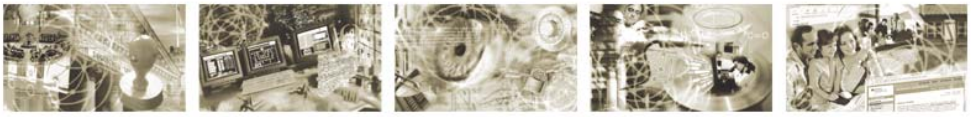
Bundesamt
für Sicherheit in der
Informationstechnik



Dokument ist noch aktuell. (Stand 2020)

Verantwortlichkeiten von IT-Herstellern, Nutzern und Intermediären

Studie im Auftrag des BSI durchgeführt von Prof. Dr. Gerald Spindler, Universität Göttingen

Bundesamt für Sicherheit in der Informationstechnik
Postfach 20 03 63
53133 Bonn
Tel.: +49 228 99 9582-0
E-Mail: recht@bsi.bund.de
Internet: http://www.bsi.bund.de/recht
© Bundesamt für Sicherheit in der Informationstechnik 2007

Autoren

Prof. Dr. Gerald Spindler, Universität Göttingen

unter Mitwirkung von:
Ass.iur. Andreas Lönner, Universität Göttingen
Ref.iur. Judith Nink, Universität Göttingen

Verantwortlichkeiten von IT-Herstellern, Nutzern und Intermediären

Prof. Dr. Gerald Spindler
Universität Göttingen

unter Mitwirkung von:
Ass. iur. Andreas Lönner, Universität Göttingen
Ref. iur. Judith Nink, Universität Göttingen

Inhaltsverzeichnis

A. Einleitung

1 Informationstechnologie durchdringt heute alle Lebensbereiche. Von der privaten Nutzung des Internets und E-Mails über die Nutzung durch gewerbliche Anwender jeglicher Art bis hin zum Einsatz von IT in kritischen Infrastrukturen wie Energie- oder Gesundheitsversorgung[1] – das private, wirtschaftliche und öffentliche Leben ist heute ohne Computertechnologie kaum vorstellbar. IT-Produkte finden sich heutzutage in jeder Form von Geräten, sei es als embedded systems in Konsumgeräten oder als spezielle Steuerungsgeräte in Industrieanlagen.

2 Vor diesem Hintergrund besitzen Sicherheitsaspekte einen überragenden Stellenwert. Der drohende volkswirtschaftliche Schaden schadhafter IT-Produkte, die Betriebsabläufe und Steuerungen zum Erliegen bringen, liegt auf der Hand. Auch aus betriebswirtschaftlicher Sicht ist die Beherrschung der bestehenden IT-Risiken von fundamentaler Bedeutung. Zu den Krisenszenarien aus unternehmerischer Sicht zählen nicht nur die vertraglichen Risiken; vielmehr ist IT-Sicherheit zu einem entscheidenden Faktor in der Wertschöpfungskette generell geworden, der die Risikoexposition eines Unternehmens, seine Kreditwürdigkeit ebenso wie seine Haftpflichtversicherungsprämien entscheidend beeinflussen kann. Auch wenn im vertraglichen Verhältnis zahlreiche Vorkehrungen gegen Krisenszenarien getroffen werden können, verbleiben sowohl gegenüber Dritten als auch für das Unternehmen intern zahlreiche Pflichten, die sich in erheblicher Weise auswirken können.

3 Dies wurde schon im Rahmen des damals befürchteten Jahr 2000-Problems deutlich[2] und hat sich seitdem eher noch verschärft.[3] Fast wöchentliche Meldungen über neu entdeckte Sicherheitslücken in Softwareprogrammen und neue Varianten von Würmern

---

1 Dazu BSI-Gutachten zur rechtlichen Analyse des Regelungsumfangs zur IT-Sicherheit in kritischen Infrastrukturen, 2005, abrufbar unter: http://www.bsi.de/fachthem/kritis/Regelungsumfang_ITSich_KRITIS.pdf; *Sonntag*, IT-Sicherheit kritischer Infrastrukturen, 2005.

2 Dazu mit weiteren Zahlenmaterial und Nachweisen *Heckeroth*, DB 1999, 702 (703); *Wohlgemuth*, MMR 1999, 59 (59); *Hohmann*, NJW 1999, 521 (521); *Heussen/Damm*, BB 1999, 481 (482); *Bartsch*, Software und das Jahr 2000 - Haftung und Versicherungsschutz für ein technisches Großproblem, S. 1 ff.; *Stretz*, in: v.Westphalen/Langheid/Streitz, Der Jahr-2000 Fehler, Rz. 1, 82 ff.; aus der schweizerischen Literatur: *Rigamonti*, SJZ 1998, 430 (431 ff.); *R. Weber*, Informatik und das Jahr 2000, 1998, S. 19 ff.

3 „Störfälle im Internet nehmen zu“, Beitrag von *Th. Stollberger* des Online-Nachrichtenservices Verivox v. 18.11.2004, abrufbar unter: http://www.verivox.de/news/ArticleDetails.asp?PM=1&aid=2542 (zuletzt abgerufen am 26.09.2006).

oder Viren werfen die Frage nach der **Pflichtenlage, Verantwortlichkeit und Haftung im geltenden Recht** der an der Herstellung, dem Einsatz und der Nutzung von IT-Produkten Beteiligten auf, angefangen beim Hersteller, über die IT-Intermediäre, die sowohl IT-Produkte einsetzen als auch selbst wiederum Dienstleistungen erbringen, wie etwa die Provider (Host-, Access-Provider), bis hin zu den IT-Anwendern, die ihrerseits bestimmten Pflichten unterliegen.

4 Aber auch **aus rechtspolitischer Sicht** stellt sich die Frage, ob das Recht mit seinen bisherigen Steuerungsinstrumenten in der Lage ist (und war), den neuen Risiken ausreichend Rechnung zu tragen. Das nunmehr seit etlichen Jahren diskutierte Problem der IT-Sicherheit scheint nach wie vor nicht bewältigt zu sein, so dass Defizite des geltenden Rechts nahe liegen.

5 Die tatsächliche Relevanz dieser Problematik steht in einem gewissen Gegensatz zur rechtlichen Durchdringung der bestehenden Sicherheitspflichten im Bereich der Informationstechnologie. Schwierigkeiten bereitet einerseits die lediglich partiell bestehende spezialgesetzliche Normierung dieser Pflichten, anderseits die starke Zersplitterung der Materie auf eine Vielzahl von Einzelgesetzen. Zudem sind bislang nur ansatzweise die traditionellen Verantwortlichkeitsnormen auf ihre Tragfähigkeit zur Bewältigung und Zuweisung von Risiken hin untersucht worden.[4]

B. Allgemeiner Teil

I. Rechtliche Grundlagen von Sicherheitspflichten

6 Ziel dieses Gutachtens ist es, einen Überblick über die derzeit bestehenden Sicherheitsanforderungen zu geben, die die Rechtsordnung – teilweise in Gestalt von Spezialgesetzen, in erster Linie jedoch durch die Auslegung bestehender allgemeiner Rechtsvorschriften – an alle Verwender von IT-Produkten stellt. Dazu ist es nötig, die für diesen Bereich in Frage kommenden Rechtsmaterien und den in ihnen niedergelegten Bestand an Rechtspflichten zu sichten. Als Pflichten kommen nicht nur öffentlichrechtlich normierte Verhaltensstandards in Betracht, sondern auch und in erster Linie zivilrechtlich begründete Sicherheitspflichten, deren (schuldhafte) Verletzung zur Haftung des Verantwortlichen führt.

---

[4] So etwa *Günther*, Produkthaftung für Informationsgüter, S. 157 ff.; *Sodtalbers*, Softwarehaftung im Internet, S. 101 ff.

7 Im **öffentlichen Recht** können grundsätzlich zwei Normenkreise voneinander unterschieden werden, die spezifische IT-Sicherheitspflichten statuieren können: Zum einen die produktbezogenen Vorschriften, zum anderen die tätigkeits- oder branchenbezogenen Vorschriften, die die Sicherheit bestimmter Anlagen oder Tätigkeiten regeln. Zu dem ersten Kreis der produktbezogenen Vorschriften gehören insbesondere als allgemeine Rahmennorm das Geräte- und Produktsicherheitsgesetz (GPSG) sowie als Beispiel für ein spezifisches produktbezogenes Gesetz das MedizinprodukteG oder das Chemikaliengesetz (ChemG). Zu dem zweiten Kreis der tätigkeits- oder anlagenbezogenen Normen zählen etwa die spezifischen Aufsichtsgesetze wie das Kreditwesengesetz oder das Versicherungsaufsichtsgesetz, die mittelbar[5] besondere Vorgaben für den Umgang mit unternehmensinternen IT-Risiken enthalten.

8 **Aus zivilrechtlicher Sicht** sind hier zunächst Pflichten innerhalb **vertraglicher Sonderverbindungen** zu nennen, deren Übernahme jedoch zur Disposition der Parteien steht. Auszuloten sind in diesem Bereich somit in erster Linie die Grenzen der Vertragsgestaltung mittels Allgemeiner Geschäftbedingungen. Besonderes Gewicht erlangen dabei die Schutz- und Nebenpflichten innerhalb von vertraglichen Beziehungen. Demgegenüber können vertragliche Hauptleistungspflichten hier nur am Rande Berücksichtigung finden, da sie nur in besonderen Fällen die IT-Sicherheit zum Gegenstand gegenseitig geschuldeter Pflichten machen. Dies schließt nicht aus, dass die Gewährleistung einer grundlegenden IT-Sicherheit zu den sog. Kardinal- oder auch vertragswesentlichen Pflichten zählt, von denen sich ein Anwender nicht freizeichnen kann.[6]

9 Diese Schutz- und Nebenpflichten entsprechen oftmals[7] den vor allem im **Deliktsrecht** dem IT-Verwender auferlegten Sicherheitspflichten, die gegenüber jedermann, also nicht nur gegenüber Vertragspartnern bestehen. In erster Linie sind hier die von der Rechtsprechung entwickelten Verkehrssicherungspflichten Gegenstand der Untersuchung. Trotz der Schuldrechtsreform mit ihrer Verlängerung der Gewährleistungsfristen im Kauf- und Werkvertragsrecht[8] und der Einführung einer allgemeinen vertragsrecht-

---

5 Über entsprechende Konkretisierungen in der Verwaltungspraxis und Auslegung von Tatbestandselementen.

6 Zu den Kardinalpflichten s. BGH NJW 1993, 335; BGH NJW-RR 1993, 560 (561); BGH NJW 2002, 673 (674); zuletzt BGH NJW-RR 2005, 1496 (1505 ff.) = WM 2005, 2002 (2013) = CR 2006, 228 (229); NJW-RR 2006, 267 (269).

7 Natürlich kann durch besondere Vertrauensbeziehungen und gerade im Vertragsverhältnis geweckten Sicherheitserwartungen eine Verschärfung der Sicherheitspflichten gegenüber den deliktischen Pflichten eintreten.

8 Die Frage, wie Software einzuordnen ist, insbesondere im Hinblick auf § 651 BGB, ist anderweitig ver-

lichen Schadensersatzhaftung spielt das Deliktsrecht nach wie vor eine wichtige Rolle: Zum einen entstehen Sicherheitsprobleme oft auch noch nach Ablauf der vertraglichen Gewährleistungsrechte; zum anderen dürften die meisten vertragsrechtlichen Schadensersatzansprüche am mangelnden Verschulden der Softwarehändler als Vertragspartner scheitern.[9] Abgesehen davon können IT-Hersteller, Intermediäre und Anwender mit Ansprüchen Dritter konfrontiert werden, die aus dem Einsatz fehlerhafter Software resultieren und die nicht auf vertraglichen Ansprüchen fußen.[10]

II. Kriterien für die Pflichtenbestimmung

10 Die verschiedenen Normen für Sicherheitspflichten verfolgen unterschiedliche Zwecke und unterliegen selbstverständlich unterschiedlichen rechtsdogmatischen Grundlagen. Während die vertragliche Haftung in erster Linie auf dem Gedanken einer besonderen, durch Vertrag begründeten Vertrauensbeziehung zwischen den Parteien beruht,[11] statuiert das Deliktsrecht Verhaltensanforderungen an jedermann.[12] Spezialgesetzliche Vorschriften sind in erster Linie an besondere Branchen gerichtet und haben insoweit einen abgegrenzten Adressatenkreis.

11 Konsequenz dieser Unterschiede hinsichtlich der Schutzzwecke und der dogmatischen Grundlagen ist daher an sich, dass die Konkretisierung der Schutzpflichten in den jeweiligen Bereichen unterschiedlichen Grundsätzen zu folgen hat. Trotz dieser Unterschiede im Einzelnen können **bestimmte Pflichtenkriterien** destilliert werden, die quasi **abstrakt für alle Pflichtenbestimmungen** gelten, da sie das Fundament für alle weiteren Pflichtenverschärfungen oder –präzisierungen bilden. Diese Grundsätze sollen hier zunächst vorgestellt werden, um in einem weiteren Schritt – als Ergebnis der Anwendung dieser Grundsätze – die konkreten Rechtspflichten der IT-Verwender aufzuzeigen. Da im Deliktsrecht die für jedermann geltenden Pflichten bestimmt werden, liegt es nahe,

---

tieft worden, s. dazu *Spindler/Klöhn*, CR 2003, 81 ff., sowie *dies*. VersR 2003, 273 ff.; dazu auch *Redeker*, CR 2004, 88 ff.; *Marly*, Softwareüberlassungsverträge, Rn. 35 ff.

9 Zu den vergleichbaren vertragsrechtlichen Fragen im Rahmen des Jahr-2000-Fehlers s. *Spindler*, DB 1999, 1991; *Wohlgemuth*, MMR 1999, 59; *v.Westphalen*, in: v.Westphalen/Langheid/Streitz, Der Jahr-2000-Fehler, Rz. 383 – 637; *Hohmann*, NJW 1999, 521 ff.; mwN. bei *Junker*, NJW 2000, 1304 (1311); s. auch LG Leipzig NJW 1999, 2975 m. Anm. *Hörl*, CR 1999, 605; allgemein zur Leistungsstörung bei Software s. *Marly*, Softwareüberlassungsverträge, Rn. 588 ff., 750 ff. et passim; *Schneider*, Handbuch des EDV-Rechts, Kap. D Rz. 728 ff. et passim.

10 Einen Anspruch aus positiver Forderungsverletzung bzw. §§ 280 I, 241 II BGB können Dritte demgegenüber nur dann geltend machen, wenn sie in den Schutzbereich des Vertrages zwischen Softwareveräußerer und –abnehmer einbezogen sind, was selten der Fall sein dürfte, aA. im Rahmen des Jahr-2000-Fehlers noch *Hohmann*, NJW 1999, 521 (524).

11 S. dazu auch *Larenz*, Schuldrecht I, § 2 I.

12 Hierzu *Larenz/Canaris*, Schuldrecht II/2, § 75.

an die Kriterien, die für Verkehrspflichten entwickelt wurden, anzuknüpfen. Denn der Maßstab der im Verkehr üblichen Sorgfalt nach § 276 BGB, der für das gesamte Schuldrecht und damit auch für vertragliche Pflichten gilt, ebenso für das Mitverschulden nach § 254 BGB (und damit die Pflichten zum Eigenschutz), entspricht strukturell weitgehend den deliktisch abgeleiteten Verkehrspflichten.[13]

1. Allgemeine Grundsätze der deliktischen Haftung, insbesondere Verkehrssicherungspflichten

12 Zentral für die Haftung ist das Konzept der Verkehrssicherungspflichten; sie sind ausschlaggebend, um Schäden, die durch mittelbare Verletzungen entstanden sind, wie etwa in der Produzentenhaftung, zuzurechnen. Sie beanspruchen aber auch allgemeine Geltung für die Ableitung von Pflichten, die aus der Beherrschung von Gefahrenquellen erwachsen. Für die Konkretisierung dieser, durch richterliche Rechtsfortbildung entwickelten Pflichten, sind insbesondere die **berechtigten Sicherheitserwartungen des Verkehrs und der zumutbare Aufwand** maßgeblich.[14]

13 Im Bereich der Produkthaftung ist dies für Hersteller (von IT-Produkten) dahingehend präzisiert worden, dass diese sich nicht nach individuellen besonderen Sicherheitserwartungen[15] oder Schadensanfälligkeiten[16] richten müssen. Ebenso wenig müssen Produkte, deren Gefahren jedermann bekannt sind, gegen Missbrauch gesichert werden; auch vor deren Fehlgebrauch muss nicht gewarnt werden.[17] Die Pflichten des Produzenten, insbesondere zur Instruktion und Warnung, werden weiter eingeschränkt, wenn die Abnehmer selbst fachkundigen Kreisen angehören und daher weitestgehend selbst die Gefahren des Produktes beurteilen können.[18] Andererseits haftet der Produzent auch für Schäden infolge eines nicht bestimmungsgemäßen Gebrauchs, sofern dieser sich noch

---

13 Vgl. zu den Kriterien der Bestimmung der im Verkehr erforderlichen Sorgfalt Bamberger/Roth-*Unberath*, § 276 BGB Rn. 20 ff.; Palandt-*Heinrichs*, § 276 BGB Rn. 15 ff.; MünchKommBGB-*Grundmann*, § 276 BGB Rn. 53 ff. sowie den Kriterien zur Bestimmung der deliktischen Verkehrspflichten Palandt-*Sprau*, § 823 BGB Rn. 45; Bamberger/Roth-*Spindler*, § 823 BGB Rn. 233 ff.; MünchKommBGB-*Wagner*, § 823 BGB Rn. 248 ff.; dezidiert für eine Gleichsetzung von deliktischer Verkehrspflichtverletzung und Außerachtlassung der im Verkehr erforderlichen Sorgfalt MünchKommBGB-*Wagner*, § 823 BGB Rn. 63 ff.

14 BGHZ 104, 323 (329) = NJW 1988, 2611; *Libertus*, MMR 2005, 507 (509); wN. bei Bamberger/Roth-*Spindler*, § 823 BGB Rn. 532.

15 *v. Bar*, in: Produktverantwortung und Risikoakzeptanz, S. 29 (31 f.).

16 OLG Hamm NJW-RR 2001, 1248 (1249) - Osteoporosegeschädigter Benutzer eines Sprungbootes.

17 BGH NJW 1990, 906.

18 BGH NJW 1992, 2016 (2018); s. aber auch BGH NJW 1996, 2224 (2226).

im Rahmen der allgemeinen Zweckbestimmung des Produktes hält[19] und vom Hersteller objektiv vorhergesehen werden kann oder nahe liegt.[20]

14 Einfluss auf die berechtigten Sicherheitserwartungen haben ferner vor allem der Preis und die Bestimmung des Produktes, einschließlich dessen allgemeiner Anpreisung in der Werbung.[21] Im Rahmen einer gewissen Bandbreite kann ein niedrigerer Preis auch ein niedrigeres Sicherheitsniveau rechtfertigen, da der Verkehr allgemein nicht von der Einhaltung höherer Standards ausgeht, sofern dies offenbar wird.[22]

15 Stets ist jedoch eine **Basissicherheit** zu gewährleisten, von deren Einhaltung der Verkehr auf jeden Fall ausgeht.[23] Eng damit verknüpft ist der Einfluss von möglichen Selbstschutzmaßnahmen:[24] Je mehr dem Produktbenutzer an **Eigenschutz** zugemutet werden kann, desto eher wird der Verkehrspflichtige nur zu Warnhinweisen verpflichtet sein. Für den Hersteller hat dies zur Folge, dass er sich auf einen objektiv zu bestimmenden Mindestsicherheitsstandard einrichten muss, der nach denjenigen Sicherheitserwartungen festzulegen ist, die allgemein bezüglich der gesamten *Produktkategorie* vorherrschen, also z.B. auch von anderen Herstellern erbracht werden.

16 Erheblich ist ferner, ab welcher Schwelle der Bedrohung von Rechtsgütern Dritter der Produzent Maßnahmen zur Sicherung ergreifen muss. Die Pflicht zum Eingreifen wird umso eher ausgelöst, **je höherrangiger die bedrohten Rechtsgüter** sind.[25] Daraus folgt, dass der Hersteller bei Bedrohung von Gesundheit und Leben bereits bei ernstlichen Verdachtsmomenten tätig werden muss; er kann nicht bis zum ersten Schadensfall abwarten[26]. Der Hersteller muss die einschlägigen Veröffentlichungen hierzu auswerten und den **Stand von Wissenschaft und Technik** berücksichtigen. Andererseits muss er sich nicht mit vereinzelt gebliebenen Auffassungen zu Gefahrenmomenten auseinander-

---

19 BGHZ 105, 346 (351) = NJW 1989, 707; BGHZ 116, 60 (65 ff.) = NJW 1992, 560; OLG Oldenburg NJW-RR 1997, 1520 (1521); MünchKommBGB-*Wagner*, § 823 BGB Rn. 588; Staudinger-*J. Hager*, Kap. F Rn. 36; dagegen *Littbarski*, NJW 1995, 217 (219).

20 BGHZ 105, 346 (351) = NJW 1989, 707; BGHZ 106, 273 (283) = NJW 1989, 1542; BGHZ 116, 60 (65 ff.) = NJW 1992, 560; BGHZ 139, 79 (84) = NJW 1998, 2905; OLG Karlsruhe VersR 1998, 63; MünchKommBGB-*Wagner*, § 823 BGB Rn. 588 (591).

21 Ausführlich dazu *Foerste*, in: v. Westphalen, ProdHaftHdb, § 24 Rn. 10, 48.

22 BGH NJW 1990, 906 (907); BGH NJW 1990, 908 (909); MünchKommBGB-*Wagner*, § 823 BGB Rn. 576; *Kötz*, Deliktsrecht,Rn. 449; Staudinger-*J. Hager*, Kap F Rn. 8.

23 BGH NJW 1990, 908 (909); *Foerste*, in: v. Westphalen, ProdHaftHbd, § 24 Rn. 10; MünchKommBGB-*Wagner*, § 823 BGB Rn. 576; *Kötz*, Deliktsrecht,Rn. 449.

24 BGHZ 104, 323 (328) = NJW 1988, 2611; BGH NJW 1990, 906; BGH NJW 1987, 372 f.; Kullmann/Pfister-*Kullmann*, Produzentenhaftung, Kz. 1520 S. 3 f.

25 BGHZ 80, 186 (192) = NJW 1981, 1603; vgl. BGHZ 104, 323 (329) = NJW 1988, 2611; MünchKommBGB-*Wagner*, § 823 BGB Rn. 591.

26 BGHZ 106, 273 (283) = NJW 1989, 1542; BGHZ 80, 186 (192) = NJW 1981 (1603).

setzen, sondern kann sich idR auf die vorherrschende Überzeugung in Fachkreisen verlassen.[27] Sind Gefahren bekannt, aber nicht die Möglichkeiten zu ihrer Vermeidung, kann das Produkt nur in Verkehr gebracht werden, wenn der Verkehr eine entsprechend reduzierte Sicherheit erwartet,[28] wobei dem Hersteller ein Anpassungsermessen bei Wandel des Gefahrenbewusstseins[29] und bei neuen technischen Entwicklungen[30] zugestanden wird. Der Hersteller muss den Weg der größeren Vorsicht wählen, wenn Unsicherheiten über die Sicherheitsvorkehrungen bestehen.[31]

17 Besonders bedeutsam für die Konkretisierung der geschuldeten Verkehrspflichten ist in diesem Zusammenhang **der Stand von Technik und Wissenschaft** hinsichtlich der Sicherheit des Produktes. Maßgeblich sind die Erkenntnisse, die zum Zeitpunkt der erforderlichen Gefahrenabwehr verfügbar waren.[32] In diesem Rahmen stellen öffentlich-rechtliche Vorschriften und **Regelwerke privater Gremien, wie DIN-Normen**, zwar wichtige, aber keineswegs abschließende Konkretisierungen des Standes der Technik im zivilrechtlichen Sinne dar,[33] da im Einzelfall eine höhere Sicherheit erforderlich sein mag oder die technische Entwicklung die Normen überholt hat.[34] Der Hersteller muss selbstverantwortlich prüfen, welche Gefahren entstehen können.[35] So binden die Sicherheitsanforderungen nach dem Gesetz über technische Arbeitsmittel und Verbraucherprodukte (GPSG)[36] oder den jeweiligen Produktsicherheitsrichtlinien als Mindest-

---

27 S. auch OLG Frankfurt NJW-RR 1995, 406.

28 *Foerste*, in: v. Westphalen, ProdHaftHdb, § 24 Rn. 84 ff.; *Schmidt-Salzer*, Produkthaftung, Bd. III/1, Rn. 4.1113 f.; Kullmann/Pfister-*Kullmann*, Produzentenhaftung, Kz. 1520 S. 4 f.; diff. *Brüggemeier*, WM 1982, 1294 (1302).

29 Insbes. bei uneinheitlichen Verbrauchererwartungen wie z.B. bei Kopfstützen, ABS-Bremssysteme oder Airbags in KfZ, vgl. *Foerste*, in: v. Westphalen, ProdHaftHdb, § 24 Rn. 89 ff.; *Schmidt-Salzer*, Produkthaftung, Bd. III/1, Rn. 4.675 ff.; ähnl. *Hollmann*, DB 1985, 2389 (2392); *Schlechtriem*, VersR 1986, 1033 (1036); abl. gegenüber dem Kriterium der Verbrauchererwartung *Möllers*, Rechtsgüterschutz im Umwelt- und Haftungsrecht, 254 ff.

30 Kullmann/Pfister-*Kullmann*, Produzentenhaftung, Kz. 1520, S. 15 f.

31 Kullmann/Pfister-*Kullmann*, Produzentenhaftung, Kz. 1520, S. 15 unter Verweis auf BGH NJW 1990, 906 (907) - und Berufung auf arzthaftungsrechtliche Grundsätze, wie z.B. BGHZ 8, 138 (140); weniger restriktiv BGH NJW 1987, 2927.

32 BGHZ 80, 186 (192) = NJW 1981, 1603.

33 Zum öffentlich-rechtlichen Verständnis ausführlich *Spindler*, Unternehmensorganisationspflichten, 505 ff.

34 BGH NJW 1998, 2814 (2815); BGH NJW 1994, 3349 (3350); LG Berlin MDR 1997, 246 (247); MünchKommBGB-*Wagner*, § 823 BGB Rn. 273; Staudinger-*J. Hager*, Kap. F Rn. 10; *Kullmann*, NJW 1996, 18 (22).

35 BGHZ 99, 167 (176 f.) = NJW 1987, 1009 (für Zubehörteile).

36 Mit dem Gesetz über technische Arbeitsmittel und Verbraucherprodukte (Geräte- und Produktsicherheitsgesetz – GPSG) wurden das Gerätesicherheitsgesetz (GSG) und das Produktsicherheitsgesetz (ProdSG) zu einem Gesetz zusammengeführt, sowie die Richtlinie über die allgemeine Produktsicherheit (Richtlinie 2001/95/EG v. 3.12.2001; ABlEG 2002 Nr. L 11 S. 4) in nationales Recht umgesetzt. Das GPSG wurde am 6. Jan. 2004 veröffentlicht (BGBl. I 2004, S. 2) und trat am 1. Mai 2004 in Kraft, GSG und ProdSG traten am 1. Mai 2004 außer Kraft; erster Überblick bei *Klindt*, NJW 2004, 465 ff.; *Potinecke*, DB 2004,

standards den Produzenten nicht und stehen höheren zivilrechtlich relevanten Sicherheitserwartungen nicht entgegen.[37] Ist für den Hersteller trotz Einhaltung der technischen Regeln und Wahrung etwaiger behördlicher Zulassungsvoraussetzungen eine von seinem Erzeugnis ausgehende Gefahr erkennbar, so hat er die darüber in Unkenntnis befindlichen Benutzer zumindest zu warnen.[38]

18 Auch **Zertifizierungen** und Prüfungen berühren hinsichtlich der materiell-rechtlichen Pflichten grundsätzlich nicht die zivilrechtliche Haftung des Herstellers. Sie können nur die Risiken und damit die Wahrscheinlichkeit eines Schadens mindern, nicht aber weitergehende Sicherheitserwartungen des Verkehrs beschränken.[39] Sie können jedoch auf der Ebene der Entlastung für bestimmte Pflichten eine Rolle spielen: Andere in den Fertigungsprozess eingeschaltete Unternehmer, wie z.B. ein Auftragsfertiger, die hinsichtlich Konstruktionsgefahren geringeren Sorgfaltspflichten als der eigentliche Hersteller unterliegen, können sich jedoch im Einzelfall damit entlasten, dass das Produkt durch den TÜV oder einen anderen Sachverständigen überprüft wurde.[40] Auf diese Auswirkungen von Zertifizierungen ist später noch zurückzukommen.[41]

19 Die Anforderungen an die Verkehrspflicht stehen in einem engen Verhältnis zu den dem Dritten abzuverlangenden Bemühungen an **vernünftigem Eigenschutz**. Nicht gegen jedes Risiko kann Schutz verlangt werden, wenn der Dritte einfacher und mit geringerem Aufwand eine Schädigung als der Pflichtige vermeiden kann.[42] Allerdings darf nicht jede Möglichkeit des Eigenschutzes dazu führen, dass die Grenze zum Mitver-

---

S. 55 ff.; *Littbarski*, VersR 2005, 448; *Lenz*, MDR 2004, 918.

37 BGH VersR 1972, 149; Kullmann/Pfister-*Kullmann*, Produzentenhaftung, Kz. 1520 S. 26; *Schmatz/Nöthlichs*, Sicherheitstechnik, Bd. I Teil 1, § 3 GSG Anm. 5.3.7; *Taschner/Frietsch*, § 1 ProdHaftG Rn. 89, Richtl. Art. 7 Rn. 31; *Wagner*, BB 1997, 2541 (2541 f.); *Niebling*, DB 1996, 80 (81); *Taupitz*, in: Produktverantwortung und Risikoakzeptanz, 119 (135), zum Einfluß des § 22 KrW-/AbfG auf den Mindestsicherheitsstand und die Sicherheitserwartungen bei Abfall s. *Gesmann-Nuissl/Wenzel*, NJW 2004, 117 ff.

38 BGHZ 99, 167 (176) = NJW 1987, 1009; BGHZ 139, 79 (83) = NJW 1998, 2905; BGH NJW 1999, 2815 (2816); krit. dazu *Littbarski*, NJW 2000, 1161 (1162).

39 Darauf deuten auch die Ausführungen der EG -Kommission hin, vgl. ein Globales Konzept für Zertifizierung und Prüfwesen - Instrument zur Gewährleistung der Qualität bei Industrieerzeugnissen -, KOM(89) 209 endg. - SYN 208, Mitteilung Nr. 89/C 267/03 der Kommission an den Rat, vorgelegt am 15.6.1989, Abl. EG Nr. C 267/3 vom 19.10.1989, S. 12 (Kapitel II Ziff.4); Präambel der Richtlinie 92/59/EWG des Rates vom 29. Juni 1992 über die allgemeine Produktsicherheit, Abl. EG Nr. L 228, S. 24; ebenso *Niebling*, DB 1996, 80 (81), allerdings nicht für sog. C-Normen des höchsten Sicherheitsstandards; auch nach § 1 II Nr. 4 ProdHaftG liegt wegen der Beschränkung auf Mindeststandards kein Zwangstatbestand vor, vgl. *Marburger*, in: FS Lukes, 97 (100).

40 BGH NJW-RR 1990, 406 f.; dazu *Kullmann*, NJW 1991, 675 (678 f.).

41 S. Rn. 145 ff.

42 Dies ist die Kernaussage der unten (Fn. 160) erwähnten Lehre vom *cheapest cost avoider*.

schulden gem. § 254 BGB verschwimmt.[43] Vielmehr muss die Prüfung eindeutig ergeben, dass der Dritte ohne großen Aufwand die Verletzung vollständig vermeiden kann, während dem Pflichtigen selbst mit hohen Kosten die vollständige Gefahrenbeherrschung nicht möglich ist. So hat die Rechtsprechung anerkannt, dass der Verkehrspflichtige darauf vertrauen kann, dass bei einer Gefahr, die mit Händen zu greifen ist und der ohne weiteres ausgewichen werden kann, der Betroffene diese erkennt und sich selbst schützt.[44] Bei jedermann erkennbaren und bekannten Gefahren, muss auf diese nicht besonders hingewiesen oder vor ihnen geschützt werden.[45] Erst recht sind Sicherungspflichten nicht gegenüber denjenigen angebracht, die gerade selbst zur Gefahrenkontrolle oder -beseitigung bestellt oder beauftragt wurden.[46]

20 Die vorstehend genannten Kriterien sind zwar auf den ersten Blick allein auf die Produkthaftung zugeschnitten; bei näherer Analyse wird jedoch deutlich, dass sie **verallgemeinerungsfähige Aussagen** enthalten, die auf das Ausmaß und die Kontrolle einer Gefahrenquelle, die bedrohten Rechtsgüter, die Zumutbarkeit von Gefahrenabwehrmaßnahmen, den Sicherheitserwartungen des Verkehrs (und gegebenenfalls des Vertragspartners) und dem möglichen Ausmaß des Eigenschutzes abstellen. Diese Maßstäbe können zwar im Einzelfall durch vertragliche Vereinbarungen modifiziert werden; doch sind sie immer wieder bei der Konkretisierung der im Verkehr erforderlichen und üblichen Sorgfalt nach § 276 BGB anzutreffen.[47]

2. Methodischer Hintergrund: Die rechtsökonomische Perspektive

---

43 Insoweit zutr. *Möllers*, VersR 1996, 153 (158); *Hasselblatt*, Die Grenzziehung zwischen verantwortlicher Fremd- und eigenverantwortlicher Selbstgefährdung im Deliktsrecht, S. 131 ff.; für eine stärkere Überlappung von Fremd- und Eigenverantwortlichkeit dagegen *Zeuner*, in: FS Medicus, S. 693 (699 ff.).

44 BGHZ 104, 323 (328) = NJW 1988, 2611; BGH NJW-RR 1989, 219 (220); OLG Köln VersR 1993, 1494 f.; MünchKommBGB-*Wagner*, § 823 BGB Rn. 251; Staudinger-*J. Hager*, Kap. E Rn. 32.

45 BGHZ 104, 323 (328 f.) = NJW 1988, 2611 – Getränkeflasche; BGH NJW 1999, 2815 (2816); BGH NJW 1986, 52 (53) – Feuerwerk Silvesternacht; BGH NJW 1985, 1076 (1077) – Nicht fertig gestellte Loggia.

46 OLG Köln VersR 1992, 470 (471) – Feuerwehr; OLG Zweibrücken BauR 1994, 781 (782), Rev. nicht angenommen, BGH Beschl. v. 5.7.1994 VI ZR 346/93 – Sicherungsposten einer Baustelle; OLG Jena VersR 1998, 903 (904), Rev. nicht angenommen, BGH Beschl. v. 24.3.1998 VI ZR 274/97 – Sachverständige zur Gefahrenbegutachtung.

47 Vgl. bspw. zum Einfluss technischer Regelwerke auf die im Verkehr erforderliche Sorgfalt Bamberger/Roth-*Unberath*, § 276 BGB Rn. 24; Palandt-*Heinrichs*, § 276 BGB Rn. 18; MünchKommBGB-*Grundmann*, § 276 BGB Rn. 64, zu Möglichkeiten des Selbstschutzes des Verletzten MünchKomm BGB-*Grundmann*, § 276 BGB Rn. 63.

21 Gerade in neuen Regelungsbereichen wie dem IT-Recht können sich die Denkmodelle der ökonomischen Rechtsanalyse als besonders nützlich erweisen.[48] Ausgangspunkt ökonomischer Denkmodelle ist die **Ressourcenknappheit.** Ziel ist eine effiziente Verteilung dieser Ressourcen.[49] Wann eine effiziente Verteilung, also **Alokationseffizienz** erreicht ist, lässt sich nach verschiedenen Kriterien messen: Nach dem **Pareto**-Kriterium besteht Allokationseffizienz, wenn eine ökonomische Situation erreicht ist, in der niemand besser gestellt werden kann, ohne jemand anderen schlechter zu stellen.[50] Weiter gefasst ist das **Kaldor-Hicks**-Kriterium. Danach ist Allokationseffizienz erreicht, wenn keine Veränderung mehr möglich ist, bei der die Gewinner ihre Gewinne höher bewerten als die Verlierer ihre Verluste.[51]

22 Die ökonomische Analyse lässt sich dabei sowohl auf der Ebene der Rechtsetzung als auch auf der Ebene der Rechtsanwendung fruchtbar machen. Auf der Ebene der Rechtsanwendung können einzelne Tatbestandsmerkmale insbesondere im Haftungsrecht auch nach ökonomischen Kriterien ausgelegt werden.[52] Auf der Ebene der Rechtssetzung ist die Grundfrage hingegen, wie Rechtsnormen gestaltet sein müssen, um eine präventiv schadensmindernde Regelungsstruktur zu erhalten.

a) Steuerungsfunktion für das Niveau der Schutzmaßnahmen

23 Bekanntermaßen entstehen durch IT-Sicherheitsprobleme Schäden mit beträchtlichem wirtschaftlichem Ausmaß. Solche Schäden können durch entsprechende Maßnahmen (z.B. Rechtebeschränkung in IT-Systemen) eingedämmt werden. Diese Maßnahmen verursachen aber wiederum selbst Kosten (z.B. Lizenzgebühren für die Schutzsoftware, Personalaufwand). Es entsteht somit ein **Optimierungsproblem**: Ab einem gewissen Aufwand für Schutzmaßnahmen ist die unter Kostengesichtspunkten optimale Struktur erreicht, denn zusätzlicher Aufwand würde höhere Kosten verursachen als Schäden verhindert würden.

24 Exemplarische Darstellung des Optimierungsproblems

---

48 *Freiwald*, Harvard Journal of Law and Technology, Vol. 14, 2001 S. 574, 580.

49 *Kübler*, in: FS Steindorff, S. 687, 689; *Salje*, Rechtstheorie 15 (1984), 277, 285.

50 *R. Zebre Jr.*, Economic Efficiency in Law and Economics, S. 3; *Behrens*, Die ökonomischen Grundlagen des Rechts, S. 83 ff.

51 *Mathis*, Effizienz statt Gerechtigkeit?, S. 70; *Baumol, W.*, Economic Theory and Operations Analysis, S. 402; *R. Zebre Jr.*, Economic Efficiency in Law and Economics, S. 4.

52 *Taupitz*, AcP 196 (1996), 114 (125 ff.); Beispiele bei *Kötz/ Schäfer*, Judex oeconomicus, 2003.

Aufwand für Schutzmaßnahmen	Erwarteter Schaden (Schadenshöhe * Wahrscheinlichkeit)	Gesellschaftliche Gesamtkosten
0	+ 40	= 40
10	+ 25	**= 35**
20	+ 20	= 40

25 Im obigen Beispiel (Tabelle): Betreibt der Akteur einen Sicherungsaufwand von 10 Einheiten, so ist der zu erwartende Schaden 25 Einheiten, Sicherungsaufwand und Schaden ergeben gesellschaftliche Gesamtkosten von 35 Einheiten. Damit ist das Optimum erreicht. Würde der Aufwand auf 0 Einheiten gesenkt oder auf 20 Einheiten gesteigert, würden die gesamtgesellschaftlichen Kosten steigen. Der zu erwartende Schaden berechnet sich dabei aus der Schadenshöhe bei einem einzelnen Schadensereignis multipliziert mit der Wahrscheinlichkeit des Eintritts eines solchen Ereignisses.

26 Mit dem Haftungsrecht ist dem Gesetzgeber ein Werkzeug an die Hand gegeben, um Anreize für einen effizienten Aufwand für Sicherungsmaßnahmen zu schaffen.[53] Denkt man Haftungsregeln zunächst hypothetisch hinweg, so sind die erwarteten Schäden im obigen Beispiel **externe Effekte**; also negative Folgen für Dritte, die der Akteur *nicht* in seine Entscheidung einbezieht.[54]

27 Eine **Verschuldenshaftung** ist aus ökonomischer Perspektive nun die Festlegung eines bestimmten Sorgfaltsstandards, dessen Nichteinhaltung zur Haftung führt.[55] Dieser Sorgfaltsmaßstab wird objektiv bestimmt und ist - juristisch beim Terminus des Verschuldens verortet[56] – nicht von den individuellen Fähigkeiten des Schädigers abhängig.[57] Im obigen Beispiel kann durch Festlegung der erforderlichen Sorgfalt bei 10 Einheiten eine Optimierung erreicht werden, da für den Akteur ein Anreiz besteht, diesen

53 MünchKommBGB-*Wagner*, Vor § 823 BGB Rn. 40.
54 *Behrens*, Die ökonomischen Grundlagen des Rechts, S. 83 ff.
55 Vgl. statt vieler *Brown*, J., Towards a Theory of Liability, 323 ff.
56 Vgl. § 276 II BGB: „Fahrlässig handelt, wer die im Verkehr erforderliche Sorgfalt außer acht lässt."
57 Wohl hM, vgl. etwa *Brüggemeier*, Deliktsrecht, Rn. 113.

Sorgfaltsmaßstab einzuhalten, weil er ansonsten haftet, also die externen Effekte zu tragen hat.

28 Diese Feststellungen lassen sich zur sogenannten marginalisierten **Learned-Hand** Formel verallgemeinern.[58] Danach ist dann kein Verschulden anzunehmen, wenn das Sorgfaltsniveau so gewählt ist, dass weitere Sorgfaltsanstrengungen (V) höhere Kosten verursachen würden als sie Schadenshöhe (S) mal Schadenswahrscheinlichkeit (q) reduzieren. Ein Verschulden ist also zu verneinen wenn: [59]

V' < S * q'

29 Ist der Sorgfaltsmaßstab durch Rechtsprechung oder gesetzliche Regelung zu hoch angesetzt, so ist es für den Schädiger nicht unbegrenzt wirtschaftlich sinnvoll, diesen einzuhalten.[60] An einem bestimmten Punkt, im obigen Beispiel ab einem Vorsorgeaufwand von 40 Einheiten, fährt der Schädiger am Besten, wenn er keine Sorgfaltsmaßnahmen trifft und die Schadenskosten i.H.v. 40 Einheiten auf sich nimmt.

30 Wird der Sorgfaltsmaßstab nicht kodifiziert, sondern mit dem unbestimmten Rechtsbegriff der Fahrlässigkeit negativ umschrieben, so liegt es in der Hand des Richters im Einzelfall,[61] ob er die Fahrlässigkeitsgrenze aufgrund obiger Erwägungen nach der Learned-Hand Formel bei 10 Einheiten ansetzt.[62]

31 Auch mit einer **Gefährdungshaftung** werden die externen Effekte **internalisiert,** d.h. es erfolgt eine Angleichung der privaten an die gesellschaftlichen Kosten.[63] Durch Einführung einer Gefährdungshaftung muss der Akteur sowohl alle Kosten für Schutzmaßnahmen als auch den erwarteten Schaden tragen: damit minimiert er schon in eigenem Interesse die gesellschaftlichen Gesamtkosten. Bezüglich der Wahl eines effizienten Sorgfaltniveaus ergibt sich also zwischen der Gefährdungshaftung und der Verschuldenshaftung (so die Gerichte hier einen effizienten Fahrlässigkeitsmaßstab festgelegt

---

58 Zuerst angewendet in United States v. Caroll Towing Co., 159 F. 2d 169 (2d Cir. 1947); vgl. *Cooter*, Journal of Economic Perspectives, Vol. 5, 1991, 11 ff., 14.

59 Vgl. dazu etwa *Cooter/Ulen,* Law & Economics, S. 334.

60 Ebenso *Schäfer/Ott*, Lehrbuch der ökonomischen Analyse des Zivilrechts, S. 172.

61 Fallbeispiele für die Anwendung ökonomischer Kriterien etwa OLG Hamm NJW RR 2002, 1459; BGH NJW 2005, 422.

62 Zuerst angewendet in United States v. Caroll Towing Co., 159 F. 2d 169 (2d Cir. 1947); vgl. *Cooter*, Journal of Economic Perspectives, Vol. 5, 1991, 11 ff., 14.

63 Diese Definition für Internalisierung findet sich auch bei *Schumann*, Grundzüge der Mikroökonomischen Theorie, S. 38 und S. 492 ff.; *K. Mathis*, Effizienz statt Gerechtigkeit?, S. 70.

haben) i.E. kein Unterschied.[64] Allerdings führt die Gefährdungshaftung auch zu einer tendenziellen Reduktion des Aktivitätsniveaus überhaupt, da gleichgültig wie viel der Schädiger an Schutzmaßnahmen durchführt, er auf jeden Fall für eintretende Schäden haftet, so dass Anreize auch zu einer Verringerung des Gefährdungsniveaus bestehen (unten Rn. 32 ff.).

b) Aussagen über die Auswahl des Haftenden

32 Die ökonomische Analyse kann aber nicht nur bei der Frage nutzbar gemacht werden, wann ein potenzieller Schädiger zu haften hat, sondern auch *wer* unter einer Vielzahl von Verursachern die Kosten tragen sollte. Anreize zur Implementierung von Schutzvorkehrungen bestehen für denjenigen, der weiß, dass er im Schadensfall haftet. Wird nun demjenigen die Haftung auferlegt, der die Schutzvorrichtungen mit niedrigstem Kostenaufwand umsetzen kann, entstehen die gesamtgesellschaftlich geringsten Kosten, der sog. „**cheapest cost avoider“**.[65]

33 Vor einer rechtlichen Umsetzung dieses Modells stellt sich aber immer zunächst die Frage, ob nicht durch Marktmechanismen von vornherein die Schutzaufwendungen dem cheapest cost avoider auferlegt werden. Letztendlich bietet es sich ja für den Schädiger an, die Schutzvorkehrungen nicht selbst zu treffen, sondern vertragliche Beziehungen bezüglich der Schutzvorkehrungen mit dem (eventuell vom Haftenden unterschiedlichen) cheapest cost avoider (gegebenenfalls sogar den Geschädigten) einzugehen. Eine solche vertragliche Optimierung ist ein Beispiel für das **Coase-Theorem**. Nach diesem erfolgt, allgemein formuliert, die Allokation (hier: der Einsatz) von Ressourcen unabhängig von der genauen Ausgestaltung der Rechtsordnung – aber nur sofern keine Transaktionskosten bestehen.[66]

34 **Transaktionskosten** sind die Kosten, die aufgewendet werden müssen um einen Vertrag abzuschließen und durchzusetzen.[67] Da entsprechende Kosten immer entstehen kann das Coase-Theorem auch anders gewendet werden: in der realen durch Transaktionskosten bestimmten Welt ist die Allokation der Ressourcen *immer* auch von der Rechtsordnung mitbestimmt.[68] Folglich behält der Grundgedanke, die rechtlich ausges-

---

64 Ebenso *Schäfer/Ott*, Lehrbuch der ökonomischen Analyse des Zivilrechts, S. 208.

65 *G. Calabresi*, The Costs of Acidents, S. 136 ff.; *Coase*, The Problem of Social Cost, S. 146 f.

66 *Thomas J. Miceli*, Economics of the Law, S. 9; *Coase*, The Problem of Social Cost, Journal of Law and Economics 3; *ders.*, in: Assmann/Kirchner/Schanze, Ökonomische Analyse des Rechts, S. 129, 148 ff.

67 *R. Coase*, The Problem of Social Cost, Journal of Law and Economics 3, S. 15.

68 *R. Coase*, Law and Economics, S. 251.

taltete Haftung am cheapest cost avoider auszurichten, praktisch immer seine Berechtigung, wird aber durch das Gedankenexperiment der idealen Welt (Coaseanischen Welt) gegenkontrolliert.[69]

c) Steuerung des Aktivitätsniveaus

35 Über eine ökonomische Analyse lassen sich also Hinweise gewinnen, wie das Haftungssystem ausgestaltet sein muss, um ein effizientes Niveau von Schutzmaßnahmen zu erreichen und Anreize setzen, dass derjenige die Schutzmaßnahmen durchführt, dem dies am kostengünstigsten möglich ist. Darüber hinaus lassen sich aber auch Aussagen darüber gewinnen, wie durch das Haftungssystem das **Aktivitätsniveau** beeinflusst werden kann: Ein rational handelnder Akteur wird bei der Abwägung von Nutzen und Kosten einer Handlung auf der Kostenseite das mögliche Haftungsrisiko mit einstellen.[70] Steigt nun das Haftungsrisiko durch schärfere Haftungsregelungen, so steigen auch die Kosten. Mit den Kosten steigt in einer funktionsfähigen Marktwirtschaft auch der Preis eines Produktes oder einer Dienstleistung. Bei ansonsten gleichen Umständen wird das teuere Produkt weniger nachgefragt. Damit wird das Aktivitätsniveau durch schärfere Haftungsregelungen gesenkt.[71]

36 Durch eine **Gefährdungshaftung** erfolgt dabei sogar eine Senkung der Aktivität auf das gesamtgesellschaftliche Optimum.[72] Denn die Gefährdungshaftung bürdet dem Schädiger alleinig das Haftungsrisiko auf. Damit fließen alle Nutzen und Kosten der Aktivität in der Person des Schädigers zusammen. Folglich ist absolute Parallelität zwischen dem Interesse des Schädigers und dem Interesse der Gesellschaft erreicht. Im Ergebnis wird der Schädiger, indem er aus eigenem Interesse handelt, gleichzeitig den Nutzen für die Gesellschaft maximieren.

37 Damit kann mittels der Gefährdungshaftung theoretisch eine stärkere Steuerungswirkung erreicht werden[73] - dass in Deutschland trotzdem die Verschuldenshaftung die Regel ist, ist historisch[74] bzw. dadurch bedingt, dass der Hauptaugenmerk auf der

---

69 Vgl. auch *Siemer*, Das Coase-Theorem, S. 82 f.

70 Zur Grundannahme des rational handelnden Akteurs vgl. *Coleman*, Foundations of Social Theory, S. 5; *Kirchgässner*, Homo Oeconomicus, S. 66 ff.; *Tietzel*, Jahrbuch der Sozialwissenschaften (1981), S. 115 ff.; *Eder*, Zeitschrift für Rechtssoziologie 8 (1987), 193 (207 ff.).

71 *Sailer*, Prävention im Haftungsrecht, S. 186.

72 Für den mathematischen Nachweis, *S. Shavell*, Economic Analysis of Accident Law, S. 23 ff., 32 ff.; vgl. auch *Sailer*, Prävention im Haftungsrecht, S. 186; Miceli, Economics of the Law, S. 28.

73 *Sailer*, Prävention im Haftungsrecht, S. 185 mwN.

74 Vgl. *Benöhr*, Die Entscheidung des BGB für das Verschuldensprinzip, Tijdschrift voor Rechtsgeschiedenis, 1978, S. 1 ff.; „Nicht der Schaden verpflichtet zum Schadensersatz, sondern die Schuld“, *Jhering*, das

Kompensationsfunktion[75] und nicht der Steuerungsfunktion des Haftungsrechts liegt. Im Übrigen ist der Unterschied in der normpraktischen Ausgestaltung geringer als soeben theoretisch skizziert, da die Steuerungswirkung durch Haftungsobergrenzen, Informationsdefizite und Versicherungsmöglichkeiten begrenzt ist:

38 **Haftungsobergrenzen** schränken die Steuerungsfunktion des Haftungsrechts ein und führen so zu einem höheren Aktivitätsniveau. So wie der Akteur Schäden bei denen er mangels Verschulden nicht haftet nicht in seine Kalkulation mit einbezieht, bezieht der Akteur bei Haftungsobergrenzen Schäden oberhalb dieser Grenzen nur mit der maximalen Haftungssumme in seine Kalkulation ein.

39 Bei einer **Verschuldenshaftung** wird dieser Effekt nicht vollständig erzielt.[76] Wie gesehen kann zwar durch richtige Wahl des Verschuldensmaßstabes ein optimales Maß an Sorgfalt erreicht werden. Allerdings wird das Aktivitätsniveau nicht auf das gesamtgesellschaftliche Optimum gesenkt. Denn für Schäden, die trotz Einhaltung der Sorgfaltspflichten entstehen, haftet der Akteur nicht. Diese werden von Dritten getragen. Ergo verursachen seine Handlungen bei ihm weniger Kosten als bei der Gesellschaft insgesamt. Und Schäden, für die er nicht haftet, wird der Akteur nicht in seine Kalkulation einbeziehen. Er wird die Handlung damit häufiger ausführen, als dies für die Gesamtgesellschaft optimal wäre.

40 Die Internalisierung der externen Effekte erfüllt auch dann keine Steuerfunktion, wenn der **Schaden nicht vorhersehbar** ist[77] - was für IT-Schäden eines der zentralen Probleme darstellt. Denn mit einem solchen Schaden kalkuliert der Akteur nicht. Ein ähnlich gelagertes Problem besteht dann, wenn der Akteur spontane Entscheidungen treffen muss – die Steuerfunktion ist größer, wenn der Akteur die Möglichkeit hat, die Situation „planend zu überdenken".[78] Durch **Versicherungen** wird das Interesse des Akteurs von dem der Allgemeinheit entkoppelt, denn durch Einschaltung der Versicherung trägt der Akteur nicht direkt den Schaden – die Steuerungswirkung ist entsprechend weiter eingeschränkt.[79]

d) Mehrpersonenkonstellationen

Schuldmoment im römischen Privatrecht, S.40.

75 *Larenz*, Lehrbuch des Schuldrechts, S. 423; vgl. auch *Sailer*, Prävention im Haftungsrecht, S. 1 mwN.

76 Vgl. *Miceli*, Economics of the Law, S. 28.

77 *Schäfer/Ott*, Lehrbuch der ökonomischen Analyse des Zivilrechts, S. 214.

78 *Weyers*, Unfallschäden, S. 466 ff.

79 Details bei *Pauly*/*Kenneth*, The Economics of Moral Hazard, S. 531.

41 In der Realität, insbesondere im IT-Bereich, wird eine effektive Schadensvermeidung häufig erst durch die Anstrengung sowohl des Akteurs als auch des Geschädigten zu erreichen sein. Bei einer Verschuldenshaftung ist der Geschädigte schon aus Eigeninteresse unabhängig von **Mitverschuldensregelungen** zu Schutzmaßnahmen angehalten.[80] Schließlich muss der Geschädigte damit rechnen, dass der Schädiger alle Sorgfaltsstandards einhält und er, der Geschädigte, somit etwaige Schäden alleine tragen muss. Bei einer Gefährdungshaftung allerdings ist eine Mitverschuldensregelung erforderlich, um Anreize für Schutzmaßnahmen durch den Geschädigten zu setzen.[81]

42 Ebenso wie die Sorgfaltsanstrengungen des Schädigers als auch des Geschädigten die Schadenswahrscheinlichkeit beeinflussen, beeinflusst in der Regel nicht nur das Aktivitätsniveau des Akteurs, sondern auch das des Geschädigten die Schadenswahrscheinlichkeit. Nach dem Theorem von *Shavell* lassen sich aber weder durch eine Verschuldenshaftung noch durch eine Gefährdungshaftung beide Aktivitätsniveaus auf das gesellschaftliche Optimum reduzieren.[82] Eine solche Steuerung tritt nämlich wie dargelegt[83] nur dann ein, wenn die jeweilige Person das volle Risiko des Schadenseintritts trifft – dieses Risiko kann aber nicht gleichzeitig sowohl dem Schädiger als auch dem Geschädigten auferlegt werden.

43 Können mehrere Personen durch ein Ereignis sowohl einen Schaden verursachen als auch geschädigt werden, so kann die Situation eintreten, dass schon ohne Haftungsregelungen gesamtgesellschaftlich effiziente Sorgfaltsmaßstäbe angewendet werden. Zur Vereinfachung soll dies an einem Beispiel aus der Schifffahrt illustriert werden[84] – wobei eine gewisse Vergleichbarkeit mit der Situation in größeren Netzwerken besteht: Angenommen, durch die Einführung von Funkgeräten lässt sich das Kollisionsrisiko zwischen zweier so ausgerüsteter Schiffe eliminieren. Ein Funkgerät kostet 5 Einheiten, der erwartete Schaden (Wahrscheinlichkeit mal Schadenshöhe) durch Kollisionen beträgt 10 Einheiten. Sind nun in der Ausgangssituation mehr als 50% der Schiffe mit einem Funkgerät ausgestattet, ist es unter Kostengesichtspunkten effektiv, neue Schiffe mit einem Funkgerät auszurüsten. Im Laufe der Zeit haben so alle Schiffe ein Funkge-

---

80 *M. Adams*, Ökonomische Analyse der Gefährdungs- und Verschuldenshaftung, S. 73 ff; *Endres*, Ökonomische Grundlagen des Haftungsrechts, S. 9 ff.

81 Ebenso *Miceli*, Economics of the Law, S. 29.

82 *Shavell*, The Journal of Legal Studies, Vol. 9, No. 1 1980, S. 1 ff.; *ders.*, Economic Analysis of Accident Law, S. 29.

83 S. Rn. 27 f.

84 Bsp. stark modifiziert nach *Schäfer/Ott*, Lehrbuch der ökonomischen Analyse des Zivilrechts, S. 231 ff.

rät. Keiner der Akteure hat Veranlassung, sein Verhalten zu ändern, weshalb ein stabiler Zustand (**Nash-Gleichgewicht**) erreicht ist.[85] Damit hat sich die gesamtgesellschaftlich effiziente Sorgfalt herausgebildet.

44 Sind allerdings in der Ausgangssituation weniger als 50% der Schiffe mit einem Funkgerät ausgestattet, ist es ineffektiv, neue Schiffe mit einem solchen auszurüsten. Es besteht wiederum ein Nash-Gleichgewicht, allerdings auf gesamtgesellschaftlich ineffizientem, niedrigem Sorgfaltsniveau. Dieses Gleichgewicht kann nun aber mit Hilfe einer Verschuldenshaftung durchbrochen werden: Wird das Fahren ohne Funkgerät als fahrlässig definiert, besteht dadurch auch bei einer Funkgerätepenetration von weniger als 50% ein Anreiz dafür, Schiffe mit einem Funkgerät auszurüsten. Das ineffiziente Nash-Gleichgewicht wird durchbrochen.

3. Anwendung auf IT-Bereiche

45 Diese allgemeinen Kriterien lassen sich ohne weiteres auch auf IT-Produkte und Dienstleistungen übertragen – allerdings mit der Maßgabe, dass der Komplexität der Produkte und der diffizilen Fehlerentdeckung Rechnung getragen werden muss.

a) Technische Standards

46 Allgemeingültige technische Standards, etwa in Gestalt von ISO-Normen, liegen – soweit ersichtlich – für IT-Produkte und erst recht für IT-Dienstleistungen bislang nicht breitflächig vor. Von Relevanz werden im Rahmen der weiteren Analyse vor allem auf Seiten der Produzenten die sog. **Common Criteria-Standards**, die sich als internationaler Standard für IT-Produkte und deren Sicherheitsbewertung (ISO-Norm)[86] herausgebildet haben.[87] Im Zusammenhang mit sog. Protection Profiles, die halbstandardisiert für Sicherheitsbedürfnisse von IT-Anwendungen erstellt werden, können diese Produktstandards rechtliche Wirkung entfalten, indem sie die nötige Mindestsicherheit für bestimmte Bereiche konkretisieren.

47 Aber auch auf der Seite der IT-Nutzer bzw. Verwender können Standards eine Rolle spielen, wie die jüngst verabschiedete ISO 27000 ff. Normenreihe, die Grundsätze für das IT-Riskmanagement aufstellt.

---

85 Es handelt sich um ein evolutorisch stabiles Nash-Gleichgewicht.

86 Gemeinsame Kriterien für die Prüfung und Bewertung von Sicherheit von Informationstechnik nach der im Jahre 2000 beschlossenen ISO-Norm 15408 bezeichnet; zur Entwicklung s. *Münch*, RDV 2003, 223.

87 Näheres dazu auch abrufbar unter: http://www.bsi.bund.de.

b) Anpassung an bestimmte Marktanforderungen

48 Ebenso spielen aber auch besondere Anforderungen in bestimmten Märkten eine Rolle, die die berechtigten Verkehrserwartungen prägen können, etwa im Gesundheits-, Sicherheits- oder Finanzsektor. Umgekehrt können an eine Massensoftware mit niedrigem Gefährdungspotential (und geringem Preis) vergleichsweise reduzierte Sicherheitsanforderungen gestellt werden. Indes ist nicht zu verkennen, dass der Trend zur Erstellung der Protection Profiles bereits diese Spezifika berücksichtigt.

c) Verhältnis zum Eigenschutz

49 Schließlich spielen im IT-Bereich die Fragen des Eigenschutzes bei der Bestimmung der Pflichten eine gewichtige Rolle: Hier gilt zunächst wiederum in Anwendung der allgemeinen Grundsätze, dass gegenüber professionellen IT-Anwendern prinzipiell reduzierte Pflichten gelten, sofern diese selbst in der Lage sind, den nötigen Eigenschutz zu gewährleisten. Allerdings versagt dies gerade dort, wo der **Code nicht zugänglich** ist oder der IT-Anwender nicht über entsprechende Kenntnisse verfügt. Ferner kommt es darauf an, ob und inwieweit allgemein bekannte Tools oder Softwareschutzmechanismen dem Nutzer zur Verfügung stehen.[88]

4. Sicherheitspflichten innerhalb von Vertragsverhältnissen

50 Im Unterschied zum Deliktsrecht zeichnet sich das Vertragsrecht dadurch aus, dass es den Parteien aufgrund der Privatautonomie hier selbst obliegt, die Pflichtensphären für die IT-Sicherheit festzulegen. Im Rahmen von Individualverträgen haben die Parteien hier weiteste Gestaltungsspielräume, die lediglich durch zwingende gesetzliche Regelungen und gesetzliche Verbote bzw. Sittenwidrigkeit (§§ 134, 138) begrenzt werden. Größerer Kontrolle unterliegt jedoch die Vertragsgestaltung durch Allgemeine Geschäftsbedingungen. Für Verträge zwischen Unternehmern und Verbrauchern statuieren die §§ 308 f. BGB zahlreiche Klauselverbote. Diese sind auch für Verträge über IT-Produkte anwendbar; für spezifische IT-Risiken treffen sie jedoch keine gesonderten Regelungen. Umso größere Bedeutung erlangt somit die Generalklausel des § 307 BGB. Danach sind Bestimmungen in Allgemeinen Geschäftsbedingungen dann unwirksam, wenn sie den Vertragspartner des Verwenders unangemessen benachteiligen. Genauere Konkretisierung erfährt diese Generalklausel durch Abs. 2 der Vorschrift, nach dem eine unangemessene Benachteiligung im Zweifel dann anzunehmen ist, wenn die vertrag-

[88] Ausführlich dazu unten Rn. 277 ff.

liche Klausel mit dem Grundgedanken der gesetzlichen Regelung nicht zu vereinbaren ist oder wesentliche Rechte und Pflichten, die sich aus der Natur des Vertrages ergeben, so einschränkt, dass die Erreichung des Vertragszweckes gefährdet ist. Insbesondere der letztgenannte Unwirksamkeitsgrund für AGB-Klauseln ist eine für IT-Verträge bedeutsame Grenze der Privatautonomie.

51 Die Regelungen der §§ 308, 309 BGB gelten nur für Verträge zwischen Verbrauchern und Unternehmern. Auf andere Verträge finden sie keine Anwendung. Indes findet gerade die allgemeine Inhaltskontrolle nach § 307 BGB – freilich mit größerem Gestaltungsspielraum – auch bei Verträgen zwischen Unternehmern Anwendung.

III. Gefahrenpotential und Gegenmaßnahmen

52 Um zu verdeutlichen, welche Risiken und daraus folgend Haftungen eintreten können, ist es notwendig, die sich bei der Nutzung von Informationstechnik, insbesondere IT-Netzen, ergebenden Gefahren näher zu beleuchten. Aus Sicht der Nutzer ist des Weiteren zu erläutern, welche Gegenmaßnahmen grundsätzlich ergriffen werden können, da sich daraus deren Pflichtenprogramm ableiten kann.

53 Werden Pflichten an eine wie auch immer geartete Zumutbarkeitsabwägung geknüpft, wird auch eine Einschätzung über die **voraussichtlichen Kosten** benötigt. Diese ist natürgemäß im vorgegebenen Rahmen dieser Untersuchung ungenau und soll nur eine Richtlinie darstellen. Notwendig ist im Rahmen einer solchen Abwägung jeweils eine Einzelfallbetrachtung und nähere technisch-betriebswirtschaftliche Analyse. So können Kosten bei größeren Systemen überdurchschnittlich skalieren, wobei auch die Gefahrensituation mit der Größe von Rechensystemen und –netzen wachsen kann.

54 Anhaltspunkte für Bedrohungspotentiale und Gefahrenlagen lassen sich aus den Aufgaben des IT-Managements im Allgemeinen und für die IT-Sicherheit im Speziellen entnehmen, die darin bestehen, die **Integrität, Verfügbarkeit und Vertraulichkeit von Daten und Diensten, sowie die Authentizität eines Senders/Empfängers sicherzustellen**:[89]

[89] Rundschreiben BaFin Nr. 18/2005 über „Mindestanforderungen an das Risikomanagement“ vom 20.12.2005, AT 7.2, S. 9 Rn. 2, abrufbar unter http://www.bafin.de/rundschreiben/89_2005/051220_anl1.pdf (zuletzt abgerufen am 20.02.2006).

- Integrität bedeutet, dass nur autorisierte und im Sinne der Systemfunktionalität gewollte Modifizierungen von Hardware, Software und Daten durchgeführt werden können.[90]

- Unter Authentizität versteht man die eindeutige Identifizierung eines Senders/Empfängers von Daten[91], wie sie z.B. in einer sog. „Public Key Infrastructure“[92] gewährleistet ist.

- Der Begriff der Verfügbarkeit meint, dass ein IT-System zum gewünschten Zeitpunkt mit den erforderlichen Funktionen und Daten zur Verfügung steht. Es handelt sich somit um eine zentrale Anforderung.

- Unter Vertraulichkeit ist der Schutz im Hinblick auf Lesen, Schreiben, Modifizieren oder Löschen von Daten vor dem unbefugten Zugriff und/oder die Weitergabe von Daten durch unbefugte Personen oder Prozesse zu verstehen.[93]

55 Für die **Netz- und Informationssicherheit** kann schließlich die Definition der EU im Rahmen der Errichtung einer europäischen Agentur zur Netz- und Informationssicherheit herangezogen werden, wonach darunter die Fähigkeit eines Netz- oder Informationssystems zu verstehen ist, Störungen oder rechtswidrige oder böswillige Angriffe abzuwehren, die die Verfügbarkeit, Integrität, Vertraulichkeit und Authentizität der gespeicherten oder übermittelten Daten und damit verbunden über das betreffende Netz angebotene Dienste beeinträchtigen können.[94]

56 Zur möglichst vollständigen Erreichung dieser Schutzziele müssen alle Beteiligten (d.h. Hersteller, Intermediäre und Nutzer von IT-Systemen) eng zusammenarbeiten und entsprechende Schutzvorkehrungen treffen. Besondere Sorgfalt ist geboten, wenn besondere Gefahrenpotentiale vorliegen, die in diesem Abschnitt beschrieben werden. Dies beinhaltet eine Abschätzung des Risikos eines Gefahrenpotentials und der möglichen Gegenmaßnahmen, jedoch keine rechtliche Bewertung.

57 Der Schwerpunkt wird nachfolgend auf Szenarien gelegt, bei denen Angreifer das Ziel verfolgen, fremde Systeme unter ihre Kontrolle zu bringen, um mit diesen kompromittierten Systemen wiederum Angriffe gegen Dritte durchzuführen. Vergleichbare Szena-

---

90 Datensicherheit in Industrie und Wirtschaft, *S&S International GmbH, uti-maco GmbH,* (1994).

91 *Singh*, in: *Bidgoli*, Handbook of Information Security, Volume 1, S. 28.

92 Zur Funktionsweise: *Radia Perlman*, in *Bidgoli*, Handbook of Information Security, Volume 1, S. 852 ff. und *Bradley S. Rubin* in; *Bidgoli*, Handbook of Information Security, Volume 2, S. 548 ff.

93 *Singh*, in: *Bidgoli*, Handbook of Information Security, Volume 1, S. 28.

94 Verordnung (EG) Nr. 460/2004 des Europäischen Parlaments und des Rates vom 10. März 2004 zur Errichtung der Europäischen Agentur für Netz- und Informationssicherheit, Abl. L 77, 13.3.2004; *Holznagel*, Recht der IT-Sicherheit, S. 11; *Eckert*, IT-Sicherheit, S. 5.

rien bzw. Schadensfälle lassen sich für zahlreiche andere Länder nachweisen, etwa für Österreich.[95]

1. Angriffe gegen Einzelsysteme

a) Systeme unter Kontrolle des Angreifers bringen

(1) Viren

58 Bis heute hat sich in der Forschung keine einheitliche Definition für den Begriff des Computervirus` durchgesetzt.[96] Grundsätzlich werden unter **Computerviren** sich selbst vermehrende Computerprogramme verstanden.[97] Viren treten niemals alleine auf, sondern benötigen einen Wirt,[98] um ausgeführt zu werden, sich zu verbreiten und evtl. vorhandene Schadfunktionen auszuführen.[99] Bei einem Wirt handelt es sich meist um ausführbare Dateien, die von einem Virus infiziert wurden oder infiziert werden können. Als Wirt können aber auch Programme dienen, die Makros enthalten.[100] Durch Infektion wird der Wirt so verändert, dass mit seiner eigenen Ausführung auch die Funktionen des Virus ausgeführt werden, wobei Viren stets versuchen, die eigene Existenz zu verdecken und gleichzeitig möglichst viele Wirte zu infizieren. Zur Reproduktion und Verbreitung sind in jedem Fall Ressourcen des Rechners erforderlich. Nicht selten ist dies sogar die einzige Schadfunktion.[101]

59 Im Gegensatz zu Computerwürmern,[102] die sich autark verbreiten können, muss ein Anwender eine mit einem Virus infizierte Datei ausführen, damit der Virus sich weiterverbreiten kann.[103] Die Verbreitung infizierter Dateien erfolgte - vor der Verfügbarkeit von weltweiten Netzwerken wie dem Internet - hauptsächlich über Wechseldatenträger wie Disketten und CD-ROMs.[104] Diese Verbreitungswege wurden jedoch nahezu komplett durch netzbasierte Verbreitungen wie E-Mail und Downloads von FTP- oder Web-Servern verdrängt.

---

95 So gingen bei einem Austausch des Kernbankensystems zur Einführung eines einheitlichen EDV-Systems für die BAWAG und die PSK tausende Buchungen verloren, s. Tageszeitung Kurier 2.10.2004.

96 *Bigdoli*, Handbook of Information Security, Volume 3, S. 95.

97 *Anonymus*, der neue hacker's guide, S. 401; *Eckert*, IT-Sicherheit, S. 45 f.

98 *Lang*, JurPC 205/2001, Rn. 50.

99 *Slade*, in: Bidgoli, Encyclopedia of Informationsystems Volume 1, 2002, S.256, 258 f., 358 f.

100 *Tita*, VW 2001, 1696; *Lang*, JurPC 205/2001, Rn. 61, *Anonymus*, der neue hacker's guide, 413.

101 *Bigdoli*, Handbook of Information Security - Volume 3, S. 95.

102 S. u. B.III.1.a)(2).

103 *Lang*, JurPC 205/2001, Rn. 50.

104 *Unbekannt*, VW 1996, 580; weiter dazu AG Köln DuD 2001, 298; LG Köln NJW 1999, 3206; *Leible/Sosnitza*, K&R 2002, 51.

60 Mögliche Gegenmaßnahmen: Virenscanner[105] sind, wie der Name bereits nahe legt, eine effektive und gängige Maßnahme, um die Infektion mit Viren zu verhindern und stellen die Grundvoraussetzung für den Schutz vor Viren dar. Neben dem Einsatz auf lokalen PCs als Wächterprogramm, welches jeden Dateizugriff auf einen möglichen Virenbefall überprüft und dem regelmäßigen Prüfen aller lokal vorhandener Dateien, ist in vernetzten Umgebungen der Einsatz zentraler Virenscanner auf den E-Mail- und Dateiservern zu empfehlen. Oberstes Gebot ist es jedoch, die Virendefinitionsinformationen für die jeweilige Antivirensoftware stets aktuell zu halten. Alle wichtigen Anbieter haben dafür standardmäßig eine automatische, webbasierte Updatefunktion in ihre Produkte implementiert, so dass der Anwender sich nach der erstmaligen Einrichtung kaum noch persönlich darum kümmern muss.

61 Einschätzung des Gefährdungspotentials: Aufgrund der Eigenschaft von Computerviren, sich nur unter Mithilfe des Anwenders weiterverbreiten zu können und durch den routinemäßigen Einsatz von Virenscannern, stellen klassische Computerviren heute keine besonders große Gefahr mehr für die IT-Sicherheit dar. Viren wurden von sich selbstständig verbreitenden Computerwürmern abgelöst,[106] die sich die weltweite Vernetzung von Computern und Schwachstellen von Software zu Nutze machen, um sich schneller und effektiver zu verbreiten als Viren.

(2) Würmer

62 Während Viren darauf ausgelegt sind möglichst viele Wirte (Dateien) zu infizieren und auf eine Verbreitung dieser infizierten Dateien durch den Anwender angewiesen sind, nutzen **Computerwürmer**[107] die Netzwerkinfrastruktur, um sich selbst zu verbreiten, indem sie Netzwerkdienste missbrauchen (bspw. massenhafter Versand von E-Mails, die u.a. den Wurm enthalten[108] oder „Erweiterungen“ gebräuchlicher Protokolle wie IRC-, P2P oder Instantmessaging-Protokolle) oder Sicherheitslücken in Netzwerkdiensten, ebenso wie in sonstiger (populärer) Software, ausnutzen.[109] Von Würmern sind auch Plattformen betroffen, die von Viren bisher verschont geblieben sind. So sind gegenwärtig auch Mobiltelefone mit fehlerhafter Implementierung des Bluetooth-

105 *Slade*, in: Bidgoli, Encyclopedia of Informationsystems Volume 1, 2002, S.263.

106 80% der bei der Bundesverwaltung erkannten Schadprogramme waren Würmer und Trojaner, BSI-Lagebericht 2005, abrufbar unter: http://www.bsi.de/literat/lagebericht/lagebericht2005.pdf, S. 17 (zuletzt abgerufen am 09.10.2006).

107 *Slade*, in: Bidgoli, Encyclopedia of Informationsystems Volume 1, 2002, S.259, 358 f.

108 *Tita*, VW 2001, 1696.

109 *Lang*, JurPC 205/2001, Rn. 41; *Eckert*, IT-Sicherheit, S. 57.

Standards bedroht.[110] Im Gegensatz zu Viren, die versuchen möglichst viele Dateien zu infizieren, nisten sich Würmer im Wirtssystem so ein, dass sie möglichst unerkannt bleiben und bei jedem Systemstart ausgeführt werden. Das Ziel von Würmern muss nicht die Ausführung von Schadfunktionen sein, sondern kann auch in der reinen Weiterverbreitung liegen, die an sich bereits großen wirtschaftlichen Schaden anrichten kann, da zur Weiterverbreitung häufig enorme Ressourcen auf Seiten der infizierten, der zu infizierenden und vermittelnden Systeme gebunden werden.

63 Mögliche Gegenmaßnahmen: Neben dem standardmäßigen Einsatz von Virenscannern, die neben Viren auch Würmer und andere schadhafte Software (sog. Malware) erkennen und deren Ausführung verhindern können, ist der Einsatz von **Firewalls**[111] zu empfehlen, die an Schnittstellen zwischen Netzen oder Computersystemen den Datenverkehr kontrollieren und regulieren können.[112] Zu unterscheiden ist zwischen sog. Personal Firewalls, die lokal auf PCs eingesetzt werden können und zentralen Firewalls, die den Zugriff zwischen Netzen beschränken können. Firewalls ermöglichen es ebenso einzelnen Anwendungen Zugriff auf Netzwerkfunktionen zu ermöglichen bzw. zu verweigern wie auch den Zugang zu Netzwerkdiensten zu regulieren. Eine häufig angewandte Strategie zur Konfiguration von Firewalls sieht vor, allen Dienste/Anwendungen den Netzwerkzugriff zu verweigern und nur die benötigten Dienste/Anwendungen freizuschalten, um die Angriffsfläche möglichst klein zu halten und somit auch der Infektion und Verbreitung von Würmern vorzubeugen.

64 Weiter lässt sich gegen die Verbreitung von Würmern empfehlen, dem **Nutzer vom Betriebssystem nur die Rechte einzuräumen, die er wirklich benötigt**. was sich bei allen modernen Plattformen (Windows, Linux, Mac OS etc.) einfach dadurch realisieren lässt, im Alltag ohne Administratorrechte zu arbeiten.

65 Zusätzlich zu dem Einsatz von Firewalls und dem Entzug überflüssiger Rechte, empfiehlt sich die Installation von Systemen, die Angriffe aufgrund typischer Angriffsmuster erkennen und entsprechende Gegenmaßnahmen auslösen können. Solche Systeme werden als **Intrusion-Detection-Systeme**[113] (IDS) bzw. als **Intrusion-Prevention-**

---

110 *Eckert*, IT-Sicherheit, S. 870 ff.; *Tanenbaum*, Computer Networks, S. 784.

111 *Chari*, in: Bidgoli, Encyclopedia of Informationsystems Volume 2, 2002, S. 313.

112 *Fuhrberg/Häger/Wolf*, Internet-Sicherheit, S. 137; *Lang*, JurPC 205/2001, Rn. 99.; zur Funktionsweise: *Tanenbaum*, Computer Networks, S. 776 ff.

113 Dazu ausführlich BSI-Studie Einführung von Intrusion-Detection-Systemen, abrufbar unter: http://www.bsi.bund.de/literat/studien/ids02/dokumente/Grundlagenv10.pdf, S. 5 ff.; *Anonymus*, der neue

Systeme (IPS) bezeichnet, wobei der Unterschied darin liegt, dass ein IDS Angriffe zwar erkennen, aber nicht verhindern kann, während IPS zusätzlich in der Lage sind Gegenmaßnahmen einzuleiten. Bei IDS und IPS wird zwischen system- oder hostbasierten und netzwerkbasierten Ansätzen unterschieden.[114] IDS werden auf dem zu überwachenden System installiert und sammeln Informationen über das System und dessen aktuellen Zustand, um anhand von in einer Datenbank hinterlegten Mustern bzw. Heuristiken,[115] Angriffe zu erkennen und dann zuvor definierte Gegenmaßnahmen (bspw. Administratoren informieren, verdächtige Prozesse beenden, Firewall-Regeln anpassen, etc.) auszulösen.[116] Netzwerkbasierte IDS werden an zentralen Netzwerkknoten eingerichtet, so dass sie in der Lage sind möglichst alle Datenpakete in einem Netzwerk zu analysieren, verdächtige Aktivitäten zu melden und ggf. Gegenmaßnahmen einzuleiten.[117] Als Maßnahme gegen einen Wurmangriff, kann ein netzwerkbasiertes IPS in der Lage sein, die erhöhte Netzwerkaktivität zu erkennen und die Firewall-Regeln so anzupassen, dass der Angriff gestoppt werden kann.

66 **Einschätzung des Gefährdungspotentials:** Die Gefahr, die von Würmern ausgeht, ist signifikant höher als die von Viren. Durch die selbstständige Weiterverbreitung nach einer Infektion und die Nutzung der Netzwerkinfrastruktur, sind Würmer in der Lage in kürzester Zeit einen enormen wirtschaftlichen Schaden anzurichten.

(3) Trojaner

67 Als **Trojanische Pferde** (kurz auch **Trojaner** genannt) werden Programme bezeichnet, die als nützliche Anwendung getarnt sind, aber zusätzliche Funktionen beinhalten, die ohne Wissen und Zutun des Anwenders ausgeführt werden.[118] Das Ziel besteht darin, heimlich Aktionen auf dem System auszuführen, so dass diese vom Anwender nicht bemerkt werden. Trojaner verbreiten sich ähnlich wie Viren meist mit Hilfe des An-

---

hacker's guide, S. 290 ff.; *Chari*, in: Bidgoli, Encyclopedia of Informationsystems Volume 2, 2002, S. 327.

114 *Peikari/Chuvakin*, Kenne Deinen Feind, S. 462 f.

115 Funktionsweise, Probleme und Beispiele bei *Zhang/Lee/Huang*, Intrusion Detection Techniques for Mobile Wireless Networks, abrufbar unter: http://citeseer.ist.psu.edu/zhang03intrusion.html, (zuletzt abgerufen am 09.10.2006).

116 *Eckert*, IT-Sicherheit, S. 676.

117 *Peikari/Chuvakin*, Kenne Deinen Feind, S. 463.

118 BSI-Lagebericht 2005, abrufbar unter: http://www.bsi.de/literat/lagebericht/lagebericht2005.pdf, S. 19 (zuletzt abgerufen am 09.10.2006); RFC 1244 Site Security Hand Book, abrufbar unter: http://www.faqs.org/rfcs/rfc1244.html, 3.9.8.1.2 (zuletzt abgerufen am 09.10.2006); *Bölscher/Kaiser/Schulenburg*, VW 2002, 565; *Lang*, JurPC 205/2001, Rn. 44.

wenders, der im Glauben eine sinnvolle Anwendung zu installieren gleichzeitig den Trojaner installiert.[119]

68 Die Unterscheidung zwischen Viren, Würmern, Trojanern und anderer Malware wie bspw. Spyware (siehe dazu mehr Rn. 72) oder Backdoors (ermöglicht Dritten unbefugten Zugang zum System) fällt häufig schwer, da sich die verwendeten Konzepte häufig überschneiden. So kann ein Wurm die Schadfunktion eines Virus besitzen und sich zusätzlich als Trojaner tarnen, um sich zu verbreiten. In der Literatur wird häufig vertreten, dass Viren Spezialfälle von Trojanern seien.[120]

69 Oftmals funktionieren Trojaner auch nach dem Client-Server-Prinzip. Der eigentliche Trojaner ist dabei nur der Server. Er nistet sich als nützliche Anwendung getarnt auf dem Zielrechner ein und sorgt für seinen eigenen automatischen Start mit dem Betriebssystem. Der potenzielle Angreifer kann nun mittels des passenden Clients aktiv bei seinem Opfer Schaden anrichten und Informationen ausspionieren.

70 **Mögliche Gegenmaßnahmen:** Zusätzlich zu den bereits oben genannten Schutzmöglichkeiten durch Virenscanner und Firewalls, ist der generelle Hinweis zum Verzicht auf Programme aus unbekannten oder unsicheren Quellen für einen Schutz gegen Trojaner sinnvoll. Benutzern von PCs eines Unternehmensnetzwerks sollte es durch entsprechende Beschränkung der Rechte in einem System grundsätzlich nicht möglich sein, selbst Software zu installieren oder Software auszuführen, die nicht explizit freigegeben ist.[121]

71 **Einschätzung des Gefährdungspotentials:** Insgesamt geht von Trojanern eine erhebliche Gefahr für die IT-Sicherheit, da der durch sie entstehende Schaden nicht unbedingt zeitnah ersichtlich sein muss.

(4) Spyware

72 Unter Spyware versteht man Programme, die keinen direkten Schaden am System des Nutzers verursachen, es dafür aber ausspionieren.[122] Wie bei der Attacke mit einem trojanischen Pferd soll auch dieser Angriff für den betroffenen Benutzer unsichtbar ablaufen, um vor der Entdeckung möglichst viele Daten über die Tätigkeiten des Benutzers zu sammeln. Spyware wird häufig zusammen mit kostenfreien Programmen instal-

119 *Slade*, in: Bidgoli, Encyclopedia of Informationsystems Volume 1, 2002, S. 260, 360.
120 *Bidgoli*, Handbook of Information Security – Volume 3, S. 97.
121 *Eckert*, IT-Sicherheit, S. 62.
122 *Chan*, in: *Bigdoli*, Handbook of Information Security – Volume 3, S. 136.

liert,[123] doch auch bereits das Besuchen einer Website, die den (u.U. automatischen) Download von bestimmter Software benötigt, um richtig angezeigt zu werden, kann zur Infizierung genügen.[124] Die gesammelten Daten werden dann an einen Dritten (meist den Anbieter des Programms) weitergeleitet – dieser kann die gesammelten Daten dann verkaufen oder mit anderen Datenbanken verschmelzen.

73 **Mögliche Gegenmaßnahmen**: Neben den bereits erwähnten Firewalls und Intrusion-Detection-Systemen (IDS), empfiehlt sich der Einsatz eines Anti-Spyware Scanners, sowie der Einsatz von Pop-Up-Blockern.[125] Zudem sollte der Nutzer das sog. „Safe and Sane Browsing“[126] verfolgen, in dem er bei der Installation von kostenfreien Programmen vorsichtig agiert.

74 **Einschätzung des Gefährdungspotenzials:** Während der Schaden, der durch eine akute Virusinfektion oder eine massive Wurmattacke ausgelöst wurde, offensichtlich ist, kann eine durch einen Trojaner eingeschleuste oder auf anderem Wege installierte Spyware Geschäftsgeheimnisse an Dritte weiterleiten, wodurch ebenfalls ein schwerwiegender Schaden entstehen kann.[127]

(5) Unsichere Konfiguration

75 Viele der oben erklärten Angriffsmöglichkeiten werden erst durch **unsichere Konfiguration** von Computersystemen ermöglicht. Dies betrifft hauptsächlich private IT-Anwender, die weder das Wissen noch die finanziellen Möglichkeiten haben, um ihre Systeme sicher einzurichten und durch Wartung auch langfristig sicher zu betreiben. Unternehmen besitzen eigene IT-Abteilungen oder nehmen Dienstleister in Anspruch, um eine sichere Konfiguration ihrer Netze und Systeme zu erreichen.

76 Der erste Schritt zu einem sicheren System ist der Einsatz aktueller Software, um bekannt gewordene und durch den Hersteller beseitigte **Sicherheitslücken** zeitnah zu schließen. Dies betrifft neben dem Betriebssystem insbesondere Schutzsoftware wie Virenscanner und Firewalls und alle durch Dritte nutzbaren Serverdienste. Ebenfalls muss die Aktualität der Anwendungssoftware (Textverarbeitung, Mediaplayer, etc.) sichergestellt sein, um indirekte Angriffe zu verhindern. Besonders Würmer nutzten in den ver-

---

123 *Chan*, in: *Bigdoli*, Handbook of Information Security – Volume 3, S. 137.
124 *Chan*, in: *Bigdoli*, Handbook of Information Security – Volume 3, S. 137.
125 *Chan*, in: *Bigdoli*, Handbook of Information Security – Volume 3, S. 141 f.
126 *Chan*, in: *Bigdoli*, Handbook of Information Security – Volume 3, S. 142 f.
127 Nach Schätzungen sind rund 15% aller Notebooks und 20% aller Desktop-Systeme mit Spyware infiziert, PC PitStop Statistics, 2004.

gangenen Jahren Sicherheitslücken, die nicht ausreichend schnell geschlossen wurden, um sich rasant zu verbreiten. Daher ist es absolut notwendig die besonders kritischen Softwarekomponenten (Betriebssystem, Schutzsoftware und Serverdienstsoftware) stets aktuell zu halten, was durchaus bedeuten kann, mehrmals täglich Aktualisierungen einzuspielen. Neben der Aktualisierung der eigentlichen Software, müssen auch die Datenbanken von Virenscannern und anderer Schutzsoftware aktuell gehalten werden, damit diese neue Malware und Angriffsmuster erkennen und die Anwender davor schützen können.

77 Der zweite Schritt zu einem sicheren System besteht in dem Anpassen der **Sicherheitseinstellungen des Computers**. Grundsätzlich kann der Rat gegeben werden, den Benutzern eines Systems immer nur die Rechte einzuräumen, die sie benötigen, um ihre Aufgaben zu erfüllen. Keinesfalls sollten Anwender mit unbeschränkten Rechten (Administrator-Rechte unter Windows) arbeiten, um zu verhindern, dass ggf. vorhandene Malware ebenfalls unbeschränkte Rechte erhält.

(6) Webbasierte Dienste

78 Durch die Verbreitung des Internets werden häufig Anwendungen als **webbasierte Dienste** angeboten; d.h. die Anzeige/Repräsentation von Anwendungen erfolgt mit Hilfe eines lokal installierten Webbrowsers, während die Logik und Datenhaltung auf zentralen Webservern geschieht.[128] Für die Repräsentation wird in der Regel die Auszeichnungssprache HTML verwendet, die vom Browser interpretiert und als Internetseite dargestellt wird. Da es sich bei HTML um keine Programmiersprache handelt, sind die Möglichkeiten der Interaktion deutlich eingeschränkt und jede Veränderung der lokalen Repräsentation (bspw. Eingabe eines Suchbegriffs) ist mit einem Anfrage-Antwort-Zyklus an den zentralen Server verbunden. Um diese Einschränkung zu umgehen, wurden die sogenannten **Aktiven Inhalte** (JavaScript,[129] Microsoft Active X, Plug-Ins wie Flash oder Java[130]) entwickelt, die Erweiterungen des Browsers darstellen und es erlauben dynamisch auf Benutzeraktionen zu reagieren. Aktive Inhalte, vor allem Active X und Java Applets werden als sog. „mobile code“[131] bezeichnet, da sie auf dem Computer des Nutzers ausgeführt werden, also vor dem

128 *Eckert*, IT-Sicherheit, S. 69 ff.; *Tanenbaum*, Computer Networks, S. 816.
129 *Seila/Miller*, in: Bidgoli, Encyclopedia of Informationsystems Volume 2, 2002, S. 693.
130 *Garfolo*, in: Bidgoli, Encyclopedia of Informationsystems Volume 2, 2002, S. 715.
131 *Opyrchal*, in : van Tilborg, Encyclopedia of Crypthography and Security, S. 657.

Ausführen vom Server zum Client übertragen werden.[132] Durch teilweise fehlerhafte Implementierungen dieser Erweiterungen in nahezu allen am Markt relevanten Browsern und der Ausnutzung dieser Schwachstellen durch Malware, sind Aktive Inhalte in den letzten Jahren zu einem ernsthaften Sicherheitsproblem geworden.[133]

79 **Mögliche Gegenmaßnahmen**: Neben der Grundvoraussetzung der Aktualität des benutzten Browsers, ist das grundsätzliche Deaktivieren der Unterstützung für Aktive Inhalte anzuraten.[134] Da viele webbasierte Anwendungen die Unterstützung von Aktiven Inhalten voraussetzen, sollten Browser eingesetzt werden, die es ermöglichen einzelnen, vertrauenswürdigen Seiten die Benutzung von Aktiven Inhalten ausdrücklich zu erlauben. Zur Verhinderung eines Angriffes durch webbasierte Anwendungen ist zusätzlich der Einsatz einer sog. „Personal Firewall" zu empfehlen, die zusätzlich zu der das gesamte Netzwerk schützenden Firewall in der Peripherie des Netzes auf dem jeweiligen Computer des Nutzers arbeitet.[135] Wie üblich ist außerdem der Einsatz eines Virenscanners von Vorteil.

80 **Einschätzung des Gefährdungspotentials**: Durch Fehler in der Implementierung von Aktiven Inhalten sind besonders Anwender gefährdet, die häufig verschiedenste Internetseiten besuchen oder webbasierte Anwendungen nutzen, deren Vertrauenswürdigkeit sie nicht kennen. Anwender, die firmeneigene Intranet-Applikationen und vertrauenswürdige Seiten mit Hilfe eines Webbrowsers besuchen, sind entsprechend weniger gefährdet. Allerdings sollte die Gefahr, die von solchen webbasierten Angriffen aufgrund des Einsatzes von unsicheren Browsern ausgeht, keinesfalls unterschätzt werden.

b) Koordination der angegriffenen Systeme (Bot-Netze)

81 Angegriffene Systeme können auch für koordinierte Angriffe verwendet werden. Hierfür hat sich der Begriff der Bot-Netze etabliert. Unter **Bot-Netzen** (Abkürzung von Roboter-Netzwerk) werden fernsteuerbare Netzwerke von PCs verstanden, welche aus untereinander kommunizierenden Bots bestehen.[136] Bei Bots handelt es sich um Software, die im Hintergrund auf den betroffenen PCs und meist ohne Kenntnis des Anwenders

---

132 *Song Fu und Cheng-Zhong Hu*, in: *Bidgoli*, Handbook of Information Security, Volume 3,S. 146; *Charles Border*, in: *Bidgoli*, Handbook of Information Security, Volume 3, S. 345.

133 Dazu BSI abrufbar unter: http://www.bsi-fuer-buerger.de/browser/02_03.htm.

134 Beispiel Netscape-Browser: *Border*, in: *Bidgoli*, Handbook of Information Security, Volume 3,S. 346.

135 *Border*, in: *Bidgoli*, Handbook of Information Security, Volume 3,S. 347; *Tanenbaum*, Computer Networks, S. 816; *Opyrchal*, in: van Tilborg, Encyclopedia of Crypthography and Security, S. 657.

136 Dazu BSI-Lagebericht 2005 abrufbar unter: http://www.bsi.de/literat/lagebericht/lagebericht2005.pdf, S. 21 (zuletzt abgerufen am 09.10.2006); *Tanenbaum*, Computer Networks, S. 818, 819, *Opyrchal*, in: van Tilborg, Encyclopedia of Crypthography and Security, S. 661.

ausgeführt wird.[137] Bots werden häufig in Folge eines Wurm- oder Trojanerangriffs eingerichtet und sind darauf vorbereitet ist, Befehle von einer zentralen Instanz zu empfangen. So werden Bot-Netze für den Versand von Spam-Mails oder koordinierte Angriffe gegen Dritte benutzt. Technisch sind Bot-Netze meist so organisiert, dass sich jeder Bot bei einem zentralen Server meldet, von dem aus der Angriff koordiniert wird, indem der Angreifer allen Bots den gleichen Befehl sendet. Dies potenziert die Wirksamkeit eines Angriffs (bspw. DoS-Angriff, siehe Rn. 87 ff.), da Bot-Netze mit mehreren tausend Bots eine enorme Bandbreitensumme besitzen können, die in der Regel die Bandbreite des Angegriffenen übersteigt. Die Struktur von Bot-Netzen ermöglicht durch gezieltes Ausschalten des zentralen Servers, die Koordination des Netzwerks und damit auch die Nutzbarkeit zu verhindern. Daher benutzen aktuelle Bot-Netze aus dem Bereich der P2P-Anwendungen bekannte verschlüsselte, dezentrale Kommunikationsstrukturen.[138]

82 Mögliche Gegenmaßnahmen: Für den Anwender eines von einem Bot befallenen PCs gleicht dies den Maßnahmen, die bereits für Computerviren und -würmer erläutert wurden.[139]

83 Einschätzung des Gefährdungspotentials: Die Gefährdung für einen von einem Bot befallenen PC bzw. dessen Anwender besteht hauptsächlich durch die von dem Bot verbrauchten Ressourcen. Bots enthalten meist keine Schad- oder Weiterverbreitungsfunktionen, damit sie dem Anwender nicht auffallen. Eine große Gefährdung stellen Bot-Netze hingegen für die Opfer eines koordinierten Bot-Netz-Angriffs dar.

2. Koordinierte Angriffe

84 Im ersten Schritt wurden Gefahrenpotentiale beschrieben, die geeignet sind, Einzelsysteme anzugreifen und unter die Kontrolle des Angreifers zu bringen. Im zweiten Schritt werden Gefahren beschrieben, die im Rahmen von koordinierten Angriffen von kompromittierten Systemen ausgehen, um Systeme Dritter zu schädigen.

a) Ausnutzung von Software-Schwachstellen (exploits)

(1) Sicherheitslücken

---

137 *Cronin*, in: van Tilborg, Encyclopedia of Crypthography and Security, S. 144, *Tanenbaum*; Computer Networks, S. 778.

138 Dazu auch abrufbar unter: http ://www.heise.de/newsticker/meldung/print/72557 (zuletzt abgerufen am 09.10.2006).

139 Zu den Gegenmaßnahmen s.u. Rn. 88.

85 Durch nicht geschlossene **Sicherheitslücken in Software**, die Internetdienste erbringt und daher über das Internet erreichbar ist, sind Angreifer in der Lage, das System zu kompromittieren. Ein solcher Fehler kann bspw. bewirken, dass der Dienst ausfällt oder der Schadcode auf dem System ausgeführt werden kann. Derartige Lücken werden häufig von Würmern ausgenutzt, um sich im System einzunisten. Erwähnt sei an dieser Stelle der Wurm „Sasser", welcher im Mai 2004 einen Systemdienst in Microsoftbetriebssystemen ab Windows NT dazu missbrauchte, den Rechner zufällig auszuschalten. Die wirtschaftlichen Schäden waren enorm.[140] Diese Art von Angriffen, ließen sich auch direkt – d.h. ohne Bot-Netze – ausführen, jedoch verhindert dieser „Umweg" die Rückverfolgungen des Angreifers. Die Ausnutzung der Lücke ist folglich der erste Schritt zum Ausführen koordinierter Angriffe.

(2) Input-Validierung

86 Ähnliche Folgen wie nicht geschlossene Sicherheitslücken kann **mangelhafte Eingabeüberprüfung** (Input-Validierung) der durch den Anwender eingegebenen Daten bei webbasierten Diensten haben.[141] Dadurch kann z.B. ein eigener Code eingeschleust werden, der anschließend direkt eine Schadfunktion ermöglicht, oder ein entsprechendes Programm nachlädt und installiert. Auf diese Art und Weise kann der Angreifer weit reichende Kontrolle über das System erlangen.[142] Die fehlende Input-Validierung ist somit ein Spezialfall der Sicherheitslücken.[143]

b) Gezielte Überlastung von Diensten (Denial-of-Service-Angriffe)

87 Ein typisches Einsatzgebiet für Bot-Netze sind sogenannte **Denial-of-Service**-Angriffe (DoS-Angriffe)[144], deren Ziel darin besteht, eine gezielte Überlastung von Diensten zu erreichen, so dass diese Dienste nicht mehr nutzbar sind.[145] Bei DoS-Angriffen wird das angegriffene System massenhaft mit Anfragen belastet, bis die Ressourcen des Systems ausgeschöpft sind und es nicht mehr auf reguläre Anfragen antworten kann.[146] Wird ein

---

140 S. dazu heise-Newsmeldung vom 6.7.2005, abrufbar unter: http://www.heise.de/newsticker/result.xhtml?url=/newsticker/meldung/61451&words=Sasser.

141 Zum Pufferüberlauf, der sowohl bei lokal ausgeführter Software, aber gerade auch für ans Netz angebundene Server gefährlich ist *Peikari/Chuvakin*, Kenne Deinen Feind, S. 171 ff.

142 *Sviatoslav Braynow*, in: Bigdoli, Handbook of Information Security, Volume 3, S. 58.

143 S. dazu auch: *Rhodenizeri*, in: Bidgoli, Encyclopedia of Informationsystems Volume 4, 2002, S. 49 ff.

144 *Kabay*, in: Bidgoli, Encyclopedia of Informationsystems Volume 1, 2002, S. 356.

145 BSI-Lagebericht 2005, abrufbar unter: http ://www.bsi.de/literat/lagebericht/lagebericht2005.pdf, S. 19 (zuletzt abgerufen am 09.10.2006); *Anonymous*, Der neue hacker's guide, 375 ff.; *Cronin*, in: van Tilborg, Encyclopedia of Crypthography and Security, S. 143.

146 *Bölscher/Kaiser/Schulenburg*, VW 2002, 565; *Kurose/Ross*, Computer Networking, S. 648.

solcher DoS-Angriff von mehreren Bots eines Bot-Netzes ausgeführt, so spricht man von einem Distributed-Denial-of-Service-Angriff (DDoS), da es sich um eine Vielzahl von Angreifern handelt, die allerdings koordiniert handeln.[147] Eine weitere Variante, die ebenfalls mit Hilfe von Bot-Netzen durchgeführt werden kann, sind sogenannte Distributed-Reflected-Denial-of-Service-Angriffe (DRDoS). Hierbei sendet der Angreifer seine Datenpakete nicht direkt an das Opfer, sondern an reguläre Internetdienste Unbeteiligter, trägt jedoch als Absenderadresse die des Opfers ein.[148] Die Antworten auf diese Anfragen stellen für das Opfer den eigentlichen DoS-Angriff dar. Für das Opfer erscheint es, als würde der Angriff von diesen Internetdiensten ausgehen - der Ursprung des Angriffs ist durch diese Vorgehensweise praktisch nicht mehr ermittelbar.[149] DoS-Situationen können auch auf anderen Wegen als durch eine gezielte Attacke auf das betroffene System entstehen: So können Fehler in der Software zu einer Überlastung des Systems führen.[150] Weiterhin können Sicherheitslücken von Viren ausgenutzt werden, um eine solche Situation herbeizuführen (so geschehen mit dem MSBlaster-Wurm).[151]

88 **Mögliche Gegenmaßnahmen**: Da die Absender der böswilligen Anfragen aufgrund der Struktur von Bot-Netzen über das gesamte Internet verteilt sind, können die böswilligen Anfragen nicht anhand ihrer Absenderadressen von regulären Anfragen durch eine Firewall unterschieden und gesperrt werden. Eine Möglichkeit besteht darin, die Anzahl der Anfragen pro Zeiteinheit und pro Absender zu begrenzen, was zwar den DoS-Angriff lindern würde, doch ggf. auch reguläre Anfragen behindern könnte.[152] Im Fall

---

147 *Anonymus*, Der neue hacker's guide, 393 f.; *Kurose/Ross*, Computer Networking, S. 649; *Todd*, Distributed Denial of Service Attacks, abrufbar unter: http://www.linuxsecurity.com/resource_files/intrusion_detection/ddos-faq.html (zuletzt abgerufen am 09.10.2006).

148 *Paxson*, An Analysis of Using Reflectors for Distributed Denial-of-Service, abrufbar unter: http://www.icir.org/vern/papers/reflectors.CCR.01/reflectors.html (zuletzt abgerufen am 09.10.2006).

149 Dazu abrufbar unter: http://de.wikipedia.org/wiki/Denial_of_Service (zuletzt abgerufen am 05.06.2007); zwar werden in der theoretischen Informatik Methoden zur Rückverfolgen (Traceback) auch bei gefälschten Adressen behandelt, ihnen ist jedoch gemein, dass sie entweder eine Erweiterung des Internet Protocol (IP) oder der Routerprogrammierung benötigen oder einen erheblichen Aufwand erfordern, den die angegriffene Maschine in der Regel nicht wird leisten können. Gegen DDoS-Angriffe wächst der Aufwand natürlich mit der Anzahl der angreifenden Systeme, bei DRDoS-Angriffen kann nur der vermeintliche Angreifer ermittelt werden; s. bspw. *Stone*, CenterTrack: An IP Overlay Network for Tracking DoS Floods, abrufbar unter: http://www.arbornetworks.com/downloads/research51/stone00centertrack_new.pdf (zuletzt abgerufen am 09.10.2006).

150 *Schulz*, in: Bigdoli, Handbook of Information Security, Volume 3, S. 206.

151 *Schulz*, in: Bigdoli, Handbook of Information Security, Volume 3,: Threats, Vulnerabilities, Prevention, Detection, and Management, S. 207.

152 Weitere mögliche Reaktionen auf einen Angriff in: Results of the Distributed-Systems Intruder Tools Workshop, abrufbar unter: http://www.cert.org/reports/dsit_workshop.pdf, S. 14 f. (zuletzt abgerufen am 05.06.2007).

eines DRDoS-Angriffs gilt im Wesentlichen das Gleiche. Zusätzlich sollten Provider an den Übergangspunkten zum Internet (Router) nur solche Datenpakete passieren lassen, deren Absenderadresse aus ihrem eigenen Adressraum stammt, damit keine Pakete mit offensichtlich gefälschten Absenderadressen in das öffentliche Internet gelangen können.[153] Weiterhin empfiehlt sich auch gegen DoS-Angriffe eine Firewall.[154] Im Falle eines DDoS- oder DRDoS-Angriffs sind die Möglichkeiten einer Firewall jedoch begrenzt.[155] Für den Fall, dass ein DoS-Angriff bereits erfolgreich stattgefunden hat, bestehen ebenfalls Möglichkeiten diesen zu beseitigen: So kann der Betreiber des betroffenen Systems z.B. in bestimmten Fällen durch sog. „Failover Systems and Devices" den Betrieb unmittelbar wieder sicherstellen.[156]

89 **Einschätzung des Gefährdungspotentials**: Die Gefahr, Opfer eines massiven DoS-Angriffs zu werden, ist trotz aller möglichen Gegenmaßnahmen relativ hoch. Besonders Unternehmen, die Dienstleistungen über das Internet anbieten, können durch einen erfolgreichen DoS-Angriff und dem damit verbundenen Ausfall der betroffenen Dienste nicht nur einen enormen wirtschaftlichen Schaden, sondern auch einen Image-Schaden erleiden. An dieser Stelle seien vor allem eBay, Yahoo und CNN als Opfer von DoS-Angriffen erwähnt.[157] Der Internet Service Provider (ISP) CloudNine.com musste in Folge eines DoS-Angriffes sogar den Betrieb einstellen.[158]

3. Ergebnis

90 Wie sich zeigt, gibt es eine Vielzahl von möglichen Angriffsszenarien. Nicht gegen alle kann sich der Nutzer effektiv wehren. Die Gefährlichsten sind jedoch durchaus mit den entsprechenden Maßnahmen abwendbar.

IV. Abgrenzung der Verantwortlichkeitssphären: Hersteller – Nutzer – Intermediäre (Dienstleister)

91 Mit dem erforderlichen Maß des Eigenschutzes im Bereich der Verkehrssicherungspflichten ist bereits eine Hauptaufgabe der Rechtsordnung im Bereich der Gewährleistung von Sicherheit – ob im IT-Sektor oder in anderen Bereichen – angesprochen: Die

153 *Schulz*, in: Bigdoli, Handbook of Information Security, Volume 3, S. 215.
154 *Schulz*, in: Bigdoli, Handbook of Information Security, Volume 3, S. 215; *Tanenbaum*, Computer Networks, S. 778.
155 *Tanenbaum*, Computer Networks, S. 778, 779.
156 *Schulz*, in: Bigdoli, Handbook of Information Security, Volume 3, S. 215, weitere präventive und reaktive Maßnahmen finden sich auf den S. 214 ff.
157 *Kurose/Ross*, Computer Networking, S. 649.
158 *Schulz*, in: Bigdoli, Handbook of Information Security, Volume 3, S. 207.

Verteilung der sicherheitsnotwendigen Anforderungen auf bestimmte Risikosphären. Potenzielle Normadressaten sind dabei drei Gruppen von Personen, die mit Informationstechnik in Berührung kommen: Die Hersteller von IT-Produkten, die Nutzer dieser Produkte sowie die Gruppe der IT-Intermediäre[159], die eine Zwischenstellung einnehmen, da sie sowohl selbst Nutzer von IT-Produkten sind als auch Dritten die Nutzung von Informationstechnik als Host-, Content- bzw. Access-Provider ermöglichen.

92 Die Auswahl einer dieser Gruppen als Adressat von Sicherheitspflichten hat prinzipiell nach deren Verantwortungsbereichen zu erfolgen, die sich wiederum in Anwendung des aus der Ökonomischen Analyse des Rechts entstammenden Kriteriums des „**cheapest cost avoider**“[160] danach bestimmen lässt, wer über die besten Gefahrabwendungsmöglichkeiten sowie Kenntnisse über mögliche Gefahren verfügt.[161]

93 Demgemäß kann vergröbert von einer **Skala** gesprochen werden, an deren einem Ende die IT-Hersteller als diejenigen stehen, die am intensivsten Schutzpflichten unterliegen, am anderen Ende die IT-Anwender, die je nach Professionalität am wenigsten in der Lage sind, IT-Risiken zu beherrschen. Allerdings ist auch hier danach zu differenzieren, ob es sich um professionelle IT-Anwender handelt, insbesondere Unternehmen, die über entsprechende Ressourcen zum Selbstschutz verfügen könnten. In der Mitte der Skala sind diejenigen Unternehmen platziert, die selbst IT-Produkte professionell einsetzen, ihrerseits aber wiederum IT-Dienstleistungen erbringen (IT-Intermediäre), insbesondere die Gruppe der Access- und Host-Provider. Sie sind zwar primär Dienstleister, doch ändert dies nichts daran, dass sie im Grundsatz ähnlichen Pflichten wie die IT-Hersteller für ihre Produkte unterliegen.

C. Verantwortlichkeit der IT-Hersteller (Produktbezogene Pflichten)

159 Eingehend zum Begriff des Intermediärs für elektronische Märkte: *Sarkar/Butler/Steinfield*, Intermediaries and Cybermediaries: A continuing role for mediating players in Electronic Markets, in: Journal of Computer Mediated Communication (JCMC), Vol. 1, Nr. 3, 1995, abrufbar unter: http://jcmc.indiana.edu/vol1/issue3/sarkar.html (zuletzt abgerufen am 09.10.2006).

160 Diese von der Lehre der ökonomischen Analyse des Rechts entwickelte Argumentationsfigur weist die Sicherheitspflichten demjenigen zu, der den eingetretenen Schaden mit dem geringsten Aufwand zu vermeiden vermag (s. dazu ausführlicher: *Schäfer/Ott*, Lehrbuch der ökonomischen Analyse des Zivilrechts, S. 227 f.; *Calabresi*, The Cost of Accidents, S. 136 ff.; von “least-cost-avoiding” sprechend *Shavell*, Foundations of Economic Analysis of Law, Kap. 8. Rn. 2.11). Im in Deutschland vorherrschenden System der Wertungsjurisprudenz können ökonomische Rationalitätsgesichtspunkte jedoch nur neben andere – in erster Linie rechtsethische – Gesichtspunkte treten. Als alleiniger Begründungsansatz für rechtliche Lösungen können sie indes nicht ausreichen. Einen kurzen Überblick über die Problematik bietet Palandt-*Heinrichs*, Einleitung Rn. 34 ff., 39.

161 Zur Verteilung von Sorgfaltsmaßnahmen allgemein s. auch MünchKommBGB-*Wagner*, Vor § 823 BGB Rn. 44.

I. Überblick

94 Die Hersteller von IT-Produkten – sei es Hard- oder sei es Software – stehen am Anfang der IT-Wertschöpfungskette. Folgerichtig gelten für Hersteller von IT-Produkten im Grundsatz dieselben Anforderungen wie für andere Hersteller auch, in erster Linie die Grundsätze der **deliktischen Produzentenhaftung** (Rn. 104 ff.) und des verschuldensunabhängigen **ProdHaftG** (Rn. 189 ff.) Neben diese Ansprüche können im Einzelfall **vertragliche Ansprüche** gegen den Hersteller treten (Rn. 98).

95 Überlagert werden die zivilrechtlichen Anforderungen durch **öffentlich-rechtliche Regulierungen im Bereich der Produktsicherheit**, insbesondere des Geräte- und Produktsicherheitsgesetzes (GPSG) als grundlegendes Gesetz. Hauptinstrument der Gewährleistung von Sicherheit sind hier in materiell-rechtlicher Hinsicht bestimmte Grundpflichten der Hersteller, in verfahrensrechtlicher Hinsicht Zertifikate für sichere Produkte, gegebenenfalls auch die Genehmigungsbedürftigkeit von Produkten. Typisch für das deutsche und europäische Produktsicherheitsrecht ist dabei der Rückgriff auf bestimmte, in einem den Vorschriften des Gesetzes entsprechenden Verfahren erlassene technische Normen, an die sich unter Umständen sogar Vermutungswirkungen knüpfen können.

96 Öffentlich-rechtliches Produktsicherheitsrecht und zivilrechtliche Produkthaftung sind dabei in doppelter Hinsicht **miteinander verzahnt**: Zum einen können die öffentlich-rechtlichen Produktsicherheitsvorschriften als Schutzgesetze gem. § 823 Abs. 2 BGB qualifiziert werden, so dass sie deliktsrechtlich flankiert werden; zum anderen können aber auch öffentlich-rechtliche Normen und erteilte Zertifizierungen unter Umständen eine Einschränkung der deliktischen Haftung herbeiführen, sei es materiell-rechtlich, sei es verfahrensrechtlich über bestimmte prozessuale Wirkungen. Umgekehrt können deliktische Produkthaftungspflichten die Bestimmung öffentlich-rechtlicher Pflichten beeinflussen.

97 Beide Bereiche sind daher von **zentraler Bedeutung** für die Pflichten und die Risiken von IT-Herstellern; beide Bereiche können in **rechtspolitischer Hinsicht** gestaltend die Verteilung der Risiken aus IT-Produkten beeinflussen.

II. Vertragliche Mängelhaftung

98 Je nach gewähltem Vertriebsweg kommen bei fehlerhaften IT-Produkten auch vertragliche Ansprüche gegen den Hersteller in Betracht. **Hardwareprodukte** werden auch im

Internet regelmäßig nicht vom Hersteller selbst, sondern von selbständigen Vertriebsgesellschaften angeboten, so dass idR kein Vertrag mit dem Hersteller zustande kommt.

99 Insbesondere im **Unternehmensbereich** (B2B-Geschäft) bei Software steht die vertragliche Haftung des IT-Herstellers klar im Vordergrund,[162] da hier häufig direkte Verträge mit den Softwareherstellern geschlossen werden. Oftmals handelt es sich auch um dauerhafte oder zumindest langfristige Vertragsverhältnisse, die eine Mischung aus Softwareherstellung und Softwarepflege umfassen,[163] wobei die Pflege häufig als Zusatzleistung angeboten wird - so etwa bei den sog. Volumenlizenzverträgen der Firma Microsoft – sei es als entgeltlicher Pflegevertrag oder unentgeltliche Zusatzleistung in Form von frei verfügbaren Patches im Internet.[164] Je nach Art des Softwarevertriebs werden z.B. bei Online-Beschaffung von Software Allgemeine Geschäftsbedingungen (AGB) genutzt,[165] die wiederum – je nach Markt- bzw. Verhandlungsmacht – Haftungs- und Gewährleistungsausschlussklauseln enthalten. Grundsätzlich gilt selbstverständlich die Privatautonomie. Soweit es sich dabei um individuelle Vereinbarungen und keine AGB handelt, muss sich die Wirksamkeit dieser Vereinbarungen daher lediglich an den Grenzen der Sittenwidrigkeit nach § 138 BGB und des gesetzlichen Verbots (§ 134 BGB) messen lassen.[166] Handelt es sich aber um Haftungs- und Gewährleistungsausschlüsse in Allgemeinen Geschäftsbedingungen, bildet die Inhaltskontrolle nach dem § 307 BGB die Grenze der Privatautonomie,[167] – selbst bei B2B-Geschäften – und sorgt dadurch dafür, dass auch in vertraglichen Beziehungen ein Mindestmaß an Sicherheit nicht abbedungen werden kann.[168]

100 In diesem Zusammenhang stellt sich die Frage, ob durch die Schuldrechtsreform auch die Haftungsfreizeichnung für **mangelbezogene Folgeschäden** – die nunmehr direkt über § 280 I BGB erfasst werden – klauselfest ist, mithin der Vertragspartner (Hersteller) für sämtliche Vermögensfolgeschäden, die seine schadhafte Software

---

162 *Spindler*, in: FS Nagel, S. 22.

163 S. dazu *Spindler*, in: FS Nagel, S. 22; *Marly*, Rn. 508; *Peter*, in: Schneider/von Westphalen, Software-Erstellungsverträge, G Rn. 7 ff.; *Baum*, CR 2002, 705 ff.; *Koch*, Versicherbarkeit von IT-Risiken, Rn. 505.

164 *Peter*, in: Schneider/von Westphalen, Software-Erstellungsverträge, G Rn. 7 ff.

165 *Schneider*, Handbuch des EDV-Rechts, J Rn. 6; *Spindler*, in: FS Nagel, S. 23.

166 *v. Westphalen*, in: Schneider/v. Westphalen, Software-Erstellungsverträge, H Rn. 6.

167 Erman-*Roloff*, § 307 BGB Rn. 1.

168 Zur Wirksamkeit derartiger Klauseln generell *v. Westphalen*, in: Schneider/v. Westphalen, Software-Erstellungsverträge, H Rn. 6; bezogen auf Gewährleistungsbeschränkungen und die wegen § 307 BGB nicht erlaubte Verkürzung der Verjährungsfrist bei Software auf ein Jahr *Bartsch*, CR 2005, 9; *Schneider*, Handbuch des EDV-Rechts, J Rn. 244.

angerichtet hat, einstehen muss oder ob er eine solche Einstandspflicht abbedingen kann. Grundsätzlich ist eine Freizeichnung für die Schadensersatzhaftung auch im Verbrauchsgüterkauf möglich, sofern kein Vorsatz vorlag oder eine Beschaffenheitsgarantie übernommen wurde.[169] Die Haftung für Mangelfolgeschäden hängt davon ab, ob der Vertragspartner den Schaden iSd § 276 BGB zu vertreten hat, d.h. ob er vorsätzlich oder fahrlässig gehandelt hat. Die Zulässigkeit der Freizeichnung unterliegt der Inhaltskontrolle der § 307 ff. BGB. Nach dem Wortlaut des § 309 Nr. 7b BGB ist eine Haftungsfreizeichnung für sonstige Schäden bei leicht fahrlässiger Pflichtverletzung zulässig. Ob dies aber auch für eine Freizeichnung bezüglich mangelbezogenen Folgeschäden gilt, ist höchst umstritten,[170] kann hier aber nicht weiter vertieft werden. Pauschale Aussagen verbieten sich hier, letztlich wird auf die Frage der Vorhersehbarkeit[171] eines konkreten Schadens abgestellt werden müssen. Klauseln, die die Haftung für Mangelfolgeschäden bei leichter Fahrlässigkeit auf vorhersehbare Schäden beschränken, dürften daher eher nicht zu beanstanden sein,[172] ebenso wenig auch Klauseln, die versuchen für Folgeschäden, eine Haftungsobergrenze einzuführen.[173]

101 Unmittelbare vertragliche Beziehungen mit dem IT-Hersteller werden auch beim Bezug von **kommerziell hergestellter Software** über das Internet in der Regel bestehen. Ein praktisch wichtiges Beispiel sind **automatische Updates** für Betriebssysteme und Anti-Virus-Programme, welche oftmals schon im Lieferumfang handelsüblicher Computer enthalten sind und deren Abonnement später auf der Hersteller-Homepage verlängert werden kann. Auch in sonstigen Fällen, in denen der Hersteller Software direkt auf seiner Homepage zum Download bereitstellt, bestehen unmittelbare vertragliche Ansprüche. Inhalt und Umfang der Pflichten des IT-Herstellers richten sich wiederum primär nach den vertraglichen Regelungen einschließlich etwaiger AGB-Klauseln, wiederum unter dem Vorbehalt der Zulässigkeit nach § 307 BGB, in deren Rahmen die deliktischen Wertungen durchaus einfließen können (ausführlich unten Rn. 529 ff.). Darüber

169 Palandt-*Weidenkaff*, § 475 BGB Rn. 14; Erman-*Grunewald*, § 475 BGB Rn. 10; *Schulze/Ebers*, JuS 2004, 466.

170 S. zum Meinungsstand *Schulze/Ebers*, JuS 2004, 466 mwN.

171 Ausführlich zur Vorhersehbarkeit *Spindler*, in: FS Nagel, S. 27.

172 So auch *Litzenburger*, NJW 2002, 1245; aA Bamberger/Roth-*Becker*, § 309 Nr. 7 Rn 20 ff. und Nr. 8 Rn. 30, 35, der die Haftung für Mangelfolgeschäden als unabdingbare Kardinalpflicht sieht, ohne die die Verwendergegenseite ihr Interesse an ordnungsgemäßer Vertragserfüllung nicht durchsetzen könne; *Intveen*, ITRB 2003, 13 f.

173 So auch tendierend *Intveen*, ITRB 2003, 14.

hinaus ist gerade bei Internet-Downloads zu beachten, dass jedenfalls im B2B-Geschäft eine Rechtswahl nach Art. 27 EGBGB zulässig ist, auch durch entsprechende AGB-Klauseln.[174] Die Wirksamkeit einer solchen Wahl richtet sich nach Art. 31 I EGBGB i.V.m. Art. 29 IV EGBGB nach demjenigen Recht, das nach der Klausel angewendet werden soll.[175] Damit wird auch die gesamte Inhaltskontrolle und ihr Ergebnis (Wirksamkeit oder Unwirksamkeit der Klausel) dem deutschen Recht entzogen und ist allein Angelegenheit des nach Art. 31 Abs. 1 EGBGB anwendbaren Rechts.[176] Der Gesetzgeber der IPR-Reform hat die nach dem früheren § 10 Nr. 8 AGBG aF vorgesehene Inhaltskontrolle von Rechtswahlklauseln bewusst ausgeschlossen, da sie in Widerspruch zu der von Art. 27 geschützten Rechtswahlfreiheit stehe.[177]

102 Sofern Software nicht unmittelbar vom Hersteller bezogen wird, sondern über einen Händler, sind die Anreize für den Hersteller, sichere Software zu produzieren, von vornherein mediatisiert. Nur soweit der Händler ihn in Regress nehmen kann, werden Schäden auf den Hersteller zurückverlagert. Handelt es sich um mangelhafte Standardsoftware, greift zwar zugunsten des Händlers die zwingende Regelung des § 478 BGB ein, so dass er stets Regress nehmen kann. Doch zeigt schon § 478 IV S. 2 BGB, dass der Hersteller den Schadensersatzanspruch bzw. den diesbezüglichen Regress abbedingen kann – so dass gerade die für IT-Schäden relevanten Mangelfolgeschäden nicht mehr vom Regress erfasst wären. Zudem kann der Händler nur dann vom Käufer auf Schadensersatz belangt werden, wenn er den Fehler und den Mangelfolgeschaden damit zu vertreten hat – dies wird indes in den seltensten Fällen gelingen, da der Händler (nicht der Hersteller!) den Code hätte kennen und zudem der konkrete Schaden hätte vorhersehbar sein müssen; meist wird es daher am Vertretenmüssen des Händlers fehlen. Abgesehen davon ist auch schon strittig, ob Software überhaupt zu den von der Verbrauchsgüterkaufrichtlinie erfassten Produkten zählt[178] – denn hier schlägt sich wie-

174 *Schmidt/Prieß*, in: Spindler/Börner, S. 175; Palandt-*Heldrich*, EGBGB Art. 27 Rn. 6.

175 BGH NJW-RR 2005, 1071, 1072; BGHZ 123, 380, 383; Staudinger-*Hausmann*, BGB, 2002, Art. 31 EGBGB Rn. 72; Palandt-*Heldrich*, Art. 31 EGBG Rn. 1, 3, Art. 27 EGBGB Rn. 8; Bamberger/Roth-*Spickhoff*, Art. 31 EGBGB Rn. 6 ff.; Erman-*Hohloch*, Art. 27 EGBGB Rn. 12, 16, Art. 31 EGBGB Rn. 6, 8; *Tiedemann*, IPRax 1991, 424 (425); *Mankowski*, RIW 2003, 2 (4); ausführlich *Heiss*, RabelsZ 65 (2001), 634 (635 ff.); *Rühl*, Rechtswahlfreiheit und Rechtswahlklausel in Allgemeinen Geschäftsbedingungen, 1999.

176 MünchKommBGB-*Martiny*, Art. 27 EGBGB Rn. 13 mwN.; Palandt-*Heldrich*, Art. 31 EGBGB Rn. 3; *Looschelders*, Internationales Privatrecht, Art. 31 Rn. 9; schon vor der Reform: *Meyer-Sparenberg*, RIW 1989, 347 (350); *Grundmann*, IPrax 1992, 1 (2); abw. nur *Heiss*, RabelsZ 65 (2001), 634 (636 ff.), der sich für allgemeine Missbrauchskontrollen ausspricht.

177 Begr. Reg E BT-Drucks. 10/504 S. 95.

178 Aus der umfangreichen Diskussion dazu: *Mankowski*, MDR 2003, 854 ff.; *Spindler*/*Klöhn*, CR 2003, 81

derum die alte Diskussion um die Sacheigenschaft von Software nieder (s. dazu Rn. 103). Bislang ist diese Frage von der Rechtsprechung nicht entschieden worden; sinnvollerweise sollte indes der Produktbegriff – vergleichbar der Diskussion im ProdHaftG (Rn.209 ff.) – auch im Verbrauchsgüterkauf entsprechend erweitert verstanden werden.[179] Schließlich kann der Regress für den gerade international wichtigen IT-Softwareverkauf durch Rechtswahl nach Art. 27 EGBGB abbedungen werden, da § 478 BGB nicht zu den international zwingenden Normen nach Art. 34 EGBGB zählt.[180]

103 Wie Software rechtlich zu qualifizieren ist, war lange Zeit, und ist es seit der Schulrechtsreform wieder, umstritten. Während vor der Schuldrechtsmodernisierung durch die stetige Rechtsprechung weitestgehend Einigkeit herrschte, dass Software zumindest wenn sie in irgendeiner Weise verkörpert ist, als Sache zu qualifizieren sei und so die Vorschriften über den Kauf (der lediglich für Sachen und Rechte gilt) anwendbar seien.[181] Durch die Schuldrechtsreform wurde § 453 BGB eingefügt, wonach die kaufrechtlichen Vorschriften nun auch auf sonstige Gegenstände anwendbar sind. In der Gesetzesbegründung wurde weiter Software als sonstiger Gegenstand genannt,[182] was ein Teil der Literatur zum Anlass nahm, die Diskussion um die Einordnung von Software erneut zu aufzunehmen, da eine Qualifikation als Sache insbesondere im Rahmen des neu formulierten § 651 BGB nach dem Wortlaut die Konsequenz hätte, dass bei Lieferung oder Erzeugung von Software nicht Werkvertragsrecht sondern Kaufrecht anzuwenden wäre. Insgesamt lassen sich zu dieser Problematik aktuell drei Strömungen herauskristallisieren: Ein Teil der Literatur verneint die Sachqualität von Software, so dass § 651 BGB schon vom Wortlaut nicht greife und Werkvertragsrecht unproblematisch bei individuell hergestellter Software Anwendung finde.[183] Andere bejahen weiterhin die Sachqualität von Software. Diese Auffassung untergliedert sich weiter in den Teil, der konsequent § 651 BGB auf individuell hergestellte bzw. angepasste Software an-

---

ff; *Marly*, Softwareüberlassungsverträge, Rn. 55 ff., 63.

179 *Spindler/Klöhn*, CR 2003, 85; *Mankowski*, MDR 2003, 857.

180 MünchKommBGB-*Lorenz*, § 478 Rn. 10; *Staudinger*, ZGS 2002, 64.

181 So die ständige Rechtsprechung: BGH GRUR 1985, 1055 (1056); 1988, 406 (408); NJW 1990, 320 (321); NJW 1993, 2436 (2437); NJW 2000, 1415 ff.; CR 2007, 75 (76); zustimmend in der Literatur: *Marly*, Softwareüberlassungsverträge, Rn. 96 ff. insb. Rn. 110; Palandt-*Heinrichs*, § 90 BGB Rn. 2; MünchKommBGB-*Holch*, § 90 Rn. 27; *Schneider*, Handbuch des EDV-Rechts, D Rn. 96; Erman-*Michalski*, § 90 BGB Rn. 3.

182 BT-Drucks. 14/6040, S. 242.

183 *Stichtenoth*, K&R 2003, 106 f.; *Junker*, NJW 2005, 2831; *Heussen*, CR 2004, 7; *Redeker*, CR 2004, 88 f.; *Diedrich*, CR 2002, 475; *Schneider*, in: Schneider/v. Westphalen, Software-Erstellungsverträge, B Rb. 39 ff.

wendet und so zum Kaufrecht gelangt[184] und den Teil, der § 651 BGB mit unterschiedlichen Begründungen (z.B. teleologische Reduktion,[185] keine „sklavische“ Anwendung des Sachbegriffs im Rahmen des § 651 BGB,[186] Schwerpunkt der Leistung[187]) auf Software nicht anwenden will und so zum Werkvertragsrecht gelangt.[188] Aufgrund der jahrelangen stetigen Rechtsprechung wird man aber wohl weiter Software als Sache qualifizieren müssen. Der XII. Zivilsenat hat jüngst ebenfalls Software aufgrund der nötigen Verkörperung eindeutig als Sache bezeichnet.[189] Um dennoch zu einer interessengerechten Lösung zu gelangen, sollte man darauf verzichten, den Sachbegriff im Rahmen des § 651 BGB derart strikt anzuwenden, um bei der Erzeugung von Individualsoftware dennoch zur Anwendbarkeit des Werkvertragsrecht zu gelangen.[190]

III. Außervertragliche Produkthaftung

1. Verschuldensabhängige Produzentenhaftung

104 Weitestgehend unstreitig ist inzwischen, dass die verschuldensabhängige Haftung nach §§ 823 ff. BGB auch auf Software als Produkt Anwendung findet, da anders als im ProdHaftG der Streit um die Sacheigenschaft der Software für die Anwendung der §§ 823 ff. BGB unerheblich ist, da es nur auf das Vorhandensein einer Gefahrenquelle ankommt, gleich welcher Natur das Produkt ist, von dem die Gefahr ausgeht.[191] Vor allem im gewerblichen Bereich spielt die verschuldensabhängige Produkthaftung nach §§ 823 ff. BGB daher eine entscheidende Rolle.

105 Die verschuldensabhängige Produkthaftung kann dabei grob in zwei Bereiche unterteilt werden, zum einen der Rechtsgutsverletzung nach § 823 Abs. 1 BGB, zum anderen der Schutzgesetzverletzung nach § 823 Abs. 2 BGB:

---

184 *Schweinoch/Roas*, CR 2004, 330; *Mankowski*, MDR 2003, 857; *Lapp*, in: Gounalakis, § 43 Rn. 6.

185 *Rücker*, CR 2006, 366 ff.

186 *Spindler/Klöhn*, CR 2003, 84.

187 *Schmidl*, MMR 2004, 592 f.

188 *Marly*, Softwareüberlassungsverträge, Rn. 53 ff. und 119; *Rücker*, CR 2006, 366 ff.; *Spindler/Klöhn*, CR 2003, 84; *Schmidl*, MMR 2004, 592 f.; *Müller-Hengstenberg/Krcmar*, CR 2002, 549 ff.; MünchKommBGB-*Busche*, § 651 BGB Rn. 12.

189 BGH, K&R 2007, 91 = CR 2007, 75 m.Anm. *Lejeune* = WM 2007, 467 sowie Anm. *Marly/Jobke*, LMK 2007, 209.

190 So auch *Spindler/Klöhn*, CR 2003, 83 f.

191 Grundlegend *Taeger*, Außervertragliche Haftung für fehlerhafte Computerprogramme, S. 239 ff.; *Günther*, Produkthaftung für Informationsgüter, S. 253 ff.; *Schneider*, Handbuch des EDV-Rechts, Kap. J Rz. 294 ff.; *Marly*, Softwareüberlassungsverträge, Rn. 1309 ff.; grundsätzlich zur Unabhängigkeit von der Sacheigenschaft: MünchKommBGB-*Wagner*, § 823 BGB Rn. 554; Erman-*Schiemann*, § 823 BGB Rn. 114.

a) Rechtsgüterbezogene Produkthaftung (§ 823 Abs. 1 BGB)

(1) Softwareversagen und Rechtsgüterschutz

106 Maßgeblich für die Anwendung der deliktischen Produzentenhaftung ist zunächst die Verletzung eines der durch § 823 Abs. 1 BGB geschützten Rechtsgüter und Rechte. Bereits auf dieser Ebene ergeben sich bereits eine Reihe von Fragen in Bezug auf IT-Produkte:

(a) Verletzung personenbezogener Rechtsgüter

107 Eine Verletzung der Rechtsgüter **Leben**, **Körper** und **Gesundheit** ist beispielsweise bei einem Brand infolge eines Kurzschlusses in der Hardware denkbar. Durch Softwarefehler werden die Rechtsgüter des § 823 Abs. 1 BGB dagegen nicht unmittelbar beeinträchtigt, allerdings können infolge von Fehlfunktionen oder Ausfällen auch Schäden an Leben, Körper, Gesundheit oder Freiheit auftreten.[192] Die Relevanz von durch **Softwarefehler** verursachten Personenschäden wird in Zukunft wohl zunehmen, wenn Steuerungsaufgaben mehr und mehr auf den Computer übertragen werden. Dies gilt besonders für den Bereich der softwaregesteuerten Arbeitsmittel und industriellen Fertigung (z.B. Software zur Steuerung chemischer Anlagen, Industrieroboter) Personenschäden können auch dort auftreten, wo die Verkehrssteuerung auf dem Einsatz von Software basiert (z.B. Flugsicherung, Verkehrsleitsysteme) oder Software im medizinischen Bereich eingesetzt wird.[193] Im privaten Bereich steigt die Bedeutung softwaregesteuerter Systeme und damit auch die Gefahr von durch Softwarefehler verursachten Personenschäden beispielsweise durch den Softwareeinsatz im privaten Pkw (z.B. Anti-Blockier-System (ABS), elektronisches Stabilitätsprogramm (ESP), automatische Fahrabstandsregelung, elektronischer Bremskraftverstärker). Als seltenes Beispiel einer Verletzung der persönlichen **Freiheit** wird der Ausfall softwaregesteuerter Fahrstühle oder Türen genannt.[194]

(b) Verletzungen des Eigentums

108 Häufiger als Personenschäden ziehen Softwarefehler Beeinträchtigungen in Form eines Eingriffs in die Sachsubstanz (Hardware), der Verfügbarkeit und Integrität von Daten,

---

192 *Koch*, NJW 2004, 801 (802); *Taeger*, Außervertragliche Haftung für fehlerhafte Computerprogramme, S. 259 f.; *Koch*, Versicherbarkeit von IT-Risiken, Rn. 185, 355, 632; *Hoeren/Pichler*, in: Loewenheim/Koch, Praxis des Online-Rechts, S. 381 (406).

193 Vgl. *Schneider/Günther*, CR 1997, 389 (392).

194 *Taeger*, Außervertragliche Haftung für fehlerhafte Computerprogramme, S. 260.

sowie von System- und Betriebsausfällen nach sich. Bei fehlender Verletzung der Sachsubstanz ist die Abgrenzung zwischen deliktsrechtlich sanktionierten **Eigentumsverletzungen** und insoweit unbeachtlichen, weil nicht ersatzfähigen, primären Vermögensschäden entscheidend. Gegenüber der Verletzung des Eigentums[195] kommt dem **Recht am eingerichteten und ausgeübten Gewerbebetrieb** nur subsidiäre Bedeutung zu.[196] Regelmäßig wird es zudem am erforderlichen betriebsbezogenen, finalen Eingriff[197] fehlen.[198] Hinsichtlich des Eigentums kann wie folgt differenziert werden:

(i) Substanzverletzungen

109 Eine Eigentumsverletzung im Sinne einer Substanzverletzung kommt in den Fällen in Betracht, in denen Geräte, Maschinen oder Anlagen mit Hilfe von Software gesteuert werden und die Software somit indirekt **in mechanischer Weise auf die Umwelt einwirkt**.[199] In diesem Zusammenhang stellt sich das Problem des sog. **Weiterfresserschadens**, wenn der Fehler einer in eine Maschine usw. eingebauten Software zu einer Beschädigung oder Zerstörung der Gesamtsache führt.[200] Nach gefestigter Rechtsprechung des BGH sind Schäden an einem ansonsten fehlerfreien Produkt, welche durch ein integriertes fehlerhaftes Teilprodukt verursacht wurden, nach § 823 Abs. 1 BGB wegen Verletzung des Eigentums am fehlerfreien Rest zu ersetzen (zum ProdHaftG s. unten Rn. 193 ff.).[201] Nachdem der BGH eine Eigentumsverletzung zunächst bei funktionaler Abgrenzbarkeit des fehlerhaften Teils bejahte, stellt er nunmehr auf die Unterscheidung zwischen dem vertraglich geschützten Äquivalenzinteresse und dem deliktisch geschützten Integritätsinteresse ab. Eine Eigentumsverletzung liegt demnach vor, wenn der Minderwert, welcher der Sache von Anfang an anhaftete, nicht mit dem eingetretenen Schaden „stoffgleich“ ist.[202] Dies wird man regelmäßig dann bejahen können,

---

195 BGHZ 138, 311 (315); Bamberger/Roth-*Spindler*, § 823 BGB Rn. 114 mwN.

196 Dazu ausführlich *Koch*, Versicherbarkeit von IT-Risiken, Rn. 360; *Sodtalbers*, Softwarehaftung im Internet, Rn. 523; *Taeger*, Außervertragliche Haftung für fehlerhafte Computerprogramme, S. 262; Staudinger-*Hager*, § 823 BGB Rn. D 67.

197 BGHZ 29, 65 (74); BGHZ 90, 113 (123); näher dazu: Bamberger/Roth-*Spindler*, § 823 BGB Rn. 108; MünchKommBGB-*Wagner*, § 823 BGB Rn. 185.

198 *Bartsch*, Software und das Jahr 2000, S. 159; s. dagegen für Virenbefall *Koch*, NJW 2004, 801 (803).

199 *Taeger*, Außervertragliche Haftung für fehlerhafte Computerprogramme, S. 260 f.

200 Ausführlich *Koch*, Versicherbarkeit von IT-Risiken, Rn. 633 ff.

201 BGHZ 67, 359 (364 f.); BGHZ 86, 256 (258); BGH NJW 1998, 1942 (1943); ausführlich Bamberger/Roth-*Spindler*, § 823 BGB Rn. 60 ff.

202 BGHZ 86, 256 (258 f.).

wenn ein Softwarefehler zur Beschädigung oder Zerstörung der Sache (z.B. Maschine, Fahrzeug usw.) führt, in die sie eingebaut ist.[203]

(ii) Verletzung der Datenintegrität und -verfügbarkeit

110 Im Grundsatz erfasst das nach § 823 Abs. 1 BGB geschützte **Eigentum** auch die Integrität von Daten,[204] da schon die **Funktionalität und innere Ordnung** des Eigentums, z.B. einer Sammlung, auch ohne Substanzschädigung geschützt wird.[205] Da jede Festplatte eine innere Ordnung der gespeicherten Daten voraussetzt, führt die Zerstörung dieser Ordnung durch Veränderung oder Löschung von Daten grundsätzlich zu einer Eigentumsverletzung.[206] Ein erheblicher Teil von Daten und Datenbanken fällt somit in den Schutzbereich von § 823 Abs. 1 BGB in den Bereich des Rechts am Eigentum.[207] Zudem werden urheberrechtlich oder andere immaterialgüterrechtlich geschützte Werke, die auch in Gestalt von Daten verkörpert sein können, ebenso wie Software gleichermaßen nach den jeweiligen Spezialregelungen, z.B. § 97 UrhG, geschützt. Darüber hinaus wird auch ein **Recht am (verkörperten) Datenbestand** als sonstiges Recht nach § 823 Abs. 1 BGB angenommen.[208] Dadurch soll der Schutz der Verfügbarkeit der Daten, auch bei ausgelagerten Daten, gewährleistet werden.[209]

111 Ermöglicht demnach eine Softwarelücke einen **Virenbefall** des Computers und werden gespeicherte Daten durch diesen Virus vernichtet, liegt eine Eigentumsverletzung gemäß § 823 Abs. 1 BGB vor. Voraussetzung für eine Eigentumsverletzung ist jedoch stets, dass die Daten auf einem Datenträger im Eigentum des Geschädigten gespeichert waren. Die Veränderung oder Vernichtung von Daten, die auf dem Rechner eines Pro-

---

203 *Sodtalbers*, Softwarehaftung im Internet, Rn. 513 ff., 518; *Taeger*, Außervertragliche Softwarehaftung für fehlerhafte Computerprogramme, S. 260 f.; Bamberger/Roth-*Spindler*, § 823 BGB Rn. 69.

204 OLG Karlsruhe NJW 1996, 200 (201); zust. *Meier/Wehlau*, NJW 1998, 1585 (1587 ff.); Staudinger-*Hager*, § 823 BGB Rn. B 60; *Imhof/Wahl*, WpK-Mitt. 1998, 136 (137); *Taeger*, Außervertragliche Haftung für fehlerhafte Computerprogramme, S. 261; aA LG Konstanz NJW 1996, 2662; AG Dachau NJW 2001, 3488.

205 BGHZ 76, 216 (220f.) = NJW 1980, 1518.

206 OLG Karlsruhe NJW 1996, 200 (201); *Bartsch*, CR 2000, 721 (723); *Spindler*, NJW 1999, 3737 (3738); *Spindler*, NJW 2004, 3145 (3146); *Meier/Wehlau*, NJW 1998, 1585 (1588); *Mankowski*, in: Ernst, Hacker, Cracker & Computerviren, Rn. 440 f.; *Koch*, Versicherbarkeit von IT-Risiken, Rn. 357 f.; *Sodtalbers*, Softwarehaftung im Internet, Rn. 511; MünchKommBGB-*Wagner*, § 823 BGB Rn. 96; Bamberger/Roth-*Spindler*, § 823 BGB Rn. 55; aA *Bauer*, PHi 1989, 98 (105 f.), nach dem die Zerstörung der Information physikalisch allenfalls eine elektronische Zustandsveränderung darstellt.

207 Dem grds. zustimmend dann aber den Weg über ein eigenes Recht am Datenbestand als gangbarer sehend *Faustmann*, VuR 2006, 260 ff.

208 *Faustmann*, VuR 2006, 262 f.; *Meier/Wehlau*, NJW 1998, 1588.

209 *Faustmann*, VuR 2006, 262.

viders gespeichert waren, genügt dagegen nicht.[210] Keine deliktischen Ansprüchen kommen wegen des fehlerhaften Programms selbst in Betracht, wenn dieses infolge des Fehlers gelöscht wird, da insoweit nur das vertraglich geschützte Äquivalenzinteresse betroffen ist.[211] Keine Verletzung der Datenintegrität im oben beschriebenen Sinne liegt auch vor, wenn ein **Trojaner** eine Schwachstelle in der Software nutzt und dadurch Daten ausgespäht werden. Denn es erfolgt keine Störung der inneren Ordnung des Datenträgers.

(iii) Beeinträchtigung der bestimmungsgemäßen Verwendung

112 Eine Eigentumsverletzung kommt auch dann in Betracht, wenn eine Beeinträchtigung der bestimmungsgemäßen Verwendung erfolgt.[212] Bei der Annahme einer Eigentumsverletzung ist indessen Vorsicht geboten, da die Grenze zum nach § 823 Abs. 1 BGB **nicht ersatzfähigen primären Vermögensschaden** nicht überschritten werden darf.[213] Die Rechtsprechung hat jedoch die **erhebliche** Beeinträchtigung der bestimmungsgemäßen Verwendung einer Sache als Eigentumsverletzung angesehen.[214] Maßgebliche Kriterien sind letztlich die **Intensität** und der **Zeitraum** der Nutzungsbeeinträchtigung.[215]

113 Insbesondere im unternehmerischen Bereich drohen durch Softwarefehler hohe Schadenssummen, wenn der **Ausfall des EDV-Systems** zu Betriebsstörungen und Produktionsausfällen führt. Ebenso kann bei privater Nutzung ein Softwaremangel die Verwendung des Computers einschränken, wobei jedoch ungleich geringere Haftungsrisiken bestehen (denkbar sind etwa Kosten zur Wiederherstellung der Betriebsbereitschaft) bzw. oftmals überhaupt kein ersatzfähiger Schaden vorliegen wird. Eine Eigentumsverletzung wird man beim Systemausfall nur in engen Grenzen annehmen können, da sich die Funktionsuntauglichkeit der Sache, die mit der Software gesteuert wird, in der Regel in einem temporären Vorgang erschöpft, der die Sache (Hardware) nicht auf Dauer ihrer Gebrauchstauglichkeit enthebt, sondern die mit einer neuen Software wieder einsatzbe-

---

210 *Spindler*, in: Hoeren/Sieber, Rn. 364.

211 *Sodtalbers*, Softwarehaftung im Internet, Rn. 518.

212 Grundlegend BGHZ 55, 153 (159) - Fleetfall; ausführlich Bamberger/Roth-*Spindler*, § 823 BGB Rn. 50 ff.

213 BGHZ 86, 152 (155); Bamberger/Roth-*Spindler*, § 823 BGB Rn. 51.

214 BGHZ 55, 153 (159 ff.); BGHZ 105, 346 (350); BGH NJW 1994, 517 (518); BGH NJW-RR 1995, 342 (342 f.); BGH NJW 1996, 2507 (2508); *Larenz/Canaris*, § 76 II 3 b, S. 387; Erman-*Schiemann*, § 823 BGB Rn. 31; Staudinger-*Hager*, § 823 BGB Rn. D 98.

215 BGH NJW 1994, 517 (518); *Sodtalbers*, Softwarehaftung im Internet, Rn. 512.

reit gemacht werden kann. Anders kann im Einzelfall zu entscheiden sein, wenn auf das System über einen längeren Zeitraum nicht zugegriffen werden kann.[216]

114 Keine Eigentumsverletzung wird man regelmäßig auch bei der **Installation eines Trojaners** auf dem Rechner bejahen können. Zwar mag mit der Präsenz dieses Schadprogramms eine gewisse psychologische Hemmschwelle hinsichtlich einer Nutzung im Internet verbunden sein. Die Gebrauchstauglichkeit des Computers wird im Übrigen (z.B. Textverarbeitung usw.) aber nicht berührt und der Trojaner kann meist innerhalb relativ kurzer Zeit entfernt werden, wodurch die volle Gebrauchsfähigkeit wiederhergestellt wird.

(c) Verletzung sonstiger Rechte

(i) Allgemeines Persönlichkeitsrecht

115 Das Allgemeine Persönlichkeitsrecht schützt auch die unzulässige Erhebung Nutzung und Verarbeitung persönlicher und personenbezogener Daten, wodurch Ansprüche auf Unterlassung, Beseitigung, Auskunft und Ersatz des materiellen und immateriellen Schadens nach den §§ 823, 1004 BGB und §§ 7, 8 BDSG ausgelöst werden können.[217] Davon umfasst wird iSd Rechts auf informationelle Selbstbestimmung, die Befugnis des einzelnen, grundsätzlich selbst darüber zu entscheiden, ob und wer über seine persönlichen und sachlichen Verhältnisse unterrichtet ist oder wird.[218] Zu denken ist hier an den Schutz bei besonders gefahrenträchtiger Informationsverwaltung, wie z.B. der Speicherung von Fingerabdrücken, politischen Einstellungen, Gesundheitsbildern, Informationen zum eigenen Vermögensstand oder der Kreditfähigkeit u.ä.[219] Derartig sensible Daten müssen entsprechend geschützt aufbewahrt werden. Lassen sich die Daten dagegen unproblematisch durch Dritte mithilfe von Trojanern etc. ausspähen, kann dies uU zur Verletzung des Allgemeinen Persönlichkeitsrechts führen.

(ii) Recht am eigenen Datum

116 Z.T. werden im Rahmen des § 823 Abs. 1 BGB eigene Rechte in Bezug auf Daten als sonstige Rechte diskutiert. So wurde in der Vergangenheit gefordert, ein „**Recht am eigenen Datum**“, das sich aus dem Recht auf informationelle Selbstbestimmung ableiten soll, als absolut geschütztes sonstiges Recht im Sinne von § 823 Abs. 1 BGB anzuer-

---

216 *Sodtalbers*, Softwarehaftung im Internet, Rn. 512; vgl. auch *Taeger*, Außervertragliche Haftung für fehlerhafte Computerprogramme, S. 261.

217 Bamberger/Roth-*Bamberger*, § 12 Rn. 160; Simitis-*Simitis*, § 7 Rn. 29 ff.

218 MünchKommBGB-*Rixecker*, Anh § 12 Rn. 102.

219 S. dazu MünchKommBGB-*Rixecker*, Anh § 12 Rn. 106.

kennen.[220] Das Recht am eigenen Datum soll ein umfassendes Selbstbestimmungsrecht des Einzelnen über ihn betreffende Informationen umfassen.[221] Die Vertreter des Rechts am eigenen Datum begründen die Notwendigkeit damit, dass das Interesse der Selbstbestimmung über personenbezogene Informationen, wie das Eigentum, gegenüber jedermann schutzwürdig sein müsse.[222] Zu Recht ist ein solches Recht aber überwiegend nicht anerkannt.[223] Das BVerfG hat im Volkszählungsurteil, in dem das Recht auf informationelle Selbstbestimmung begründet wurde, ausdrücklich betont, dass der Einzelne kein Recht auf absolute und unbeschränkbare Herrschaft über seine Daten hat und auch personenbezogene Information nicht ausschließlich dem Betroffenen allein zugeordnet werden können.[224] Diese Aussage steht daher in Widerspruch zur Annahme eines absolut geschützten Rechts am eigenen Datum.

(iii) Recht am Unternehmen

117 Bei fahrlässigen Datenlöschungen könnte eine Verletzung des als sonstiges Recht iSd § 823 Abs. 1 BGB anerkannten Rechts am eingerichteten und ausgerichteten Gewerbebetrieb in Betracht kommen. Voraussetzung für eine Verletzung dieses Rechts ist aber das Korrektiv der Betriebsbezogenheit. Das bedeutet, dass sich der Eingriff gegen den Betrieb als solchen richten muss und nicht lediglich vom Gewerbebetrieb ablösbare Rechtspositionen beeinträchtigen darf.[225] Bei fahrlässigen Datenlöschungen, die z.B. aufgrund von Stromunterbrechung erfolgen, fehlt es daher meist an der Betriebsbezogenheit, so dass dem Recht am eingerichteten und ausgeübten Gewerbebetrieb in Bezug auf Daten wenig Bedeutung zukommt.[226]

(2) Verantwortlichkeit für von Dritten verursachte Verletzungen?

118 Steht die Verletzung eines Rechtsguts fest, bedarf es ferner der Zurechnung der Verletzung zum Hersteller. Während normalerweise das Produkt und sein Fehler selbst die

---

220 Entwickelt von *Meister*, Datenschutz im Zivilrecht, S. 121 ff. noch vor der Anerkennung des Rechts auf informationelle Selbstbestimmung im Volkszählungsurteil; grds. demgegenüber positiv äußernd *Bruns*, Informationsansprüche gegen Medien, 65 f.; ergebnisoffen BGHZ 91, 231 (237 ff.).

221 *Meister*, Datenschutz im Zivilrecht, S. 114 f.

222 *Meister*, Datenschutz im Zivilrecht, S. 124.

223 *Meier/Wehlau*, NJW 1998, 1585 (1588 f.); *Spindler/Klöhn*, VersR 2003, 410 (412); Bamberger/Roth-*Spindler*, § 823 BGB Rn. 93; Staudinger-*Hager*, § 823 Rn. C 173; *Wente*, 97; Simitis-*Simitis*, Einleitung Rn. 26; *Ehmann*, AcP 188 (1988), 266 f.; ausführlich *Sodtalbers*, Softwarehaftung im Internet, Rn. 524 f.

224 BVerfGE 65, 1 (43 f.) – Volkszählungsurteil.

225 St. Rspr. BGH NJW 1951, 643 (644); NJW 1952, 660 (661) – Constanze I; NJW 1959, 479 (481) – Stromkabel; NJW 1983, 810; NJW 1998, 2141; NJW-RR 2005, 673 (675); Bamberger/Roth-*Spindler*, § 823 Rn. 108; MünchKommBGB-*Wagner*, § 823 Rn. 185.

226 *Meier/Wehlau*, NJW 1998, 1589; *Faustmann*, VuR 2006, 262; LG Konstanz NJW 1996, 2662.

entsprechende Rechtsgutsverletzung herbeiführen, etwa schadhafte Bremsen bei einem Kfz, die zu einem Unfall mit Verletzungsfolgen führen, sind bei IT-Produkten oftmals Einflüsse Dritter im Spiel, die Zurechnungsfragen aufwerfen:

(a) Haftung für Verhalten Dritter (Hacker)

119 Grundsätzlich treffen den Beherrscher der Gefahrenquelle Sicherungspflichten auch dann, wenn erfahrungsgemäß mit einem Fehlverhalten Dritter zu rechnen ist.[227] Beispiele hierfür sind Sicherungsvorkehrungen des Grundstückseigentümers gegen missbräuchliches Verhalten Dritter,[228] eines Veranstalters gegen Übergriffe der Zuschauer auf Nachbargrundstücke,[229] die Beseitigung von durch mutwillige Aktionen auf eine Fahrbahn geratenen Hindernisse[230] oder die Sicherung von Kraftfahrzeugen gegen Benutzung durch Unbefugte.[231] Demgemäß ist sowohl im allgemeinen Deliktsrecht[232] als auch in der Produkthaftung anerkannt, dass der Beherrscher der Gefahrenquelle – der Software – auch für Schäden einstehen muss, die erst durch das vorsätzliche Ausnutzen der durch das Produkt entstandenen latenten Gefahr durch Dritte entstehen.[233] **Überträgt** man diese **Grundsätze auf** die **IT-Produkthaftung**, wird die Verantwortlichkeit von Softwareproduzenten bei IT-Sicherheitslücken ihrer Programme nicht dadurch ausgeschlossen, dass letztlich Dritte, wie Programmierer von Viren oder Würmern oder Hacker, die Schäden verursachen. Eine solche latente Gefahr besteht insbesondere bei Sicherheitslücken, die von Hackern ausgenutzt werden können.[234]

(b) Haftung für Fremdprodukte und -dienste (Zubehör; Kompatibilitäten)

120 Eng damit verwandt, aber nicht gleichbedeutend ist die Haftung für **fremde Software**, die in Verbindung mit der eigenen Software eingesetzt wird – in Übertragung der von der Rechtsprechung entwickelten Haftung des Herstellers für fremd produziertes **Zube-**

---

227 BGHZ 165 (170) = NJW 1962, 1565; BGH NJW 1990, 1236 (1237); OLG Köln VersR 1992 (1241).

228 So sind Lichtroste gegen ein Abheben zu sichern BGH NJW 1990, 1236 (1237); anders OLG Frankfurt Rev. nicht angenommen BGH VersR 1998, 250 (Ls.) für einen Schacht im Schotterstreifen.

229 BGH NJW 1980, 223.

230 BGHZ 37, 165 (170) = NJW 1962, 1565; OLG Koblenz NVwZ 2002, 745 – Fahrbahnverschmutzung durch Sand.

231 BGH NJW 1971, 459 (460).

232 Bamberger/Roth-*Spindler*, § 823 BGB Rn. 245 mwN; MünchKommBGB-*Wagner*, § 823 BGB Rn. 255 f.

233 BGH NJW 1990, 1236 (1237).

234 *Mankowski*, in: Ernst, Hacker, Cracker & Computerviren, Rn. 442; *Bartsch*, CR 2000, 721 (721 ff.).

hör, die hier zumindest eine Produktbeobachtungspflicht annimmt;[235] dementsprechend sind diese Komplexe im Rahmen der Produktbeobachtung zu thematisieren.

121 Allerdings muss von vornherein der Anwendungsbereich der Produkthaftung eingegrenzt werden: Denn für **mangelnde Kompatibilität** mit einzelnen Fremdprodukten kann keine deliktische Haftung eingreifen, da damit der Bereich des deliktisch geschützten Integritätsinteresses verlassen würde.[236] Denn die Inkompatibilität der eigenen Hard- und Software mit einzelnen Fremdkomponenten liegt bereits beim Erwerb vor, so dass von vornherein mangelhaftes Eigentum erworben wurde. Allein das Äquivalenzinteresse ist damit betroffen, für dessen Ausgleich ausschließlich das Gewährleistungsrecht sorgt.[237]

(3) Pflichten vor Inverkehrgabe: IT-Sicherheitslücken als Konstruktionsfehler

122 In der Produkthaftung unterscheidet man typischerweise Konstruktions- und Fabrikationsfehler, für die gehaftet werden muss,[238] während für Entwicklungsfehler keine Haftung eingreift.[239] Bei Hardwareprodukten können beide Fehlerkategorien auftreten. Dagegen spielt für Software eindeutig der Konstruktionsfehler die maßgebliche Rolle, wird doch Software digital eins-zu-eins kopiert, so dass nur in seltenen Fällen eine fehlerhafte Fabrikation ursächlich für eine Rechtsgutsverletzung sein dürfte, z.B. wenn Software-CDs/DVDs fehlerhaft kopiert wurden.

123 Maßgeblich sind daher **Konstruktionsfehler**, wenn bei der Inverkehrgabe des Produktes nicht der Stand von Wissenschaft und Technik[240] berücksichtigt wurde, da der ge-

---

235 Grundlegend dazu BGH v. 9.12.1986 – VI ZR 65/86 – Honda, BGHZ 99, 167 = MDR 1987, 396 = CR 1987, 230; dazu *Ulmer*, ZHR 152, 564 (570 ff.); *Foerste*, in: v. Westphalen, ProdHaftHdb, § 25 Rz. 176 ff.; Kullmann/Pfister-*Kullmann*, Rz. 1520, S. 52; *Pfister*, EWiR 1987, 235.

236 BGHZ 86, 256 (258 ff.) = NJW 1983, 810 (811) = JZ 1983, 499 m. Anm. *Stoll*; MünchKommBGB-*Wagner*, § 823 BGB Rn. 122; Bamberger/Roth-*Spindler*, § 823 BGB Rn. 60 mwN.

237 BGHZ 39, 366 (367) = NJW 1963, 1827; BGHZ 67, 359 (364) = NJW 1977, 379; BGHZ 86, 256 (259) = NJW 1983, 810; BGHZ 96, 221 (228) = NJW 1986, 922; BGH NJW 1992, 1678; 1994, 2231 (2232); 2001, 1346 (1347) – Grundstück mit Schlacke führt zur Beschädigung von darauf stehenden Bauwerken; OLG Düsseldorf NJW-RR 1997, 1344 (1346); OLG Koblenz NJW-RR 1998, 374; Bamberger/Roth-*Spindler*, § 823 BGB Rn. 60; Staudinger-*J. Hager*, Kap. B Rn. 108; Soergel-*Spickhoff*, Vor § 823 BGB Rn. 49; *Hinsch*, VersR 1992, 1053.

238 Bamberger/Roth-*Spindler*, § 823 BGB Rn. 494 ff.; MünchKommBGB-*Wagner*, § 823 BGB Rn. 581 ff., 584 ff.

239 Bamberger/Roth-*Spindler*, § 823 BGB Rn. 493; MünchKommBGB-*Wagner*, § 823 BGB Rn. 264, 579f.; *Foerste*, in: v.Westphalen, ProdHaftHdB, § 24 Rn. 18, 82 ff.

240 Zur Relevanz des Standes von Wissenschaft und Technik für die Produkthaftung bei fehlerhaften Computerprogrammen *Littbarski*, in: Kilian/Heussen, Kap. 180 Rn. 53.

samten Serie der Software derselbe Fehler anhaftet.[241] Ähnlich der Produktbeobachtungspflicht ist der Hersteller gehalten, alle allgemein oder ihm speziell zugänglichen Erkenntnisquellen auszuschöpfen.[242] **Entscheidend** ist demnach, ob dem Softwarehersteller bereits **bei der Inverkehrgabe die Sicherheitslücken bekannt** sein mussten. Die Kenntnis wird auch bereits durch eine einzelne Mitteilung über eine Sicherheitslücke an den Softwarehersteller begründet, selbst wenn sie geheim gehalten wird, da nicht auszuschließen ist, dass andere ebenfalls diese Lücke entdecken und ausnützen. Umgekehrt führen **Sicherheitslücken, die erst später bekannt werden**, nicht dazu, dass dem Hersteller ein Konstruktionsfehler anzulasten wäre; hier handelt es sich vielmehr um einen **Entwicklungsfehler**, so dass allein nachträgliche Pflichten im Rahmen der Produktbeobachtung eingreifen können.

124 Ferner ist der Hersteller selbstverständlich gehalten, seine Konstruktion, Fertigung oder Instruktion[243] zu ändern, um den Fehler in Zukunft zu verhindern.[244] Sind Gefahren bekannt, aber nicht die Möglichkeiten zu ihrer Vermeidung, kann das Produkt im Prinzip nicht in den Verkehr gebracht werden.[245] Allerdings ist dem Hersteller ein Anpassungsermessen bei Wandel des Gefahrenbewusstseins[246] und bei neuen technischen Entwicklungen[247] zuzugestehen. Der Hersteller muss den Weg der größeren Vorsicht wählen, wenn Unsicherheiten über die Sicherheitsvorkehrungen bestehen.[248] Auch wenn Software ein äußerst komplexes Produkt darstellt, dessen Fehlerbehebung erheblichen

---

241 Eingehend zum Konstruktionsfehler als Programmierfehler *Taeger*, Außervertragliche Haftung für fehlerhafte Computerprogramme, S. 244 ff.; *Günther*, Produkthaftung für Informationsgüter, S. 300 f.; *Meier/Wehlau*, CR 1990, 95 (96); *Reese*, DStR 1994, 1121 (1123).

242 BGHZ 116, 60 (70 f.); BGH NJW 1990, 906 (907 f.); BGH NJW 1952, 1091; *Kullmann*, NJW 2002, 30 (32); Kullmann/Pfister-*Kullmann*, Kz. 1520 S. 14; Bamberger/Roth-*Spindler*, § 823 BGB Rn. 494 mwN.

243 Bei der Instruktion käme es z.B. darauf an, dass der Nutzer eindringlich auf die Notwendigkeit von periodischen Sicherheitsupdates hingewiesen wird.

244 BGH NJW 1990, 906 (908); BGH NJW 1994, 3349 (3350); MünchKommBGB-*Wagner*, § 823 BGB Rn. 602; *Michalski*, BB 1998, 961 (964).

245 Vgl. *Foerste*, in: v. Westphalen, ProdHaftHdb, § 24 Rn. 84 ff., 86; Kullmann/Pfister-*Kullmann*, Kz. 1520 S. 4 f.; diff. *Brüggemeier*, WM 1982, 1294 (1302).

246 Insbes. bei uneinheitlichen Verbrauchererwartungen wie z.B. bei Kopfstützen, ABS-Bremssysteme oder Airbags in Kfz, vgl. *Foerste*, in: v. Westphalen, ProdHaftHdb, § 24 Rn. 89, 90 ff.; ähnlich *Hollmann*, DB 1985, 2389 (2392); *Schlechtriem*, VersR 1986, 1033 (1036); abl. gegenüber dem Kriterium der Verbrauchererwartung *Möllers*, Rechtsgüterschutz im Umwelt- und Haftungsrecht, S. 254 ff.

247 Kullmann/Pfister-*Kullmann*, Kz. 1520 S. 15 f.

248 Kullmann/Pfister-*Kullmann*, Kz. 1520 S. 15 unter Verweis auf BGH NJW 1990, 906 (907) - und Berufung auf arzthaftungsrechtliche Grundsätze, wie z.B. BGHZ 8, 138 (140); weniger restriktiv BGH NJW 1987, 2927; ähnlich LG Itzehoe JurPC 87/2003, 17 f.

Aufwands bedarf, führt dies nicht daran vorbei, dass bekannte Sicherheitsprobleme unverzüglich beseitigt werden müssen, bevor das Produkt auf den Markt gebracht wird.[249]

125 Der Hersteller darf nicht sehenden Auges Software, auch bereits vorhandener Versionen, weiterhin in Umlauf bringen, von denen er weiß, dass sie fehlerbehaftet sind. Ebenso wenig kann der Hersteller darauf vertrauen, dass bei der Installation fehlerhafter Software gleichzeitig die nötigen **Sicherheitspatches** aus dem Internet eingespielt und übertragen werden; denn es ist nicht auszuschließen, dass schon während dieser Zeit der Nutzer Angriffen ausgesetzt ist oder dass die entsprechenden Server der IT-Hersteller nicht erreichbar bzw. überlastet sind. Problematisch ist allerdings oft, dass die Software bereits in der ersten Vertriebsstufe (Großhändler) etwa auf Hardware aufgespielt wird (OEM-Versionen) und der Softwarehersteller häufig außerhalb von Vertriebsbindungen und –systemen keine Kontrolle mehr darüber hat, bei wem sich welche Versionen der Software befinden. Hier ist die Software bereits in Verkehr gebracht und nicht mehr im unmittelbaren Einflussbereich des Produzenten, so dass nur die nachträglichen Pflichten des Herstellers eingreifen (s. Rn. 127 ff.).

126 Fraglich kann daher nur sein, **wie viel Zeit** dem Hersteller eingeräumt werden kann, **um die Sicherheitslücke zu beseitigen**; hier ist mit Sicherheit zu bedenken, dass Software ein komplexes Produkt darstellt und die Korrektur solcher Lücken nicht mit der Aktualisierung von Virenscannern verglichen werden kann, da es um das Einpassen neuer Codes in vorhandene Software geht. Andererseits kann der Softwarehersteller sich nicht darauf berufen, dass ihm die nötigen Ressourcen zur Anpassung fehlen, da er zumindest in den letzten Jahren angesichts sich häufender Sicherheitslücken allgemein damit rechnen muss, dass neue Probleme auftauchen. Welcher Zeitraum hier angemessen ist, kann nur im Einzelfall beurteilt werden; dabei werden als Ausgangspunkt die in der Branche üblichen Anpassungszeiten, aber auch eine „best practice“ herangezogen werden müssen, da ein niedriger Sicherheitsstandard nicht maßgeblich sein kann. Zudem sind Schadensumfang und –ausmaß sowie die Bedeutung der Software einschließlich der Vorteilsziehung für den Softwarehersteller im Sinne einer Kosten-Nutzen-Abwägung in die Beurteilung einzubeziehen.

(4) Pflichten nach Inverkehrgabe

249 *Meier/Wehlau*, CR 1990, 95 (97); *Bauer*, PHi 1989, 38 (47); s. auch *Schneider/Günther*, CR 1997, 389 ff.; *Bartsch*, CR 2000, 721 (722 ff.).

127 Nach Inverkehrgabe wird der Hersteller nicht vollständig von seiner Verantwortung für das Produkt frei. Vielmehr muss er bei Kenntnis von Schäden durch das Produkt die zu diesem Zeitpunkt erforderlichen und ihm zumutbaren Gefahrenabwehrmaßnahmen ergreifen. Zu Schäden muss es noch nicht gekommen sein.[250] Anknüpfungspunkt für die Haftung des Produzenten ist die Verletzung der **Produktbeobachtungspflicht**.[251] Haftungsgrund ist die Schaffung einer andauernden Gefahrenquelle, deren Ursachen aus der Sphäre des Herstellers stammen, unabhängig davon, welcher Fehlerkategorie sie angehören.[252]

(a) Produktbeobachtungs- und Warnpflichten

(i) Grundsätze

128 Für bereits vor Bekanntwerden der Sicherheitslücken vertriebene Software ist der Hersteller zur Produktbeobachtung, insbesondere zur Sammlung und Auswertung zugänglicher[253] Literatur und Erkenntnisse über mögliche Defekte seiner Software,[254] und zur Warnung, gegebenenfalls auch zum Rückruf verpflichtet. Gerade aus dem Wissen um die objektive Unvermeidbarkeit von Programmierungsfehlern („Bugs“) erwächst eine Pflicht des Herstellers zur besonders sorgfältigen Produktbeobachtung.[255] Bei drohenden Gefahren für Leib und Leben ist sogar bereits ein ernstzunehmender Verdacht hinreichend, um Warnpflichten auszulösen[256]; bei Sachschäden und nicht akuter Bedrohung kann sich der Produzent im Falle eines Verdachts zunächst auf eigene Ermittlungen und aktive Beobachtung des Produktes beschränken, ohne vor dem Produkt oder dessen spezifische Verwendung warnen zu müssen.[257]

129 Allerdings darf der Hersteller nicht abwarten, bis die Gefahr zur Gewissheit feststeht; bei sich häufenden Beschwerden muss der Hersteller vor den Gefahren warnen.[258] Häu-

---

250 OLG Karlsruhe VersR 1998, 63; hierzu *Kullmann*, NJW 1997, 1746 (1750).

251 Vgl. *v. Bar*, in: Produktverantwortung und Risikoakzeptanz, S. 29 (33).

252 *Foerste*, in: v. Westphalen, ProdHaftHdb, § 24 Rn. 292; *Michalski*, BB 1998, 961 (962 f.); Staudinger-*J. Hager*, § 823 BGB F Rn. 20 f.

253 International tätige Unternehmen sind etwa zur weltweiten Informationsbeschaffung und –auswertung verpflichtet, s. BGHZ 80, 199 (203) = NJW 1981, 1606; *Foerste*, in: v. Westphalen, ProdHaftHdb, § 24 Rn. 296.

254 Zu den Anforderungen an die Produktbeobachtungspflicht grundlegend BGHZ 80, 199 (202 f.); BGH NJW 1990, 906 (907 f.); *Foerste*, in: v. Westphalen, ProdHaftHdb, § 24 Rn. 245, 290 ff.; Kullmann/Pfister-*Kullmann*, Kza 1520 S. 54 f.

255 AA LG Köln NJW 1999, 3206: Keine Pflicht zur Warnung bei nachträglichen Erkenntnissen über Virenbefall einer Diskette.

256 BGHZ 80, 186 (192) = NJW 1981, 1603; OLG Frankfurt NJW-RR 1995, 406 (408); OLG Frankfurt NJW-RR 2000, 1268 (1270); OLG Karlsruhe VersR 1998, 63 (64 f.).

257 BGHZ 80, 186 (192)= NJW 1981, 1603; *Kullmann*, NJW 1996, 18 (23).

258 BGH NJW-RR 1995, 342 (343).

fig werden **IT-Sicherheitslücken durch Dritte** festgestellt und öffentlich bekannt gemacht; ab diesem Zeitpunkt kann sich der Hersteller nicht mehr nur auf eine passive Beobachtung beschränken, sondern muss selbst tätig werden.

(ii) Kontraproduktive öffentliche Sicherheitswarnungen?

130 Allerdings ist bei der Pflichtenbestimmung auch zu berücksichtigen, dass öffentliche Warnungen in kontraproduktiver Weise geradezu Dritte herausfordern können, eine IT-Sicherheitslücke zu nutzen, wie dies offenbar bei dem Wurm Sasser der Fall war. Sind die Lücken nur dem Hersteller bekannt geworden, etwa aufgrund eigener Tests oder aufgrund einer vertraulichen Mitteilung eines Dritten, muss ihm ein Ermessen zugestanden werden, ob er eine öffentliche Warnung ausspricht oder versucht, über Sicherheitspatches, die die Lücke nicht offen legen, das Sicherheitsproblem zu beseitigen. Insbesondere wenn der Hersteller aufgrund seiner Vertriebsstrukturen die Möglichkeit hat, die Verwender seiner Software individuell anzusprechen, ist eine öffentliche Warnung nicht geboten, sogar unter Umständen pflichtwidrig. Mehren sich jedoch die Hinweise Dritter, so dass anzunehmen ist, dass die Kenntnis von der Lücke sich verbreiten könnte, oder kann der Hersteller den Weg seines Produktes nicht nachverfolgen, ist der Hersteller gehalten, eine öffentliche Warnung auszusprechen, da nicht mehr auszuschließen ist, dass die Sicherheitslücke in erheblichem Umfang ausgenutzt wird und dadurch Schäden bei Nutzern entstehen. Denn der Hersteller kann nicht mehr davon ausgehen, dass seine Sicherheitspatches Beachtung finden oder der Nutzer sich genügend lang im Netz befindet, damit etwa eine automatische Updateerkennung eingreift.

131 Die **Warnhinweise** müssen **geeignet** sein, die in Betracht kommenden Verkehrskreise anzusprechen und auf die vom Produkt ausgehende Gefahr aufmerksam zu machen, wobei angesichts der heutigen Massenverbreitung einiger EDV-Programme nicht davon ausgegangen werden kann, dass alle Nutzer computerbezogene Zeitschriften beziehen oder entsprechende Online-Foren besuchen;[259] ebenso wenig genügt eine passive, produktspezifische Warnung in der Internet-Homepage des Herstellers. Vielmehr muss der Hersteller von weit verbreiteten Produkten zahlreiche Kanäle gleichzeitig zur Warnung nutzen.[260] Sofern es sich indes um gewerbliche Abnehmer mit Kenntnissen im EDV-Bereich handelt, treffen den Hersteller die Warnpflichten von vornherein nicht in der-

259 Vgl. *Marly*, Softwareüberlassungsverträge, Rn. 1311; allgemein: Kullmann/Pfister-*Kullmann*, Kza 1520 S. 61 ff.; *Foerste*, in: v. Westphalen, ProdHaftHdb, § 24 Rn. 251ff. mwN.

260 Ausführlich dazu *Marly*, Softwareüberlassungsverträge, Rn. 1311.

selben Intensität wie bei anderen Abnehmern, da diesen die Problematik grundsätzlich vertraut ist.[261]

(iii) Herausgabe des Quellcodes

132 Eine deliktsrechtlich[262] begründete Herausgabepflicht des Quellcodes ist in aller Regel nicht anzunehmen. Denn die Pflicht des Herstellers ist darauf gerichtet, eine Schädigung anderer Rechtsgüter des Softwarenutzers abzuwenden, was allein schon durch den Nichtgebrauch der Software erreicht wird; Maßnahmen zur Fehlerbehebung an der Software selbst sind dagegen auf das Äquivalenzinteresse gerichtet.[263]

(iv) Ende des Supports bei älteren Produkten?

133 Im schnelllebigen IT-Markt ist schließlich von besonderem Interesse, wann die Produktbeobachtungspflicht endet; so stellen auch bekannte Softwarefirmen wie Microsoft nach ca. 5-7 Jahren den Support für ihre Produkte ein. Hier ist zu differenzieren:

134 Allgemein gilt, dass die **Produktbeobachtungspflicht** selbst nach längerer Bewährung eines Produktes nur dort enden kann, wo keine Langzeitschäden zu befürchten sind. Insoweit kann allerhöchstens von einer graduellen Abschwächung der Beobachtungspflichten und Orientierung an anderen Arten von Schäden, wie Spätschäden, ausgegangen werden.[264]

---

261 Vgl. etwa zu abgeschwächten Instruktionspflichten gegenüber gewerblichen Abnehmern BGH NJW 1996, 2224 (2225 f.); Kullmann/Pfister-*Kullmann*, Kza 1520 S. 47 f.

262 Zu Ausnahmen im Werkvertragsrecht vgl. BGH NJW-RR 2004, 782: Die Herausgabepflicht beurteilt sich nach den Umständen des Einzelfalls. Neben der Höhe des vereinbarten Werklohns kann dabei insbesondere dem Umstand Bedeutung zukommen, ob das Programm zur Vermarktung durch den Besteller erstellt wird und dieser zur ihm obliegenden Wartung und Fortentwicklung des Programms des Zugriffs auf den Quellcode bedarf; BGH NJW 1987, 1259 (1259 f.); LG München I CR 1989, 990 (991); LG Köln CR 2003, 484: grundsätzlich Übergabe des Quellcodes weder bei Individual- noch bei Standardsoftware Leistungspflicht des Herstellers; LG Köln CR 2000, 505 = NJW-RR 2001, 1711: Herausgabe bei Individualsoftware, wenn kein Wartungsvertrag besteht; OLG Karlsruhe CR 1999, 11: Herausgabepflicht, wenn Dokumentation zur Bedienung und Wartung geschuldet ist; abl. für Standardsoftware OLG München CR 1992, 208 (209): ohne Vereinbarung grundsätzlich keine Herausgabe des Quellcodes; *Schneider*, CR 2003, 317 (318 f.); *Ernst*, MMR 2001, 208 (211); *Schneider*, Handbuch des EDV-Rechts, A Rn. 90 ff., 99, H Rn. 24 f., 76 ff, J Rn. 328; *Brandi-Dohrn*, Gewährleistung bei Hard- und Softwaremängeln, S. 32 f.; auf den Einzelfall abstellend *Köhler/Fritzsche*, in: Lehmann, Rechtsschutz und Verwertung von Computersoftware, Kap. XIII Rz. 146 f.; *Seffer/Horter*, ITRB 2005, 169; *Conrad*, ITRB 2005, 12; *Hoeren*, CR 2004, 721; ebenso wohl *Marly*, Softwareüberlassungsverträge, Rn. 64 ff.; *Malzer*, CR 1989, 991 (992).

263 Dies wird von *v. Westphalen/Langheid/Streitz*, Rz. 829 f. zu wenig berücksichtigt.

264 Zutr. *Foerste*, in: v. Westphalen, ProdHaftHdb, § 24, Rn. 298; *Hölzlwimmer*, Produkthaftungsrechtliche Risiken des Technologietransfers durch Lizenzverträge, S. 40; *v. Bar*, in: Produktverantwortung und Risikoakzeptanz, S. 29, 40; Staudinger-*Hager*, § 823 BGB F Rn. 21; aA LG Frankfurt NJW 1977, 1108; *Löwe*, DAR 1978, 288 (290); *Dietrich*, Produktbeobachtungspflicht und Schadenverhütungspflicht der Produzenten, S. 121 f.: Produktbeobachtungspflicht endet spätestens nach 10 Jahren; diff. *Pauli*, PHi 1985, 134 (139), der von einem späteren Wiederaufleben der Produktbeobachtungspflicht bei Schäden ausgeht.

135 Indes ist mit der Produktbeobachtungspflicht **nicht der „Support“ (Patches) zu verwechseln**: Denn selbst eine länger wirkende Produktbeobachtungspflicht besagt bei älteren Softwareprodukten nichts darüber, zu welchen Maßnahmen der Hersteller gehalten ist – hier könnte etwa eine allgemeine Warnung vor Sicherheitslücken genügen.

(v) Produktbeobachtung für Fremdsoftware

136 Die Produktbeobachtungspflicht erstreckt sich nach der Rechtsprechung auch auf Gefahren, die durch die Kombination des eigenen mit fremden Produkten, insbesondere mit auf dem Markt angebotenen Zubehörteilen entstehen können.[265] Die Produktbeobachtungspflicht hängt hier entscheidend von der Art und Größe der geschaffenen Gefahr ab: Sind Leib und Leben bedroht, hat der Hersteller über die Pflicht zur Sammlung und Verwertung einschlägiger Informationen hinaus bei konkretem Anlass auch die durch die Kombination entstandenen Gefahren sowie die durch Verwendung von fehlerhaftem Zubehör mit dem Produkt entstehenden Risiken[266] selber zu überprüfen.[267] Diese Pflichten reduzieren sich erheblich, sofern nicht hochrangige Rechtsgüter bedroht sind oder der Markt zu unübersichtlich ist, um allen Gefahren nachgehen zu können.[268] Auch kann sich ein Hersteller grundsätzlich auf den eigenverantwortlichen Umgang weiterer Produzenten mit einem Vorprodukt verlassen.[269]

137 Die Rechtsprechung schießt indes über ihr Ziel hinaus: Eine generelle **Ausdehnung der Beobachtungspflichten auf Zubehörteile oder Kombinationsgefahren** kann nicht allein damit begründet werden, dass der Hersteller ohnehin zur Beobachtung der Produkte verpflichtet ist; grundsätzlich ist der Hersteller nur für die Gefahren verantwortlich, die er selbst geschaffen hat, nicht aber für Gefahrenerhöhungen, die durch Dritte verursacht werden,[270] erst recht, wenn die Zubehörprodukte wesentlich später nach Entwicklung, Konstruktion und Fabrikation auf den Markt gebracht werden. Jedenfalls muss es als

---

265 BGHZ 99, 167 (172 ff.) = NJW 1987, 1009; BGH NJW 1995, 1286 (1287 f.); ausführlich dazu *Ulmer*, ZHR 152, 564 (575 ff.), der sich allerdings dogmatisch auf die Herausforderungsfälle im Schadensrecht stützt; dem BGH zust. *Kunz*, BB 1994, 450 (451); *Dietrich*, Produktbeobachtungspflicht und Schadenverhütungspflicht der Produzenten, S. 76 ff.; ausführlich *Klinger*, Die Produktbeobachtungspflicht bezüglich Fremdzubehörteilen, S. 56 ff.

266 Vgl. *Kunz*, BB 1994, 450 (451 f.); anders *Ulmer*, ZHR 152, 564 (575 ff.): nur Kombinationsrisiken, nicht Fehlerfreiheit des Zubehörs.

267 Zumindest hinsichtlich der von Marktführern angebotenen Zubehörteile, BGHZ 99, 167 (174 f.) = NJW 1987, 1009; *Michalski*, BB 1998, 961 (963); *Birkmann*, DAR 1990, 124 (128).

268 BGHZ 99, 167 (175 f.) = NJW 1987, 1009; *v. Bar*, in: Produktverantwortung und Risikoakzeptanz, S. 29, 35.

269 OLG Stuttgart VersR 2001, 465 (467): Zimmermann, der einen Holzbalken hergestellt hat, auf das korrekte Anstreichen durch einen Maler, Rev. n. angen. BGH Beschl. v. 24.10.2000 – VI ZR 89/00.

270 Ähnlich *Ulmer*, ZHR 152, 564 (579); zust. *v. Bar*, in: Produktverantwortung und Risikoakzeptanz, S. 29, 36.

ausreichend angesehen werden, wenn der Hersteller den Produktbenutzer dahingehend instruiert, dass nur von ihm selbst freigegebene bzw. als unbedenklich eingestufte Zubehörteile gefahrlos benutzt werden können und dass die Benutzung nicht autorisierten Zubehörs auf Gefahr des Benutzers erfolgt.[271] Anders ist dies zu beurteilen, wenn der Hersteller etwa selbst Schnittstellen für andere Programme vorsieht oder es sich um allgemein gebräuchliche Programme handelt, mit dem der Hersteller von vornherein rechnen muss.

138 Demgemäß ist die **Haftung für fremde Software weitgehend ausgeschlossen**; sie kann allenfalls in Betracht kommen, wenn die fremde Software, wie Plug-Ins, Add-Ons etc. spezifisch auf das Produkt des Herstellers zugeschnitten ist. Nur dann wird man überhaupt von einer solchen Produktbeobachtungspflicht ausgehen können.

(b) Rückrufpflichten

139 Auch wenn in den Grundzügen größtenteils anerkannt, fehlt bislang eine klare dogmatische Grundlage für die Pflicht, das Produkt zurückzunehmen und gegen ein funktionstüchtiges auszutauschen,[272] da sie das vertragsrechtlich geregelte Äquivalenzinteresse berührt.[273] Nur dann, wenn erhebliche Folgen für Gesundheit und Eigentum zu befürchten sind und Warnhinweise entsprechende Schäden nicht ohne weiteres verhindern können, kann eine entsprechende Fehlerbehebung[274] anstelle eines Warnhinweises in Betracht kommen.[275] Im Vordergrund der Herstellerpflichten steht aber die Vermeidung von Schäden an anderen Rechtsgütern durch den weiteren Gebrauch des Produktes, so dass in fast allen Fällen eine ausdrückliche Warnung genügt, die den Softwarenutzer von der weiteren Verwendung des Produktes abhält; alles andere wäre auf das Äquivalenzinteresse gerichtet. Modifiziert werden kann diese Lage allenfalls durch das öffentlich-rechtliche Produktsicherheitsrecht.[276]

---

271 In der Tendenz auch BGHZ 99, 167 (174) = NJW 1987, 1009.

272 Zusammenfassend MünchKommBGB-*Wagner*, § 823 BGB Rn 603 ff.; Staudinger-*J. Hager*, § 823 Rz. F 20 f.; Bamberger/Roth-*Spindler*, § 823 BGB Rn 516 ff.; *Pieper*, BB 1991, 985; *v. Bar*, 25 Jahre Karlsruher Forum, S. 80 ff.; *Hager*, VersR 1984, 799 ff.; *Herrmann*, BB 1985, 1801 ff.; *Schwenzer*, JZ 1987, 1059 ff.; *Sack*, BB 1985, 1801 ff.

273 Zu Recht abl. *Foerste*, in: v. Westphalen, ProdHaftHdb, § 24 Rn. 260 ff., 266, 274, 280 mwN.

274 *Bartsch*, Der Jahr-2000-Fehler, S. 157 f.; *Imhof/Wahl*, WpK-Mitt. 1998, 136 (139) weisen zutreffend darauf hin, dass eine Deinstallation der Software im Sinne eines physischen Rückrufs wenig Sinn machen würde.

275 Vgl. OLG Frankfurt NJW-RR 2000, 1268 (1272); OLG München NJW-RR 1999, 1657, Rev. n. angen. BGH 27.5.1999 – III ZR 103/98; BGH NJW 1990, 2560; *Foerste*, DB 1999, 2199 (2199 f.); *Schwenzer*, JZ 1987, 1059 (1061 f.); Kullmann/Pfister-*Kullmann*, Kza 1520 S. 62 f.; MünchKommBGB-*Wagner*, § 823 BGB Rn. 605; *v. Bar*, in: Produktverantwortung und Risikoakzeptanz, S. 29 (40 f.).

276 Vgl. § 5 I Nr. 1 c) GPSG = § 4 II ProdSG aF: öffentlich-rechtliche Produktbeobachtungspflicht des Her-

140 Unklar ist auch, ob mit der Rückrufpflicht auch eine **Pflicht zur kostenlosen Beseitigung der Gefahr** einhergeht[277] und welche Kosten ersetzt verlangt werden können: Die Rspr. tendiert dazu, den Schaden auf die Kosten des Ausbaus der fehlerhaften Teile zu beschränken, nicht jedoch die Kosten für den Einbau neuer, fehlerloser Teile zu erstatten.[278] Während der Hersteller bei zuvor unterlassenem Rückruf für einen eingetretenen Schaden ersatzpflichtig ist,[279] fehlt es grundsätzlich an einer Rechtsgutsverletzung und einem Schaden, wenn lediglich die Gefahr einer Schädigung besteht.[280] Jedoch ist der Hersteller verpflichtet, Gefahren für von § 823 Abs. 1 BGB geschützte Rechtsgüter zu vermeiden, so dass zumindest ein Anspruch aus § 1004 BGB anzunehmen ist. Daher hat der Hersteller die Kosten in vollem Umfang[281] jedenfalls für die Rücknahme des Produktes zu tragen, wenn von dem Produkt Gefahren für andere Rechtsgüter drohen.[282] Bei einem drohenden Schaden allein am Produkt selbst genügt eine Warnung des Produktbenutzers, da ansonsten das Äquivalenzinteresse und die Erwartung, das Produkt nutzen zu können, geschützt würde.[283]

141 Dementsprechend kann aus dem Produkthaftungsrecht prinzipiell keine Pflicht abgeleitet werden, dass Patches oder ein Support zur Verfügung gestellt wird, da es genügen würde, dass der Kunde das Produkt nicht mehr benutzt, um seine Integritätsinteressen zu wahren. Eine Pflicht zur fortdauernden Softwarepflege kann daher deliktisch nicht abgeleitet werden.

---

stellers sowie § 8 Abs. 4 Nr. 7 GPSG = § 9 ProdSG aF: behördliche Anordnung des Rückrufs; zur Rückrufpflicht aufgrund von § 823 BGB Abs. 2 i.V.m.. § 8 Abs. 4 Nr. 7 GPSG bzw. § 9 ProdSG aF; vgl. Bamberger/Roth-*Spindler*, § 823 BGB Rn. 522.

277 Etwa durch Reparatur oder Austausch des Produktes, so OLG Düsseldorf NJW-RR 1997, 1344 (1345); OLG Karlsruhe NJW-RR 1995, 594 (597); *J. Hager*, VersR 1984, 799 (800); *Mayer*, DB 1985, 319 (320); G. *Hager*, AcP 184 (1984), 413 (423 ff.) mit dem Hinweis, dass auch in der Praxis so verfahren wird; ausführlich *Koch*, AcP 203 (2003), 603 ff.

278 OLG Stuttgart NJW 1967, 572; zust. OLG Düsseldorf NJW-RR 1997, 1344 (1346).

279 BGH VersR 1971, 80 (81); BGHZ 80, 199 (203) = NJW 1981, 1606; BGH NJW 1994, 517 (518 f.); BGH NJW-RR 1995, 342.

280 Abl. deswegen wohl (obiter dictum) OLG München NJW-RR 1999, 1657, Rev. n. angen. BGH 27.5.1999 – III ZR 103/98.

281 *Dietrich*, Produktbeobachtungspflicht und Schadenverhütungspflicht der Produzenten, S. 223 f.; abw. *Foerste*, in: v. Westphalen, ProdHaftHdb § 24 Rn. 285: ausnahmsweise Kostenteilung.

282 OLG Düsseldorf NJW-RR 1997, 1344 (1345); OLG Karlsruhe NJW-RR 1995, 594 (597); MünchKommBGB-*Wagner*, § 823 BGB Rn. 605; Staudinger- *Hager*, § 823 BGB F Rn. 26; *G. Hager*, AcP 184 (1984), 413 (423) ff.; *J. Hager*, VersR 1984, 799 (802); *Mayer*, DB 1985, 319 (320); *Dietrich*, Produktbeobachtungspflicht und Schadenverhütungspflicht der Produzenten, S. 236; nur bei Gefahren für Leib und Leben: *Schwenzer*, JZ 1987, 1059 (1063); *Michalski*, BB 1998, 961 (965).

283 Zutr. *Foerste*, DB 1999, 2199 (2200); *Taschner/Frietsch*, Einführung Rn. 89; ähnlich *Pieper*, BB 1991, 985 (988) mit dem Hinweis, dass andernfalls eine „deliktische Gewährleistung" entstünde; anders *v. Westphalen*, DB 1999, 1369 (1370); *Koch*, AcP 203 (2003), 603 (624 ff., 631f.), will Ersatz der Aus- und Einbaukosten unter Ausschluss von Materialkosten gewähren.

(5) Herstellerpflichten und technische Standards

142 Art und Umfang der Pflichten von IT-Herstellern werden nicht nur durch die Erwartungen des Verkehrs, sondern auch maßgeblich vom Erkenntnisstand von Wissenschaft und Technik mitbestimmt. Die Rechtsprechung rekurriert hierbei vielfach an die dem öffentlichen Sicherheitsrecht als Eingriffsvoraussetzung für Behörden entstammenden Kategorien der „anerkannten Regeln der Technik", den „Stand der Technik" sowie den „Stand von Wissenschaft und Technik",[284] ohne die Verwendung dieser Begriffe näher zu erläutern. Im Ergebnis ausschlaggebend für die Pflichtenbestimmung ist das konkrete Gefährdungspotential eines Produkts.[285]

143 Untergrenze der Sorgfaltsanforderungen bilden jedenfalls die **anerkannten Regeln der Technik**, d.h. die in den Kreisen der betreffenden Techniker bekannten und als richtig anerkannten Regeln, welche in der Praxis erprobt, dort verbreitet und bewährt sind.[286] Nach oben werden die Sorgfaltsanforderungen begrenzt durch den **Stand von Wissenschaft und Technik** im Zeitpunkt des Inverkehrbringens des Produkts,[287] welcher das realisierbare Ergebnis neuester naturwissenschaftlicher Forschung und ingenieurwissenschaftlicher Erfahrungssätze, deren Akzeptanz durch die Mehrheit der Praktiker noch aussteht widerspiegelt.[288] Für danach nicht voraussehbare Gefahren (Entwicklungsfehler) haftet der Hersteller nicht.[289]

144 Für die Ausfüllung dieser unbestimmten Rechtsbegriffe und damit die Pflichtenbestimmung im Bereich der Produkthaftung von herausragender Bedeutung sind Standards, welche in **überbetrieblichen technischen Normen** niedergelegt sind:

(a) Haftungsrechtliche Bedeutung technischer Normen

---

284 BGH NJW 1971, 1313 (anerkannte Regeln der Technik); BGH DB 1972, 1335 (Stand der Technik); BGH NJW 1981, 1603 (Stand von Wissenschaft und Technik); ausführlich zur Abgrenzung der Begriffe BVerfG NJW 1979, 359, (362); *Marburger*, Die Regeln der Technik im Recht, §§ 14-16.

285 Dazu ausführlich *Finke*, Die Auswirkungen der europäischen Normen und des Sicherheitsrechts auf das nationale Haftungsrecht, S. 9 ff.

286 *Marburger*, Die Regeln der Technik im Recht, S. 157, 162 f., 439; *Foerste*, in: v.Westphalen, ProdHaftHdB, § 24 Rn. 16; *Wilrich*, § 2 GPSG Rn. 107; *Vieweg*, in: Schulte, Handbuch des Technikrechts, S. 353.

287 *Foerste*, in: v.Westphalen, ProdHaftHdB, § 24 Rn. 18 f.; *Spindler*, Unternehmensorganisationspflichten, S. 796.

288 BVerfG NJW 1979, 359, (362); OLG Köln NJW-RR 1991, 1077 (1079); *Marburger*, Die Regeln der Technik im Recht, S. 164 f.; *Foerste*, in: v. Westphalen, ProdHaftHdB, § 24 Rn. 16.

289 Bamberger/Roth-*Spindler*, § 823 BGB Rn. 493; MünchKommBGB-*Wagner*, § 823 BGB Rn. 264, 579f.; *Foerste*, in: v.Westphalen, ProdHaftHdB, § 24 Rn. 18, 82 ff.

145 Technischen Normen werden von privaten Normungsorganisationen wie beispielsweise dem deutschen DIN e.V. erlassen und sind folglich keine Rechtsnormen.[290] Nach Auffassung der Rechtsprechung handelt es sich vielmehr um **auf freiwillige Anwendung angelegte Empfehlungen** der privaten Normungsorganisationen.[291] Da die technischen Regeln keine (rechtliche) Bindungswirkung entfalten, ist der Hersteller ferner nicht gehindert, das erforderliche Sicherheitsniveau auf abweichende, aber gleich geeigneten oder besseren, als dem in der technischen Norm vorgezeichnetem Wege **(alternative Sicherheitslösungen)** zu erreichen.[292]

146 Die Bedeutung überbetrieblicher technischer Normen im Haftungsrecht liegt nach ständiger Rechtsprechung des BGH darin, dass sie anerkannte Regeln der Technik wiedergeben und daher **zur Bestimmung des nach der Verkehrsauffassung zur Sicherheit Gebotenen in besonderer Weise geeignet** sind.[293] Technische Normen können herangezogen werden, um den Inhalt von Verkehrspflichten zu konkretisieren. Die technischen Regeln können indes nur als der zu fordernde **Mindeststandard** herangezogen werden, der nicht ausschließt, dass die Zivilgerichte im Einzelfall über die dort niedergelegten Verhaltensanforderungen hinausgehen.[294] Sie bestimmen mithin die Sorgfaltsanforderungen nicht abschließend und binden die Zivilgerichte mangels Rechtsnormqualität nicht.[295]

147 Die technischen Normen geben jedoch **nicht in jedem Fall die anerkannten Regeln der Technik** wieder;[296] sie können im Einzelfall auch hinter ihnen zurückbleiben.[297] Der Hersteller muss daher nach Ansicht des BGH grundsätzlich selbständig prüfen, ob

---

290 *Reiff*, in: Marburger, Technische Regeln im Umwelt- und Technikrecht, S. 159; Bamberger/Roth-*Spindler*, § 823 BGB Rn. 255; MünchKommBGB-*Wagner*, § 823 BGB Rn. 578.

291 BGH NJW 2004, 1449 (1450); BGHZ 139, 16 (19); BGHZ 103, 338 (341); *Röthel*, in: Marburger, Technische Regeln im Umwelt- und Technikrecht, S. 31 (45); *Reiff*, in: Marburger, Technische Regeln im Umwelt- und Technikrecht, S. 159.

292 Bamberger/Roth-*Spindler*, § 823 BGB Rn. 257; *Foerste*, in: v.Westphalen, ProdHaftHdB, § 24 Rn. 20; MünchKommBGB-*Wagner*, § 823 BGB Rn. 273, 578.

293 BGH NJW 2004, 1449 (1450); BGH NJW-RR 2002, 525 (526); BGH NJW 2001, 2019 (2020); BGH VersR 1988, 632 (633); Bamberger/Roth-*Spindler*, § 823 BGB Rn. 255; MünchKommBGB-*Wagner*, § 823 BGB Rn. 272; *Reiff*, in: Marburger, Technische Regeln im Umwelt- und Technikrecht, S. 159, 161 ff.

294 BGH NJW 2004, 1449 (1450); BGH VersR 1987, 102 (103); *Reiff*, in: Marburger, Technische Regeln im Umwelt- und Technikrecht, S. 161; Bamberger/Roth-*Spindler*, § 823 BGB Rn. 20, 255; Soergel-*Krause*, Anh II § 823 BGB Rn. 49; MünchKommBGB-*Wagner*, § 823 BGB Rn. 272; Staudinger-*Hager*, § 823 BGB Rn. G 34; *Vieweg*, in: Schulte, Handbuch des Technikrechts, S. 355.

295 Bamberger/Roth-*Spindler*, § 823 BGB Rn. 255; *Vieweg*, in: Schulte, Handbuch des Technikrechts, S. 360.

296 BGH NJW 1987, 372 (373); *Foerste*, in: v.Westphalen, ProdHaftHdB, § 24 Rn. 37.

297 BGHZ139, 16 (20); OLG Nürnberg NJW-RR 2002, 1538; *Reiff*, in: Marburger, Technische Regeln im Umwelt- und Technikrecht, S. 161 f.

und welche Sicherungsmaßnahmen erforderlich sind.[298] Die Einhaltung der einschlägigen technischen Norm entlastet nur dann, wenn sie die jeweiligen Gefahren ausreichend berücksichtigt, also z.B. auch besonders gefährdete Verkehrskreise mit einbezieht.[299] Über die normierten Standards hinausgehende Sicherheitsmaßnahmen wird man dann fordern müssen, wenn die technischen Normen veraltet sind, besonderen Gefahrenlagen zu begegnen ist oder sich das Produkt an einen besonders gefährdeten Nutzerkreis wendet.[300] Insbesondere für DIN-Normen besteht bei Einhaltung der in technischen Normen geregelten Standards jedoch eine **tatsächliche Vermutung für die Wiedergabe der anerkannten Regeln der Technik**, die nicht unterschritten werden dürfen.[301]

148 Keine anderen Grundsätze gelten auch für **europäisch harmonisierte Normen** im Rahmen des sog. **„New Approach"**. Auch technische Normen, welche von den europäischen Normungsorganisationen CEN, CENELEC und ETSI erarbeitet werden, bleiben rechtliche unverbindliche Empfehlungen privater Organisationen[302], welche auf freiwillige Einhaltung angelegt sind (so ausdrücklich § 2 Abs. 16 GPSG).[303] Bei harmonisierten Normen wird wegen der an sie anknüpfenden Vermutungswirkung (s. z.B. § 4 Abs. 1 Satz 2 GPSG) zwar verbreitet von einer Bindungswirkung oder gar einer „Rechtswirkung" gesprochen.[304] Diese Bindungswirkung ist indes auf die Prüfung der Konformität mit den Richtlinienanforderungen beschränkt (Adressaten sind insoweit Marktüberwachungsbehörden und Verwaltungsgerichte), welche zivilrechtlich – wie ausgeführt – nur den zu fordernden Mindeststandard markieren[305], die zivilrechtliche Sorgfalt aber nicht

---

298 BGH NJW 2001, 2019 (2020); BGH NJW 1982, 1049; *Köhler*, BB 1985 Beil. 4, 10 (10 f.); *Marburger*, VersR 1983, 587 (603).

299 BGH NJW 1987, 372; OLG Zweibrücken NJW 1977, 111 f.; *Marburger*, VersR 1983, 597 (600); *Spindler*, Unternehmensorganisationspflichten, S. 805.

300 Bamberger/Roth-*Spindler*, § 823 BGB Rn. 255, 489; Soergel-*Krause*, Anh II § 823 BGB Rn. 46; *Foerste*, in: v.Westphalen, ProdHaftHdB, § 24 Rn. 41.

301 BGH NJW 1988, 2667 (2668); BGH VersR 1984, 270; BGH VersR 1972, 767 (768); OLG Celle NJW 2003, 2544; *Köhler*, BB 1985 Beil. 4, 10 (11); Bamberger/Roth-*Spindler*, § 823 BGB Rn. 255; *Foerste*, in: v.Westphalen, ProdHaftHdB, § 24 Rn. 38, 41; *Spindler*, Unternehmensorganisationspflichten, S. 803, 805.

302 CEN und CENELEC sind Vereine nach belgischem Recht, ETSI ist ein Verein nach französischem Recht, s. dazu *Röthel*, in: Marburger, Technische Regeln im Umwelt- und Technikrecht, S. 31 (41).

303 Siehe auch *Europäische Kommission*, Leitfaden für die Umsetzung der nach dem neuen Konzept und dem Gesamtkonzept verfassten Richtlinien, 2000, S. 7, 9, abrufbar unter http://ec.europa.eu/enterprise/newapproach/legislation/guide/document/guidepublicde.pdf; *Röthel*, in: Marburger, Technische Regeln im Umwelt- und Technikrecht, S. 31 (45 f.); *Taupitz*, in: Produktverantwortung und Risikoakzeptanz, S. 119 (124); *Wilrich*, Einleitung Rn. 39.

304 *Roßnagel*, DVBl. 1996, 1181 (1184); *Spindler*, Unternehmensorganisationspflichten, S. 161 f. mwN.

305 Siehe *Taschner/Frietsch*, Art. 7 ProdHaft-RL Rn. 31: „Es handelt sich bei diesen Sicherheitsanforderungen gemeinschaftsrechtlichen Charakters [...] um Mindestanforderungen auf EG-Ebene. Ihr Ziel ist in erster Linie die Herstellung des freien Warenverkehrs auf dem Gemeinsamen Markt durch Beseitigung technischer Handelshemmnisse. Die Beseitigung von Gefährdungen für den Verwender technischer Gerä-

abschließend definieren. Auch die Einhaltung der in harmonisierten Normen niedergelegten Sicherheitsanforderungen vermag den Produkthersteller daher in Bezug auf die zivilrechtliche Haftung nicht in jedem Fall zu entlasten.[306] Dies wird auf europarechtlicher Ebene schließlich durch das Nebeneinander von Produktsicherheits- und Produkthaftungsrichtlinie verdeutlicht.[307]

149 Nicht zu unterschätzen ist indes die **faktische Autorität** harmonisierter wie rein nationaler Normen für die Bestimmung der Verkehrspflichten, so dass die Einhaltung der Normvorgaben den Hersteller im praktischen Ergebnis oftmals gleichbedeutend mit der Wahrung der im Verkehr erforderlichen Sorgfalt sein wird.[308] In der Tat gehen die Gerichte nur in seltenen Fällen über die Anforderungen der einschlägigen technischen Norm hinaus.[309] Dagegen werden Pflichtverstöße oftmals schon allein deshalb bejaht, weil technische Normen missachtet wurden.[310]

(b) Technische Standards für den IT-Bereich: Common Criteria und Protection Profiles

150 Bislang existieren im IT-Bereich keine allgemeingültigen Sicherheitsstandards, so dass hinsichtlich der Sicherheitserwartungen des Verkehrs praktisch keine Konkretisierung durch technische Normen erfolgt.[311] Vor allem der rasante Fortschritt in der Softwareentwicklung behindert dabei die Versuche zur Festlegung eines allgemeingültigen Sicherheitsstandards, der nicht sofort wieder überholt ist.[312]

151 Zunehmend werden IT-Produkte nach den sog. **Common Criteria-Standards** zertifiziert und geprüft, die sich als internationaler Standard für IT-Produkte herausgebildet haben.[313] Im Zusammenhang mit sog. Protection Profiles, die halbstandardisiert für Si-

---

te ist lediglich von zweitrangigem Interesse."

306 *Taupitz*, in: Produktverantwortung und Risikoakzeptanz, S. 119 (132 ff., insbes. 135, 136); *Wandt*, Internationale Produkthaftung, Rn. 646; Bamberger/Roth-*Spindler*, § 823 BGB Rn. 489.

307 *Taupitz*, in: Produktverantwortung und Risikoakzeptanz, S. 119 (135); Bamberger/Roth-*Spindler*, § 823 BGB Rn. 489.

308 MünchKommBGB-*Mertens*, 3. Aufl. 1997, § 823 BGB Rn. 30.

309 *Reiff*, in: Marburger, Technische Regeln im Umwelt- und Technikrecht, S. 155 (166). Ein Beispiel ist BGH NJW 1985, 164, wo das Gericht über die einschlägigen DIN-Normen und die Bestimmungen der Bayerischen VersammlungsstättenVO hinausging. Siehe auch BGH VersR 1987, 783 zur Abweisung einer Unterlassungsklage gegen die Stiftung Warentest, die ein Produkt trotz Einhaltung der maßgeblichen DIN-Norm mit „mangelhaft" bewertet hatte.

310 S. z.B. BGH NJW-RR 2002, 525.

311 *Sodtalbers*, Softwarehaftung im Internet, Rn. 273; *Hoeren*, in: von Westphalen, Vertragsrecht und AGB-Klauselwerke, IT-Verträge, Rn. 94.

312 Bereits in der Begründung zum ProdHaftG wird auf das Problem veralteter Normen hingewiesen: BT-Drucks. 11/2447, 19; ferner *Bartl*, § 3 ProdHaftG, Rn. 43.

313 Näher dazu unter http://www.bsi.bund.de.

cherheitsbedürfnisse von IT-Anwendungen erstellt werden, können diese Produktstandards (mittelbar) rechtliche Wirkung entfalten, indem sie die nötige Mindestsicherheit für bestimmte Bereiche konkretisieren. Als Common Criteria werden die „Gemeinsamen Kriterien für die Prüfung und Bewertung von Sicherheit von Informationstechnik" nach der im Jahre 2000 beschlossenen ISO-Norm 15408 bezeichnet,[314] die den amerikanischen Standard TCSEC sowie den europäischen Standard ITSEC ablösen sollen. Sie stellen ein weltweit anerkanntes Rahmenwerk für die Bewertung von Softwareprodukten dar.[315] Ziel ist eine vergleichbare Überprüfung und entsprechend auch Zertifizierung von IT-Produkten mit unterschiedlich modellierbarer Prüfungsintensität.[316] Common Criteria definieren somit an sich keine Überprüfung für IT-Produkte, sondern legen für die Bewertung eine gemeinsame Basis fest. Dafür definieren die Common Criteria 11 Funktionalitätsklassen sowie deren Abhängigkeiten, die für ein Produkt sicherheitsrelevante Vorgänge beschreiben. Die Funktionalitätsklassen sind allgemeine Grundfunktionen der Sicherheitsarchitektur eines zu zertifizierenden Produkts bzw. einer Produktklasse wie z.B. der Schutz der Benutzerdaten, die Privatsphäre, Kommunikation oder Sicherheitsprotokollierung.[317] Diese Grundfunktionen sind getrennt zu bewerten.

152 Allein für sich genommen würden jedoch die Common Criteria keine Sicherheitsbewertung erlauben. Hierzu sind **Protection Profiles** erforderlich, die Dokumente darstellen, in denen Anwender auf der Basis der 11 Funktionsklassen ihre Sicherheitsbedürfnisse benutzerorientiert formal beschreiben und anschließend registrieren können.[318] Protection Profiles stellen produktunabhängige Profile zur Bewertung bestimmter IT-Produkte dar. Aus ihnen kann für konkrete Produkte ein sogenanntes Security Target, sprich spezielle Sicherheitsvorgaben, erstellt werden, gegen das dann die Evaluation durchgeführt werden kann.[319] Ein Protection Profile besteht u.a. aus der Beschreibung des Sicherheitsproblems, der Spezifizierung von Sicherheitszielen sowie der notwendigen Anforderungen an das Produkt, um den Sicherheitszielen genügen zu können.[320]

---

314 Zur Entwicklung s. *Münch*, RDV 2003, 223.

315 *Mackenbrock*, http://www.bsi.de/cc/cc_20d.htm; *Ernestus*, DuD 2003, 68; *Probst*, DSB 2003, Heft 5, 10.

316 *Probst*, DSB 2003, Heft 5, 10.

317 Common Criteria v3.0 Rev. 2 Teil 1, http://www.bsi.bund.de/cc/CCMB2005V3T2.pdf, Rn. 119 ff.

318 *Ernestus*, DuD 2003, 68; *Probst*, DSB 2003, Heft 5, 10; *Roßnagel*, Freundesgabe für Büllesbach, S. 131 (141); eine Liste der aktuell registrierten Schutzprofile findet sich unter http://www.bsi.de/cc/pplist/pplist.htm.

319 *Mackenbrock*, http://www.bsi.de/cc/cc_20d.htm.

320 Common Criteria v3.0 Rev. 2 Teil 1, http://www.bsi.bund.de/cc/CCMB2005V3T1.pdf, Rn. 272; dazu auch *Probst*, DSB 2003, Heft 5, 10 ff.

153 Zusammen können Common Criteria und Protection Profiles den nötigen Mindest-IT-Sicherheitsstandard bezogen auf ein bestimmtes Anwendungsgebiet ergeben. Für eine bestimmte Produktklasse stellt ein Protection Profile, sofern es vorliegt, eine entsprechende Normierung für diese Produktklasse dar. Damit können sie als Orientierung für die Pflichtenbestimmung dienen und wirken als Mindeststandard bzw. als Festlegung der allgemein **anerkannten Regeln der Technik** im Sinne der Überzeugung aller Fachleute in einem Technikgebiet (zum Begriff der anerkannten Regeln der Technik s. Rn. 146). Anders formuliert, können durch die Festlegung von Protection Profiles die Mindestanforderungen an alle Produkte, die die im Protection Profile enthaltenen Ziele erfüllen sollen, im Wege eines Mindeststandards bzw. der Schwelle der zu erfüllenden Anforderungen bei Produktion und Vertrieb eines entsprechenden Produkts im Sinne eines Pflichtenprogramms wie bei anderen Normierungen verbindlich festgelegt werden. Damit kommt den Protection Profiles im Zusammenspiel mit den Common Criteria aber auch eine erhebliche Bedeutung hinsichtlich der Konkretisierung der im Verkehr erwarteten Sicherheit zu – was sich im Bereich der mit der Einhaltung (oder Verletzung) der allgemein anerkannten Regeln der Technik verknüpften Vermutungswirkungen auswirkt.[321]

(c) Zwischenergebnis

154 Nach dem derzeitigen Stand können Standards grundsätzlich nur sektorspezifisch Wirkung entfalten. Dies wird vor allem bei Softwarestandards wie z.B. den Common Criteria und den Protection Profiles deutlich. Es wird zwar versucht, die Profile möglichst allgemein zu halten, dennoch betreffen sie nur einen speziellen Anwendungsfall.

155 Allerdings entspricht gerade eine sektorspezifische Regelung den allgemeinen Regeln der Produkthaftung, etwa wenn die Haftung des Herstellers durch besonderes Expertenwissen auf Seiten des Nutzers oder besondere Einsatzgebiete (die aber dem Hersteller bekannt sein müssen) beeinflusst werden kann. Die Standardisierungen können demnach rechtlich beachtlich als Konkretisierung der Verkehrspflichten und der geschuldeten Sorgfalt herangezogen werden, wenn sie auf das aktuell hergestellte Produkt passen. Sollte nur ein Teil des Profiles nicht aussagekräftig genug oder nicht allein anwendbar sein, so treffen den Hersteller die Pflichten des Standards nicht. Sofern jedoch ein entsprechend anwendbarer Standard besteht, kann er auch sektorspezifisch angewendet werden.

---

321 S. unten Rn 174 ff.

(6) Haftungsrechtliche Bedeutung von Zertifikaten

156 Im Gegensatz zum öffentlichen Produktsicherheitsrecht, das dem Zertifikat Vermutungswirkungen beimisst,[322] sind dessen zivil- bzw. haftungsrechtliche Auswirkungen gesetzlich nicht ausdrücklich geregelt und bislang **nicht abschließend geklärt**. Hierbei sind zwei grundlegende Fragen zu unterscheiden: erstens, ob Zertifikaten – seien es Zertifikate des BSI oder privater Zertifizierungsunternehmen – eine haftungsbefreiende Wirkung zukommt (dazu Rn. 157 ff.) und – zweitens –, ob Zertifizierungen geeignet sind, die Sicherheitserwartungen der Nutzer von IT-Produkten für die Bestimmung des Inhalts der Herstellerpflichten maßgebend zu beeinflussen (dazu Rn.162 ff.).

(a) Keine pauschale Haftungsfreizeichnung durch Zertifizierung

157 Zertifikate bewirken keine pauschale Entlastung des Herstellers im Sinne einer abschließenden Definition der vom Hersteller einzuhaltenden Sicherheitsanforderungen. Selbst einer **behördlichen Genehmigung oder Zulassung** wird eine pauschale Rechtfertigungswirkung gegenüber der zivilrechtlichen Haftung von der ganz hM versagt, da diese jeweils nur den **Mindeststandard** konkretisieren, den Hersteller im Übrigen aber nicht von eigenverantwortlichen Gefahrenerforschung und Gefahrenabwehr befreien.[323] Auch insoweit gilt, dass der zivilrechtliche Sorgfaltsmaßstab „deliktsautonom“ zu bestimmen ist und die haftungsrechtliche Verantwortung nicht vom Hersteller auf den Zertifizierer übergeht.[324]

158 So hat beispielsweise der BGH der behördlichen Betriebserlaubnis für ein Kfz eine entlastende Wirkung zugunsten des Herstellers versagt.[325] Durch die behördliche Genehmigung geht die Verantwortung grundsätzlich nicht vom Hersteller auf die Behörde über.[326] Er darf sich folglich nicht darauf verlassen, eine Genehmigungs- oder Zulassungsbehörde werde etwaige Mängel aufdecken und dann die Genehmigung bzw. Zulassung versagen.[327] Rechte Dritter werden durch öffentlich-rechtliche Genehmigungen nur insoweit ausgeschlossen, als verwaltungsrechtliche Fachgesetze

---

322 S. § 8 Abs. 2 Satz 3, 4 GPSG für das CE-Kennzeichen und das GS-Zeichen und unten Rn. 253 ff.

323 *Spindler*, Unternehmensorganisationspflichten, S. 833; Bamberger/Roth-*Spindler*, § 823 BGB Rn. 253, 490; Soergel-*Krause*, Anh II § 823 BGB Rn. 48, Anh III § 823 BGB Rn. 16; MünchKommBGB-*Wagner*, § 823 BGB Rn. 275 f.; Staudinger-*Hager* § 823 BGB, E Rn. 34; *Laranz/Canaris*, § 76 III 4 f, S. 416; *Foerste*, in v.Westphalen, ProdHaftHdb, § 24 Rn. 94.

324 Bamberger/Roth-*Spindler*, § 823 BGB Rn. 490; Soergel-*Krause*, Anh II § 823 BGB Rn. 48.

325 BGH NJW 1987, 1009 (1011); BGH NJW 1987, 372 (373).

326 BGH NJW 1987, 372 (373); Kullmann/Pfister-*Kullmann*, Kz. 1520, S. 5; *Foerste*, v.Westphalen, ProdHaftHdB, § 24 Rn. 94; *Schmidt-Salzer*, Produkthaftung², III/1, Rn. 4.761.

327 BGH NJW 1987, 372 (373); BGH NJW 1987, 1009 (1011).

eine Präklusion privater Rechte Dritter ausdrücklich anordnen (z.B. § 14 BImSchG; § 11 WHG).[328]

159 Diese Grundsätze gelten erst Recht für Prüfungen und Zertifizierungen durch den **TÜV** oder sonstige private Zertifizierungsunternehmen. Insbesondere die Verleihung des **GS-Zeichens** („Geprüfte Sicherheit", s. § 7 GPSG und unten Rn. 250) kann den Hersteller damit nicht *pauschal* entlasten.[329] Außerhalb des Bereichs der Produkthaftung hat das OLG Hamm TÜV-Gerätesicherheitsprüfungen im Rahmen der Konkretisierung der berechtigen Sicherheitserwartungen als Indiz herangezogen und einer TÜV-Genehmigung für den Betrieb einer Anlage eine indizielle Bedeutung dafür zugesprochen, dass die Anlage den Sicherheitserwartungen der Benutzer entspricht.[330]

160 Auch **Zertifizierungen und Prüfungen nach der Neuen Konzeption der EU** über Produktsicherheit berühren nicht die zivilrechtliche Haftung des Herstellers.[331] Auch insoweit ist zu bedenken, dass sich die Konformitätsbewertung jeweils nur auf die in den Richtlinien festgelegten Sicherheitsanforderungen bezieht, welche nur den Mindeststandard wiedergeben und nicht zwangsläufig identisch mit dem zivilrechtlichen Verkehrspflichten sind.[332] Das **CE-Kennzeichen** (unten Rn. 248) mag zwar als „formales Schutzschild"[333] gegen behördliche Maßnahmen wirken, enthält aber keine Qualitätsaussage[334] und kann den Hersteller keinesfalls von der Produkthaftung entlasten. Dies gilt unabhängig davon, ob der Hersteller selbst oder eine (neutrale) benannte Stelle die Konformitätsbewertung durchgeführt hat.[335] § 6 Abs. 4 MPG (als Umsetzung der Medizin-Produktrichtlinie, die dem New Approach folgt) stellt ausdrücklich klar, dass die

---

328 Bamberger/Roth-*Spindler*, § 823 BGB Rn. 19; MünchKommBGB-*Wagner*, § 823 BGB Rn. 275, 307 f.; *Wagner*, Öffentlich-rechtliche Genehmigung und zivilrechtliche Rechtswidrigkeit, S. 123 ff.; *Foerste*, in v. Westphalen, ProdHaftHdb, § 24 Rn. 95.

329 Siehe BGH NJW-RR 1990, 406 f.; s. auch OLG Celle NJW 2003, 2544 (2545); MünchKommBGB-*Wagner*, § 823 BGB Rn. 578.

330 OLG Hamm NJW-RR 2001, 1248 (1249): Die Einhaltung der normativen Voraussetzungen (TÜV-Genehmigung) für den Betrieb einer Anlage (hier: Nautic-Jet-Sprungboot) spricht indiziell dafür, dass die Anlage den Sicherheitserwartungen der Benutzer entspricht.

331 *Niebling*, DB 1996, 80 (81); *Niebling*, Die CE-Kennzeichnung, S. 23 f.; *Foerste*, in: v.Westphalen, ProdHaftHdb, § 24 Rn. 94; Bamberger/Roth-*Spindler* § 823 BGB Rn. 490; *Wilrich*, § 6 GPSG Rn. 31.

332 S. dazu *Taupitz*, in: Produktverantwortung und Risikoakzeptanz, S. 119 (134 ff.).

333 So *Wilrich*, § 4 GPSG Rn. 26, § 8 GPSG Rn. 18.

334 *Klindt*, EuZW 2002, 133 (135 Fn. 27); *Niebling*, DB 1996, 80; *Niebling*, Das CE-Kennzeichen, S. 15; *Wilrich*, § 6 GPSG Rn. 6.

335 S. dazu auch *Europäische Kommission*, Leitfaden für die Umsetzung der nach dem neuen Konzept und dem Gesamtkonzept verfassten Richtlinien, S. 45: „Die Gesamtverantwortung für die Konformität eines Produktes mit allen Anforderungen der anzuwendenden Richtlinie verbleibt jedoch immer beim Hersteller, selbst wenn einige Etappen der Konformitätsbewertung unter der Verantwortung einer benannten Stelle durchgeführt werden".

Durchführung eines Konformitätsbewertungsverfahrens die zivil- und strafrechtliche Verantwortlichkeit unberührt lässt.

161 Die dargestellten Grundsätze gelten auch für Zertifikate des BSI oder privater Zertifizierungsunternehmen in Bezug auf **IT-Produkte**. Zertifizierungen können auch hier in aller Regel nicht per se haftungsbefreiend wirken. Der Aussagegehalt einer Zertifizierung anhand technischer Normen, welche – wie oben (Rn. 146) ausgeführt – stets nur den Mindeststandard widerspiegeln, beschränkt sich naturgemäß auf die Dokumentation der Einhaltung der (Mindest-)Anforderungen der technischen Norm. Von der Frage der pauschalen Haftungsentlastung ist die Bedeutung von Zertifikaten im Rahmen des Nachweises der Einhaltung der erforderlichen Sicherheitsanforderungen zu unterscheiden (dazu unten Rn. 181 ff.).

(b) Verschärfung der Haftung durch Zertifizierung?

(i) Grundsätze

162 Schwieriger ist die Frage, inwiefern sich Zertifikate auf die Sicherheitserwartungen der maßgeblichen Verkehrskreise auswirken können. In beschränktem Umfang dürften Zertifikate bei der Bestimmung des Inhalts von Verkehrspflichten relevant werden, sofern Produktzertifikate Einfluss auf die Erwartungen der Nutzer nehmen. Mit Zertifikaten können – insbesondere bei Werbung mit dem Zertifikat – beim Kunden oder Verbraucher **erhöhte Erwartungen hinsichtlich Sicherheit und Qualität** begründet werden, an denen sich das jeweilige zertifizierte Unternehmen festhalten lassen muss, wenn seine Produkte oder seine Produktionstätigkeit von diesen Erwartungen abweichen.[336] Zertifikate können die Einhaltung eines generell höheren Sicherheitsniveaus suggerieren, da durch eine entsprechende Sicherheitsorganisation die Wahrscheinlichkeit von Fehlern beim Pflichtigen verringert werden soll. Dabei kommt es nicht auf die objektive Geeignetheit solcher Zertifikate zur Feststellung einer ordnungsgemäßen Produktbeschaffenheit an, sondern nur, wie im Rahmen von Werbeaussagen, auf deren generelle Eignung, gesteigerte Sicherheitserwartungen bei den Adressaten hervorzurufen.

163 Auch Zertifikate hinsichtlich des **Qualitätsmanagements wie DIN EN ISO 9000 ff.** können durchaus für sich eine deutliche Aussage auch für den Bereich der Werbung enthalten. Die Werbung mit dem Zertifikat ist relativ leicht mit der Werbung in Ein-

336 *Spindler*, Unternehmensorganisationspflichten, S. 815; vgl. *Wagner/Janzen*, BFuP 1994, 573 (596 f); insofern auch *Kassebohm/Malorny*, ZfB 1994, 693 (701 f).

klang zu bringen, dass ein hoher Qualitätsstandard bei der Softwareerstellung verfolgt wird. Unter Zugrundelegung ähnlicher Erfahrungen bzw. Kenntnis z.B. über den Automobilbereich können leicht Parallelen gezogen werden, die eine zumindest laienhafte Bewertung eines Qualitätsmanagement im Softwarebereich ermöglichen. Damit können Zertifikate **im Bereich Qualitätsmanagement** durchaus **Einfluss auf die Sicherheitserwartungen** nehmen.[337]

(ii) Anwendung auf IT-Hersteller

164 Derzeit wird man davon auszugehen müssen, dass die Sicherheitserwartung der Nutzer aufgrund von **Zertifikaten für IT-Produkte** erst dann signifikant steigen, wenn sich einzelne Prüfmethoden in einem Produktbereich durchgesetzt haben und in Nutzerkreisen einen entsprechenden Bekanntheitsgrad erreicht haben. Beispielsweise die Zertifikat-Angabe, dass ein Produkt einem gewissen Protection Profile mit einer bestimmten Vertrauenswürdigkeitsstufe genügt, kann erst dann die Sicherheitserwartungen der Nutzer maßgeblich beeinflussen, **wenn Existenz *und* Inhalt der Zertifizierung weitgehend bekannt** sind.

165 Bei den Common Criteria erfolgt eine **Zertifizierung anhand eines Protection Profile** und den entsprechenden Zertifikatsbedingungen wie z.B. besonderer Konfigurationen. Zudem kann der Hersteller auch die Vertrauenswürdigkeitsstufe des Zertifikats wählen. Der tatsächliche Inhalt eines Zertifikats ergibt sich somit aus dem Dreigespann von Profil, Bedingungen und Vertrauenswürdigkeitsstufe. Zwar können das Profil und die Stufe als objektivierter Maßstab angesehen werden, dennoch verkompliziert sich die Aussage erheblich. Nimmt man die vom Hersteller vorgegebenen Bedingungen hinzu, so lassen sich bereits bei demselben Produkt keine eindeutigen Aussagen mehr treffen. Die Aussage, ein Produkt an sich entspreche einem Profil in einer bestimmten Vertrauenswürdigkeitsstufe, könnte also nur als allgemeingültig angesehen werden, wenn das Zertifikat sich auf die Auslieferungskonfiguration beziehen würde, und Änderungen an der Konfiguration nicht auch Änderungen des Sicherheitsstandards nach sich ziehen würden. Eine sinngemäße Übertragung einer vom Nutzerkreis vorgestellten Sicherheitsstufe von einem Produkt auf ein anderes der gleichen Produktklasse wird damit erheblich erschwert. Selbst unter Annahme der Bekanntheit der Common Criteria und des Profils wäre somit eine Einordnung schwierig. Hinzu kommt die **Unbekanntheit** der Common Criteria sowie die Vielzahl der möglichen Protection Profiles.

337 Ausführlich *Spindler*, Unternehmensorganisationspflichten, S. 815 f.

166 Zur angemessenen Bewertung des Evaluierungsergebnisses muss auch der **Evaluierungsreport** berücksichtigt werden.[338] Insbesondere Prüftiefe, Prüfmethoden und –bedingungen geben erst gemeinsam eingehend Auskunft über die Qualität des Zertifikats. Der Hersteller des Produkts kann sich bzw. sein Produkt nämlich unterschiedlich strengen Evaluationen unterziehen. Das erhaltene Zertifikat sagt demnach nur unter Berücksichtigung auch des Prüfungsumfangs etwas über den eingehaltenen Standard aus. Bei Betrachtung dieser Bewertungskriterien als Grundlage für eine gesteigerte Sicherheitserwartung durch den Einsatz eines Zertifikats wird deutlich, dass der durchschnittliche Nutzer aus der bloßen Konfrontation mit einem solchen Standard **ohne weitergehende Informationen bzgl. Inhalt und Verlässlichkeit der Sicherheitsprüfung** häufig **keinerlei Rückschlüsse** ziehen kann. Der Einsatz eines Produktzertifikats im Bereich der IT-Produkte kann also in der Regel die Sicherheitserwartungen der entsprechenden Kreise nicht steigern.

167 Die Normenreihe **DIN EN ISO 9000 ff.** stellt auch im IT-Bereich ein branchenübergreifendes Qualitätssicherungsmodell dar, dessen Anwendung auf die Softwareentwicklung in DIN EN ISO 9000-3 vermittelt wird. Sowohl auf Seiten des Softwareherstellers, als auch auf Seiten des -einkäufers ist die Regelung zur unabhängigen Überprüfung der Qualitätssicherungsmaßnahmen auf große Resonanz gestoßen.[339] Dennoch sind diese Normen für die Sicherheitserwartung der Käufer und somit für die Haftung nach § 823 Abs. 1 BGB insofern nur von begrenzter Bedeutung, als dass sie praktisch nur bei Softwarekäufen zwischen Unternehmen und im Wesentlichen auch nur bei Individualsoftware herangezogen werden.[340] Nur in diesem abgesteckten Rahmen kann die Einhaltung der Sicherheitsnormen auch die Verkehrserwartung beeinflussen.

168 Zusätzlich stellen die Normen **nur Anforderungen an das Software-Produktionsverfahren**: Da Softwareprodukte aufgrund ihrer Komplexität praktisch nicht fehlerfrei zu konstruieren sind,[341] zielt das effektive Qualitätsmanagement darauf ab, die Bedingungen bzw. ein Umfeld dafür zu schaffen, möglichst hochwertige und fehlerarme Produkte zu schaffen. Inhaltlich wird jedoch im Unterschied zu Produktsi-

338 Ebenso *Fuhrberg/Häger/Wolf*, Internet-Sicherheit, Kap. 2.4.2 (S. 46).

339 *Sodtalbers*, Softwarehaftung im Internet, Rn. 274; *Thaller*, ISO 9001, S. 25; *Wilhelm*, DuD 1995, 330 (331, 335).

340 *Burgartz/Blum*, QM-Optimizing der Softwareentwicklung, S. 178; *Sodtalbers*, Softwareentwicklung im Internet, Rn. 275.

341 OLG Hamburg CR 1986, 83 (84); LG Heidelberg CR 1989, 197 (198); *Taeger*, Außervertragliche Haftung für fehlerhafte Computerprogramme, S. 37, 40 f.; MünchKommBGB-*Wagner*, § 3 ProdHaftG Rn. 15.

cherheitszertifikaten nicht die Eigenschaft und Qualität der Software selbst unter sicherheitstechnischen Aspekten überprüft, weshalb die Einhaltung der Normen nicht automatisch einen bestimmten Sicherheitsstandard der Software sichern kann.[342] Die Zertifizierung dient demnach nur der Einhaltung von Qualitätsstandards.

(7) Beweislast

(a) Produkthaftungsrechtliche Beweislastverteilung

169 Auch für IT-Produkte greifen die von der Rechtsprechung entwickelten Regeln zur Beweislastumkehr zugunsten des Geschädigten ein. Danach obliegt dem Geschädigten der Beweis der Rechtsgutsverletzung, des Produktfehlers sowie der Nachweis, dass der Produktfehler im Organisationsbereich des Herstellers entstanden ist und bereits im Zeitpunkt des Inverkehrbringens vorlag.[343] Hinsichtlich der **objektiven Verkehrspflichtverletzung** als auch des **Verschuldens** greift zugunsten des Geschädigten eine Beweislastumkehr ein,[344] wonach sich der Hersteller in Bezug auf alle seine Hilfskräfte zu entlasten hat.[345]

170 Keine Beweiserleichterung nicht aber dafür greift dagegen hinsichtlich des Umstandes, dass bei ordnungsgemäßer **Instruktion** der Schaden nicht eingetreten wäre.[346] Auch bei Verletzungen der **Produktbeobachtungspflicht** greift keine Beweislastumkehr zugunsten des Geschädigten hinsichtlich des objektiven Pflichtverstoßes ein, da hier nur allgemein zugängliche Informationen in Rede stehen, zu denen der Geschädigte notfalls durch Sachverständigengutachten ebenso Zugang wie der Hersteller hat.[347]

171 Die von der Rechtsprechung entwickelte **Befundsicherungspflicht** des Herstellers, sich vor Inverkehrgabe seiner Produkte über den Status bzw. Befund seiner Produkte und deren etwaige Fehlerhaftigkeit zu vergewissern, und der damit verbundenen Beweislastumkehr hinsichtlich des Vorliegens eines Fehlers bei Inverkehrgabe des

---

342 *Wilhelm*, DuD 1995, 330 (335); *Sodtalbers*, Softwarehaftung im Internet, Rn. 275; *Koch*, Computer-Vertragsrecht, Rn. 287.

343 Bamberger/Roth-*Spindler*, § 823 BGB Rn. 553; MünchKommBGB-*Wagner*, § 823 BGB Rn. 612.

344 Vgl. BGHZ 80, 186 (196 f.); bestätigt wiederum in BGH NJW 1996, 2507 (2508); BGH NJW 1999, 1028; *Foerste*, in: v.Westphalen, ProdHaftHdB, § 30 Rn. 46 ff.; MünchKommBGB-*Wagner*, § 823 BGB Rn. 608; Staudinger-*Hager*, § 823 BGB Rn. F 43.

345 BGH NJW 1968, 247 ff.; MünchKommBGB-*Wagner*, § 823 BGB Rn. 609.

346 Vgl. BGH DB 1999, 891 (891); OLG Frankfurt NJW-RR 1999, 27 (30).

347 Vgl. die in BGHZ 80, 186 (195 ff.); s. auch BGHZ 116, 69 (72 f.) aufgestellten Grundsätze, wonach ab Inverkehrgabe der Geschädigte die Verletzung der Pflicht zu beweisen hat; *Prütting*, in: Produktverantwortung und Risikoakzeptanz, S. 49 (52); krit. demgegenüber *Foerste*, in: v. Westphalen, ProdHaftHdb, § 30 Rn. 89; MünchKommBGB-*Wagner*, § 823 BGB Rn. 611; *Tiedtke*, in: FS Gernhuber, S. 471 (480 f.).

Produktes[348] kann nicht übertragen werden. Denn diese Pflicht beschränkt sich auf diejenigen Produkte, deren erhebliche Risiken für den Verbraucher „in der Herstellung geradezu angelegt sind und deren Beherrschung deshalb einen Schwerpunkt des Produktionsvorganges darstellt, so dass über die übliche Warenendkontrolle hinaus besondere Befunderhebungen des Herstellers erforderlich sind“[349]. Gerade daran fehlt es aber bei den stets identischen Produkten im Bereich des Softwarevertriebs.[350]

172 Die Beweislast für die **Kausalität** des Produktfehlers bzw. der Verkehrspflichtverletzung des Herstellers für die eingetretene Rechtsgutsverletzung trägt der Geschädigte.[351] Eine Beweislastumkehr greift ferner grundsätzlich **nicht** ein. Der Geschädigte muss daher beispielsweise den Einwand des Herstellers, der Schaden sei auf einen Fehlgebrauch des Produktnutzers zurückzuführen, widerlegen.[352] Doch kann im Einzelfall ein **Beweis des ersten Anscheins** in Betracht kommen, wenn es beispielsweise im Zusammenhang mit der Verwendung des betreffenden Produkts zu parallelen Schadensfällen gekommen ist (zur Nichteinhaltung technischen Normen unten Rn. 179).[353]

173 Gerade bei **IT-Produkten** ist der Nachweis der haftungsbegründenden Kausalität in der Praxis für den Geschädigten schwer zu führen, da er häufig mit dem Einwand konfrontiert wird, dass sein Schaden auf anderen Ursachen – insbesondere anderer schadhafter Software oder mangelhafter Installation – beruht. Gerade in diesem Zusammenhang kommt daher Beweiserleichterungen besondere Bedeutung zu.

(b) Beweisrechtliche Bedeutung technischer Normen

174 Die Rechtsprechung geht zunächst davon aus, dass für technische Normen eine tatsächliche Vermutung für die Wiedergabe der anerkannten Regeln der Technik eingreift (oben Rn. 147). Zumindest im Ausgangspunkt lässt sich die **Einhaltung einer technischen Norm** daher mit der Einhaltung der im Verkehr erforderlichen Sorgfalt

---

348 BGHZ 104, 323 (332 ff.); BGH NJW 1993, 528 (529); bestätigt in BGHZ 129, 353 (361 f., 365 f.); ausführlicher dazu Bamberger/Roth-*Spindler*, § 823 BGB Rn. 500 f. mwN.

349 So BGH NJW 1993, 528 (529); OLG Dresden NJW-RR 1999, 34, Rev. vom BGH nicht angenommen, Beschl. v. 26. Mai 1998 VI ZR 294/97, referiert bei *Kullmann*, NJW 1999, 96 (101); *Kullmann*, NJW 1994, 1698 (1705); Kullmann/Pfister-*Kullmann*, Kz. 1520 S. 35 f.; krit. *Rolland*, Produkthaftungsrecht Teil II Rn. 42a: kaum kalkulierbar.

350 Ausführlicher dazu *Spindler*, NJW 1999, 3737 (3741 f.).

351 BGH NJW 1989, 1542 (1545); BGH NJW 1992, 560 (562f.); MünchKommBGB-*Wagner*, § 823 BGB Rn. 614.

352 *Foerste*, in: v.Westphalen, ProdHaftHdB, § 30 Rn.95.

353 *Foerste*, in: v.Westphalen, ProdHaftHdB, § 30 Rn. 99 ff.; MünchKommBGB-*Wagner*, § 823 BGB Rn. 614; Staudinger-*Hager*, § 823 BGB Rn. F 39.

gleichsetzen, wobei überwiegend wohl von einem starken **Indiz** für die Wahrung der Sorgfalt[354], zum Teil aber auch eine tatsächliche Vermutung (Anscheinsbeweis) angenommen wird.[355] Einschränkend gilt hier jedoch, dass die Einhaltung einer technischen Norm die Gewährleistung des erforderlichen Sicherheitsstandards nur dann indiziert, wenn die technische Norm die jeweiligen Gefahren ausreichend berücksichtigt hat, also z.B. auch besonders gefährdete Verkehrskreise einbezog.[356] Hierzu ist der Zweck der betreffenden technischen Norm durch Auslegung zu ermitteln.[357] Ebenso bewahrt die Befolgung der Norm nicht vor dem Rechtswidrigkeitsvorwurf, wenn eine technische Norm nicht dem Stand der Technik entspricht, insbesondere wenn die technische Regel falsch oder unzureichend ist.[358] Begründete Zweifel an der Richtigkeit von technischen Regeln, z.B. wegen neuerer technischer Erkenntnisse, zwingen zur Aufklärung des technischen Sachverhalts durch den Pflichtigen.[359] In ähnlicher Weise verfährt die österreichische Rechtsprechung,[360] indem die normgerechte oder sonstigen technischen Standards entsprechende übliche Herstellungsart die Fehlerfreiheit des Produkts indizieren soll.

175 Zum Teil wird auch angenommen, dass die Einhaltung von technischen Standards geeignet ist, den Pflichtigen **von einem Verschulden zu entlasten**,[361] auch wenn mitunter grundsätzliche Zweifel an der Objektivität und Neutralität privater Normierungsgremien

354 Ausdrücklich OLG Celle NJW 2003, 2544; Soergel-*Krause*, Anh III § 823 BGB Rn. 16; *Foerste*, in: v. Westphalen, ProdHaftHdB, § 24 Rn 41; *Vieweg*, in: Schulte, Handbuch des Technikrechts, S. 362; *Reiff*, in: Marburger, Technische Regeln im Umwelt- und Technikrecht, S. 167.

355 So *Marburger*, Die Regeln der Technik im Recht, S. 464; *Marburger*, VersR 1983, 597 (602 f.).

356 Vgl. BGH NJW 1987, 372 – Zinkspray – für Technische Regeln für Druckgase TRG 300 vom Mai 1978; OLG Zweibrücken NJW 1977, 111 f; *Marburger*, VersR 1983, 597 (600); *Brüggemeier*, DeliktsR, Tz. 579; *Foerste*, in: v.Westphalen, ProdHaftHdb, § 24 Rn. 41; *Schmidt-Salzer*, Produkthaftung², Bd. III/1, Rn. 4.756. S. dagegen als Negativbeispiel OLG Saarbrücken VersR 1997, 377 (378 f), das DIN-Normen praktisch als eine Art gesetzliche Konkretisierung von Verkehrspflichten behandelt.

357 BGH VersR 2002, 247; BGH NJW 2001, 2019 (2020); *Reiff*, in: Marburger, Technische Regeln im Umwelt- und Technikrecht, S. 167 ff.

358 BGH NJW 1987, 372 (373); BGH NJW 1984, 801; MünchKommBGB-*Mertens*, 3. Aufl. 1997, § 823 BGB Rn. 28, der allerdings in diesem Fall zum Wegfall des Verschuldensvorwurfs tendiert.

359 BGH NJW 1982, 1049; *Köhler*, BB 1985, Beil. Nr. 4, 10 (10 f); *Marburger*, Die Regeln der Technik im Recht, S. 462 ff, 466; *Marburger*, VersR 1983, 597 (603).

360 OGH 6 Ob 73/04k; 3 Ob 547/95; 6 Ob 157/98a.

361 So für die ISO 9000 ff *Heussen/Schmidt*, CR 1995, 321 (328); *Schlutz*, PHI 1996, 122 (123, 135); *Adams/Löhr*, QZ 36 (1991), 24 (26); allgemeiner wohl auch *Marburger*, AcP 192 (1992), 1 (11); *Möllers*, Rechtsgüterschutz im Umwelt- und Haftungsrecht, S. 244; *Möllers*, DB 1996, 1455 (1460 f); *Cosack*, Umwelthaftung im faktischen GmbH-Konzern, S. 61; vorsichtiger *Ensthaler/Füßler/Nuissl*, Juristische Aspekte des Qualitätsmanagements, S. 195: ISO 9004 grundsätzlich geeignet, aber ergänzungsbedürftig; generell für die Einhaltung von technischen Regelwerken als Wahrung der erforderlichen Sorgfalt *Marburger*, VersR 1983, 597 (602 f); *v. Westphalen*, DB 1987, Beil. Nr. 11 S. 10. Gegen ein Entfallen des Verschuldensvorwurfs *Reiff*, in: Marburger, Technische Regeln im Umwelt- und Technikrecht, S. 168.

bestehen.[362] Jedenfalls hat die Rechtsprechung stets betont, dass die Haftung des Verkehrspflichtigen trotz Einhaltung einer DIN-Norm eingreifen kann, wenn die (technische) Entwicklung über sie hinweggegangen ist oder sich bei der Benutzung Gefahren zeigen, die in den DIN-Normen noch nicht berücksichtigt sind.[363] Der Pflichtige muss daher stets prüfen, ob die technische Norm in der gegebenen Situation anwendbar ist und ob sie für den konkreten Fall ausreicht, insbesondere über die technischen Regelwerke hinaus neuere Erkenntnisse berücksichtigen, vor allem wenn die betreffende Norm älteren Ursprungs ist, oder Divergenzen zwischen verschiedenen Normen bestehen.[364] Gerade wenn die technische Norm keine abschließende Erfassung sämtlicher relevanten Fragen enthält, muss der Anwender sorgfältig untersuchen, ob er weitere Maßnahmen für den konkreten Einzelfall zu treffen hat.[365]

176 Bei **Nichteinhaltung der technischen Regeln** wird zum Teil ein Anscheinsbeweis für eine Verkehrspflichtverletzung bejaht,[366] was in dieser Pauschalität indes nicht zutrifft, da technische Normen keine zwingenden Verhaltensnormen und abweichende, technisch ebenso sichere Lösungen folglich zulässig sind.[367] Der BGH bejaht im Falle der Nichteinhaltung einer technischen Norm zwar keinen Anscheinsbeweis für die Pflichtwidrigkeit, geht aber zumindest von einer starken **Indizwirkung** des Verstoßes gegen technische Normen für das Vorliegen einer Verkehrspflichtverletzung aus.[368]

---

362 Abl. daher generell zur Haftungsentlastung durch Einhaltung von DIN-Normen bzw. allgemein anerkannten Regeln der Technik *Huth*, Die Bedeutung technischer Normen, S. 210 ff.

363 BGH NJW 1994, 3349 (3350); OLG Hamm VersR 1996, 1517 (1518).

364 BGH NJW 1984, 801 (802); BGH NJW 1987, 372 (373); im Werkvertragsbereich BGH NJW 1998, 2814 (2815); *Foerste*, in: v. Westphalen, ProdHaftHdB, § 24 Rn. 42; *Schmidt-Salzer*, Produkthaftung[2], Bd. III/1, Rn. 4.754 f; *Hollmann*, DB 1985, 2389 (2395); RGRK[12-]*Steffen*, § 823 BGB Rn. 277; Kullmann/Pfister-*Kullmann*, Kz 1520 S. 13 f; *Schmatz/Nöthlichs*, Sicherheitstechnik, Bd. I Teil 1, § 3 GSG Anm. 5.3.3 zur Produkthaftung; *Falke*, Rechtliche Aspekte der Normung in den EG-Mitgliedsstaaten und der EFTA, S. 451 f.; restriktiver *Marburger*, Die Regeln der Technik im Recht, S. 467 f; *Marburger*, VersR 1983, 597 (602 f.) mwN., der eine generelle Prüfungspflicht nur für die besondere Risikolage annimmt, nicht aber hinsichtlich der Richtigkeit der Regel; dagegen *Huth*, Die Bedeutung technischer Normen, S. 208 f.

365 Vgl. *Schmidt-Salzer*, Produkthaftung[2], Bd. III/1, Rn. 4.757; *Marburger*, VersR 1983, 597 (603); *Huth*, Die Bedeutung technischer Normen, S. 219 ff.; insoweit auch *Bayer*, Auswirkungen eines zertifizierten Qualitätsmanagementsystems, S. 102, 105; übertragen auf die Arzthaftung im Hinblick auf Qualitätsmanagementsysteme *Steffen*, in: FS Deutsch, S. 799 (807 f.).

366 *Reiff*, in: Marburger, Technische Regeln im Umwelt- und Technikrecht, S. 171 mwN.

367 *Reiff*, in: Marburger, Technische Regeln im Umwelt- und Technikrecht, S. 171; *Spindler*, Unternehmensorganisationspflichten, S. 805.

368 BGH VersR 1984, 270 (271); in einer Reihe von Entscheidungen bejaht der BGH die Pflichtwidrigkeit ganz maßgeblich aufgrund des Verstoßes gegen technische Normen: BGH NJW 2004, 1449 (1450); BGH NJW 2001, 2019 (2020); BGH NJW 1991, 2019 (2021); ebenso im Ergebnis die Literatur, wonach das Unterschreiten der technischen Normen regelmäßig eine Verkehrspflichtverletzung darstellt, Soergel-*Krause*, Anh III § 823 BGB Rn. 16; *Foerste*, in: v. Westphalen, ProdHaftHdB, § 24 Rn. 39; MünchKommBGB-*Wagner*, § 823 BGB Rn. 578; Bamberger/Roth-*Spindler*, § 823 BGB Rn. 257.

177 In der Literatur wird überwiegend eine differenzierende Betrachtungsweise zugrunde gelegt. Die Nichteinhaltung einer technischen Norm ist danach regelmäßig mit der Verletzung einer Verkehrspflicht gleichzusetzen, wenn jegliche Sicherheitsmaßnahmen unterlassen werden oder das Sicherheitsniveau der technischen Norm durch die vom Verkehrspflichtigen gewählte Lösung unterschritten wird.[369] Dem Verkehrspflichtigen steht es aber jederzeit frei, das erforderliche Sicherheitsniveau durch gegenüber der technischen Norm **alternative Lösungen** zu erreichen (Rn. 145). Er trägt in diesem Fall aber die Beweislast dafür, dass die gewählte Sicherheitsleistung den Vorgaben der technischen Norm äquivalent ist.[370] Die Beweislastverschiebung zu Lasten des Herstellers für die Erreichung eines gleichwertigen Sicherheitsniveaus kam im praktischen Ergebnis einer Vermutung für eine Verkehrspflichtverletzung bei der Abweichung von technischen Regelwerken recht nahe.[371]

178 Für den Bereich der **Produkthaftung** ist bei Nichteinhaltung technischer Normen in Bezug auf den Nachweis der *Sorgfaltswidrigkeit* des Herstellerhandelns zu bedenken, dass die Darlegungs- und Beweislast für die Verletzung der äußeren und inneren Sorgfalt ohnehin beim Hersteller liegt (Rn. 169), dieser sich also vom Vorwurf der objektiven Verkehrspflichtverletzung und des Verschuldens entlasten muss. Hier wird der Hersteller in (seltenen) Einzelfällen versuchen nachzuweisen, dass die von ihm gewählte Alternativlösung gleiche oder höhere Sicherheit gegenüber der Norm bietet.[372]

179 Die Beweislast hinsichtlich der **Kausalität** des Produktfehlers bzw. der Verletzung der Herstellerpflichten obliegt im Grundsatz dem Geschädigten (Rn. 172). Steht fest, dass der Hersteller eine technische Norm verletzt hat, spricht nach BGH ein **Anscheinsbeweis** dafür, dass die Schädigung, die in örtlichem und zeitlichem Zusammenhang mit dem Verstoß eingetreten ist, durch die Pflichtverletzung verursacht wurde.[373] Der Schä-

---

369 *Reiff*, in: Marburger, Technische Regeln im Umwelt- und Technikrecht, S. 171; *Spindler*, Unternehmensorganisationspflichten, S. 805; *Foerste*, in: v. Westphalen, ProdHaftHdB, § 24 Rn. 20; *Marburger*, Die Regeln der Technik im Recht, S. 470.

370 MünchKommBGB-*Wagner*, § 823 BGB Rn. 578; *Köhler*, BB 1985 Beilage 4, S. 10 (11); *Reiff*, in: Marburger, Technische Regeln im Umwelt- und Technikrecht, S. 172; *Spindler*, Unternehmensorganisationspflichten, S. 806; *Foerste*, in: v. Westphalen, ProdHaftHdB, § 24 Rn. 20; *Marburger*, Die Regeln der Technik im Recht, S. 472.

371 *Spindler*, Unternehmensorganisationspflichten, S. 806.

372 *Vieweg*, in: Schulte, Handbuch des Technikrechts, S. 361.

373 BGH NJW 2001, 2019 (2020); BGH NJW 1991, 2021 (2022); *Reiff*, in: Marburger, Technische Regeln im Umwelt- und Technikrecht, S. 162, 172ff.; *Foerste*, in: v. Westphalen, ProdHaftHdB, § 30 Rn. 103; Bamberger/Roth-*Spindler*, § 823 BGB Rn. 280; Staudinger-*Hager*, § 823 BGB Rn. E 72; Soergel-*Krause*, Anh II § 823 BGB Rn. 74; MünchKommBGB-*Wagner*, § 823 BGB Rn. 272, 316; Palandt-*Sprau*, § 823 BGB Rn. 80; *Marburger*, Die Regeln der Technik im Recht, S. 448 ff., insb. 453 f.

diger muss den Anscheinsbeweis erschüttern, indem er darlegt und beweist, dass der Schaden auch dann eingetreten wäre, wenn er die Norm eingehalten hätte. Der BGH geht wohl zum Teil von einer Beweislastumkehr aus, wenn er davon spricht, die „Bekl. hätten daher *darzulegen und zu beweisen*, dass die Schäden nicht auf der Verletzung anerkannter Regeln der Technik beruhen".[374]

180 Zusammengefasst haben technische Standards damit eine **dreifache Wirkung**:

- Sie begründen eine Vermutung dafür, dass sie die anerkannten Regeln der Technik wiedergegeben.
- Ihre Befolgung begründet starkes Indiz (nach aA einen Anscheinsbeweis) dafür, dass der Pflichtige die im Verkehr erforderliche Sorgfalt eingehalten hat, sofern keine besonderen Gefahrenlagen vorlagen.
- Ihre Verletzung begründet ein starkes Indiz (nach aA einen Anscheinsbeweis) dafür, dass der Pflichtige die im Verkehr erforderliche Sorgfalt verletzt hat. Steht die Nichteinhaltung einer technischen Norm fest, spricht ein Anscheinsbeweis dafür, dass die Schädigung, die in örtlichem und zeitlichem Zusammenhang mit dem Verstoß eingetreten ist, durch die Pflichtverletzung verursacht wurde

(c) Beweisrechtliche Bedeutung von Zertifikaten

(i) Grundsätze

181 In diesem Rahmen ist auch die beweisrechtliche Bedeutung von erteilten Zertifikaten einzuordnen. Wie oben (Rn. 157) dargestellt, können Zertifikate den Hersteller zwar nicht pauschal von der Haftung entlasten, doch kann ihnen im Einzelfall eine beweisrechtliche Bedeutung zukommen. Auch hier ist indessen Zurückhaltung angebracht. Zudem ist – wie im österreichischen Recht – genau darauf abzustellen, wofür das Zertifikat erteilt wurde, ob für ein Herstellungsverfahren, ein Produkttyp oder für das Produkt selbst; das Zertifikat kann allenfalls für den jeweiligen Bereich eine entlastende Wirkung entfalten.[375]

182 So begründet nach der Rechtsprechung des BGH die **Betriebserlaubnis** für ein Kfz **keine Vermutung für die ordnungsgemäße Beschaffenheit des Produkts**, sondern besagt nur, dass der Kontrollbeamte nichts Vorschriftswidriges gefunden hat. Der Hersteller von Fahrzeugen oder Fahrzeugteilen, für die eine allgemeine Betriebserlaubnis erteilt ist, darf sich folglich nicht darauf verlassen, dass die Zulassungsstelle etwaige

374 BGH NJW 2001, 2019 (2020); dazu *Reiff*, in: Marburger, Technische Regeln im Umwelt- und Technikrecht, S. 173 f.

375 S. dazu die Entscheidung des OGH 10 Ob 98/02p.

Mängel entdeckt.[376] Ein Hersteller wird sich allenfalls dann auf eine behördliche Prüfung verlassen dürfen, wenn durch die gesetzlichen Genehmigungsvoraussetzungen und die personelle und technische Ausstattung der Behörde sowie deren Prüfverfahren gewährleistet ist, dass das Produkt nach den neuesten Erkenntnissen von Wissenschaft und Technik gefahrlos verwendet werden kann.[377]

183 Für eine Prüfung durch den **TÜV** und die Vergabe des **GS-Zeichens** hat der BGH entschieden, dass ein *Hersteller*, der seine Produkte selbst konstruiert, aufgrund der Prüfung nicht ohne Weiteres von seiner Haftung für konstruktive Mängel freigestellt wird.[378] In einer neueren Entscheidung geht das OLG Oldenburg davon aus, dass der Endhersteller seine Pflicht zur stichprobenartigen Materialprüfung von Zulieferprodukten im Hinblick auf die große Anzahl der zu verarbeitenden Zulieferteile durch ein eigenes Materialprüfungszertifikat, durch ein entsprechendes TÜV-Zertifikat oder durch ein aussagekräftiges Prüfzertifikat des Herstellers der Zulieferprodukte erbringen könne.[379] Umgekehrt kann die **fehlende TÜV-Zulassung** eine Beweiserleichterung für den Geschädigten (welcher den Produktfehler zu beweisen hat, s. Rn. 169) bieten, indem der Hersteller die sicherheitstechnische Ordnungsmäßigkeit des Produktes zu beweisen hat.[380]

184 Für *andere* in den Herstellungsprozess und den Vertrieb von Produkten eingeschaltete Unternehmer, die in Bezug auf Konstruktionsgefahren geringere Sorgfaltspflichten als der eigentliche Hersteller und Konstrukteur des Produktes zu erfüllen haben, können Zertifikate wie das GS-Zeichen weitergehende entlastende Wirkung entfalten.[381] So kann sich ein **Importeur** in Bezug auf seine Pflicht zu stichprobenartiger Untersuchung unter Umständen damit entlasten, dass er ein eingeführtes Gerät durch einen Sachverständigen überprüfen lässt oder es gem. § 3 Abs. 4 GSG aF (jetzt § 7 GPSG) von einer zugelassenen Prüfstelle auf ihre Sicherheit untersuchen lässt.[382] Entsprechendes gilt für den **Auftragsfertiger** im Rahmen der horizontalen Arbeitsteilung, welcher von dem

---

376 BGH NJW 1987, 1009 (1011); BGH NJW 1987, 372 (373); BGH NJW-RR 1990, 406 f.; Kullmann/Pfister-*Kullmann*, Kz. 1520, S. 5.

377 Kullmann/Pfister-*Kullmann*, Kz. 1520, S. 5; *Foerste*, in: v. Westphalen, ProdHaftHdB, § 24 Rn. 96.

378 BGH NJW-RR 1990, 406 f. unter Hinweis auf BGH NJW 1987, 1009 (1011); BGH NJW 1987, 372 (373); s. auch OLG Celle NJW 2003, 2544; MünchKommBGB-*Wagner*, § 823 BGB Rn. 578.

379 OLG Oldenburg NJW-RR 2005, 1338 (1339).

380 OLG Stuttgart bei *Schmidt-Salzer*, Entscheidungssammlung Produkthaftung, II.117 (1 f) – Schleifscheibe; *Schmidt-Salzer*, Produkthaftung, Bd. III/1, Rn. 4.887.

381 Bamberger/Roth-*Spindler*, § 823 BGB Rn. 490.

382 BGH NJW-RR 1990, 406 f.; *Foerste*, in: V.Westphalen, ProdHaftHdB, § 26 Rn. 61; Soergel-*Krause*, Anh III § 823 BGB Rn. 16.

Hersteller des Endprodukts beauftragt worden ist, bestimmte Produktteile unter Verwendung der ihm von dem Endprodukthersteller zur Verfügung gestellten Formen herzustellen.[383]

185 Die in der industriellen Praxis häufig anzutreffenden Zertifikate nach **DIN ISO 9001 ff.** können dem Hersteller nicht seinen Entlastungsbeweis abnehmen,[384] da kein Auditorenteam in den für die Qualitätszertifizierungen üblichen, kurzen Zeitspannen in der Lage sein dürfte, alle möglichen Fehlerquellen einer Betriebsorganisation zu überprüfen.[385] Der Nachweis einer lückenlosen Qualitätsregelung reicht im Bereich der Produkthaftung angesichts der erforderlichen Entlastung hinsichtlich sämtlicher Hilfspersonen,[386] durch deren individuelle Fehlleistung der Produktfehler entstanden oder unentdeckt sein kann, nicht aus.[387] Ebenso wenig darf sich derjenige, der Verkehrspflichten im Wege vertraglicher Arbeitsteilung delegiert, allein auf die Zertifizierung des Übernehmers verlassen.[388]

(ii) Anwendung auf IT-Hersteller

186 Ausgehend von den oben dargestellten Grundsätzen wird man auch Zertifikaten für **IT-Produkte** im zivilen Haftungsrecht nur eine **eingeschränkte beweisrechtliche Bedeutung** beimessen können (zur Bedeutung im öffentlichen Produktsicherheitsrecht siehe unten Rn. 253 ff.). Insbesondere kann ein Zertifikat den konstruktionsverantwortlichen Hersteller regelmäßig nicht entlasten. Bei der Herstellung von Hardwarekomponenten in horizontaler Arbeitsteilung können die oben genannten Grundsätze (Rn. 184) zum Tragen kommen.[389] Gleiches gilt für Software, die allerdings kaum typische Fabrikationsfehler aufweisen wird, da sie 1:1 vom Original kopiert wird, daher allenfalls Kopierfehler etc. eine Rolle spielen können.

187 Der Zertifizierung anhand anerkannter technischer Normen, welche die anerkannten Regeln der Technik wiedergeben, wird im Einzelfall **indizielle Bedeutung** für den

---

383 BGH NJW-RR 1990, 406 f.; *Kullmann* NJW 1991, 675 (678 f.).

384 Anders wohl *Kassebohm/Malorny*, BB 1994, 1361 (1365).

385 Zutr. *Wagner/Janzen*, BFuP 1994, 573 (596); *Kassebohm/Malorny* ZfB 1994, 693, (701,704).

386 BGH NJW 1968, 247 ff.

387 *Bayer*, Auswirkungen eines zertifizierten Qualitätsmanagementsystems, S. 97 ff.; Bamberger/Roth-*Spindler*, § 823 BGB Rn. 560; skeptisch zur Wirkung der Zertifizierung auch *Heussen/Schmidt*, CR 1995, 321 (329).

388 *Merz*, in: v.Westphalen, ProdHaftHdb, § 44 Rn. 57; ähnlich aus strafrechtlicher Sicht *Goll/Winkelbauer*, in: v.Westphalen, ProdHaftHdb, § 48 Rn. 51.

389 Die Herstellung von Software erfolgt regelmäßig nicht im Wege der Arbeitsteilung, sondern alleine durch einen Hersteller.

Nachweis der Normkonformität des Produkts zukommen. Denn wenn Ist-Standards als technische Normen und Mindeststandard eine Aussage über die allgemein anerkannten Regeln der Technik treffen, so ist unter Anwendung der allgemeinen Grundsätze zumindest von einer Indizwirkung zugunsten des Herstellers auszugehen, wenn er die Einhaltung eben dieses Standards mit einem Zertifikat belegen kann.[390] Auch hier gilt aber, dass sich die allgemein anerkannten Regeln der Technik bereits über die Festlegungen des Standards hinaus entwickelt haben können, so dass trotz Zertifikat eine Prüfung im Einzelfall erfolgen muss.

b) Produkthaftung infolge Schutzgesetzverletzung (§ 823 Abs. 2 BGB): öffentlich-rechtliche Produktsicherheitsnormen

188 Die verschuldensabhängige Produkthaftung nach § 823 Abs. 1 BGB wird durch zahlreiche Schutzgesetze flankiert, deren Verletzung nach § 823 Abs. 2 BGB eine Haftung nach sich ziehen kann. Von Bedeutung sind indes für die Produkthaftung im wesentlichen nur die öffentlich-rechtlichen Normen zur Produktsicherheit, allen voran das als Rahmengesetz für die Produktsicherheit gedachte **Geräte- und Produktsicherheitsgesetz** (GPSG),[391] daneben aber auch Spezialgesetze wie das Medizinproduktegesetz,[392] die individuellen Schutz entfalten können. Da das GPSG als Schutzgesetz nach § 823 Abs. 2 BGB zu qualifizieren[393] und Software nicht vom GSPG ausgenommen ist (näher unten Rn. 209 ff.),[394] sind entsprechende zivilrechtliche Schadensersatzansprüche grundsätzlich denkbar.[395] Ein Anspruch des Produktbenutzers besteht aufgrund des eingeschränkten Schutzbereichs des GPSG jedoch nur bei Personenschäden,[396] so dass der Anwendungsbereich des GPSG bei fehlerhaften IT-Produkten gering sein dürfte (unten Rn. 209 ff.). Bei fehlerhaften Medizinprodukten mit Softwaresteuerung (s. § 3 Nr. 1 MPG) können ggf. die Vorschriften des MPG als Schutzgesetz zur Anwendung gelangen.

---

390 Bamberger/Roth-*Spindler*, § 823 BGB Rn. 491.

391 Näher unten Rn. 206 ff.; allgemein zum GPSG *Klindt*, NJW 2004, 465 ff.; *Potinecke*, DB 2004, 55 ff.

392 *Deutsch/Spickhoff*, Medizinrecht, Rn. 1248; *Foerste*, in: v. Westphalen, ProdHaftHdb, § 32 Rn. 13; Bamberger/Roth-*Spindler*, § 823 BGB Rn. 190.

393 Zum Schutzgesetzcharakter des GPSG s. *Potinecke*, DB 2004, 55 (60); *Spindler*, NJW 2004, 3145 (3148); *Molitoris*, in: RAnwHdb, C.14 Rn. 221; *Klindt*, GPSG, § 4 GPSG Rn. 75; *Reinicke/Tiedtke*, Rn. 1024; noch zum alten ProdSG: *G. Wagner*, BB 1997, 2541 (2542); *Nickel/Kaufmann*, VersR 1998, 948 (951 f.); *v. Westphalen*, DB 1999, 1369 (1371); *Marburger*, FS Deutsch, 271 (288).

394 Zur alten Rechtslage nach dem ProdSG Kullmann/Pfister-*Kullmann*, Kz. 2705, S. 8 f.

395 Noch zur alten Rechtslage: Kullmann/Pfister-*Kullmann*, Kza 2705 S. 3, 14; *Wagner*, BB 1997, 2541 (2541 f.).

396 *Klindt*, GPSG, § 4 GPSG Rn. 8; Bamberger/Roth-*Spindler*, § 823 BGB Rn. 159.

2. Verschuldensunabhängige Produkthaftung (ProdHaftG)

189 Neben die Haftung nach Deliktsrecht (s. § 15 Abs. 2 ProdHaftG) tritt die verschuldensunabhängige Haftung nach dem ProdHaftG[397], welches der Umsetzung der EG-Produkthaftungsrichtlinie[398] dient. In seiner praktischen Bedeutung bleibt das ProdHaftG wegen seiner engeren Voraussetzungen hinter der deliktischen Haftung zurück. Das ProdHaftG kann nach § 14 ProdHaftG vertraglich nicht abbedungen werden (§ 14 ProdHaftG).

a) Produktbegriff des ProdHaftG (§ 2 ProdHaftG)

190 § 2 ProdHaftG definiert als Produkt „jede bewegliche Sache, auch wenn sie einen Teil einer anderen beweglichen Sache oder einer unbeweglichen Sache bildet sowie Elektrizität“. Als bewegliche Sache fällt **Hardware** unproblematisch unter den Produktbegriff des § 2 ProdHaftG. Gleiches gilt für alle Arten körperlicher **Datenträger** als solcher.[399] Nach wie vor ist die Frage umstritten, ob **Software** unter den Produktbegriff des ProdHaftG fällt. Rechtsprechung zu dieser Frage existiert soweit ersichtlich nicht. Teilweise wird die Produkteigenschaft von Software verneint, da es sich hierbei um keine bewegliche Sache (vgl. § 2 ProdHaftG), sondern um ein immaterielles Gut handele.[400] Das Computerprogramm als solches sei von dem körperlichen Datenträger zu unterscheiden. Das ProdHaftG finde zwar Anwendung, wenn die Gefahr von der Körperlichkeit der Sache ausgehe, nicht aber wenn sie von der Software herrühre, welche in der Sache verkörpert ist.[401]

191 Die wohl überwiegende Meinung bejaht dagegen zu Recht die Produkteigenschaft von auf einem Datenträger wie Disketten, CD-Rom, Festplatten u. ä. gespeicherter und damit **verkörperter Software**.[402] Denn die Software ist mit dem Datenträger fest

---

397 Gesetz über die Haftung für fehlerhafte Produkte (Produkthaftungsgesetz – ProdHaftG) vom 15.12.1989, BGBl. I 1989, S. 2191.

398 Richtlinie 85/374/EWG des Rates vom 25.7.1985 zur Angleichung der Rechts- und Verwaltungsvorschriften der Mitgliedsstaaten über die Haftung für fehlerhafte Produkte, ABl. EG Nr. L, S. 210.

399 *Taschner/Frietsch*, § 2 ProdHaftG Rn. 22; Staudinger-*Oechsler*, § 2 ProdHaftG Rn. 68.

400 So *Redeker*, NJW 1992, 1739 f.; *Müller-Hengstenberg*, NJW 1994, 3128 (3131); *Honsell*, JuS 1995, 211 (212); *Taschner/Frietsch*, § 2 ProdHaftG Rn. 22.

401 *Beckmann/Müller*, MMR 1999, 14 (15); *Redeker*, NJW 1992, 1739 f.; *Bauer*, PHi 1989, 98 (101).

402 *Spindler/Klöhn*, VersR 2003, 410 (412); *Spindler*, MMR 1998, 119 (120); *Mankowski*, in: Ernst, Hacker, Cracker & Computerviren, Rn. 441; *Marly*, Softwareüberlassungsverträge, Rn. 1303; *Sodtalbers*, Softwarehaftung im Internet, Rn. 161; *Koch*, Versicherbarkeit von IT-Risiken, Rn. 607; *Taeger*, Außervertragliche Haftung für fehlerhafte Computerprogramme, S. 160 ff.; *v. Westphalen*, Vertragsrecht und AGB-Klauselwerke, IT-Verträge, Rn. 92; *Taschner/Frietsch*, § 2 ProdHaftG Rn. 23; Palandt-*Sprau*, § 2 ProdHaftG Rn. 1; Erman-*Schiemann*, § 2 ProdHaftG Rn. 2; MünchKommBGB-*Wagner*, § 2 ProdHaftG

verbunden und bildet mit dieser eine bewegliche Sache. Es genügt mithin, wenn die Software auf irgendeinem Datenträger beim Benutzer gespeichert ist.[403] Diese Ansicht stimmt mit der vertragsrechtlichen Rechtsprechung des BGH zur Sacheigenschaft von Software überein[404] und trägt auch der Verkehrsauffassung Rechnung, welche den Datenträger unter Einschluss der Software als bewegliche Sache ansieht.[405] Eine Unterscheidung zwischen **Individual- und Standardsoftware** wird dabei nicht getroffen.[406] In einer Stellungnahme zu der dem ProdHaftG zugrunde liegenden EG-Produkthaftungsrichtlinie 85/374/EWG geht auch die Kommission der Europäischen Gemeinschaften davon aus, dass Software als Produkt im Sinne der Richtlinie anzusehen ist.[407]

192 Streitig ist die Produktqualität von **online übertragener Software**.[408] Denkbar wäre es, die Übertragung von Daten mittels elektromagnetischer Ströme als Unterfall des Produktes „**Elektrizität**“ einzuordnen, welche in § 2 S. 1 ProdHaftG ausdrücklich als Produkt im Sinne des ProdHaftG genannt wird.[409] Allerdings bietet die Elektrizität als einzige Ausnahme keinen Raum für die Annahme einer Regelungslücke und damit für Analogien.[410] Entscheidend ist demnach letztlich die Auslegung des Begriffs der beweglichen Sache in § 2 ProdHaftG. Nach wohl hM ist der Sachbegriff des § 90 BGB aus der Auslegung des § 2 ProdHaftG zugrunde zu legen.[411] Eine Ansicht in der Literatur verneint die Produkteigenschaft online übertragener Software daher auch unter Hin-

---

Rn. 15; Staudinger-*Oechsler*, § 2 ProdHaftG Rn. 64.

403 *Spindler/Klöhn*, VersR 2003, 410 (412); MünchKommBGB-*Wagner*, § 2 ProdHaftG Rn. 15.

404 Dazu BGH NJW 1993, 2436 (2437); BGH NJW 1990, 320 (321).

405 *Taschner/Frietsch*, § 2 ProdHaftG Rn. 23.

406 *Marly*, Softwareüberlassungsverträge, Rn. 1303; *Taeger*, Außervertragliche Haftung für fehlerhafte Computerprogramme, S. 168; *v. Westphalen*, in: v. Westphalen, ProdHaftHdb, § 73 Rn. 39; Staudinger-*Oechsler*, § 2 ProdHaftG Rn. 69; a. A. MünchKommBGB-*Wagner*, § 2 ProdHaftG Rn. 15.

407 Stellungnahme der Kommission der Europäischen Gemeinschaften auf die Schriftliche Anfrage Nr. 706/88 von Herrn Gijs de Vries an die Kommission: Produkthaftung für Computerprogramme v. 08.05.1989, ABl. EG Nr. C 114, S. 42.

408 Dafür *Spindler/Klöhn*, VersR 2003, 410 (412); *Spindler*, MMR 1998, 119 (121); *Wagner*, NJW 1996, 2899 (2904); *Taeger*, CR 1996, 257 (261 f.); *Sodtalbers*, Softwarehaftung im Internet, Rn. 164 ff.; *Koch*, Versicherbarkeit von IT-Risiken, Rn. 607; *Mankowski*, in: Ernst, Hacker, Cracker & Computerviren, Rn. 441; *v. Westphalen*, in: v. Westphalen, ProdHaftHdb, § 73 Rn. 40; MünchKommBGB-*Wagner*, § 2 ProdHaftG Rn. 16; dagegen Erman-*Schiemann*, § 2 ProdHaftG Rn. 2; Staudinger-*Oechler*, § 2 ProdHaftG Rn. 65, 69a; *Taschner/Frietsch*, § 2 ProdHaftG Rn. 22.

409 So etwa *v. Westphalen*, in: v. Westphalen, ProdHaftHdb, § 73 Rn. 40 (für online übertragene Software); *Höckelmann*, Die Produkthaftung für Verlagserzeugnisse, S. 141 ff. (für online übertragene Verlagserzeugnisse); für eine Analogie zur Elektrizität *Meyer*, ZUM 1997, 26 (28, 33).

410 *Wagner*, NJW 1996, 2899 (2900); *Spindler*, in: Spindler, Rechtsfragen bei Open Source, Kap. E Rn. 11; *Spindler*, MMR 1998, 119 (120 f.); *Taschner/Frietsch*, § 2 ProdHaftG Rn. 22; Staudinger-*Oechsler*, § 2 ProdHaftG Rn. 12, 67.

411 *Taschner/Frietsch*, § 2 ProdHaftG Rn. 17; Kullmann/Pfister-*Kullmann*, Kz. 3603 S. 1; Palandt-*Sprau*, § 2 ProdHaftG Rn. 1; Staudinger-*Oechsler*, § 2 ProdHaftG Rn. 11.

weis auf die fehlende gegenständliche Verkörperung auf einem Datenträger.[412] Diese Argumentation greift indessen zu kurz. Im Hinblick auf den verbraucherschützenden Zweck des ProdHaftG kann die Frage der Anwendbarkeit der verschuldensunabhängigen Haftung nicht davon abhängen, ob bereits die Übertragung in körperlicher Form erfolgte. Entscheidend ist vielmehr, dass zumindest beim Nutzer der Software eine dauerhafte Verkörperung durch Speicherung auf einem Datenträger erfolgt.[413] Für die Anwendbarkeit des ProdHaftG ist demnach danach zu **differenzieren**, ob die Software lediglich zeitweise während der Benutzung der Dienste des Service Providers genutzt werden kann oder ob der Nutzer sie durch Download auf seinen eigenen Rechner dauerhaft verwenden kann.[414] Ein Provider, welcher dem Kunden lediglich **vorübergehend die Nutzung einer Software ermöglicht**, ohne diese auf den Rechner herunter zu laden, unterliegt nicht der Haftung nach dem ProdHaftG, der Provider erbringt hier letztlich nichts anderes als eine Dienstleistung,[415] welche nicht in den Anwendungsbereich des Gesetzes fällt.[416] Bei **dauerhafter Verkörperung** auf dem Rechner findet die Materialisierung erst beim Kunden statt, indem die Software oder die Information auf der Festplatte oder einem anderen Medium gespeichert wird.[417] Eine Verkörperung und damit ein Produkt im Sinne des § 2 ProdHaftG liegt dann vor. Zwar hat hier erst der Kunde durch eigenen Willensentschluss die Körperlichkeit des Produktes herbeigeführt, so dass man an der Herstellung des Produktes im Organisationsbereich des Herstellers zweifeln könnte. Doch liegt das entscheidende Moment der Inverkehrgabe des Produktes „Software“ in der vom Anbieter offerierten Möglichkeit, die Software herunterzuladen.[418] Denn ab diesem Zeitpunkt kann der Kunde das Produkt jederzeit wiederbenutzen, wobei er nicht mehr auf die Netzverbindung angewiesen ist. Die Rechtslage kann hier nicht anders beurteilt werden, als wenn dem Kunden nur noch eine unwesentliche Fertigungshandlung obliegt, um das Endprodukt „herzustellen“, etwa bei zusammenschraubbaren Fertigmöbeln.

b) Rechtsgutsverletzung

412 Staudinger-*Oechsler*, § 2 ProdHaftG Rn. 11, 66.

413 *Wagner*, NJW 1996, 2899 (2900); *Spindler/Klöhn*, VersR 2003, 410 (412); *Spindler*, MMR 1998, 119 (120); *Mankowski*, in: Ernst, Hacker, Cracker & Computerviren, Rn. 441; *Taeger*, Außervertragliche Haftung für fehlerhafte Computerprogramme, S. 160 ff.; MünchKommBGB-*Wagner*, § 2 ProdHaftG Rn. 16.

414 *Spindler*, in: Spindler, Rechtsfragen bei Open Source, Kap. E Rn. 11 f.; *Spindler*, MMR 1998, 119 (121); MünchKommBGB-*Wagner*, § 2 ProdHaftG Rn. 16.

415 MünchKommBGB-*Wagner*, § 2 ProdHaftG Rn. 16.

416 Dazu *Taschner/Frietsch*, § 2 ProdHaftG Rn. 8; Staudinger-*Oechsler*, § 2 ProdHaftG Rn. 42.

417 Abl. daher *Smith/Hamill*, PHI 1988, 85.

418 MünchKommBGB-*Wagner*, § 2 ProdHaftG Rn. 16.

193 Wie auch der Anspruch aus § 823 Abs. 1 BGB beruht die Haftung nach ProdHaftG auf der Verletzung der dort aufgezählten Rechtsgüter. Der Hersteller ist demnach zum Schadensersatz verpflichtet, wenn durch einen Fehler seines Produkts ein Mensch getötet, Körper oder Gesundheit verletzt oder eine Sache beschädigt werden (§ 1 Abs. 1 Satz 1 ProdHaftG). Primäre Vermögensschäden, welche nicht an eine Rechtsgutsverletzung anknüpfen, werden nicht ersetzt. Hinsichtlich der Haftung für die Verletzung von **Leben, Körper und Gesundheit** durch fehlerhafte IT-Produkte kann auf die Ausführungen zu **Rn. 105 ff.** verwiesen werden.[419]

194 Der Begriff des **Sachschadens** entspricht nach wohl hM dem der Eigentumsverletzung bei § 823 Abs. 1 BGB (ausführlich oben **Rn. 109**).[420] Im Hinblick auf den Wortlaut des Art. 9 lit. a der EG Produkthaftungsrichtlinie wird zum Teil eine Beschränkung auf Substanzverletzungen angenommen.[421] Die abschließende Entscheidung dieser Streitfrage muss letztlich aber einer Klärung durch den EuGH vorbehalten bleiben.[422] Eine bedeutsame Einschränkung erfährt der sachliche Schutzbereich des ProdHaftG im Bereich der Sachschäden durch § 1 Abs. 1 Satz 2 ProdHaftG. Sachbeschädigungen weren jedoch nur erfasst, wenn eine **andere Sache** als das fehlerhafte Produkt beschädigt (Rn. 109 ff.) und diese anderen Sachen ihrer Art nach gewöhnlich für den **privaten Ge- und Verbrauch** bestimmt und hierzu von dem Geschädigten hauptsächlich verwendet worden sind:

(1) Andere Sache

195 Nach dem ProdHaftG ersatzfähig sind – in **Abgrenzung von der vertraglichen Gewährleistung**[423] – allein Schäden an anderen Sachen als dem fehlerhaften Produkt. Für die Abgrenzung ist die Verkehrsauffassung maßgeblich.[424] Eine „andere Sache“ im Sinne der Vorschrift liegt ohne weiteres vor, wenn eine von dem fehlerhaften Produkt **körperlich getrennte Sache** beschädigt wird. Im IT-Bereich ist dies etwa bei einer mechanischen Einwirkung auf eine andere Sache infolge fehlerhafter Steuerungssoftware im privaten Pkw denkbar (z.B. Auffahrunfall). Wird die fehlerhafte Software selbst

419 S. dazu *Taschner/Frietsch*, § 2 ProdHaftG Rn. 22.
420 Palandt-*Sprau*, § 1 ProdHaftG Rn. 5; MünchKommBGB-*Wagner*, § 823 BGB Rn. 6 f.
421 *Koch*, Versicherbarkeit von IT-Risiken, Rn. 608.
422 So zu Recht MünchKommBGB-*Wagner*, § 1 ProdHaftG Rn. 7.
423 *Larenz/Canaris*, § 84 I 1 c, S. 646; MünchKommBGB-*Wagner*, § 1 ProdHaftG Rn. 9.
424 BT-Drucks. 11/2447, S. 13; *Taschner/Frietsch*, § 1 ProdHaftG Rn. 38.

durch ihren Fehler gelöscht und damit zerstört, kann dieser Schaden nicht über das ProdHaftG liquidiert werden.[425]

196 Streitig ist im Rahmen des ProdHaftG die Behandlung von **Weiterfresserschäden** (dazu bereits Rn. 109),[426] also die Frage, inwieweit ein fehlerhaftes Teilprodukt im Verhältnis zum Endprodukt eine andere Sache sein kann. Unter Hinweis auf §§ 1 Abs. 1 Satz 2, 2 Satz 2, 4 ProdHaftG wird in der Literatur zum Teil vertreten, dass auch Schäden am Endprodukt ersatzfähig seien.[427] Andere stellen darauf ab, ob das Teilprodukt aus Sicht des Betroffenen im Markt als eigenständige Ware behandelt wird.[428] Die ganz hM lehnt eine Übertragung der Weiterfresser-Rechtsprechung zur deliktischen Produzentenhaftung auf das ProdHaftG indessen ab,[429] da das in Verkehr gebrachte Endprodukt nach der Verkehrsauffassung insgesamt das „fehlerhafte Produkt" sei.[430] Eine Haftung für Eigentumsverletzungen aufgrund von Softwarefehlern scheidet danach auf Grundlage des ProdHaftG jedenfalls dann aus, wenn die **Software in das fertige Endprodukt integriert** war. Nach überwiegender Auffassung gilt dies auch dann, wenn der Hersteller des Endprodukts nicht mit dem Hersteller der Software identisch ist.[431] Nicht nach dem ProdHaftG ersatzfähig sind danach Datenschäden durch fehlerhafte Software, wenn die Software auf einem handelsüblichen Computer vorinstalliert war. Ebenso sind Schäden am privaten Pkw des Nutzers, in den eine fehlerhafte Software (z.B. automatische Fahrabstandsregelung) eingebaut worden ist, nicht ersatzfähig.[432]

197 Anders liegt der Fall, wenn ein Teil einer Sache erst **nachträglich als Ersatz oder Zusatz mit dem Rest- oder Endprodukt verbunden** worden ist.[433] Dies dürfte beispielsweise dann gelten, wenn Software getrennt vom Rechner erworben und auf dem

---

425 *Sodtalbers*, Softwarehaftung im Internet, Rn. 317.

426 Ausführlich zum Streitstand MünchKommBGB-*Wagner*, § 1 ProdHaftG Rn. 10 ff.; Staudinger-*Oechsler*, § 1 ProdHaftG Rn. 10 ff.

427 *Taeger*, Außervertragliche Haftung für fehlerhafte Computerprogramme, S. 196 f.; *v. Westphalen*, in: v. Westphalen, ProdHaftHdb, § 72 Rn. 7 ff.

428 *Larenz/Canaris*, § 84 I 1 c, S. 646; Staudinger-*Oechsler*, § 1 ProdHaftG Rn. 20.

429 *Koch*, Versicherbarkeit von IT-Risiken, Rn. 610; *Sodtalbers*, Softwarehaftung im Internet, Rn. 324 f.; *Tiedtke*, NJW 1990, 2961 (2964); *Taschner/Frietsch*, § 1 ProdHaftG Rn. 38 ff.; Palandt-*Sprau*, § 1 ProdHaftG Rn. 6; Erman-*Schiemann*, § 1 ProdHaftG Rn. 3; MünchKommBGB-*Wagner*, § 1 ProdHaftG Rn. 14.

430 BT-Drucks. 11/2447, S. 13; *Sodtalbers*, Softwarehaftung im Internet, Rn. 323.

431 *Tiedtke*, NJW 1990, 2961 (2964); MünchKommBGB-*Wagner*, § 1 ProdHaftG Rn. 13.

432 So auch *Koch*, Versicherbarkeit von IT-Risiken, Rn. 610; *Sodtalbers*, Softwarehaftung im Internet, Rn. 324 f.

433 BT-Drucks. 11/2447, S. 13; *Taschner/Frietsch*, § 1 ProdHaftG Rn. 40; Staudinger-*Oechsler*, § 1 ProdHaftG Rn. 20a.

Rechner installiert wurde, wobei es nach Rn. 196 nicht darauf ankommt, ob die Software von einem Datenträger auf den Computer überspielt oder online übertragen wurde.

(2) Privater Gebrauch

198 Durch die Beschränkung des Schutzbereichs auf die Beschädigung privat genutzter Sachen, fällt die Beschädigung **gewerblich**, **beruflich** und **freiberuflich** genutzter Sachen insgesamt **nicht** in den Schutzbereich der verschuldensunabhängigen Produkthaftung.[434] Dies beruht zum einen auf der Erwägung, dass im unternehmerischen Bereich besonders hohe Vermögensfolgeschäden drohen, zum anderen ist einem Unternehmen eher als einem Privaten ein Abschluss einer Versicherung gegen derartige Schäden zumutbar.[435]

c) Verursachung durch einen Fehler des Produkts

199 Ein Produkt ist gemäß §3 ProdHaftG fehlerbehaftet, wenn es nicht die Sicherheit bietet, die unter Berücksichtigung aller Umstände, insbesondere seiner Darbietung, des Gebrauchs, mit dem billigerweise gerechnet werden kann und des Zeitpunktes, in dem es in den Verkehr gebracht wurde, berechtigterweise erwartet werden kann. Die Kriterien zur Bestimmung der Fehlerhaftigkeit von IT-Produkten entsprechen insoweit den zur deliktischen Produzentenhaftung gemachten Ausführungen,[436] so dass insoweit auf Rn. 105 ff. verwiesen wird.

d) Haftungsausschlussgründe

200 Die Haftung nach dem ProdHaftG ist ausgeschlossen, wenn einer der Ausschlussgründe des § 1 Abs. 2 ProdHaftG erfüllt ist. Die Beweislast hierfür trägt der Hersteller (§ 1 Abs. 4 Satz 2 ProdHaftG). Hinsichtlich der Herstellung und des Vertriebs von Software kann der Haftungsausschlussgrund des **§ 1 Abs. 2 Nr. 3 ProdHaftG** Bedeutung erlangen, soweit die Software „weder für den Verkauf oder Vertrieb mit wirtschaftlichem Zweck hergestellt noch im Rahmen einer beruflichen Tätigkeit hergestellt oder vertrieben“ wird. Bei unentgeltlicher Überlassung von Software scheidet eine verschuldensunabhängige Haftung folglich von vornherein aus. Dies betrifft zum einen **Freeware** und frei zugängliche **Open Source Software**, welche von Programmieren in ihrer Freizeit

---

434 *Hoeren*, in: v. Westphalen, Vertragsrecht und AGB-Klauselwerke, IT-Verträge, Rn. 95; *Taschner/Frietsch*, § 2 ProdHaftG Rn. 33; *Larenz/Canaris*, § 84 I 1 c, S. 647; *Koch*, Versicherbarkeit von IT-Risiken, Rn. 609.

435 *Larenz/Canaris*, § 84 I 1 c, S. 647.

436 Dazu auch *Koch*, Versicherbarkeit von IT-Risiken, Rn. 614, 637; Palandt-*Sprau*, § 3 ProdHaftG Rn. 2 ff.; MünchKommBGB-*Wagner*, § 3 ProdHaftG Rn. 29.

erstellt und im Internet zum kostenlosen Download bereitgestellt wird.[437] Dagegen findet das ProdHaftG auf **Shareware** Anwendung, da damit zumindest mittelbar ein wirtschaftlicher Zweck verfolgt wird.[438] Gemäß § 1 II Nr. 5 ProdHaftG wird nach dem Produkthaftungsgesetz zudem nicht für Fehler gehaftet, die nach dem Stand von Wissenschaft und Technik vom Hersteller nicht erkannt werden konnten, als der das Produkt in Verkehr brachte (**Entwicklungsfehler**).[439] Demgemäß kann bei objektiv bei Inverkehrgabe nicht erkennbaren Programmierungsfehlern keine Haftung eingreifen, so dass angesichts der wohl nicht zu erreichenden Fehlerlosigkeit bei Software von vornherein eine Reihe von Softwarefehlern nicht zur Haftung führen. Anders als nach Deliktsrecht besteht nach dem ProdHaftG damit auch keine verschuldensunabhängige Einstandspflicht für Fehler bei der Produktbeobachtung.[440]

e) Beweislast

201 Für die verschuldensunabhängige Produkthaftung gilt, dass sie lediglich dem Geschädigten den Nachweis der Pflichtwidrigkeit des Herstellers abnimmt, indem die Schadensersatzpflicht allein schon beim Vorliegen eines fehlerhaften Produktes, das kausal für die Rechtsgutsverletzung geworden ist, abnimmt. Dem Geschädigten obliegt aber nach wie vor die Darlegungs- und Beweislast dafür, dass das Produkt fehlerhaft war und genau dieser Fehler für die Rechtsgutsverletzung verantwortlich war (Kausalität).[441] Damit treten aber genau dieselben Probleme wie im Bereich der verschuldensabhängigen Produkthaftung auf, insbesondere hinsichtlich des Kausalitätsnachweises. Hinzuweisen ist in diesem Rahmen auf die für das österreichische Recht vertretene Auffassung, dass der Hersteller nur darlegen muss, dass das Produkt zur Zeit, zu der es in Verkehr gebracht worden war, wahrscheinlich noch nicht den schadenskausalen Fehler hatte.[442] Dieser erleichterte Beweis soll grundsätzlich mit den getroffenen Feststellungen erbracht sein, dass das Produkt dem Stand der Technik entspricht und etwa das technische Prüfzeichen einer für die Prüfung anerkannten Anstalt aufweist.[443] Dies soll auch

---

437 *Koch*, Versicherbarkeit von IT-Risiken, Rn. 611; *Marly*, Softwareüberlassungsverträge, Rn. 1306; *Spindler*, in: Spindler, Rechtsfragen bei Open Source, Kap. E Rn. 15.

438 *Koch*, Versicherbarkeit von IT-Risiken, Rn. 611; *v. Westphalen*, in: v. Westphalen, ProdHaftHdb, § 72 Rn. 56.

439 *Marly*, Softwareüberlassungsverträge, Rn. 1306.

440 *Marly*, Softwareüberlassungsverträge, Rn. 1310; Palandt-*Sprau*, § 3 ProdHaftG Rn. 12; MünchKommBGB-*Wagner*, § 3 ProdHaftG Rn. 36, § 1 ProdHaftG Rn. 61.

441 Palandt-*Sprau*, § 1 ProdHaftG Rn. 9, 25; MünchKommBGB-*Wagner*, § 1 ProdHaftG Rn. 76 ff.; Bamberger/Roth-*Spindler*, § 823 Rn. 552; ferner OLG Düsseldorf NJW-RR 1997, 1344 (1345).

442 OGH 6 Ob 157/98a.

443 Dabei handelte es sich um den Zeichengenehmigungsausweis der VDE-Prüfstelle (Verband Deutscher

den Verweis auf die Einhaltung relevanter Normen und Standards (ISO, ÖNORM etc.) umfassen.

f) Rechtsfolgen

202 Der Umfang des zu ersetzenden Schadens richtet sich im Ausgangspunkt nach den §§ 249 ff. BGB. Zu ersetzen sind hierbei entgegen einer in der Literatur vertretenen Meinung auch **Sachfolgeschäden**.[444] Hierbei bestehen gegenüber dem Deliktsrecht jedoch zwei wichtige Einschränkungen. Bei Sachbeschädigungen (also auch Datenschäden[445]) hat der Geschädigte einen **Selbstbehalt** von € 500 selbst zu tragen (11 ProdHaftG). Allgemein beschränkt § 10 Abs. 1 ProdHaftG die Haftung auf einen **Höchstbetrag** von 85 Millionen €. Im Einzelfall kommt eine Kürzung des Schadensersatzanspruchs wegen Mitverschuldens des Geschädigten in Betracht (§§ 6 ProdHaftG, 254 BGB) (siehe dazu oben zur deliktischen Produzentenhaftung Rn.188).

3. Zusammenfassung

203 Eine **verschuldensabhängige** Produkthaftung aufgrund des § 823 Abs. 1 BGB kommt im IT-Bereich in Betracht, soweit ein geschütztes Rechtsgut verletzt wird. Besondere Schwierigkeiten bereitet hierbei noch immer die nicht abschließend geklärte Einordnung von Datenschäden als Eigentumsverletzung. Ebenso von Unsicherheit geprägt ist die Abgrenzung primärer Vermögensschäden von einer die Eigentumsverletzung begründenden Beeinträchtigung der bestimmungsgemäßen Verwendung des Produkts. Im Bereich der Pflichten liegt der Schwerpunkt auf der Abgrenzung von Entwicklungs- zu Konstruktionsfehlern: vor allem die zum Zeitpunkt der Inverkehrgabe nicht bekannten Gefahrenpotentiale aufgrund zukünftiger Entwicklungen führen nicht zu einer Haftung der IT-Hersteller, wohl aber Sicherheitslücken, die zu diesem Zeitpunkt erkennbar gewesen wären. Technische Standards wie die Common Criteria und Protection Profiles können hier zur Konkretisierung herangezogen werden, wenngleich sie nur ein Mindestmaß der zu erwartenden Sicherheit darstellen, über die im Einzelfall hinaus zivilrechtlich höhere Anforderungen gestellt werden können, wenn dem Hersteller entsprechende Gefahrenszenarien bekannt sein können. Schließlich kann das Deliktsrecht auch nicht über Rückrufpflichten dazu herangezogen werden, um Pflichten zur nachträgli-

---

Elektrotechniker) für einen Elektroofen.

444 *Koch*, Versicherbarkeit von IT-Risiken, Rn. 627; *Taschner/Frietsch*, § 1 ProdHaftG Rn. 42; *v.Westphalen*, in: v. Westphalen, ProdHaftHdb, § 71 Rn. 28 ff.; MünchKommBGB-*Wagner*, § 1 ProdHaftG Rn. 3 f.

445 *Marly*, Softwareüberlassungsverträge, Rn. 1307.

chen Verbesserung der Software zu begründen („Patches“) – denn hier ist oftmals das Äquivalenzinteresse berührt, das gerade nicht vom Deliktsrecht erfasst wird.

204 Im Bereich der **verschuldensunabhängigen** Produkthaftung ist die Einordnung von Software als Produkt noch immer von Unsicherheiten gekennzeichnet. Die Reichweite der Haftung wird stark eingeschränkt, indem allein Sachschäden an anderen Sachen als dem fehlerhaften Produkt ersatzfähig sind, und auch dann nur, wenn es sich um privat genutzte Sachen handelt; Schäden an gewerblich genutzten Sachen scheiden demnach von vornherein aus. Damit wird der Bereich der verschuldensunabhängigen Produkthaftung erheblich eingeschränkt, da zahlreiche Produkthaftungsfälle sich im B2B-Sektor abspielen.

205 Schließlich ist beiden Bereichen gemein, dass für die Frage der Kausalität keine Beweislastumkehr eingreift, in der Regel auch nicht für das Vorliegen eines Fehlers der Software bei Inverkehrgabe.

IV. Öffentlich-rechtliche Produktsicherheit, insbesondere das GPSG

206 Die zivilrechtliche Regulierung der Produktsicherheit wurde schon seit langer Zeit öffentlich-rechtlich flankiert durch allgemeine und sektorspezifische Normen zur Produktsicherheit. Die bisher im Gerätesicherheitsgesetz (GSG)[446] und im Produktsicherheitsgesetz (ProdSG)[447] nebeneinander geregelten sicherheitsrechtlichen Anforderungen an Produkte wurden mit Inkrafttreten des neuen Geräte und Produktsicherheitsgesetz (GPSG)[448] am 1.5.2004 in einem einheitlichen Gesetz zusammengefasst. Das GPSG dient zugleich der Umsetzung der Richtlinie 2001/95/EG des Europäischen Parlaments und des Rates vom 3.12.2001 über die allgemeine Produktsicherheit.[449] Neben dieser allgemeinen Produktsicherheitsregelung bestehen nach wie vor sektorspezifische Produktsicherheitsnormen, wie etwa das Medizinproduktegesetz (MPG)[450], die hier nicht näher thematisiert werden können. Zahlreiche dieser Produktsicherheitsnormen gehen zurück auf europarechtliche Vorgaben zur weiteren Integration des Binnenmark-

446 Gesetz über technische Arbeitsmittel (Gerätesicherheitsgesetz - GSG) vom 14.6.1968, BGBl. I, S. 717.

447 Gesetz zur Regelung der Sicherheitsanforderungen an Produkte und zum Schutz der CE-Kennzeichnung (Produktsicherheitsgesetz – ProdSG) vom 22.4.1997, BGBl. I, S. 934.

448 Gesetz über technische Arbeitsmittel und Verbraucherprodukte (Geräte- und Produktsicherheitsgesetz – GPSG) vom 6.1.2004, BGBl. I, S. 2, ber. S. 219.

449 ABl. EG Nr. L 11, S. 4 ff.

450 Gesetz über Medizinprodukte (Medizinproduktegesetz – MPG) vom 7.8.2002, BGBl. I, S. 2304.

tes, die insbesondere den sog. New Approach (dazu unten Rn. 1.c)(1)(b)) umgesetzt haben, um zu einer möglichst flexiblen und aktuellen Harmonisierung im Produktsicherheitsbereich zu gelangen.

207 **Ziel des GPSG** ist es, Schutz vor unsicheren Produkten hinsichtlich des Verbraucher- und Arbeitnehmerschutzes zu gewährleisten und den freien Wahrenverkehr mit sicheren Produkten sicherzustellen.[451] Das GPSG soll insbesondere das gemeinsame „Dach" für alle Verbraucherprodukte im Sinne der Produktsicherheitsrichtlinie bilden und als Auffanggesetz für sonstige Produkte fungieren, für die es keine Spezialnormierung gibt.

1. Anwendungsbereich und Anforderungsprofil des GPSG

208 Gem. § 1 Abs. 1 S. 1 GPSG gilt das Gesetz für das „Inverkehrbringen und Ausstellen von Produkten, das selbständig im Rahmen einer wirtschaftlichen Unternehmung erfolgt." Die private Weitergabe eines Produkts wird folglich nicht vom GPSG erfasst. Das Gesetz statuiert in §§ 4 und 5 GPSG besondere Pflichten beim Inverkehrbringen von Produkten für Hersteller, Importeure, Händler und vom Gesetz gleichgestellte Personen und regelt zusätzlich nachgelagerte Pflichten zum Produktrückruf und zur Beobachtung.

a) Produktbegriff

209 Gefahren die aus der Benutzung **fehlerhafter Hard- und Software** herrühren, könnten prinzipiell vom Schutzumfang des GPSG erfasst sein. Allerdings müsste das GPSG hierzu überhaupt auf Hard- und Software Anwendung finden: Während die Voraussetzung des „Herstellens" und des anschließenden Vertriebs von Hard- und Software im Rahmen einer wirtschaftlichen Unternehmung[452] in aller Regel erfüllt sein werden und insofern das Merkmal des Inverkehrbringens i.S.v. § 2 Abs. 8 GPSG vorliegt, ist fraglich, ob es sich bei Hard- und Software um Produkte im Sinne des GPSG handelt.

(1) Grundsätze

210 Weder die Produktsicherheitsrichtlinie noch das GPSG selbst enthalten eine Definition des Produktbegriffes.[453] Beide Regelungen setzen den Begriff des Produkts vielmehr voraus und grenzen ihren Anwendungsbereich auf bestimmte Produktarten ein (Art. 2 Richtlinie 2001/95/EG, § 2 GPSG). Der vom GPSG verwendete Produktbegriff umfasst

451 *Runte/Potinecke*, CR 2004, 725; *Wilrich*, Einleitung Rn. 1 ff.; *Littbarski*, VersR 2005, 448 f.
452 Für Open Source Software kann dies indes fraglich sein.
453 *Klindt*, GPSG, § 2 GPSG Rn. 3.

gemäß der in § 2 Abs. 1 GPSG enthaltenen Begriffsbestimmung technische Arbeitsmittel und Verbraucherprodukte.

211 Nach der in § 2 Abs. 2 GPSG enthaltenen Legaldefinition sind **technische Arbeitsmittel** verwendungsfertige Arbeitseinrichtungen, die bestimmungsgemäß ausschließlich bei der Arbeit verwendet werden, sowie deren Zubehörteile. Da insofern auf die Verwendung zu geschäftsmäßigen Zwecken abgestellt wird, fallen Produkte, die von Verbrauchern in Anlehnung an § 13 BGB weder zur gewerblichen noch zur selbständigen beruflichen Tätigkeit genutzt werden, aus dem Definitionsbereich der technischen Arbeitsmittel heraus.[454]

212 **Verbraucherprodukte** sind demgegenüber gem. § 2 Abs. 3 GPSG „Gebrauchsgegenstände und sonstige Produkte, die für Verbraucher bestimmt sind oder unter vernünftigerweise vorhersehbaren Bedingungen von Verbrauchern benutzt werden können, selbst wenn sie nicht für diesen bestimmt sind". Insbesondere sind also neben solchen Produkten, die bestimmungsgemäß innerhalb einer Lieferkette an private Endverbraucher abgegeben werden, auch sog. **Migrationsprodukte** in den Anwendungsbereich des GPSG mit einbezogen, also solche, die ursprünglich nicht für Verbraucher bestimmt waren, die jedoch in vorhersehbarer Weise von Verbrauchern benutzt werden.

213 Inwieweit IT-Produkte in den Anwendungsbereich des GPSG fallen, ist weithin ungeklärt. Unter Berücksichtigung der Beschränkung des Anwendungsbereichs des GPSG auf technische Arbeitsmittel und Verbraucherprodukte ist hierbei zwischen Hardware und Software zu unterscheiden.

(2) Hardware

214 Hardware-Teile (z.B. Computer, Laptops, Monitore, Drucker, Keyboards und anderes Zubehör) fallen als körperliche Gegenstände unproblematisch unter den Produktbegriff des GPSG.[455] Da auch Migrationsprodukte, also Gebrauchsgegenstände, die nicht zwingend für Verbraucher bestimmt sind, aber deren Verwendung durch Verbraucher vernünftigerweise erwartet werden kann,[456] unter den Begriff der Verbraucherprodukte zu subsumieren sind, ist unbeachtlich, wenn die Hardware auch am Arbeitsplatz Verwendung findet. Handelsübliche Hardware wird daher regelmäßig ein Verbraucherpro-

454 *Geiß/Doll*, B § 2 GPSG Rn. 12; *Zscherpe/Lutz*, K&R 2005, 499; *Runte/Potinecke*, CR 2004, 725 (726).

455 *Runte/Potinecke*, CR 2004, 725; *Hoeren/Ernstschneider*, MMR 2004, 507; *Zscherpe/Lutz*, K&R 2005, 499 (500); *Wilrich*, § 2 Rn. 4; *Klindt*, GPSG, § 2 GPSG Rn. 13.

456 *Hoeren/Ernstschneider*, MMR 2004, 507.

dukt im Sinne von §§ 2 Abs. 3, 5 GPSG und nicht technisches Arbeitsmittel nach § 2 Abs. 2 GPSG sein.[457] Als technische Arbeitsmittel können im IT-Bereich vor allem computergestützte Steuerungseinrichtungen für Fertigungsprozesse eingestuft werden.[458] Denn diese entsprechen den in der Vorgängerregelung des § 2 Abs. 1 GSG als Arbeitseinrichtungen beispielhaft aufgezählten Werkzeugen, Arbeitsgeräten, usw. Ob auch nicht handelsübliche Hardware, wie etwa bestimmte Arten von Servern oder Hochleistungsrechnern, die bestimmungsgemäß ausschließlich im geschäftlichen Bereich eingesetzt werden, technische Arbeitseinrichtungen sind,[459] ist angesichts der genannten Beispiele zumindest zweifelhaft, soweit von diesen Geräten keine Gefahren aufgrund mechanischer Einwirkung auf Arbeitnehmer oder Dritte ausgehen.[460]

(3) Software

215 Probleme bereitet dagegen die Einordnung von Software als lediglich geistiger Leistung, da für den Produktbegriff – ähnlich wie im ProdHaftG (Rn. 190 ff.) – in der Regel auf die Verkörperung abgestellt wird.[461] Das Abstellen auf die Verkörperung bei technischen Arbeitsmitteln legte im alten Gerätesicherheitsgesetz bereits der Titel „Geräte“ nahe.[462] Die Beispiele im neuen GPSG in der Legaldefinition von technischen Arbeitsmittel in § 2 Abs. 1 GPSG, die sich wiederum ausschließlich auf Geräte beziehen, legen es nahe, auch weiter auf die Verkörperung abzustellen. Ähnliches gilt für den Begriff des Verbraucherprodukts. Dieser kann laut der Gesetzesbegründung alles sein, was aus einem Herstellungsprozess hervorgeht, von technischen Gegenständen bis hin zu Stoffen.[463] Dadurch wird deutlich, dass auch hier die Körperlichkeit klar im Vordergrund steht. Wenn die geistige Leistung daher auf einem Speichermedium verkörpert ist, ist zumindest der Datenträger ein vom GPSG erfasstes Produkt.[464] Darüber hinaus ist allerdings fraglich, ob das geistige Werk selbst – und nicht nur der Datenträger an sich – erfasst wird. Im Unterschied zum **MPG**, in dessen § 3 Nr. 1 MPG ausdrücklich auch Software in den Anwendungsbereich einbezogen wird, enthält das GPSG keine ausdrückliche Regelung. Im Umkehrschluss ließe sich behaupten, dass körperlich nicht fi-

457 *Zscherpe/Lutz*, K&R 2005, 499 (500); *Hoeren/Ernstschneider*, MMR 2004, 507 f.
458 *Hoeren/Ernstschneider*, MMR 2004, 507 (508).
459 So *Zscherpe/Lutz*, K&R 2005, 499 (500).
460 Dazu *Hoeren/Ernstscheider*, MMR 2004, 507.
461 S. Rn 190 ff.; *Klindt*, GPSG, § 2 GPSG Rn. 13; *Wilrich*, § 2 GPSG Rn. 4; *Runte/Potinecke*, CR 2004, 725; ferner *Hoeren/Ernstschneider*, MMR 2004, 508.
462 S. *Runte/Potinecke*, CR 2004, 726.
463 BT-Drucks. 15/1620, S. 26.
464 *Hoeren/Ernstschneider*, MMR 2004, 507 (508); *Wilrich*, § 2 Rn. 10.

xierte Software nicht vom Geräte- und Produktsicherheitsgesetz erfasst sein soll.[465] Allerdings kann diese Argumentation kaum überzeugen, da aus der Formulierung in § 3 Nr. 1 MPG, nach der Medizinprodukte als „alle einzeln oder verbunden verwendeten Instrumente […] einschließlich der für ein einwandfreies Funktionieren des Medizinproduktes eingesetzten Software“ definiert werden, lediglich ersichtlich ist, dass Software kein „Instrument“ ist.

216 Die Einordnung von Software unter das GPSG bedarf insofern einer differenzierteren Betrachtung, bei der zwischen sogenannter „embedded Software“, also solcher, die in ein Endprodukt integriert ist und Steuerungsfunktionen erfüllt, und solcher, die selbständig zu nutzen ist, unterschieden werden muss

(a) Im Endprodukt integrierte Software

217 Soweit die in ein Endprodukt integrierte Steuerungssoftware betroffen ist, nimmt diese als Teil eines ganzen Produkts an der Produkteigenschaft desselben teil.[466] Insofern lässt sich hinsichtlich der **Steuerungssoftware** die Produkteigenschaft bejahen, sofern das Gesamtprodukt entweder technisches Arbeitsmittel oder Verbraucherprodukt im Sinne des GPSG ist. Im Bereich der Verbraucherprodukte wird hierbei in Zukunft wohl der Automobilsektor verstärkt eine Rolle spielen, wenn Steuerungsaufgaben mehr und mehr auf den Computer übertragen werden (z.B. ABS, ESP, automatische Fahrabstandsregelung) und bei Fehlfunktionen Personen (Verwender, Dritte) geschädigt werden können. Gleiches ist im häuslichen Bereich denkbar, wenn Geräte in zunehmendem Maß durch Software gesteuert werden („Vernetztes Haus“).

(b) Selbständige Software

218 Schwieriger ist hingegen die Beurteilung der übrigen **„selbständigen“ Software**. Die Literatur geht in Anlehnung an die zum Produktbegriff des § 2 ProdHaftG entwickelten Grundsätze (dazu oben Rn. 190 ff.) zum Teil davon aus, dass Software zumindest dann in den Anwendungsbereich des GPSG fällt, wenn sie auf einem Datenträger gespeichert und somit verkörpert ist.[467] Mangels Definition des Produktbegriffs in der Richtlinie und dem GPSG hat sich die Auslegung des Gesetzes an Sinn und Zweck dieser Normen zu orientieren. Ohne Rücksicht auf die engere Definition des Sachbegriffs in § 90 BGB

---

465 Hinsichtlich Art. 1 Abs. 2 lit. a) Medizinproduktrichtlinie: *Schieble*, Produktsicherheitsgesetz und europäisches Gemeinschaftsrecht, S. 124.

466 *Runte/Potinecke*, CR 2004, 725 (726); *Zscherpe/Lutz*, K&R 2005, 499 (500).

467 *Hoeren/Ernstschneider*, MMR 2004, 507 (508); *Zscherpe/Lutz*, K&R 2005, 499 (500); offen lassend *Wilrich*, § 2 GPSG Rn. 10.

ist folglich entscheidend auf das Ziel der Produktsicherheitsrichtlinie, Verbraucher und Arbeitnehmer vor Gesundheitsschäden durch unsichere Konsumgüter zu schützen, abzustellen. Soweit Software also „gefährlich" sein kann, wird man sie somit als Produkt im Sinne der Produktsicherheitsrichtlinie und des GPSG einordnen müssen, denn der Hersteller von Software kann grundsätzlich ein vergleichbar hohes Gefährdungspotential schaffen, wie der Hersteller anderer Produkte.[468] Dies gilt auch für online übertragene Software.[469] Unerheblich ist auch, ob es sich um Standard- oder Individualsoftware handelt.[470]

219 Während es inzwischen wohl der vorherrschenden (zutreffenden) Auffassung entsprechen dürfte, dass selbständige Software jedenfalls für **Verbraucher** als Produkt im Sinne des GPSG zu qualifizieren ist,[471] ist fraglich, inwieweit von ihr eine vom GPSG erfasste Gefährdungslage für geschützte Rechtsgüter ausgeht (s. Rn. 221 ff.).

220 Zweifelhaft ist die Rechtslage für den Bereich der **technischen Arbeitsmittel**. § 2 Abs. 2 GPSG definiert Arbeitsmittel als „verwendungsfertige Arbeits*einrichtungen*" und deren „*Teile*", „Zubehör*teile*" sowie „Schutzausrüstung". Der Wortlaut legt somit eine Beschränkung der technischen Arbeitsmittel auf körperliche Gegenstände nahe. Dies wird auch durch die Vorgängerregelung des § 2 Abs. 1 GSG bestätigt, welcher als Beispiele für Arbeitseinrichtungen Werkzeuge, Arbeitsgeräte, Arbeits- und Kraftmaschinen, Hebe- und Fördereinrichtungen sowie Beförderungsmittel nennt. Der Wortlaut des 1968 erlassenen GSG (früher: „Maschinenschutzgesetz") orientiert sich indessen weithin an den Gefährdungslagen der industriellen Arbeitswelt und berücksichtigt die Entwicklungen der Computertechnologie und ihren Einfluss auf die Arbeit nicht. Soweit der Einsatz selbständiger Software Sicherheit und Gesundheit von Menschen gefährden kann (Rn. 221 ff.), käme nach Sinn und Zweck des GPSG daher grundsätzlich zumindest eine analoge Anwendung der Bestimmungen über technische Arbeitsmittel in Betracht.

b) Persönlicher und sachlicher Schutzbereich

221 Schutzziel des GPSG ist – neben dem Schutz des Wettbewerbs durch Gewährleistung des Handels mit sicheren Produkten – der Arbeitsschutz und der Schutz der Verbraucher. Der Kreis der vom GPSG geschützten Produktverwender ist danach auf

468 *Runte/Potinecke*, CR 2004, 725 (727); *Zscherpe/Lutz*, K&R 2005, 499 (500).
469 *Klindt*, GPSG, § 2 GPSG Rn. 13.
470 *Zscherpe/Lutz*, K&R 2005, 499 (500); *Klindt*, GPSG, § 2 GPSG Rn. 13.
471 *Zscherpe/Lutz*, K&R 2005, 499 (500); *Hoeren/Ernstschneider*, MMR 2004, 507; zum GPSG *Klindt*, GPSG, § 2 GPSG Rn. 12 f..

Verbraucher und Arbeitnehmer, die an oder mit technischen Arbeitsmitteln arbeiten, beschränkt.[472] In persönlicher Hinsicht schützt das Gesetz neben dem Produktverwender jedoch auch jeden Dritten (Bystander), der mit den Produkten in Berührung kommt, oder in ihren Gefahrenbereich gelangt, ohne sie selbst zu nutzen (vgl. § 4 Abs. 1, 2 GPSG).[473]

222 Es bezweckt jedoch nur den Schutz vor Gefährdungen der Sicherheit und Gesundheit von Verwendern und Dritten (vgl. § 4 GPSG). **Eigentums- und Vermögensschäden** sind daher grundsätzlich **nicht** vom Schutzumfang des GPSG erfasst.[474] In der Literatur wird zwar vereinzelt vertreten, der Begriff „Sicherheit" (vgl. § 4 Abs. 1, 2 GPSG) sei nicht auf die Sicherheit von Leib und Leben beschränkt, sondern umfasse auch den Schutz des Eigentums und damit beispielsweise die unberechtigte Löschung von Daten.[475] Sicherheit bezieht sich nach § 4 Abs. 1, 2 GPSG jedoch auf die Sicherheit der Verwender und Dritter und damit auf deren persönliche Integrität.[476] Das Begriffspaar „Gesundheit und Sicherheit" ist insoweit nicht anders auszulegen, als die gleichlautende Formulierung in der Vorgängerregelung des § 6 Abs. 1 Satz 1 ProdSG[477]; im gleichen Sinne hatte auch der BGH zum alten § 3 GSG entschieden.[478] Entsprechend ist der Begriff „Gefahr" in der nur für Verbraucherprodukte geltenden Vorschrift des § 5 GPSG auszulegen (vgl. § 5 Abs. 2 GPSG). Allerdings kann der Schutzbereich im europäisch-harmonisierten Bereich auf Grundlage von § 3 Abs. 1 GPSG per Rechtsverordnung auf weitere Rechtsgüter erstreckt werden.[479] Im nicht harmonisierten Bereich ist der Schutzumfang hingegen auf die Abwehr von Personenschäden beschränkt. Das Gesetz bezweckt demnach nicht die Sicherung der Qualität von Produkten allgemein.[480]

223 Damit ergeben sich **im Hinblick auf IT-Produkte bereits wesentliche Einschränkungen**, da in der Mehrzahl der Schadensfälle Eigentum und Vermögen betroffen sein werden, Personenschäden dagegen eher die Ausnahme bilden – wenngleich durch Soft-

472 *Wilrich*, Einleitung Rn. 2, 4.
473 *Wilrich*, Einleitung Rn. 5.
474 *Wilrich*, Einleitung Rn. 6.
475 *Runte/Potinecke*, CR 2004, 725 (728). Zur Frage der Eigentumsverletzung bei unberechtigter Löschung von Daten siehe Rn. 110 ff.
476 *Wilrich*, Einleitung Rn. 6; ebenso zu § 6 ProdSG: *Klindt*, GPSG, § 4 GPSG Rn. 8.
477 MünchKommBGB-*Wagner*, § 823 BGB Rn. 619; *Wagner*, BB 1997, 2541 (2542); *Klindt*, GPSG, § 6 ProdSG Rn. 5; *Foerste*, in: v. Westphalen, ProdHaftHdB, § 90 Rn. 26, § 91 Rn. 6; Kullmann/Pfister-*Kullmann*, Kz. 2705, S. 8f.
478 BGH NJW 2006, 1589 (1590); BGH NJW 1983, 812 (813) – Hebebühne; MünchKommBGB-*Wagner*, § 823 BGB Rn. 618; *Peine*, § 3 Rn. 158.
479 Hierzu: *Wilrich*, Einleitung Rn. 6, § 3 Rn. 3.
480 *Wilrich*, Einleitung Rn. 9; noch zum GSG: *Peine*, § 3 Rn. 79.

ware verursachte Personenschäden grundsätzlich denkbar sind (s. Rn. 107). Insbesondere der praktisch relevante Bereich der Gefährdung des Eigentums- oder Vermögens (beispielsweise infolge der Vernichtung von Daten oder des Ausfalls von IT-Systemen) von Unternehmen fällt jedoch von vorn herein aus dem Schutzbereich des GPSG heraus. Personenschäden durch Software dürften vor allem im Bereich der Arbeit vorkommen, wenn als **technische Arbeitsmittel** einzuordnende Maschinen aufgrund von Softwarefehlern oder (bei Vernetzung) Sicherheitslücken Arbeitnehmer oder Dritte schädigen. Bei **embedded Software** dürften in Zukunft jedoch auch bei als Verbraucherprodukt einzuordnender Software zunehmend Gefahren für die Sicherheit und Gesundheit von Personen denkbar sein.

224 Beim gegenwärtigen Stand der technischen Entwicklung dürften Gefahren für die Sicherheit und Gesundheit der Produktverwender oder Dritter aufgrund von **selbständiger Software** insbesondere im Verbraucherbereich im Regelfall ausscheiden. Die von Verbrauchern verwendete (selbständige) Software dient größtenteils administrativen (Beispiel: Textverarbeitung, Tabellenkalkulation usw.) oder Unverhaltungszwecken (z.B. Computerspiele), ohne dass mit ihrer Anwendung unmittelbare Einwirkungen auf die reale Welt verbunden wären. Produktfehler werden in diesem Bereich somit kaum jemals in Personenschäden resultieren.

c) Anforderungen an die Produktsicherheit (§ 4 GPSG)

225 Gem. § 4 GPSG dürfen Produkte nur in Verkehr gebracht und ausgestellt werden, soweit sie den Anforderungen an die Produktsicherheit genügen. Hinsichtlich der Anforderungen ist zu unterschieden zwischen Produkten, welche europäischen Vorgaben entsprechen müssen („harmonisierter Bereich“, dazu (1)) und solchen, die lediglich nationalen Anforderungen unterliegen (dazu (2)).

(1) Harmonisierter Bereich (§ 4 Abs. 1 GPSG)

226 § 4 Abs. 1 GPSG bezieht sich auf Produkte, welche einer Rechtsverordnung nach § 3 Abs. 1 GPSG unterfallen und damit einen Teil des europäischen Harmonisierungskonzeptes im Bereich der Produktsicherheit, des sogenannten **New Approach** (Neues Konzept)[481], darstellen.

(a) Rechtsverordnungen nach § 3 Abs. 1 GPSG

481 Ausführlich zum New Approach *Klindt*, EuZW 2002, 133 ff.

227 Die in den Harmonisierungsrichtlinien festgelegten europäischen Anforderungen an Produkte werden durch die nach § 3 Abs. 1 GPSG zu erlassenen Rechtsverordnungen in deutsches Recht umgesetzt. Das GPSG dient derzeit der Umsetzung von nicht weniger als 14 Richtlinien des sog. **New Approach** der Europäischen Kommission.[482] Bei den Richtlinien können die Kategorien sektoral und vertikal unterschieden werden.[483] **Sektorale Richtlinien** enthalten produktbezogene Vorgaben, also Anforderungen an bestimmte Produktgruppen.[484] Demgegenüber sind **vertikale Richtlinien** gefahrbezogen und stellen einheitliche, sektoral übergreifende Anforderungen an Produkte.[485]

228 Für den **IT-Bereich** sind hier insbesondere

- die Erste Verordnung zum Geräte- und Produktsicherheitsgesetz (Verordnung über das In-Verkehr-Bringen elektrischer Betriebsmittel zur Verwendung innerhalb bestimmter Spannungsgrenzen)[486],
- die Zweite Verordnung zum Geräte und Produktsicherheitsgesetz (Verordnung über die Sicherheit von Spielzeug)[487] und
- die neunte Verordnung zum Geräte- und Produktsicherheitsgesetz (Maschinenverordnung)[488]

von Bedeutung. Der Vollständigkeit halber sei aufgrund der offenkundigen Relevanz der Regelwerke für IT-Produkte auch das Gesetz über Medizinprodukte[489] und das Gesetz über die elektromagnetische Verträglichkeit von Geräten[490] erwähnt.

229 Während § 8 Abs. 1 MPG eine eigenständige Vermutungsregel statuiert, ist fraglich, ob das **EMVG** an der in § 4 Abs. 1 GPSG festgesetzten Privilegierung teilhaben kann. Zwar stellt das Gesetz keine Rechtsverordnung nach § 3 Abs. 1 GPSG dar, so dass es gemäß dem Wortlaut von § 4 Abs. 1 GPSG nicht dessen Anwendungsbereich unterliegt. Allerdings setzt das EMVG die EG-Richtlinie 89/336/EWG zur Angleichung der Rechtsvorschriften der Mitgliedstaaten über die elektromagnetische Verträglichkeit in

---

482 *Wilrich*, Einl. Rn. 44.

483 Eingehend *Wilrich*, Einl. Rn. 44 ff.

484 Abgedeckt sind derzeit: einfache Druckbehälter, Spielzeug, Bauprodukte, Maschinen, persönliche Schutzausrüstung, nicht selbsttätige Waagen, aktive implantierbare medizinische Geräte, Gasverbrauchseinrichtungen, Warmwasserheizkessel, Explosivstoffe für zivile Zwecke, Medizinprodukte, Sportboote, Aufzüge, elektrische Haushaltskühl- und Gefriergeräte, Druckgeräte, In-vitro-Diagnostika sowie Telekommunikationseinrichtungen und Satellitenfunkanlagen.

485 Dazu gehören derzeit die Niederspannungsrichtlinie, die Richtlinie zur elektromagnetischen Verträglichkeit und die Richtlinie bezüglich Geräten und Schutzsystemen in explosionsgefährdeten Bereichen.

486 BGBl. I 1979, 629, zuletzt geändert durch Art. 10 des Gesetzes vom 6.1.2004, BGBl. I, 2, 219.

487 BGBl. I 1989, 2541, zuletzt geändert durch Art. 11 des Gesetzes vom 6.1.2004, BGBl. I, 2.

488 BGBl. I 1993, 704, zuletzt geändert durch Art. 14 der Verordnung vom 23.12.2004, BGBl. I, 3758.

489 BGBl. I 1994, 1963, neugefasst durch Bekanntmachung vom 7.8.2002, BGBl. I, 3146, zuletzt geändert durch Art. 109 der Verordnung vom 25.11.2003, BGBl. I, 2304.

490 BGBl. I 1998, 2882, zuletzt geändert durch Art. 3 Abs. 5 des Gesetzes vom 7.7.2005, BGBl. I 1970.

nationales Recht um, so dass hiermit folglich ebenfalls europäisch harmonisiertes Recht vorliegt und unter Berücksichtigung von Sinn und Zweck der Privilegierung Produkte, die in den Anwendungsbereich des EMVG fallen, entsprechend § 4 Abs. 1 GPSG zu beurteilen sind.[491]

230 Indes ist festzuhalten, dass bislang außerhalb von bestimmten Wirtschaftsbereichen **keine speziellen Produktsicherheitsrichtlinien und Verordnungen für den IT-Bereich** gelten. Insbesondere für die Softwareherstellung existieren keine europarechtlich harmonisierten Anforderungen. Demgemäß können insoweit auch keine Vermutungswirkungen im Zusammenhang mit der Einhaltung technischer Regelwerke eingreifen, da hierfür die rechtliche Grundlage bislang fehlt.

(b) Konformitätsvermutung

231 Produkte, welche in den harmonisierten Bereich fallen, dürfen gemäß § 4 Abs. 1 GPSG nur in Verkehr gebracht werden, wenn sie den in den Rechtsverordnungen nach § 3 Abs. 1 GPSG (= GPSGV) vorgesehenen Anforderungen an Sicherheit und Gesundheit und sonstigen Voraussetzungen für ihr Inverkehrbringen entsprechen und Sicherheit und Gesundheit der Verwender oder Dritter oder sonstige aufgeführte Rechtsgüter bei bestimmungsgemäßer Verwendung oder vorhersehbarer Fehlanwendung nicht gefährdet werden.

232 Bei einem entsprechend einer harmonisierten Norm hergestellten Produkt wird (widerleglich) **vermutet**, dass es den betreffenden Anforderungen an Sicherheit und Gesundheit genügt (§ 4 Abs. 1 Satz 2 GPSG). **Harmonisierte Normen** in diesem Sinne sind gemäß § 2 Abs. 16 GPSG nicht verbindliche technische Spezifikation, die (1) von einer europäischen Normenorganisation nach den in der Richtlinie 98/34/EG des Europäischen Parlaments und des Rates vom 22.6.1998 über ein Informationsverfahren auf dem Gebiet der Normen und technischen Vorschriften[492] festgelegten Verfahren angenommen und (2) deren Fundstelle im Amtsblatt der Europäischen Gemeinschaften veröffentlicht wurde.

233 Die Einhaltung der harmonisierten technischen Normen ist für den Hersteller **freiwillig**; er ist an sie nicht gebunden und kann das von der EU-Richtlinie geforderte Sicherheitsniveau auf einem anderen technischen Weg erreichen. Die Vermutungswirkung bildet

---

491 Zustimmend *Hoeren/Ernstschneider*, MMR 2004, 507 (509).

492 ABl. EG Nr. L 204 S. 37.

jedoch einen **Anreiz** zur Einhaltung der technischen Normen.[493] Entscheidet sich der Hersteller nicht nach den Vorgaben einer harmonisierten Norm zu produzieren, trägt er die Beweislast dafür, dass sein Produkt den Vorgaben der einschlägigen Richtlinie entspricht.[494] Diese Kombination von Freiwilligkeit und positiver Vermutungswirkung kann auch als „sanfter Zwang" zur normgerechten Produktion bezeichnet werden.[495]

(2) Nichtharmonisierter Bereich (§ 4 Abs. 2 GPSG)

234 Außerhalb des durch vertikale und sektorale Richtlinien harmonisierten Bereichs (oben (1)), wenn somit keine Rechtsverordnung nach § 3 Abs. 1 GPSG vorliegt, richtet sich die Zulässigkeit der Inverkehrgabe nach § 4 Abs. 2 GPSG.

(a) Pflichten der IT-Hersteller

235 Nach § 4 Abs. 2 Satz 1 GPSG müssen Produkte so beschaffen sein, dass bei ordnungsgemäßer Verwendung oder vorhersehbarer Fehlanwendung Sicherheit und Gesundheit von Verwendern oder Dritten nicht gefährdet werden. Diese allgemeinen Sicherheitsanforderungen werden in § 4 Abs. 2 Satz 2 Nr. 1 bis 4 GPSG (siehe auch Art. 2 lit. b, 3 Abs. 3 Produktsicherheitsrichtlinie 2001/95/EG) näher konkretisiert. § 4 Abs. 2 Satz 3 GPSG betont ausdrücklich, dass bei der Beurteilung der Produktsicherheit Normen und andere technische Spezifikationen zugrunde gelegt werden können.

236 Bei der Bestimmung der Pflichten der IT-Hersteller nach dem GPSG ist zu berücksichtigen, dass die Herstellerpflichten – und daran anschließend die Befugnisse der zuständigen Behörde – grundsätzlich an eine **Gefahr für die Sicherheit und Gesundheit der Produktverwender und Dritter** anknüpfen (§ 4 GPSG). Sie bleiben daher wegen der Ausklammerung von Eigentums- und Vermögensschäden zwangsläufig hinter den zivilrechtlichen Pflichten aus § 823 Abs. 1 BGB (dazu ausführlich oben Rn.119 ff.) zurück, welche auch den Schutz des Eigentums und des Rechts am eingerichteten und ausgeübten Gewerbebetrieb (Recht am Unternehmen) umfassen.[496] Gegenüber einem IT-Hersteller können nach GPSG folglich nur dann behördliche Anordnungen ergehen, wenn dies zur Vermeidung von Personenschäden erforderlich ist.

493 *Wilrich*, § 4 GPSG Rn. 28.
494 *Wilrich*, Einleitung Rn. 39.
495 *Spindler*, Unternehmensorganisationspflichten, S. 159.
496 Dies wird zu wenig berücksichtigt von *Runte/Potinecke*, CR 2004, 725 (728), die beispielsweise auch Informationspflichten zur Datensicherung aus dem GPSG ableiten (die Autoren fassen jedoch – anders als die wohl überwiegende Meinung – unter den Begriff der Sicherheit auch Eigentums- und damit Datenschäden).

237 Aus dem GPSG ergeben sich hinsichtlich der Pflichten der Hersteller von Hardware keine wesentlichen Unterschiede gegenüber den Herstellern anderer technischer Geräte. Sie trifft daher insbesondere die Pflicht, dem Produkt eine Gebrauchsanleitung in deutscher Sprache beizufügen (für den nicht harmonisierten Bereich § 4 Abs. 4 Nr. 2 GPSG).[497] Die Anforderungen an den Schutz der persönlichen Integrität der Verwender und Dritter bilden hierbei – wie in anderem Zusammenhang (oben Rn. 146) bereits ausgeführt – den öffentlich-rechtlich geforderten Mindeststandard ohne die zivilrechtlichen Verkehrspflichten abschließend mitzubestimmen. Besondere Bedeutung aus dem Anforderungskatalog des § 4 Abs. 2 Satz 2 GPSG für die Herstellerpflichten dürfte im Bereich der IT-Hersteller (Hard- und Software) die Einwirkung des Produkts auf andere Produkte, deren Verwendung zu erwarten war (Nr. 2), haben. Insbesondere Softwarehersteller haben daher ggf. etwaige Kompatibilitätsprobleme mit anderen Programmen zu berücksichtigen.

(b) „Nationaler New Approach“

238 In § 4 Abs. 2 Satz 4 GPSG vollzieht der deutsche Gesetzgeber die europäische Konzeption für den nicht harmonisierten Bereich als eine Art **„nationalen New Approach“**[498] nach. Auch im nicht harmonisierten Bereich gilt somit eine Freiwilligkeit der Produktion nach technischen Normen. § 4 Abs. 2 Satz 3 GPSG formuliert lediglich, dass bei der Beurteilung der Produktsicherheit Normen und andere technische Spezifikationen zugrunde gelegt werden können. Aber auch hier gilt die aus dem New Approach stammende Vermutungswirkung zugunsten normkonform hergestellter Produkte. Nationales Gegenstück der europäischen harmonisierten Norm ist hier eine Norm oder sonstige technische Spezifikation, die (1) vom Ausschuss für technische Arbeitsmittel und Verbraucherprodukte (§ 13 GPSG) ermittelt **und** (2) von der beauftragten Stelle[499] im Bundesanzeiger bekannt gemacht wurde (§ 4 Abs. 2 Satz 4 GPSG). Anders als im europäischen Recht wird indes die Normsetzung nicht an private Normungsgremien wie das DIN oder die CEN delegiert, sondern in dem besagten gesetzlich geregelten Ausschuss vorgenommen.

d) Besondere Pflichten bei Verbraucherprodukten (§ 5 GPSG)

497 *Hoeren/Ernstschneider*, MMR 2004, 507 (510).
498 *Klindt*, NJW 2004, 465 (466).
499 Bundesanstalt für Arbeitsmedizin und Arbeitsschutz, siehe § 2 Abs. 14 und § 12 GPSG.

239 Soweit Hard- und Software als Verbraucherprodukt im Sinne von § 2 Abs. 3 GPSG einzuordnen sind, treffen den Hersteller die besonderen Pflichten nach § 5 GPSG. Der Hersteller ist daher insbesondere verpflichtet, über von dem Produkt ausgehende Gefahren zu informieren (§ 5 Abs. 1 Nr.1a GPSG), seinen Namen und seiner Adresse auf dem Produkt anzubringen (§ 5 Abs. 1 Nr. 1b GPSG) und Vorkehrungen zu treffen, damit er imstande ist, zur Vermeidung von Gefahren geeignete Maßnahmen zu veranlassen, bis hin zur Rücknahme des Verbraucherprodukts, der angemessenen und wirksamen Warnung und dem Rückruf (§ 5 Abs. 1 Nr.1c GPSG). Gehen von den in Verkehr gebrachten Produkten Gefahren für die Gesundheit und die Sicherheit von Personen aus, hat der Hersteller unverzüglich die zuständige Behörde zu informieren (§ 5 Abs. 2 GPSG).

240 Die genannten Pflichten sind ohne weiteres auf die Hersteller von Hardware anwendbar. Ihre **Übertragung auf Software stößt dagegen auf Schwierigkeiten**. Beispielsweise ist die Informationspflicht nach Nr.1a wohl nur schwer auf Software zu übertragen, denn Software weist an sich keine gefährliche Beschaffenheit auf, sondern wird erst infolge eines Programmierfehlers oder nachträglicher Einflussnahme zu einer Gefahr. Die Identifikation des Herstellers (Nr.1b) kann bei online übertragener Software nur durch einen Hinweis im Programm selbst erfolgen.[500] Ein Rückruf von Software erscheint dagegen kaum denkbar. Im Regelfall werden bei erkannten Sicherheitsrisiken unter Verhältnismäßigkeitsgesichtspunkten eine Warnung der Verwender und die Zurverfügungstellung eines Updates ausreichen.[501]

2. Normungsverfahren nach dem GPSG

241 Die Vermutungswirkung zugunsten normkonformer Produkte gilt freilich nur für die Konformität mit solchen Normen, die den Anforderungen des GPSG an Normgeber und Verfahren entsprechen. Auch hier wird zwischen harmonisiertem und nicht harmonisiertem Bereich unterschieden.

a) Verfahren im harmonisierter Bereich

242 Gem. § 2 Abs. 16 GPSG gilt die Vermutungswirkung für solche Normen, die von einer **europäischen Normenorganisation** nach dem Verfahren der Richtlinie 98/34/EG (über ein Informationsverfahren auf dem Gebiet der Normen und technischen Vorschriften)[502] angenommen und im Amtsblatt der Europäischen Gemeinschaften veröffentlicht wor-

500 *Runte/Potinecke*, CR 2004, 725 (729).
501 *Runte/Potinecke*, CR 2004, 725 (729).
502 Richtlinie 98/34/EG des Europäischen Parlaments und des Rates vom 22.06.1998, ABl. Nr. L 204, S. 37.

den sind. In concreto handelt es sich bei den Normenorganisationen gemäß Anhang I der Richtlinie 98/34/EG um das CEN (Europäische Komitee für Normung), das CENELEC (Europäisches Komitee für Elektrotechnische Normung) sowie das ETSI (Europäisches Institut für Telekommunikationsstandards). Auch die nationalen Normungsgremien, die in Anhang II der Richtlinie 98/34/EG aufgelistet sind, sind nach Maßgabe von Art. 2, 3 RiLi 98/34/EG in den Normierungsprozess eingebunden. Deutsche Normungsgremien sind gegenwärtig das Deutsche Institut für Normung e.V. (DIN) und die Deutsche Elektrotechnische Kommission im DIN und VDE (DKE). Allerdings kann die Kommission gem. Art. 2 Abs. 4 der Richtlinie 98/34/EG auf Grundlage der Mitteilung eines Mitgliedstaates den Anhang II ändern und gegebenenfalls den Kreis der involvierten nationalen Normungsgremien erweitern.

243 Beschließt ein nationales Normungsgremium die Aufnahme einer neuen Norm in das Normungsprogramm, so hat es die europäischen und nationalen Normungsgremien sowie die Kommission davon zu unterrichten, Art. 2 Abs. 1 Richtlinie 98/34/EG. Über diese nationalen Normungsaktivitäten berät ein ständiger Ausschuss, der aus von den Mitgliedsstaaten ernannten Vertretern besteht, in Zusammenarbeit mit Vertretern der europäischen und nationalen Normungsgremien, Art. 5, 6 Abs. 1 RiLi 98/34/EG. Soweit der Ausschuss dies für sinnvoll erachtet, regt er bei der Kommission die Erarbeitung einer europäischen Norm durch ein europäisches Normungsgremium an, Art. 6 Abs. 3 Richtlinie 98/34/EG.

b) Verfahren im nicht harmonisierten Bereich

244 Im nicht harmonisierten Bereich kommt die Vermutungswirkung gem. § 4 Abs. 2 S. 4 GPSG solchen Normen zu, die vom Ausschuss für technische Arbeitsmittel und Verbraucherprodukte ermittelt und von einer beauftragten Stelle im Bundesanzeiger bekannt gemacht worden sind.

245 Dem **Ausschuss für technische Arbeitsmittel und Verbraucherprodukte (AtAV)** obliegt gemäß § 13 Abs. 2 Nr. 2 die Ermittlung von Normen mit Vermutungswirkung im Sinne des § 4 Abs. 2 Satz 4 GPSG. Er ist beim Bundesministerium für Wirtschaft und Arbeit (BMWA) angesiedelt,[503] § 13 Abs. 1 GPSG. Dem Ausschuss gehören „sachverständige Personen aus dem Kreis der zuständigen Behörden für Sicherheit und Gesundheit des Bundes und der Länder, der zugelassenen Stellen (§ 2 Abs. 15 GPSG), der Träger der

[503] Laut Gesetz ist dieses zuständig. Allerdings existiert das BMWA durch eine Umstrukturierung nicht mehr. Zuständige Behörde ist nunmehr das Bundesministerium für Arbeit und Soziales (BMAS).

gesetzlichen Unfallversicherung, des Deutschen Instituts für Normung e.V., der Kommission Arbeitsschutz und Normung, der Arbeitgebervereinigungen, der Gewerkschaften und der beteiligten Verbände an", insbesondere Hersteller und Verbraucher wären nur dann berechtigt, Vertreter in den Ausschuss an das BSI als für Sicherheit zuständige Bundesoberbehörde zu entsenden, wenn Fragen der Sicherheit und Gesundheit in seine Zuständigkeit fielen (s. § 3 BSIG).

246 Während der alte Ausschuss für technische Arbeitsmittel (AtA) ein reines Beratungsgremium war, ist seit der Einführung des GPSG zum einen die Zuständigkeit für Verbraucherschutz hinzugekommen, zum anderen ist er nunmehr ein **echter Regelungsausschuss**,[504] wobei sich seine Funktion jedoch in der Ermittlung von Normen und Spezifikationen erschöpft und nicht auch die Aufstellung von Normen umfasst.[505] Grund dafür ist die im Zuge des *nationalen* New Approach eingeführte Vermutungswirkung in § 4 Abs. 2 GPSG.[506]

247 Die Bundesanstalt für Arbeitsmedizin und Arbeitsschutz ist als **beauftragte Stelle** im Rahmen des Normungsverfahrens lediglich für die Bekanntmachung im Bundesanzeiger zuständig. Auch dies ist Voraussetzung für das Eingreifen der Vermutungswirkung. An der Ermittlung der Normen hat sie jedoch keinen Anteil.

3. Zertifizierung

a) CE-Kennzeichen

248 Durch die **CE-Kennzeichnung**[507] (Abkürzung für „Communautés Européenes") erklärt der **Hersteller bzw. Importeur selbst**, dass das Produkt entsprechend der Bestimmungen der auf ihn anwendbaren EU-Richtlinien hergestellt wurde und somit im Europäischen Binnenmarkt in Verkehr gebracht werden darf.[508] Die CE-Kennzeichnung ist obligatorisch, sofern das Produkt einer Richtlinie unterfällt, die eine CE-Kennzeichnung

504 Amtl. Begründung GPSG, BT-Drucks. 15/1620, S. 33 f.

505 *Klindt*, § 13 GPSG Rn. 5.

506 *Wilrich*, § 13 GPSG Rn. 4.

507 Richtlinie 93/68/EWG des Rates vom 22. Juli 1993 zur Änderung der Richtlinien 87/404/EWG (einfache Druckbehälter), 88/378/EWG (Sicherheit von Spielzeug), 89/106/EWG (Bauprodukte), 89/336/EWG (elektromagnetische Verträglichkeit), 89/392/EWG (Maschinen), 89/686/EWG (persönliche Schutzausrüstungen), 90/384/EWG (nichtselbsttätige Waagen), 90/385/EWG (aktive implantierbare medizinische Geräte), 90/396/EWG (Gasverbrauchseinrichtungen), 91/263/EWG (Telekommunikationsendeinrichtungen), 92/42/EWG (mit flüssigen oder gasförmigen Brennstoffen beschickte neue Warmwasserheizkessel) und 73/23/EWG (elektrische Betriebsmittel zur Verwendung innerhalb bestimmter Spannungsgrenzen), ABl. L 220 vom 30.8.1993, S. 1–22 und *Europäische Kommission*, Leitfaden für die Umsetzung der nach dem neuen Konzept und dem Gesamtkonzept verfassten Richtlinien, abrufbar unter: http://ec.europa.eu/enterprise/newapproach/legislation/guide/document/guidepublicde.pdf.

508 *Wilrich*, § 6 GPSG Rn. 5.

vorschreibt. Es handelt sich dabei indes um kein Zeichen der Qualität oder der Sicherheit des Produkts,[509] sondern allein um eine Kennzeichnung zur Erleichterung des freien Warenverkehrs in der EU und dem EWR (europäischer **„Reisepass" für Produkte**).[510] Die Marktüberwachungsbehören können bei mit dem CE-Kennzeichen versehenen Produkten von der Einhaltung der wesentlichen Sicherheitsanforderungen der EU-Richtlinien ausgehen und müssen Maßnahmen gegen die betreffenden Produkte grundsätzlich unterlassen.[511]

249 Voraussetzung für die CE-Kennzeichnung ist, dass der Hersteller vor dem ersten Inverkehrbringen ein **Konformitätsbewertungsverfahren** nach dem EU-Modulsystem[512] durchführt, an dessen Ende die EG-Konformitätserklärung des Herstellers steht, dass er die grundlegenden Gesundheits- und Sicherheitsanforderungen der betreffenden EU-Richtlinien erfüllt. Welche Module im Einzelnen zur Anwendung kommen, legen die Richtlinien unter Berücksichtigung des Gefahrenpotentials des Produkts fest, wobei grundsätzlich zwischen Herstellererklärung, Prüfung durch eine benannte Stelle und dem Erfordernis eines zertifizierten Qualitätssicherungssystems[513] unterschieden werden kann.[514] Zuständig für die **Akkreditierung** der benannten Stellen sind in Deutschland die Zentralstelle der Länder für Sicherheitstechnik (ZLS)[515] und die Zentralstelle der Länder für Gesundheitsschutz bei Arzneimitteln und Medizinprodukten (ZLG)[516].

b) GS-Zeichen

250 Das **GS-Zeichen** hat seine gesetzliche Grundlage in § 7 GPSG (vormals § 3 Abs. 4 GSG). Es handelt sich um ein rein nationales Zeichen, welches die hohen deutschen Sicherheitsstandards kenntlich machen soll.[517] Das GS-Zeichen steht für „geprüfte Si-

---

509 *Niebling*, DB 1996, 80 (81); *Niebling*, Die CE-Kennzeichnung, S. 23 f.; *Foerste*, in: v. Westphalen, ProdHaftHdb, § 24 Rn. 94; Bamberger/Roth-*Spindler* § 823 BGB Rn. 490.

510 *Wilrich*, § 6 GPSG Rn. 7.

511 *Finke*, Die Auswirkungen der europäischen technischen Normen und des Sicherheitsrechts auf das nationale Haftungsrecht, S. 89; *Wilrich*, § 4 GPSG Rn. 26.

512 93/465/EWG: Beschluss des Rates vom 22. Juli 1993 über die in den technischen Harmonisierungsrichtlinien zu verwendenden Module für die verschiedenen Phasen der Konformitätsbewertungsverfahren und die Regeln für die Anbringung und Verwendung der CE- Konformitätskennzeichnung, ABl. EG Nr. L 220 vom 30.8.1993 S. 23 (Modulbeschluss).

513 Entspricht ein Qualitätssicherungssystem den Organsationsnormen EN 29000ff. (= ISO 9000ff.), wird vermutet, dass die Anforderungen an ein ordnungsgemäßes Qualitätssicherungssystem erfüllt sind, siehe Modulbeschluss 93/465/EWG (Fn. 512) Modul D, 3.3; Modul E, 3.3.

514 *Kaufmann*, DB 1994, 1033 (1034); *Roßnagel*, DVBl 1996, 1181 (1183); *Finke*, Die Auswirkungen der europäischen technischen Normen und des Sicherheitsrechts auf das nationale Haftungsrecht, S. 90, 206.

515 Siehe http://www.zls-muenchen.de/.

516 Siehe http://www.zlg.de/.

517 *Klindt*, § 7 GPSG Rn. 1.

cherheit“ und wird auf Antrag des Herstellers durch eine von der Zentralstelle der Länder für Sicherheitstechnik (ZLS) **anerkannte GS-Stelle**[518] (§ 11 GPSG) für technische Arbeitsmittel und verwendungsfertige Gebrauchsgegenstände vergeben.

251 Voraussetzung der Zertifizierung ist der Nachweis der Übereinstimmung des geprüften Produkts mit den Anforderungen des GPSG sowie anderer Rechtsvorschriften hinsichtlich der Gewährleistung von Sicherheit und Gesundheit durch eine Baumusterprüfung, sowie der Nachweis, dass die Voraussetzungen eingehalten werden, die bei der Herstellung der technischen Arbeitsmittel und verwendungsfertigen Gebrauchsgegenstände zu beachten sind, um ihre Übereinstimmung mit dem geprüften Baumuster zu gewährleisten (§ 7 Abs. 1 GPSG). In regelmäßigen Abständen führt die Zertifizierungsstelle zudem Fertigungskontrollen durch, wobei überprüft wird, ob das Produkt noch dem geprüften Baumuster entspricht (§ 7 Abs. 2 GPSG).

4. Anordnungsbefugnisse der Marktüberwachungsbehörden

a) Verwaltungsrechtliche Befugnisse

252 Die nach Landesrecht zuständigen Marktüberwachungsbehörden (s. § 8 Abs. 1 Satz 1 GPSG) haben das Inverkehrbringen von Produkten sowie in Verkehr gebrachte Produkte aufgrund eines Überwachungskonzeptes zu überwachen (§ 8 Abs. 2 GPSG). Hat die Behörde den begründeten Verdacht, dass ein Produkt nicht den Anforderungen nach § 4 GPSG entspricht, ist sie gehalten, die erforderlichen Maßnahmen zu treffen (§ 8 Abs. 4 GPSG. Die Behörde kann nach GPSG insbesondere:

- Maßnahmen anzuordnen, die gewährleisten, dass ein Produkt erst in den Verkehr gebracht wird, wenn es den Anforderungen nach § 4 Abs. 1 und 2 entspricht,
- anzuordnen, dass ein Produkt von einer zugelassenen Stelle oder einer in gleicher Weise geeigneten Stelle überprüft wird,
- anzuordnen, dass geeignete, klare und leicht verständliche Warnhinweise über Gefährdungen, die von dem Produkt ausgehen, angebracht werden,
- das Inverkehrbringen eines Produkts für den zur Prüfung zwingend erforderlichen Zeitraum vorübergehend zu verbieten,

518 Z.B. TÜV, VDE. Siehe die Liste der zugelassenen Stellen unter http://www.zls-muenchen.de/.

- zu verbieten, dass ein Produkt, das nicht den Anforderungen nach § 4 Abs. 1 und 2 entspricht, in den Verkehr gebracht wird,
- die Rücknahme oder den Rückruf eines in Verkehr gebrachten Produkts, das nicht den Anforderungen nach § 4 GPSG entspricht, anzuordnen, ein solches Produkt sicherzustellen und, soweit eine Gefahr für den Verwender oder Dritten auf andere Weise nicht zu beseitigen ist, seine unschädliche Beseitigung zu veranlassen,
- anzuordnen, dass alle, die einer von einem in Verkehr gebrachten Produkt ausgehenden Gefahr ausgesetzt sein können, rechtzeitig in geeigneter Form, insbesondere durch den Hersteller, auf diese Gefahr hingewiesen werden,
- selbst die Öffentlichkeit warnen, wenn andere ebenso wirksame Maßnahmen, insbesondere Warnungen durch den Hersteller, nicht oder nicht rechtzeitig getroffen werden.

Bei allen Maßnahmen der Behörden gilt aus Gründen der Verhältnismäßigkeit das Prinzip des **Vorrangs von Eigenmaßnahmen** der für das Inverkehrbringen zuständigen Person (§ 8 Abs. 4 Satz 4 GPSG).

b) Vermutungswirkung von Zertifikaten

253 Gemäß § 8 Abs. 2 Satz 3 GPSG geht die zuständige Marktüberwachungsbehörde bei Produkten, welche einer Verordnung nach § 3 Abs. 1 GPSG unterliegen und mit **CE-Kennzeichen** (Rn. 248 ff.) versehen sind davon aus, dass sie den dort genannten Anforderungen entsprechen. Im Hinblick auf verwaltungsrechtliche Anordnungen bewirkt das CE-Kennzeichen damit eine Vermutung zugunsten der **Verkehrsfähigkeit** des Produkts („Unschuldsvermutung“).[519] Abgesehen von Stichproben dürfen diese Produkte damit nicht Gegenstand einer systematischen Marktkontrolle werden.[520]

254 Das CE-Kennzeichen bewirkt in Verbindung mit § 8 Abs. 2 Satz 3 GPSG indes nur einen formalen Schutz gegen behördliche Anordnungen.[521] Im Rahmen des in den EU-Richtlinien geregelten **Schutzklauselverfahrens** (s. auch Art. 95 Abs. 5 EG) kann die Behörde gegenüber Produkten, welche ihrer Ansicht nach die wesentlichen Anforde-

519 *Europäische Kommission*, Erläuterung zur Maschinenrichtlinie, Rn. 181, 182, S. 50 f., siehe http://ec.europa.eu/enterprise/mechan_equipment/machinery/guide/guide_de.pdf.

520 Entschließung des Rates vom 7. Mai 1985 über eine neue Konzeption auf dem Gebiet der technischen Harmonisierung und der Normung, ABl. EG Nr. C 136 vom 4.6.1985 S. 1, Anhang II (Modellrichtlinie) B. II. 2; *Wilrich*, § 8 GPSG Rn. 18.

521 *Wilrich*, § 8 GPSG Rn. 18.

rungen nicht einhalten, *vorläufige* Maßnahmen treffen.[522] Sie muss dann aber die Europäische Kommission über Maßnahmen, welche den freien Warenverkehr beeinträchtigen informieren, damit die Kommission in die Lage versetzt wird, die Berechtigung er Maßnahmen einzuschätzen und ggf. eine Überprüfung der harmonisierten Normen in die Wege zu leiten.[523]

255 Bei technischen Arbeitsmitteln und verwendungsfertigen Gebrauchsgegenständen, die mit dem **GS-Zeichen** nach § 7 Abs. 1 GPSG versehen sind (dazu Rn. 108 ff.), ist davon auszugehen, dass diese den Anforderungen an Sicherheit und Gesundheit nach § 4 Abs. 1 und 2 GPSG sowie anderen Rechtsvorschriften entsprechen (§ 8 Abs. 2 Satz 4 GPSG). Über § 4 Abs. 2 Satz 4 GPSG hinaus wird damit die Übereinstimmung des Produkts mit *allen* gesetzlichen Anforderungen vermutet.[524] In der Praxis bedeutet ein zu Recht vergebenes GS-Zeichen damit eine deutliche Erschwernis für behördliches Vorgehen gegen das betreffende Produkt.[525]

5. Zusammenfassung

256 Das öffentliche Produktsicherheitsrecht erfasst sowohl Hard- als auch Softwareprodukte. Für Hardwareprodukte ergeben sich keine grundlegenden Besonderheiten gegenüber anderen elektrischen Geräten. Demgegenüber ist der Anwendungsbereich für Softwareprodukte von vornherein deutlich beschränkt, da der Schutzzweck des GPSG auf Personenschäden beschränkt ist und insbesondere Datenschäden somit nicht erfasst werden.

V. Ergebnis

257 Aus rechtspolitischer Sicht sind insbesondere folgende Defizite zu beklagen:

---

522 Dazu Entschließung des Rates vom 7. Mai 1985 über eine neue Konzeption auf dem Gebiet der technischen Harmonisierung und der Normung, ABl. EG Nr. C 136 vom 4.6.1985 S. 1, Anhang II (Modellrichtlinie) B. VII; *Finke*, Die Auswirkungen der europäischen technischen Normen und des Sicherheitsrechts auf das nationale Haftungsrecht, S. 90; *Wilrich*, § 9 GPSG Rn. 8.

523 *Europäische Kommission*, Leitfaden für die Umsetzung der nach dem neuen Konzept und dem Gesamtkonzept verfassten Richtlinien, S. 58 ff.: Hält die Kommission die Maßnahmen für gerechtfertigt, setzt sie den betreffenden Mitgliedstaat sowie die übrigen Mitgliedstaaten umgehend davon in Kenntnis, andernfalls fordert sie den betreffenden Mitgliedstaat auf, seine Maßnahmen aufzuheben und unverzüglich das Nötige zu veranlassen, damit die Produkte im Gebiet des betreffenden Staates wieder zum freien Warenverkehr zugelassen werden. Wird die Schutzklausel aufgrund einer Lücke in einer harmonisierten Norm, auf die sich eine Konformitätsvermutung gründet, in Anspruch genommen, leitet die Kommission die Angelegenheit nach Anhörung der betroffenen Parteien an den gemäß Richtlinie 98/34/EG eingerichteten Ausschuss für Normen und technische Vorschriften und ggf. – sofern dies in der den Harmonisierungsrichtlinien vorgesehen ist – spezielle Sektorausschüsse weiter.

524 *Wilrich*, § 4 GPSG Rn. 44, § 8 GPSG Rn. 19: die Vermutung nach § 4 Abs. 2 Satz 4 GPSG bezieht sich dagegen nur auf die „betreffenden Anforderungen" der Norm oder technischen Spezifikation.

525 *Wilrich*, § 8 GPSG Rn. 19.

- die verschuldensabhängige Produkthaftung greift grundsätzlich nur bei Rechtsgutsverletzungen ein; hier bestehen noch zahlreiche Unsicherheiten über die Reichweite. Insbesondere bei Vermögensschäden sowie Betriebsausfallschäden besteht die Gefahr, dass derartige Schäden nicht von der verschuldensabhängigen Produkthaftung erfasst werden,
- das Produkthaftungsrecht sieht grundsätzlich keine Pflichten vor, dass ein IT-Hersteller „Patches“ zur Verfügung stellt; er kann sich mit Warnungen begnügen,
- die Verantwortlichkeit für Schnittstellen zu anderen Programmen ist nach wie vor ungeklärt,
- Im verschuldensunabhängigen Produkthaftungsrecht ist nach wie vor ungeklärt, ob Software als Produkt überhaupt erfasst wird. Zudem ist auch hier der Kreis der erfassten Schäden auf Eigentumsschäden bei Verbrauchern sowie Körperschaden allgemein begrenzt.

258 Im öffentlich-rechtlichen Produktsicherheitsrecht fehlt es bislang vor allem auf europäischer Ebene an entsprechenden sektorspezifischen Richtlinien für den IT-Bereich; auf nationaler Ebene ist die Verengung des GPSG auf Gefahren für Leib und Leben (Gesundheit) zu beklagen, die zahlreiche IT-Risiken unberücksichtigt lässt. Ebenso wenig sind allgemeine technische Regeln nach dem nationalen Normungsverfahren im GPSG zu verzeichnen.

D. Verantwortlichkeit der IT-Nutzer

I. Grundsätzliche Überlegungen

1. Die Doppelrolle von IT-Nutzern

259 Den Pflichten der IT-Hersteller, aber auch anderer IT-Verwender in der Wertschöpfungskette, stehen mögliche Pflichten der IT-Nutzer zum Selbstschutz gegenüber. Im Zivilrecht findet dieser Gedanke des zumutbaren Selbstschutzes seinen Niederschlag in erster Linie in § 254 BGB.

260 Damit würde sich indes die Problematik kaum erschöpfen: Denn anders als in klassischen Wertschöpfungsketten, bei denen definitiv von einem Endverbraucher gesprochen werden kann, der ein Produkt „konsumiert“, ist die Situation in der IT-Branche anders. IT-Nutzer verwenden typischerweise die IT-Produkte ihrerseits, um andere Produkte herzustellen oder Dienstleistungen zu erbringen. Selbst wenn die IT-Nutzer nicht eigenständig in anderen Wertschöpfungsketten eingeschaltet sind, stehen sie doch in vielfältiger Weise in Interaktion mit anderen IT-Nutzern, oftmals durch ihre Anbindung an entsprechende Netze wie das Internet und die damit gegebenen Kommunikationsmöglichkeiten. Daher wäre es verkürzt, sich nur auf die Selbstschutz- und Schadensminderungspflichten der IT-Nutzer im Verhältnis zu IT-Herstellern oder –Intermediären zu

konzentrieren; vielmehr können die IT-Nutzer auch Pflichten gegenüber Dritten treffen, die unmittelbar mit dem Einsatz von IT-Produkten zusammenhängen. Die IT-Nutzer befinden sich daher in einer **Doppelrolle**, die im Folgenden immer im Blickfeld zu behalten ist. Allerdings werden diese Pflichten hinsichtlich ihrer Konkretisierung (Sorgfaltsstandards nach § 276 BGB) oftmals gleichbedeutend sein mit den über § 254 BGB zu definierenden Pflichten.[526] Um den Rahmen der hier vorliegenden Untersuchung nicht zu sprengen, können daher oft die jeweiligen Pflichten gemeinsam behandelt werden, sofern nicht aus besonderen Gründen eine Differenzierung geboten ist.

261 In diesem Rahmen sind **Differenzierungen je nach den Gruppen der verschiedenen IT-Nutzer** geboten, insbesondere ob es sich um private (Rn. 275 ff.) oder kommerzielle IT-Nutzer (Rn. 331 ff.) handelt, bei letzteren wiederum nochmals in bestimmte Sektoren mit unterschiedlichen Risikopotentialen unterteilt, etwa für den Finanzsektor (D.III.4.) oder für Berufsgruppen, die besonderen Pflichten unterliegen (D.V.).

262 Die Unterteilung ist sowohl für die zivilrechtliche Pflichtenbestimmung wie für die öffentlich-rechtlichen Vorgaben relevant. Während in der zivilrechtlichen Bewertung häufig Zumutbarkeitserwägungen in wirtschaftlicher Hinsicht betrachtet werden, die regelmäßig nur kommerzielle Anwender wegen ihrer wirtschaftlichen Leistungsfähigkeit und den entsprechenden angemessenen Erwartungen der Allgemeinheit treffen, werden auch öffentlich-rechtliche Pflichten meist an bestimmte Mindestkriterien geknüpft. Hier kann als qualifizierendes Merkmal z.B. das Vorliegen eines gewerblichen Handelns oder aber, wie im Datenschutz, die Verarbeitung von Daten über den persönlichen oder familiären Bereich hinaus in Betracht kommen,[527] was im Ergebnis fast immer nur bei kommerziellen Nutzern der Fall sein wird.

2. Die Abgrenzung der IT-Nutzung (Definition)

263 Zunächst ist zu klären, wer als privater Nutzer anzusehen ist: Als normative Anknüpfungspunkte hierfür könnten zunächst §§ 13, 14 BGB dienen, aber auch europarechtliche Vorgaben sowie Regelungen des Produkthaftungsrechts. Diese Differenzierungen beanspruchen auch für das öffentliche Recht Gültigkeit, sofern dieses zwischen privaten und gewerblichen Abnehmern unterscheidet – auch wenn grundsätzlich die eigenständi-

526 Objektiver Maßstab (hM) Bamberger/Roth-*Unberath*, § 254 BGB Rn. 10; MünchKommBGB-*Oetker*, § 254 BGB Rn. 35; Palandt-*Heinrichs*, § 254 BGB Rn. 8; Erman-*Kuckuk*, § 254 BGB Rn. 24; *Looschelders*, Schuldrecht AT, Rn. 1023.

527 S. dazu näher unten Rn. 404 ff.

gen Definitionen der jeweiligen öffentlich-rechtlichen Norm zu berücksichtigen sind. Bereits hier wird die oben (Rn. 259) angesprochene Doppelfunktion deutlich:

a) Privater Nutzer, Verbraucher und Unternehmer

264 §§ 13, 14 BGB regeln die **Verbraucher- bzw. Unternehmereigenschaft**. Hierfür wird grundsätzlich an den Abschluss eines Rechtsgeschäfts, also an eine konkrete rechtlich wirksame Handlung angeknüpft.[528] Unter entsprechender Anwendung wäre demnach privater Nutzer derjenige, dessen schädigende Handlungen in den privaten Bereich einzuordnen sind, der also konkret für den eigenen Bedarf gehandelt hat. In Abgrenzung dazu wäre ein Nutzer als kommerzieller Nutzer einzustufen, sofern seine Handlungen einen Bezug zu seinem Geschäft aufweisen.

265 Allerdings erscheint diese Differenzierung im hier diskutierten Zusammenhang **zunächst nur bedingt zielführend**. Denn die Abgrenzung von privaten und kommerziellen Nutzern wirft vor allem für die Eigenverantwortlichkeit der IT-Nutzer gegenüber Dritten aufgrund der **Heterogenität der Computernutzung** eine Reihe von Problemen auf: Häufig lässt sich eine konkrete Handlung des Nutzers direkt nicht ausmachen, da sein Rechnersystem ohne sein weiteres Zutun etwa schädigende Angriffe auf Dritte durchführen kann. Die Handlung des Nutzers, an die für die Qualifizierung nach §§ 13, 14 BGB angeknüpft würde, müsste also im Augenblick der Beeinträchtigung des eigenen Rechnersystems ermittelt werden, obwohl die Schädigung eventuell viel später erfolgt. Grenzt man nach der jeweilig vorliegenden Handlung ab, so hätte dies zur Folge, dass der Nutzer eines einzigen Computersystems **unterschiedlichen Pflichtbereichen** unterworfen wäre. Das System wäre also eventuell in bestimmten Situationen als konform mit eventuellen Sicherungspflichten einzustufen, während dieselbe Rechnereinheit in ihrer Konfiguration auch einen Pflichtverstoß (mangels Sicherheit) darstellen könnte.

266 Diese augenscheinlich widersprüchliche Einordnung ist jedoch hinzunehmen. Zunächst sind viele Pflichten, die dem Nutzer obliegen – **dauerhafter und grundlegender Natur** – die die Person in allen Funktionen und Rollen treffen, etwa die Einrichtung eines Virenscanners und dessen regelmäßiges Update.[529] Darüber hinaus kann darauf abgestellt werden, **in welcher Funktion der Nutzer am Verkehr teilnimmt**: Ist er etwa nicht mit anderen IT-Nutzern verbunden (was indes selten der Fall sein dürfte), reduzie-

---

528 Bamberger/Roth-*Schmidt-Räntsch*, § 13 BGB Rn. 5; MünchKommBGB-*Micklitz*, § 13 BGB Rn. 4; rechtsvergleichend zum Verbraucherbegriff *Faber*, ZEuP 1998, 854.

529 Dazu sogleich.

ren sich entsprechend seine Pflichten. Wird er seine IT-Produkte dagegen auch gewerblich oder gar in Bereichen mit besonderem Gefahrenpotential einsetzen, so kann er sich nicht darauf berufen, dass eine Schädigung in seinem privaten Bereich seinen Ausgang nahm, etwa durch Befall seines Rechners in seiner Privatsphäre mit einem Virus, dessen schädigende Wirkung sich dann später über den Rechner des IT-Nutzers an andere fortsetzte.

b) Arbeitnehmer

267 Diese Problematik stellt sich insbesondere bei der hier vorzunehmenden Abgrenzung bei **Arbeitnehmern**. Diese handeln regelmäßig im Rahmen des Betriebs und können dabei auch Kundenkontakt haben. Möglicherweise fehlt ihnen jedoch die Berechtigung, Schutzmaßnahmen überhaupt zu ergreifen (Admin-Rechte). Selbst wenn sie die Berechtigung haben, so sind die Pflichten dem Betriebsinhaber zuzuweisen, nicht aber dem einzelnen Arbeitnehmer. Auch ist möglich, dass der Arbeitnehmer an seinem privaten Computer arbeitet und mit diesem dem kommerziellen Betrieb zuzuordnen sein könnte. Fraglich ist, ob die Pflichten, die sie bei der Handlung am Arbeitsplatz haben könnten, auch im rein privaten Bereich weiter gelten müssten. Zwar könnte sich hier die Zurechnung der Gefahrenquellen zum Betriebsinhaber wiederum wegen fehlender Zugriffsmöglichkeiten auf den (privaten) Rechner des Nutzers schwierig gestalten; doch würde damit verkannt, dass der Betriebsinhaber es in der Hand hat, überhaupt den Einsatz von privaten Rechnern zuzulassen, einschließlich von Richtlinien zur entsprechenden Konfiguration von Sicherheitsmaßnahmen.

268 Auch hier ist auf den Anknüpfungspunkt einer möglichen Pflicht abzustellen. Der Arbeitnehmer, der nicht am betriebseigenen Systemen arbeitet, kann tatsächlich während seiner Tätigkeit für das Unternehmen nicht gegenüber anderen Mitarbeitern zu Lasten des Geschädigten privilegiert werden. Seine Pflichten bezüglich der IT-Sicherheit des Systems erfolgen aber regelmäßig nicht aufgrund eigenen überlegenen Wissens, sondern weil er im Rahmen des Verantwortungsbereichs des Unternehmens auch besondere Gefährdungen auszuschließen hat. Insofern wird ihm ein überlegenes Wissen bzw. eine Organisationsstruktur des Unternehmens zugerechnet,[530] was wiederum auch die Zuordnung zum Unternehmen ermöglicht. Der Arbeitnehmer muss im Rahmen des Organisationsverbundes seines Unternehmens die notwendigen Anstrengungen zum Schutz seiner Kunden und Dritter treffen; verantwortlich ist indes hierfür der Arbeitgeber als

530 BGH NJW 1995, 1339 (1341); BGH NJW 1993, 1066; BGHZ 135, 202 mwN.

Herrscher über die Gefahrenquellen insgesamt. Diese Organisationsstruktur steht dem Arbeitnehmer dagegen im privaten Umfeld nicht zur Verfügung. Daher kann ihm ein entsprechendes Wissen, das ihm im Rahmen seines Arbeitsumfeldes zur Verfügung steht (oder stünde), nicht zugerechnet werden, so dass Arbeitnehmer auch an mobilen Rechnersystemen (Laptops, PDAs etc.), die sowohl privat als auch beruflich genutzt werden, nicht zwangsläufig als kommerzielle Nutzer einzustufen sind, wenn sie privat handeln.

269 Handelt der Arbeitnehmer dagegen **von seinem beruflichen Umfeld aus, jedoch in privater Funktion**,[531] profitiert er von den Sicherungsvorkehrungen seines Arbeitgebers und muss sich die entsprechenden Sicherungsmöglichkeiten zurechnen lassen.

270 **Gleiches gilt für Arbeitnehmer**, die **von zu Hause** oder allgemein mit einem eigenen Computersystem arbeiten: Auch sie treffen bei „privater" Nutzung die gleichen Pflichten wie bei der Nutzung als Arbeitnehmer, sofern sie sich die entsprechenden Sicherungsinfrastrukturen ihrer Arbeitgeber zunutze machen können. Bei sog. **Telearbeitern** wäre schließlich zu überlegen, ob nicht eine Abgrenzung nach dem Umfang der nichtprivaten Nutzung eines Computersystems angebracht wäre, wie sie bereits bei der Unternehmereigenschaft im Sinne von §§ 13, 14 BGB eine Rolle spielt,[532] und auch im Produkthaftungsrecht angewandt wird.[533] Wenn also ein überwiegender Teil der Rechnernutzung kommerziell erfolgt, wäre der Nutzer als kommerzieller Nutzer anzusehen.

c) Expertenwissen

271 Keine Probleme bei der Einordnung als privater oder kommerzieller Nutzer bereitet das Vorliegen von **Expertenwissen**. Dem IT-Experten können grundsätzlich schon aufgrund vorhandener Verantwortlichkeitsregelungen im Einzelfall weitergehende Pflichten obliegen.

d) Zwischenergebnis

---

531 Nach Berichten aus der Praxis ist etwa der Einsatz von digitaler Signaturen zum Online-Banking daran weitgehend gescheitert, dass die Kunden das Online-Banking vom Arbeitsplatz aus durchführen wollten – hier aber kein Signaturkarteneinsatz möglich ist, sondern nur das PIN-TAN-Verfahren (LEGAL-IST Workshop zu Privacy, Identity, Management, 17.3.2006, Göttingen). Schon allein diese Tatsache zeigt, dass die private Nutzung am Arbeitsplatz nicht zu unterschätzen ist.

532 OLG Naumburg WM 1998, 2158; Erman-*Saenger*, § 13 BGB Rn. 17; *Pfeiffer*, NJW 1999, 169 (173); aA Bamberger/Roth-*Schmid-/Räntsch*, § 13 BGB Rn. 12.

533 *Taschner/Frietsch*, § 1 ProdHaftG, Rn. 32 f.; *v. Westphalen*, in: v. Westphalen, ProdHaftHdb, Bd. 2, § 72 Rn. 29.

272 Die Pflichten eines Nutzers sind damit nicht einheitlich zu definieren, sondern rollenabhängig; sie können je nach Umfeld und Möglichkeiten erheblich differieren. Als privater Nutzer kann daher unter Zugrundelegung der EG-Produkthaftungsrichtlinie 85/374/EWG nur derjenige definiert werden, „wer die Sache nutzt oder verbraucht, ohne damit seinen Lebensunterhalt zu verdienen oder sonstige Zwecke zu verfolgen, die außerhalb einer privaten Existenz und Tätigkeit liegen."[534] Nicht privat ist demnach zunächst, wer gewerblich oder freiberuflich handelt.[535]

273 Da es sich um die Abgrenzung von privater und kommerzieller Nutzung von Informationstechnik handelt, müsste die kommerzielle Tätigkeit demnach entweder im Erbringen von Diensten *mit* dem System liegen oder die Tätigkeit *mittels* Informationstechnik erbracht bzw. gefördert werden. Auch Handlungen bezüglich Rechnersystemen, die also nicht direkt mit einem eventuell angebotenen Produkt zu tun haben, aber dennoch im weiteren Sinne für die Ausübung der Tätigkeit genutzt werden, sind somit erfasst. Hierzu könnte beispielsweise eine computergestützte Verwaltung, Consumer-Relationship-Management-Systeme u.ä. zählen.

274 Privater Nutzer kann zudem **nur eine natürliche Person** sein, juristischen Personen fehlt es insoweit am „Privatleben".[536] Die Produkthaftungsrichtlinie stellt demnach auf die Nutzung einer Sache ab. Die genutzte Sache wäre vorliegend ein Rechnersystem, auf das sich eventuelle Pflichten beziehen würden. Als privater Nutzer ist demnach negativ abgegrenzt anzusehen, wer als natürliche Person ein Rechnersystem nicht (überwiegend) gewerblich oder freiberuflich nutzt. Der Arbeitnehmer unterfällt nur im Rahmen seiner Arbeitnehmertätigkeit den Pflichten für kommerzielle Nutzer.

II. Private IT-Nutzung

275 Private Nutzer treffen im Bereich der IT-Sicherheit regelmäßig keine **vertraglichen Pflichten**. Eine wichtige Ausnahme bildet jedoch die Teilnahme am **E-Commerce**, insbesondere die den Bankkunden treffenden Pflichten beim Online-Banking (dazu ausführlich unten Rn. 280 ff.). Regelmäßig wird es jedoch – gerade im Verhältnis zwischen Privaten – an vertraglichen Beziehungen fehlen, so dass eine Haftung Privater nur auf

534 Schmidt-Salzer/Hollmann-*Schmidt-Salzer*, Art. 9 RL, Rn. 47.
535 *v. Westphalen*, in: v. Westphalen, ProdHaftHdb, Bd. 2, § 72 Rn. 21 ff.
536 *Faber*, ZEuP 1998, 854 (883); *Taschner/Frietsch*, § 1 ProdHaftG Rn. 36; ebenso der Verbraucherbegriff in § 13 BGB, MünchKommBGB-*Micklitz*, § 13 BGB Rn. 10.

außervertragliche Ansprüche gestützt werden kann. Spezialgesetzlich normierte Pflichten bestehen für Private im IT-Sektor soweit ersichtlich nicht.

1. Vorsätzliche Verletzungshandlungen

276 Als vorsätzliche Schädigungshandlungen kommen im Bereich der IT-Sicherheit vor allem **Hacking**, **Denial-of-Service-Attacken** und die bewusste **Weiterverbreitung von Viren** in Betracht.[537] Gegenüber dem privaten Nutzer als Täter kommen in diesem Fällen Schadensersatzansprüche wegen der Verletzung von Schutzgesetzen (§ 823 Abs. 2 BGB) und wegen vorsätzlich sittenwidriger Schädigung (§ 826 BGB) in Betracht, so dass ohne Rücksicht auf eine Rechtsgutsverletzung im Sinne von § 823 Abs. 1 BGB auch primäre Vermögensschäden ersatzfähig sind. Relevantes Schutzgesetz in diesem Bereich ist neben strafrechtlichen Normen, wie beispielsweise § 202a StGB (Ausspähen von Daten) oder § 303a StGB (Datenveränderung), vor allem § 43 Abs. 2 Nr. 4 BDSG. Danach handelt ordnungswidrig, wer die Übermittlung personenbezogener Daten, welche nicht allgemein zugänglich sind, durch unrichtige Angaben erschleicht.[538] Soweit dem Geschädigten hiernach ein Anspruch zusteht, wird eine Inanspruchnahme des Täters jedoch häufig an praktischen **Durchsetzungsproblemen** scheitern.

2. Sicherheitspflichten privater IT-Nutzer gegenüber Dritten

277 Mangels eines entsprechenden Vorsatzes wird eine Haftung privater Nutzer oftmals nur auf die Verletzung **deliktischer Verkehrspflichten** gestützt werden können. Der folgende Abschnitt befasst sich mit deliktischen Verkehrspflichten privater Nutzer, die dabei herausgearbeiteten Wertungen können jedoch auch im vertraglichen Bereich herangezogen werden (zum Online-Banking unten Rn. 535 ff.).[539] Die Sorgfaltspflichten privater Nutzer können in doppelter Hinsicht relevant werden: Zum einen bei Schädigung Dritter infolge unterlassener Sicherungsmaßnahmen (Rn. 278 ff.), zum anderen spiegelbildlich im Rahmen des Mitverschulden (Rn. 314 ff.).

a) Rechtsgutverletzung

278 Die Haftung nach § 823 Abs. 1 BGB beruht auf der schuldhaften Verletzung eines der dort aufgezählten Rechtsgüter oder absoluten Rechte. Hinsichtlich der Verletzung der

---

537 Ausführlich dazu *Mankowski*, in: Ernst, Hacker, Cracker & Computerviren, Rn. 500 ff., 512 ff.

538 Dazu *Gola/Schomerus*, § 43 BDSG Rn. 23; *Mankowski*, in: Ernst, Hacker, Cracker & Computerviren, Rn. 502.

539 S. dazu Palandt-*Heinrichs*, § 280 BGB Rn. 28; MünchKommBGB-*Ernst*, § 280 BGB Rn. 104; Bamberger/Roth-*Grüneberg/Sutschet*, § 241 BGB Rn. 92.

Rechtsgüter **Leben**, **Körper**, **Gesundheit** und **Freiheit** kann im Wesentlichen auf die zur Produkthaftung gemachten Ausführungen verwiesen werden (oben **Rn. 107**). Ein Eingriff in diese Rechte dürfte bei privaten IT-Nutzern kaum vorkommen, ist aber nicht völlig auszuschließen. Deutlich mehr praktische Relevanz dürfte bei privaten Nutzern eine **Eigentumsverletzung** wegen Störung der Integrität von Daten (z.B. infolge der Weiterverbreitung von Viren) haben (**oben Rn. 108 ff.**).

279 Denkbar ist zudem eine Beeinträchtigung der bestimmungsgemäßen Verwendung eines Computersystems. Problematisch ist in diesem Zusammenhang etwa die Teilnahme an Attacken, die nur die **Funktionsfähigkeit des Systems** beeinträchtigen, aber im Grunde keine Datenveränderung vornehmen. Hierzu gehört beispielsweise die durch unterlassene Sicherungsmaßnahmen ermöglichte Instrumentalisierung des Rechners eines privaten Nutzers für eine Denial-of-Service-Attacke.[540] Zur Eigentumsverletzung wegen Nutzungsstörungen ausführlich oben (Rn. 112). Richtet sich der Denial-of-Service-Angriff gegen ein **gewerbliches Unternehmen**, so kommt abgesehen von den genannten Rechten die Beeinträchtigung des Rechts am eingerichteten und ausgeübten Gewerbebetrieb als Auffangrecht[541] in Betracht. Allerdings bestehen hier oftmals Probleme hinsichtlich der notwendigen Betriebsbezogenheit.[542]

b) Verkehrspflichten

280 Der private Nutzer muss die Rechtsgutsverletzung durch zurechenbares und pflichtwidriges **Handeln** oder **Unterlassen** verursacht haben. Eine bewusste Schädigungshandlung wird dabei die Ausnahme darstellen. Regelmäßig wird der Privatnutzer entweder fahrlässig zur Schädigung Dritter beitragen, etwa indem er Viren und andere Schadprogramme über seinen Rechner weiter verbreitet. Besondere Bedeutung erlangt zudem die Haftung für Unterlassen, wenn der private Nutzer seinen PC nicht im Rahmen des Zumutbaren gegen Angriffe geschützt hat und Angreifer die Sicherheitslücke zum Schaden Dritter ausnutzen, indem sie seinen Rechner als Werkzeug instrumentalisieren (z.B. aufgrund von Bot-Netzen). Anknüpfungspunkt für die Haftung wird damit im Regelfall entweder eine sog. mittelbare Verletzungshandlung oder ein Unterlassen des Privatnutzers sein, was in den Wertungen eng bei einander liegt.[543] Da der Verletzungserfolg in

---

540 Dazu *Möller/Kelm*, DuD 2000, 292; zur Risikoverteilung AG Gelnhausen CR 2006, 209; s.o. Rn. 87 f. (Bedrohungspotentiale Denial-of-Service-Attacks).

541 *Koch*, NJW 2004, 801 (803) mwN.

542 Dazu bereits oben Rn. 108.

543 Dazu Bamberger/Roth-*Spindler*, § 823 BGB Rn. 23; *Medicus*, Bürgerliches Recht, Rn. 646; *La-*

beiden Fällen nicht unmittelbar durch die Handlung des Schädigers, sondern durch eine Reihe von Zwischenursachen vermittelt wird, ist Voraussetzung der Haftung jeweils die Verletzung einer Verkehrspflicht.[544]

(1) Zurechnungskriterien

281 Derjenige, der eine Gefahrenquelle schafft, ist grundsätzlich verpflichtet, die notwendigen und zumutbaren Vorkehrungen zu treffen, um eine Schädigung anderer zu vermeiden. Ihn treffen diesbezüglich Verkehrspflichten.[545] Andererseits gibt es keine allgemeine Rechtspflicht, andere vor Schäden zu bewahren, so dass die Annahme von Verkehrspflichten besonderer Begründung bedarf.[546] Während für IT-Hersteller (Rn. 94 ff.) und auch IT-Intermediäre (Rn. 651 ff.) weitgehend Einigkeit darüber besteht, dass sie Verkehrspflichten zumindest aufgrund ihrer Herrschaft über Gefahrenquellen treffen, ist die Bestimmung von Inhalt und Umfang der den privaten Nutzer treffenden Pflichten im IT-Bereich noch weitgehend ungeklärt.

282 Eine Zurechnung von Verkehrspflichten kommt grundsätzlich bei der **Beherrschung einer besonderen Gefahrenquelle** sowie bei der Schaffung einer besonderen Gefahrenlage aus **vorangegangenem Tun** in Betracht.[547] Der IT-Nutzer hat als Besitzer die Verfügungsgewalt über sein Computersystem.[548] Ist der Computer durch einen vorherigen Angriff kompromittiert und führt selbst entsprechende Angriffe aus, sei es durch Versendung von E-Mails mit Viren oder aber durch die Teilnahme an Denial-of-Service-Attacken,[549] so geht von dieser Computeranlage eine Gefährdung für die Computer und Daten und ggf. weitere Rechtsgüter Dritter aus. Damit besteht hier durchaus ein Anknüpfungspunkt in Gestalt der Beherrschung einer Gefahrenquelle.[550]

283 Allerdings ist zweifelhaft, ob der Nutzer für alle möglichen Schäden einstehen sollte, die von seinem Computer ausgehen, etwa im Rahmen eines Bot-Netzes und davon aus-

---

renz/Canaris, § 75 II 3 c, S. 368, § 76 III 1 c, S. 401 f.

544 *Kötz/Wagner*, Deliktsrecht, Rn. 108.

545 BGH NJW-RR 2003, 1459; BGH NJW 1990, 1236; BGH NJW-RR 2002, 525 mwN.

546 BGH NJW 1987, 2510; Palandt-*Sprau*, § 823 BGB Rn. 46; Bamberger/Roth-*Spindler*, § 823 BGB Rn. 227; *Koch*, NJW 2004, 801 (803); *Libertus*, MMR 2005, 507 (508).

547 *Larenz/Canaris*, § 76 III 4 b; *Koch*, NJW 2004, 801 (803); ähnl. auch *Libertus*, MMR 2005, 507 (508).

548 Dabei werden zunächst entsprechende Admin-Rechte unterstellt. Der reine Nutzer ohne Berechtigung, Software zu installieren, hat in der Regel keine Möglichkeit, auf die Konfiguration des Systems Einfluß zu nehmen, damit auch nicht auf dessen Sicherheitsniveau.

549 S.o. Rn. 52 ff.; zur Verteilung des Risikos zwischen Serverinhaber und –vermieter bei DoS-Attacken AG Gelnhausen CR 2006, 208.

550 Ebenso *Koch*, NJW 2004, 801 (803); *Libertus*, MMR 2005, 507 (509); implizit auch *Schmidbauer*, abrufbar unter: http://www.i4j.at/news/aktuell36.htm.

gehenden Denial-of-Service-Attacks oder Virenverbreitung. Denn für den Nutzer ist es im Rahmen des Internets praktisch nicht vorhersehbar, wer durch die jeweiligen Handlungen bzw. Viren geschädigt werden kann. Anders formuliert kann die Haftung hier unabsehbar ausufern. Im deutschen Recht ergibt sich eine erste Eingrenzung durch die bei gewerblich Geschädigten erforderliche Betriebsbezogenheit des Eingriffs, die bei derartigen Gefährdungen nicht vorliegen wird. Dennoch verbleibt bei Schädigung von Daten ein für den Einzelnen fast unübersehbares Haftungsrisiko, das sich in praxi wohl nur aufgrund des erforderlichen Kausalitätsnachweises relativiert – denn das deutsche Haftungsrecht verlangt ansonsten keinen Vorsatz oder keine Pflichtwidrigkeit hinsichtlich des Schadens selbst bzw. bezüglich des haftungsausfüllenden Tatbestandes.

(2) Sicherheitserwartungen des Verkehrs

284 Grundsätzlich lassen sich gegen die vielen Bedrohungen Gegenmaßnahmen ergreifen. Zur genaueren Konkretisierung des Inhalts und Umfangs der Verkehrspflicht ist in erster Linie auf die berechtigten **Sicherheitserwartung der betroffenen Verkehrskreise** abzustellen,[551] zu deren Bestimmung die Möglichkeit und Zumutbarkeit der Gefahrenvermeidung einerseits auf der Versenderseite, andererseits auf der Empfängerseite gegeneinander abzuwägen ist.[552] Für die Bestimmung der Reichweite der Pflichten des Nutzers kommt es auf eine **objektivierte Betrachtung** anhand einer Nutzergruppe an, nicht auf die individuellen Fähigkeiten und Ressourcen des individuellen Nutzers. Angesichts der Entwicklung des Internet zum Massenphänomen wird man sich indes vor überspannten Sorgfaltsanforderungen an einen vermeintlich „typischen Internetnutzer“ hüten müssen, da das Wissen um Einstellungen, Softwareverwendung und Risiken bei privaten Nutzern (insbesondere zwischen den Altersgruppen) zum Teil erheblich variiert.[553] Ebenso ist im schnelllebigen IT-Sektor stets zu berücksichtigen, dass sich die Verkehrserwartungen mit zunehmender Verbreitung eines Risikobewusstseins und der Kenntnis möglicher Gegenmaßnahmen wandeln können.[554]

285 Im Einzelnen ist daher in einem ersten Schritt darauf abstellen, ob das Problem überhaupt weithin **bekannt** ist (dazu Rn. 286 f.).[555] Für die Beurteilung der **Zumutbarkeit**

---

551 BGH NJW-RR 2002, 525 (526); BGH NJW 1978, 1629; NJW 1990, 906 (907); Bamberger/Roth-*Spindler*, § 823 BGB Rn. 234; *Schwerdtfeger/Gottschalck*, in: Schwarz/Peschel-Mehner, Kap. 2 Rn. 246.

552 *Koch*, NJW 2004, 801 (804); *Libertus*, MMR 2005, 507 (509); Bamberger/Roth-*Spindler*, § 823 BGB Rn. 234.

553 Dazu bereits *Spindler*, JZ 2004, 1128 (1129).

554 *Spindler*, JZ 2004, 1128 (1129).

555 *Leible/Wildemann*, K&R 2004, 288 (289); vgl. *Schmidbauer*, abrufbar unter:

kann in einem zweiten Schritt zwischen der technischen Zumutbarkeit und der wirtschaftlichen Zumutbarkeit unterschieden werden (dazu Rn. 290 ff.).

(3) Bekanntheit des Problems

286 Verkehrspflichten privater Nutzer können nicht mit dem pauschalen Hinweis auf die Komplexität der modernen Informationstechnologie verneint werden. Wenn der BGH in der vielbeachteten **Dialer-Entscheidung** eine Pflicht zur Installation von Dialerschutzprogrammen verneinte,[556] so lag dies vor allem daran, dass Dialer damals noch weitgehend unbekannt (und Schutzvorkehrungen technisch aufwändig) waren.[557] Entgegen zuvor ergangenen instanzgerichlichen Entscheidungen[558] stellte der III. Zivilsenat fest, dass für den Nutzer keine Pflicht zur Überwachung des eigenen Computersystems besteht, solange kein konkreter Hinweis auf einen Missbrauch besteht.[559] Verallgemeinert man diesen Gesichtspunkt, so kommt es grundsätzlich darauf an, ob ein verständiger objektiver Nutzer nicht von einer entsprechenden Gefahr wusste oder zumindest damit rechnen musste.[560] Grund hierfür ist auch, dass der **Bekanntheitsgrad die Verkehrserwartung beeinflusst**. Im zu entscheidenden Fall war für den Nutzer nicht erkennbar, dass eine Beeinträchtigung des Systems stattgefunden hatte bzw. diese nicht einfach beseitigt werden konnte. Hinzu kam, dass der Nutzer auch grundsätzlich nicht misstrauisch sein und demgemäß keine Sicherungsmaßnahmen (z.B. Dialer-Schutzprogramm) ergreifen musste.[561]

287 Ob allerdings angesichts der weiteren Entwicklung heute noch davon ausgegangen werden kann, dass die Allgemeinheit bzw. ein verständiger Nutzer keine Kenntnis von den Gefahren der Informationstechnologie und den möglichen Schutzmechanismen hat, ist zweifelhaft.[562] Wie die **technische Entwicklung** ist auch der den Nutzer treffende

---

http://www.i4j.at/news/aktuell36.htm; BGH VersR 1972, 70 (71); *Härting/Schirmbacher*, CR 2004, 334 (337); dem hat sich der BGH im Dialer Urteil, NJW 2004, 1590 jedoch nicht angeschlossen, sondern hat im konkreten Fall eine ergänzende Vertragsauslegung vorgenommen.

556 BGH NJW 2004, 1590 = JZ 2004, 1124 m. Anm. *Spindler*.

557 So auch *Ernst*, CR 2006, 590 (593).

558 LG Berlin ZAP 2002, 565; KG Berlin NJW-RR 2003, 637; s. auch AG München JurPC Web-Dok. 391/2002; AG Dillenburg CR 2003, 686.

559 BGH NJW 2004, 1590 = JZ 2004, 1124 m. Anm. *Spindler*. Dem folgend für Schutzmaßnahmen gegen Trojaner LG Stralsund CR 2006, 487 (489) mit zu Recht krit. Anm. *Ernst*, CR 2006, 590 ff.

560 Vgl. auch LG Köln NJW 1999, 3206.

561 BGH NJW 2004, 1590 (1592) = JZ 2004, 1124 m.Anm. *Spindler*.

562 *Leible/Wildemann*, K&R 2004, 288 (289); ähnl. Argumentation für Viren *Schmid*, abrufbar unter: http://www.bwl.tu-darmstadt.de/jus4/lehre/IuD-I_ws_05/ws_0506_vorl_ueb_iud_1_modul_6_060123.pdf, 43.

Sorgfaltsmaßstab einer steten Veränderung unterworfen.[563] Gegenwärtig wird man auch vom durchschnittlichen IT-Nutzer zumindest die Kenntnis grundlegender Sorgfaltsmaßnahmen im IT-Verkehr erwarten können. Dazu gehört beispielsweise die Verwendung von Anti-Virus-Programmen (im Einzelnen unten Rn. 295 ff.).

288 **Wann** indes ein Sicherheitsproblem im Einzelfall als **allseits bekannt** unterstellt werden kann, ist bislang wenig geklärt. Ein Problem wird nicht bereits dann weithin bekannt sein, wenn Fachzeitschriften darüber berichten; gerade angesichts der massenweisen Verbreitung von IT-Produkten kann hier etwa nicht auf Computerzeitschriften abgestellt werden, selbst wenn diese sich an einen breiten Leserkreis wenden. Vielmehr muss auch derjenige, der sich nicht direkt und gezielt informiert, die Möglichkeit gehabt haben, von der Problematik Kenntnis zu erlangen, etwa bei umfangreicher Berichterstattung in Print-, Rundfunk- und TV-Medien. Zusätzlich müssen aber auch die generellen Lösungsmöglichkeiten bekannt sein, z.B. durch die Installation entsprechender Abwehrprogramme.

(4) Zumutbarkeit der Schutzmaßnahmen

289 Wirtschaftlich aufwändige, aber auch technisch anspruchsvolle Lösungen, die den Normalnutzer überfordern, können nicht verlangt werden. Gerade im Privatbereich muss danach gefragt werden, ob dem potenziell Pflichtigen, also dem Durchschnittsnutzer, die Ergreifung der Sicherungsmaßnahmen überhaupt von seinen Fähigkeiten her möglich ist, etwa wenn technische Lösungen nur durch zahlreiche, teils komplizierte Schritte zu erreichen sind. Fehlbedienungen können z.B. bei Firewalls durchaus gerade den gegenteiligen Effekt hervorrufen und das System anfälliger für Angriffe machen.[564]

(a) Technische Zumutbarkeit

290 Technisch zumutbar ist der Einsatz einer Lösung, wenn sie auch für den Nichtfachmann mit geringem Einarbeitungsaufwand installiert werden kann. Die Anforderungen an private Nutzer dürfen hierbei insbesondere im technischen Bereich (z.B. der Konfiguration von Firewalls) nicht übertrieben streng gehandhabt werden (siehe im Einzelnen unten Rn. 294 ff.).[565] Entfernungsanleitungen (Removal tools), die einen Eingriff in Systemkomponenten, z.B. die Beendigung von Systemdiensten oder die Bearbeitung von Systemdatenbanken (registries), erfordern, können durch den Durchschnittsnutzer gerade

563 Dazu schon *Spindler*, JZ 2004, 1128 (1129); zust. *Kind/Werner*, CR 2006, 353 (355).
564 S.u. Rn. 63 ff.
565 Dazu auch *Ernst*, CR 2006, 590 (593).

nicht befolgt werden. Problematisch sind auch Lösungen, die eine ständige Aufmerksamkeit des Nutzers erfordern. Diese kann verlangt werden, sofern auch komplizierte Vorgänge für den Nutzer einfach erklärt werden können, und die Handlungsmöglichkeiten deutlich und eindeutig sind. Sofern allerdings der Nutzer die Bewertung von Systemeinstellungen oder Netzwerkaktionen vornehmen muss, diese häufig notwendig werden, und Entscheidungen bzw. Einstellungen die Sicherheit des gesamten Systems kompromittieren können, also im Grunde ein IT-Experte eingesetzt werden müsste, kann dies nicht von einem Durchschnittsnutzer verlangt werden. Es ist jedoch zumutbar, ein entsprechendes Programm zu installieren, das Schutzmaßnahmen bereitstellt, sofern es die genannten Kriterien der Einfachheit erfüllt.

(b) Wirtschaftliche Zumutbarkeit

291 Zwischen technischer und wirtschaftlicher Zumutbarkeit besteht ein enger sachlicher Zusammenhang. Wirtschaftlich zumutbar ist die Ergreifung von Sicherungsmaßnahmen jedenfalls dann, wenn sie nicht vollkommen außerhalb jedes vernünftigen Verhältnisses zu dem mit der Maßnahme verbundenen Sicherheitsgewinn steht. So können monatlich zu entrichtende Beträge durchaus angemessen sein, sofern sie nicht ein bestimmtes Maß überschreiten, z.B. für ein monatliches Virenscan-Update.

292 Zur Lösung von IT-Sicherheitsproblemen ist stets auch der Einsatz entsprechender **Experten** denkbar. Allerdings sind die Kosten hierfür meist unverhältnismäßig hoch. Der Private wird in aller Regel nur Maßnahmen ergreifen, welche ihm ohne fremde Hilfe möglich sind. Eine Pflicht zur kostenpflichtigen Heranziehung von Fachkräften dürfte bei privaten Nutzern indessen unzumutbar sein.

(c) Allgemeines Lebensrisiko

293 Zur Begründung einer Verkehrspflicht müssen von der beherrschten Gefahrenquelle bzw. der geschaffenen Gefahrenlage besondere, über das allgemeine Lebensrisiko hinausgehende Gefahren ausgehen.[566] Bei einem weit verbreiteten und damit auch weithin bekannten Problem könnte man davon ausgehen, die Gefahr einem solchen Angriffs zum Opfer zu fallen, werde bei Nutzung des Internet in Kauf genommen, so dass Schäden in den Verantwortungsbereich des zum Selbstschutz verpflichteten Geschädigten fallen.[567] Zum gegenwärtigen Zeitpunkt wird man so weit allerdings nicht gehen kön-

---

566 Erman-*Schiemann*, § 823 BGB Rn. 20; Staudinger-*Hager*, § 823 BGB Rn. 33; vgl. auch BGH NJW 1996, 1533; BGH NVwZ-RR 1994, 400 (401).

567 Zu Viren *Libertus*, MMR 2005, 507 (509).

nen. Auch wenn bei Internetnutzern ein entsprechendes Selbstverständnis vorhanden sein sollte und ein Virenbefall mithin als „übliches Risiko“ der Internetnutzung angesehen würde, kann hierauf keine rechtliche Wertung gestützt werden, so dass Sicherungspflichten privater Nutzer generell zu verneinen wären.

c) Einzelfragen

294 Für die eingangs beschriebenen Bedrohungs- und Abwehrszenarien (oben Rn. 52 ff.) ist im Folgenden zu klären, ob eine Verkehrspflicht des privaten Nutzers besteht. Dazu ist im Einzelnen zu prüfen, ob

- die Tatsache, dass es ein Sicherheitsproblem und eine generelle Lösung gibt, weithin bekannt ist,
- die Ergreifung der Lösung technisch
- und wirtschaftlich zumutbar ist.

(1) Virenscanner

295 Eine Gefährdung der IT-Sicherheit durch Viren erfolgt vom Privatnutzer in der Regel durch den unbeabsichtigten Versand mit E-Mails oder durch Weitergabe auf verseuchten Datenträgern.[568] Der virenbefallene Rechner des Privatnutzers stellt hierbei eine besondere Gefahrenquelle dar, welche die Zurechnung einer Verkehrspflicht rechtfertigt.[569] Die Gefahr durch Viren und die erforderlichen Schutzmaßnahmen sind als weithin bekannt anzusehen.[570] Bereits mehrfach wurde über diese Problematik auch in den Medien berichtet.[571] Fachzeitschriften thematisieren diesen Bereich zudem regelmäßig. Außerdem wird meist auch darauf hingewiesen, dass mit sogenannten Virenscannern eine relativ einfach zu handhabende Vorsorgemöglichkeit besteht. Der Nutzer muss lediglich ein entsprechendes Programm kaufen oder kostenfrei im Internet herunterladen und installieren. Bei neu erworbenen Computern gehört ein vorinstalliertes Virenschutzprogramm zum üblichen Lieferumfang. Die Verwendung eines Antivirenschutzprogramms ist dabei auch dem Durchschnittsnutzer sowohl technisch als auch wirtschaftlich zumutbar. [572] Technische Vorkenntnisse sind nicht erforderlich, da die Standardprogramme entsprechende Nutzerführungen enthalten. Wirtschaftliche Argumente

---

568 *Mankowski*, in: Ernst, Hacker, Cracker & Computerviren, Rn. 516.

569 *Koch*, NJW 2004, 801 (803); *Libertus*, MMR 2005, 507 (509).

570 LG Köln NJW 1999, 3206; *Koch*, NJW 2004, 801 (802); *Libertus*, MMR 2005, 507 (509); *Schmidbauer*, abrufbar unter: http://www.i4j.at/news/aktuell36.htm; *Schultze-Melling*, CR 2005, 7; *Schneider/Günther*, CR 1997, 389 (394); *Spindler*, JZ 2004, 1128 (1129); *Tita*, VW 2001, 1781 (1784).

571 OLG Hamburg MMR 2005, 119 (120); *Göttert*, VW 2001, 1972.

572 *Mankowski*, in: Ernst, Hacker, Cracker & Computerviren, Rn. 516.

gegen den Einsatz von Virenscannern dürften schon deshalb nicht verfangen, weil solche kostenlos im Internet als Freeware zum Download bereit stehen.[573] Allerdings muss im Einzelfall genau geprüft werden, ob diese Programme weithin bekannt und einfach verfügbar sowie installierbar sind.

296 Problematisch ist indessen, wie häufig der Nutzer seinen Virenschutz **aktualisieren** muss. Hierzu ist zunächst zu beachten, dass auch die aktuellste Virendefinitionsdatei keinen absoluten Schutz bietet. Werden neue Viren erstellt, so brauchen auch die Virenlabore der Antivirensoftwarehersteller einige Zeit, um hierauf zu reagieren. In dieser Zeit ist selbst ein ständig aktuell gehaltenes Computersystem vor dem speziellen Virus ungeschützt.[574] Zudem stellen die Hersteller von Antiviren-Software nicht ständig neue Updates zur Verfügung. Teilweise werden die automatischen Updates z.B. im wöchentlichen Rhythmus bereitgestellt. Weiter bedeutet ein Update regelmäßig den Download größerer Dateien. Zwar nimmt die Verbreitung breitbandiger Internetzugänge zu. Es kann gegenwärtig aber noch nicht davon ausgegangen werden, dass der Durchschnittsnutzer einen solchen besitzt. Daher dürfte es derzeit überzogen sein, eine ständige Pflicht zur Aktualisierung des privaten Systems zu fordern.[575] Grundsätzlich ist damit **maximal eine wöchentliche Aktualisierung** zumutbar.

297 Im Ergebnis lässt sich danach festhalten, dass dem privaten IT-Nutzer die Pflicht zur Einrichtung, Wartung und wöchentlichen Aktualisierung eines Virenscanners obliegt.[576]

(2) Firewall

298 Ein weiteres Abwehrprogramm ist die sog. Firewall, welche insbesondere der Abwehr von Angriffen aus Netzwerken dient und damit wichtig für die generelle Sicherheit des Computers ist.[577] Durch eine Firewall wird einerseits der Zugriff auf Programme und Systemfunktionen von außen bereits im Aufbau blockiert. Andererseits ermöglichen die sog. Personal Firewalls darüber hinaus die Freigabe oder Verweigerung von Netzzugriffsrechten lokaler Programme. So kann z.B. ein Programm, das auf Ressourcen im

573 *Ernst*, CR 2006, 590 (593).
574 *Heibey*, in: Roßnagel, Handbuch Datenschutzrecht, Kap. 4.5 Rn. 131.
575 *Schmidbauer*, abrufbar unter: http://www.i4j.at/news/aktuell36.htm; wöchentlich oder kürzer *Koch*, NJW 2004, 801 (807); ebenso BSI, IT-Grundschutzhandbuch 2005, M 4.3.
576 Ebenso *Ernst*, CR 2006, 590 (593); *Mankowski*, in: Ernst, Hacker, Cracker & Computerviren, Rn. 516. Abzulehnen LG Stralsund CR 2006, 487 (489).
577 Vgl. LG Köln JurPC Web-Dok. 62/2004, wonach zu einem Sicherheitskonzept auch eine Firewall gehört; *Schneider/Günther*, CR 1997, 389 (394).

Internet zuzugreifen versucht, hieran durch entsprechende Regeln gehindert werden. Firewalls dienen damit auch dem Schutz vor Trojanern.

299 Die Unsicherheit des Betriebs von Computern im Internet bzw. die Angreifbarkeit ist weithin bekannt. Dies bezieht sich zwar hauptsächlich auf Viren, aber zumindest die abstrakte Kenntnis des Nutzers von der Gefährlichkeit ohne besondere Kenntnis der Gründe ist vorhanden. Ob daraus allerdings auch darauf geschlossen werden kann, dass auch die Lösung, nämlich die Einrichtung einer Firewall, bekannt ist, ist eher fraglich. Mit aktuellen Betriebssystemen wird meist eine integrierte Firewall geliefert. Beim Einsatz von sogenannten Internetroutern für den breitbandigen Internetzugang ist zudem häufig eine Firewall in die Hardware integriert, die zumindest die größten Gefahren minimiert. Weder dieser Schutz noch die zurzeit beigelegten Firewalls sind allerdings zum absoluten Schutz geeignet, da sie nur eine rudimentäre Funktionalität bieten. So können z.B. die sog. „well-known Ports“ bzw. „trusted Ports“, also die Ports von 0 bis 255 bzw. 1024, offen sein.[578] Wenn hier fehler- oder schadhafte Software auf Verbindungen wartet, so bieten die integrierten Lösungen keinen bzw. kaum Schutz.[579] Programme, die aktive Inhalte ausführen und denen Zugang zum Netz gewährt wurde, bergen die weitere Gefahr, dass selbstverständlich auch die aktiven Inhalte, die für die Firewall nicht vom Programm unterscheidbar sind, die entsprechende Berechtigung zum Netzzugriff haben.[580] Hier bietet die Firewall keinen Schutz.

300 Hinzu kommt die schwierige Bedienbarkeit der Programme.[581] Firewalls arbeiten auf der Basis eines bestimmten Regelsatzes. Anhand dieser Regeln entscheiden sie, ob bestimmte Kommunikationsvorgänge erlaubt werden sollen. Da die Kommunikationspartner und -programme vorher nicht bekannt sind, muss hierfür der Nutzer gefragt werden. Die zugehörigen Nachrichten sind jedoch meist kryptisch und unverständlich. Viele Firewalls geben z.B. an, dass von einer bestimmten IP-Adresse aus eine Anfrage an den eigenen Rechner gestellt wurde, oder dass ein lokales Programm Zugriff auf eine entfernte IP-Adresse wünscht. Aufgrund der Vielzahl der Programme und Dienste können Firewalls auch keine direkte Aussage darüber treffen, ob der Zugriff gefährlich ist. Der Nutzer muss also anhand der netzwerkspezifischen Informationen entscheiden. Die Be-

578 *Eckert*, IT-Sicherheit, S. 88; BSI, IT-Grundschutzhandbuch 2005, M 2.76

579 Zu den Folgen der Überwindung von Firewalls *Quack-Grobecker/Funke*, VW 1999, 157 (158).

580 Vgl. *Eckert*, IT-Sicherheit, S. 72.

581 „Aufstellen und Aktualisieren der Filterregeln ist keine einfache Aufgabe.“ BSI, IT-Grundschutzhandbuch 2005, M 2.76.

antwortung ist damit schwierig. Hinzu kommt, dass die Antworten direkt der Regelerstellung dienen. Blockiert der Nutzer also aus Vorsicht eine wichtige Anwendung, so ist diese möglicherweise nicht mehr einsatzfähig bzw. kann erst durch die komplizierte Entfernung der Regel wieder in einen funktionsfähigen Zustand versetzt werden. Durch solche Erfahrungen kann der Nutzer veranlasst sein, auch bei gefährlichen Programmen Zugriffsrechte zu erteilen. Mit der Gewährung von Rechten kann der Nutzer die Firewall sogar vollkommen deaktivieren, ohne dass er dies merkt.[582] Sofern nämlich eine hochpriorisierte Regel den generellen Netzwerkzugriff erlaubt, so greifen auch schützende Regeln nicht mehr. Dennoch signalisiert die Firewall Bereitschaft.

301 Es **fehlt** somit bereits an der **Bekanntheit** unter privaten Nutzern,[583] dass Firewalls als Lösungsmöglichkeit zur Verfügung stehen. Zusätzlich ist die **Benutzung kompliziert** und daher auch technisch dem Durchschnittsnutzer nicht zumutbar, während wegen der geringen Kosten eine wirtschaftliche Zumutbarkeit wohl gegeben wäre. Eine grundsätzliche Pflicht zum Einsatz von Firewalls besteht demnach zumindest für Privatnutzer nicht.

(3) System- und Programmupdates

302 Ein weiteres großes Sicherheitsproblem stellen Lücken im Betriebssystem oder Teilen desselben dar. Aufgrund der hohen Komplexität von Betriebssystemen bzw. Programmen sind Fehler nicht auszuschließen.[584] Einerseits können lokal ausgeführte Programme solche Lücken nutzen, um ihre Zugriffsrechte auf dem Computersystem unbefugt zu erhöhen, andererseits können solche Lücken durchaus auch von außen über ein Netzwerk bzw. das Internet ausgenutzt werden. Damit sind System- und Programmupdates eine Abwehrmaßnahme auch gegen Trojaner. Indem z.B. Webseiten speziell präpariert werden und einen Fehler in einem Programm auslösen, können sie eigene Computeranweisungen ausführen, die z.B. ein Virus oder andere Malware installiert. Schließlich besteht die Möglichkeit, dass eine nicht ausführbare Datei, beispielsweise ein Bild oder eine Musikdatei so präpariert wird, dass ein Fehler im Programm hervorgerufen wird, der ebenso ausgenutzt wird. Das angreifende „Programm“ erwirbt damit automatisch

582 Vgl. zur automatischen Anpassung der Regeln mittels Intrusion Detection-Systemen und der anschließenden Einschränkung von Diensten BSI, IT-Grundschutzhandbuch 2005, M 5.71 (2747); zu den möglichen Folgen von bestimmten Freigaben der Firewall *Klapdor*, VW 2005, 507.

583 Nur für kommerzielle Nutzer *Schneider/Günther*, CR 1997, 389 (394).

584 OLG Hamburg CR 1986, 83 (84); LG Heidelberg CR 1989, 197 (198); *Gorny*, CR 1986, 673 (675); *Engel*, CR 1986, 702 (708); *Bömer*, CR 1989, 361; *Taeger*, Außervertragliche Haftung für fehlerhafte Computerprogramme, 1995, S. 37, 40 f.; MünchKommBGB-*Wagner*, § 3 ProdHaftG Rn. 15; *Heussen*, CR 2004, 1 (3); mit Einschränkungen auch *Kilian*, CR 1986, 187 (190).

die Rechte des aktuellen Benutzers und kann weitere Programme nachinstallieren, die in dessen Benutzerkontext und mit seinen Rechten laufen. Falls auf der Anlage dann sogar noch Systemlücken bestehen, kann das Programm seine Nutzerrechte erhöhen und damit vollen Zugriff erlangen.[585] Zusätzlich kann es sich eventuell sogar vor Abwehrprogrammen verbergen.

303 Auch hier stellt das kompromittierte System eine Gefahrenquelle dar, die nur der Nutzer beherrschen kann. Es ist somit zu klären, ob dem Nutzer die Verkehrspflicht obliegt, solche Angriffe abzuwehren, indem er wichtige Systemupdates und Programmupdates beschafft und installiert. Während das Wissen über Viren relativ verbreitet ist, ist das Bewusstsein, dass auch ein gegen Viren geschütztes System durchaus verwundbar ist, beim durchschnittlichen privaten Nutzer noch kaum vorhanden. Anderes wird man aber dann annehmen müssen, wenn ein auf dem System laufender Dienst an Updates erinnert bzw. diese sogar automatisch oder halb-automatisch herunterlädt und installiert.[586] In diesem konkreten Fall kann von einer Bekanntheit und ebenso der technischen Zumutbarkeit ausgegangen werden.[587]

304 Aus Nutzersicht ist es zum Teil jedoch gar nicht erwünscht, dass jedes Programm, das er installiert hat, nach Updates fragt, da dadurch grundsätzlich auch die Gefahr besteht, dass Daten über das Nutzerverhalten oder ähnliches übertragen werden. Man könnte dann zwar eine Pflicht des Nutzers annehmen, sich selbst über vorhandene Updates zu informieren. Dies kann jedoch bei der Vielzahl der Programme nicht geleistet werden, zumal er häufig gar nicht weiß, dass eine Firewall oder ein ähnliches Programm den Internetzugriff des Programms unterdrückt.

305 Die wirtschaftliche Zumutbarkeit ist besonders bei größeren Updates schwierig zu beantworten, da diese über langsame Internetanbindungen bzw. Telefonleitungen auch hohe Kosten verursachen können.[588] Aus diesem Grunde sind auch größere Systemupdates durchaus wirtschaftlich zumutbar. Allerdings kann sich hier im Einzelfall durchaus eine Unzumutbarkeit ergeben, etwa wenn die Updates von Programmen derart umfangreich sind, dass sie mit einer (zu dem entsprechenden Zeitpunkt) verkehrsüblichen

---

585 Zu sog. Root-Kits, die eben diese Techniken verwenden, *Kühnhauser*, DuD 2003, 218 f.

586 Zu automatisierten Software-Updates *Probst*, DuD 2003, 508.

587 Ähnl. *Probst*, DuD 2003, 508: „Im Bereich der Endanwender kann die Automatisierung, dass die [...] aus Unwissenheit [...] unterbliebene Systemwartung überhaupt erfolgt."

588 Als Beispiel habe ein Update eine Größe von ca. 50 MB, der Nutzer hat ein normales Modem und überträgt damit ca. 5 KByte/s, wobei er bei seinem Internetprovider 3 Cent/min bezahlt. Die Übertragung wird ca. 3 Stunden benötigen und damit ca. 5 € kosten.

Datenverbindung nicht zu bewältigen sind, wie dies etwa noch für den Service Pack 2 für das Betriebssystem Windows XP der Fall war.

306 Im Ergebnis wird man unter Einbeziehung der durch ungesichterte private Rechner drohenden Schäden (Multiplikatorwirkung[589]) zumindest die Zumutbarkeit von wichtigen System-und Programmupdates bejahen müssen, die automatisiert oder halbautomatisch, also durch einen im System verankerten Update-Dienst, installiert werden können.

(4) Nutzung von Nutzerkonten mit eingeschränkten Rechten

307 Eine weitere Möglichkeit, die Gefahren zumindest zu minimieren, ist die Arbeit unter einem Benutzerkonto mit eingeschränkten Rechten.[590] Als Folge könnte ein erfolgreicher Angriff diejenigen eingeschränkten Nutzerrechte erlangen, sofern er nicht andere Lücken zur Erhöhung ausnutzt.[591] Damit kann eine dauerhafte Verankerung des Schadprogramms im System verhindert oder zumindest erschwert werden. Während bei Unix-Systemen die Arbeit als Nutzer die Regel ist, und nur in Ausnahmefällen Administratorrechte genutzt werden, ist dies bei Windows-Betriebssystemen anders. Hier arbeitet der Hauptnutzer regelmäßig mit Administratorrechten. Viele Programme sind auch ohne diese Rechte gar nicht lauffähig, so dass der Betrieb nur eingeschränkt möglich ist, wenn der Nutzer nicht ständig zwischen dem Administratorkonto und dem eingeschränkten wechseln will.

308 Diese Möglichkeit ist jedoch **keineswegs als weithin bekannt** einzustufen. Der Durchschnittsnutzer ist sich dieser Möglichkeit gar nicht bewusst und kann deshalb auch die entsprechenden Maßnahmen, die auch spezielle Anleitungen oder Expertenwissen und einigen Aufwand erfordern und damit auch technisch nicht zumutbar wären, nicht ergreifen. Es besteht somit keine Verkehrspflicht für private Nutzer, im Regelfall mit eingeschränkten Rechten zu arbeiten.

(5) Intrusion Detection-Systeme

309 In Erweiterung zu Firewalls dienen Intrusion Detection-Systeme der Erkennung von Angriffen, die auch aus dem internen Netzwerk unterstützt werden.[592] Sie überwachen

589 *Mankowski*, in: Ernst, Hacker, Cracker & Computerviren, Rn. 516.
590 S. dazu *Endres*, c't Archiv 23/2005, 112.
591 S.o. Rn. 85.
592 *Heibey*, in: Roßnagel, Handbuch Datenschutzrecht, Kap. 4.5 Rn. 133.

den Netzwerkverkehr sowie die Systemkonfiguration und melden dem Nutzer verdächtige Aktionen oder Veränderungen.[593] Intrusion Detection-Systeme sind allerdings bereits ihrer Bestimmung nach nur für größere Netzwerke geeignet. Die Anpassung an das jeweilige System sowie die entsprechende Überwachung erfordern jedenfalls Expertenwissen bzw. Kenntnis von der Funktionsweise der Kommunikation in Netzwerken. Beim Einsatz von Intrusion Detection-Systemen fallen in der Regel personenbezogene Daten an, die datenschutzrechtlichen Vorgaben sind demnach einzuhalten.[594] Unabhängig davon, ob diese Sicherungswerkzeuge also dem Durchschnittsnutzer bekannt sind, ist dem privaten Nutzer der Einsatz von Intrusion Detection-Systemen jedenfalls nicht technisch zumutbar.

(6) Malware-Entfernungsprogramme

310 Verfügbar sind auch Programme zur Entfernung von sog. Malware,[595] die sich bereits im System tatsächlich eingenistet hat. Dadurch kann insbesondere Schadensfällen bei Dritten – z.B. durch die Weiterverbreitung von Viren – vorgebeugt werden. Der Einsatz der entsprechenden Programme ist durchaus anwenderfreundlich. Zudem sind die Entfernungsprogramme meist kostenlos erhältlich. Zweifelhaft ist jedoch, ob die Existenz dieser Programme bereits so bekannt ist, dass auch dem normalen Nutzer der Einsatz zuzumuten ist. Mangels der notwendigen Bekanntheit ist der private Nutzer nicht verpflichtet, Malware-Entfernungsprogramme einzusetzen.

(7) Verhalten im E-Mail-Verkehr

311 Von den Verkehrspflichten des privaten Nutzers im technischen Bereich zu unterscheiden sind Verhaltenspflichten bei der Nutzung von E-Mail und Internet. So enthalten Spam-E-Mails häufig Anhänge, welche beim Öffnen unbemerkt ein Virusprogramm oder ein trojanisches Pferd auf dem Rechner des Nutzers installieren. Neben der Gefahr für den eigenen Datenbestand besteht hierbei die Möglichkeit der Weiterverbreitung des Schadprogramms auf andere Nutzer. Immer stärker in den Vordergrund tritt zudem gegenwärtig der Identitätsmissbrauch im Internet unter Verwendung von heimlich auf dem Rechner des Privatnutzers installierten Trojanern (s. dazu die Ausführungen zum Online-Banking Rn. 479 ff.).

---

593 S.o. Rn. 65.

594 Dazu eingehend BSI-Studie „Einführung von Intrusion-Detection-Systemen – Rechtliche Aspekte“, abrufbar unter: http://www.bsi.bund.de/literat/studien/ids02/dokumente/Rechtv10.pdf.

595 Zum Begriff s.o. Rn. 63, 68.

312 Auch der private Nutzer ist daher verpflichtet, **unbekannte und verdächtige Anhänge** im Zweifelsfall **ungeöffnet zu löschen** bzw. nur nach Verifizierung des Absenders zu öffnen. Das Wissen um die Bedrohungen durch E-Mail-Anhänge darf heute zum allgemeinen Kenntnisstand des durchschnittlichen Internetnutzers gezählt werden. Besondere IT-Kenntnisse sind zur Durchführung der Maßnahme nicht erforderlich. Eine allgemeine Pflicht, präventiv alle **E-Mails mit unbekanntem Absender zu löschen**, wird man demgegenüber **nicht** annehmen können, denn sie würde die E-Mail-Korrespondenz auf Bekannte beschränken und damit in ihrer Reichweite erheblich beschneiden. Auch wenn sich pauschale Aussagen verbieten, da Unternehmen im E-Mail-Verkehr mit privaten Nutzern Adressen durchaus wechseln, etwa wenn eine neue Domain erworben wurde, oder auch private Nutzer (als Korrespondenten) häufig ihre Adresse wechseln können, dürften doch meist bei privaten Nutzern seriöse E-Mails unbekannter Herkunft eher die Ausnahme und Spam-E-Mails die Regel bilden.

(8) Ergebnis

313 Zum jetzigen Zeitpunkt sind lediglich der Einsatz von Virenscannern sowie entsprechende Aktualisierungen als eine grundsätzliche Verkehrspflicht des Nutzers einzuordnen. Hinzu kommen grundlegende Verkehrspflichten im E-Mail-Verkehr.

3. Schadensminderungs- und Selbstschutzpflichten

314 Schließlich ist für die Verteilung der Verantwortungsbereiche das Ausmaß an Selbstschutz und Schadensabwendungspflichten des Geschädigten im Rahmen von § 254 BGB relevant,[596] für die die zuvor erörterten Pflichten quasi spiegelbildlich herangezogen werden können. Schädiger und Geschädigter sind im Grunde der gleichen Risikosituation ausgesetzt. Setzen beide keine entsprechenden Schutzmaßnahmen ein, so hängt es lediglich vom Zufall ab, welches System zuerst infiziert wird. Während also grundsätzlich eine Verkehrspflicht zum Einsatz von Virenscannern besteht, liegt eine gleichartige Pflicht nach § 254 BGB vor.[597]

---

596 Dabei kann die an sich von Gesetzes wegen vorgesehene Unterscheidung zwischen dem Mitverschulden des Geschädigten nach § 254 Abs. 1 BGB und seiner Schadensabwendungs- und -minderungspflicht nach § 254 Abs. 2 BGB offen bleiben, da insoweit Einigkeit darüber herrscht, dass § 254 Abs. 2 BGB nur einen besonderen Anwendungsfall des allgemeineren § 254 Abs. 1 BGB darstellt, vgl. MünchKommBGB-*Oetker*, § 254 BGB Rn. 68; Palandt-*Heinrichs*, § 254 BGB Rn. 32; *Lange/Schiemann*, Schadensersatz, § 10 X 1; der Streit um die dogmatische Einordnung des § 254 BGB (näher dazu *Greger*, NJW 1985, 1130 ff.) spielt hier keine Rolle.

597 *Spindler*, CR 2005, 741 (744); *Schneider/Günther*, CR 1997, 389 (394); *Libertus*, MMR 2005, 507 (511); *Koch*, NJW 2004, 801 (804); *Schmidbauer*, abrufbar unter: http://www.i4j.at/news/aktuell36.htm; iE *Mankowski*, in: Ernst, Hacker, Cracker und Computerviren, Rn. 530 f.

a) Warnpflichten des Geschädigten

315 § 254 Abs. 2 Satz 1 BGB hält ausdrücklich dazu an, den Schuldner (bzw. Schädiger) auf die Gefahr eines ungewöhnlich hohen Schadens aufmerksam zu machen, die der Schuldner weder kannte noch kennen musste, damit dieser in die Lage versetzt wird, dem Schaden seinerseits zu begegnen.[598] Die Pflicht zur Warnung entsteht für den Geschädigten aber nur dann, wenn er selbst Schädigung und Schadenshöhe vorhersehen kann[599] und er bessere Erkenntnismöglichkeiten als der Schädiger hat.[600] Für IT-Sicherheitslücken kommt dies vor allem dann zum Tragen, wenn allgemein erhältliche, anwendungsneutrale Software, wie Office- oder Betriebssysteme, zum Einsatz in Bereichen mit Gefährdungspotential für hochrangige Rechtsgüter kommen. Denn einerseits hat der Hersteller (nicht der Händler!) oftmals keine Kenntnis von dem jeweiligen Gefährdungspotential seines Produktes; andererseits sind grundsätzlich die Gefahren durch einem breiten Publikum[601] bekannt gewordene IT-Sicherheitslücken dem Nutzer erkennbar. Stets aber muss die Verletzung der Warnpflicht nach § 254 Abs. 2 Satz 1 BGB ursächlich für die Entstehung des Schadens und der Schadenshöhe sein; hätte der Schädiger die Warnung nicht beachtet[602] oder keine Maßnahmen ergreifen können, trifft den Geschädigten auch nicht der Vorwurf nach § 254 Abs. 2 Satz 1 BGB. Die Beweislast hierfür obliegt dem Geschädigten.[603]

b) Selbstschutzpflichten

316 Der Pflicht zur Erfassung der Risiken und der Einleitung von Maßnahmen zur Problembewältigung entspricht die allgemeine Pflicht des Softwarebenutzers zum Selbstschutz.[604] So könnte der IT-Anwender gehalten sein, die allgemein üblichen Vorkehrungen zum Viren- und Wurmschutz zu treffen, indem er Virenscanner bei sich einsetzt und auf dem Laufenden hält.[605] Die Missachtung dieser etwaigen Pflichten würde folgerichtig ein Mitverschulden gemäß § 254 BGB begründen.

---

598 So BGH VersR 1960, 526 (527).

599 Vgl. BGH VersR 1964, 950 (951); Staudinger-*Schiemann*, § 254 BGB Rn. 76; MünchKommBGB-*Oetker*, § 254 BGB Rn. 70.

600 BGH VersR 1953, 14; *Lange/Schiemann*, Schadensersatz, § 10 IX 2.

601 Hier gelten spiegelbildlich die Anforderungen wie zu den Warnpflichten des Herstellers. Allein das Bekanntwerden in einschlägigen Fachkreisen oder EDV-Zeitschriften genügt nur bei Nutzern mit einschlägigen Kenntnissen oder EDV-Abteilungen.

602 BGH NJW 1989, 290 (292).

603 BGH VersR 1996, 380 (381).

603 BGH DB 1956, 110 f.; Palandt-*Heinrichs*, § 254 BGB Rn. 74.

604 Ähnl. *v. Westphalen*, PHI 1998, 222 (223)

605 *Burg/Gimnich*, DRiZ 2003, 381 (384 f.); *Günther*, Produkthaftung für Informationsgüter, 303 f.; *Schnei-*

317 Zur Feststellung einer solchen Pflicht zum Selbstschutz sind die eingangs dargestellten Kriterien bzgl. der Pflichtenbestimmung im IT-Bereich maßgeblich. Demnach sind die berechtigten Sicherheitserwartungen des Verkehrs und der zumutbare Aufwand für die Bestimmung der Selbstschutzpflichten entscheidend. Es ist eine wertende Interessenabwägung vorzunehmen, bei der das Ausmaß der drohenden Gefahr, sowie die Möglichkeit und Zumutbarkeit der Gefahrenvermeidung auf Seiten des Gefahrverursachers und des Selbstschutzes auf Seiten des Gefährdeten unter Berücksichtigung von Vertrauensschutzgesichtspunkten gewichtet werden müssen.[606] Unter Berücksichtigung dieses Maßstabs wird angesichts des allgemein bekannten Risikos von Computerviren und der geringen Kosten für die Einrichtungen eines aktuellen Virenschutzprogramms teilweise ausdrücklich auch für Privatpersonen die Zumutbarkeit von Selbstschutzmaßnahmen bejaht und eine Schadensbegrenzungspflicht angenommen.[607]

318 Für eine solche Verpflichtung privater IT-Nutzer spricht insbesondere der Umstand, dass das Ausmaß des drohenden Schadens entscheidend von der dem IT-Hersteller regelmäßig unbekannten Tatsache abhängt, welche Daten sich auf der verwendeten Hardware befinden und wofür diese benutzt werden.[608] Der IT-Anwender kann folglich das Schadensrisiko wesentlich besser abschätzen und durch entsprechende Vorkehrungen auffangen. Richtigerweise ist allerdings unter Bezugnahme auf das Kriterium der Zumutbarkeit der Gefahrenvermeidung zwischen den verschiedenen IT-Anwendern zu differenzieren: Während professionellen IT-Anwendern bei entsprechenden Kenntnissen und Ressourcen derartige Selbstschutzmaßnahmen zumutbar sind,[609] sind die Voraussetzungen bei privaten IT-Nutzern höher. Der Einsatz von Virenscannern ist ihnen aber zuzumuten (oben Rn. 297).

319 Neben dem Zumutbarkeitskriterium kann hier als maßgeblicher Anknüpfungspunkt für diese Differenzierung auch der Gedanke der **Vorteilsziehung** herangezogen werden: Nicht alle IT-Anwender nutzen Softwareprodukte in gleichem Maße und profitieren dementsprechend davon. Der Gedanke der Vorteilsziehung ist in Rechtsprechung und Lehre gleichermaßen als Anknüpfungspunkt zur Bestimmung von Art und Ausmaß der

---

der/Günther, CR 1997, 389 (394); *Koch*, NJW 2004, 801 (804 ff .); *Schmidbauer*, Schadensersatz wegen Viren, abrufbar unter http://www.i4j.at/news/aktuell36.htm (zuletzt abgerufen am 22.2.2006).

606 Vgl. *Koch*, NJW 2004, 801 (804); *Libertus*, MMR 2005, 507 (509).

607 So bezüglich der Risiken im E-Mail-Verkehr: *Koch*, NJW 2004, 801 (807): In Anlehnung an die Rechtsfigur der Betriebsgefahr im Straßenverkehr will der Autor einen Mitverschuldensanteil von 25 % bei ungenügenden Virenschutzvorkehrungen veranschlagen.

608 *Koch*, NJW 2004, 801 (804 f.); *Libertus*, MMR 2005, 507 (509).

609 S. unten Rn. 375 ff.

Verkehrspflichten, sowie als Rechtfertigungsgrund zur haftungsrechtlichen Ungleichbehandlung von Privaten und Unternehmern anerkannt.[610] Letztere profitieren in besonderem Maße vom Einsatz von Software und erlangen somit nicht unerhebliche betriebswirtschaftliche Vorteile. Insofern ist unter Berücksichtigung des Gedankens der Vorteilsziehung bzgl. der Bestimmung der Selbstschutzpflichten des Softwarebenutzers folgerichtig zwischen professionellen IT-Anwendern und privaten IT-Anwendern zu unterscheiden. Privaten Softwarebenutzern ist demnach eine Pflicht zu Selbstschutzmaßnahmen unter anderen Voraussetzungen aufzuerlegen.

320 Diese Rechtsauffassung hat der BGH auch in seinem Urteil zu Mehrwertdiensten hinsichtlich einer Pflicht zum Einsatz von Dialerschutzprogrammen deutlich zum Ausdruck gebracht, indem er ausgeführt hat, dass privaten IT-Nutzern eine routinemäßige Überprüfung auf Dialer ohne besondere Verdachtsmomente sowie die Überwachung des Aufbaus von Verbindungen ins Internet nicht obliege.[611] Des Weiteren hat er klargestellt, dass privaten IT-Nutzern keine Pflicht zur Verwendung und Aktualisierung eines Dialerschutzprogrammes treffe.[612] Anders ist dies aber zu beurteilen, wenn die Gefahr sowie die Lösung allgemein bekannt sind. Demgemäß entfällt die Pflicht zu Selbstschutzmaßnahmen zumindest bei privaten Softwarenutzern, wenn nicht Problem und Lösung bekannt und die Ergreifung technisch und wirtschaftlich zumutbar ist.[613]

321 Bei Programmen mit bekannten Sicherheitslücken muss der Nutzer, insbesondere ein Unternehmen, dieses Programm sperren und darf es nicht mehr einsetzen. Benutzt er dennoch sehenden Auges die fehlerhafte Software und entstehen hierdurch aufgrund von Hackerangriffen Schäden, so kann sich ein völliger Ausschluss des Schadensersatzanspruchs ergeben.[614]

322 Schließlich sind Nutzer grundsätzlich auch zum Einspielen von kostenlos zur Verfügung gestellten **Patches** verpflichtet, so dass sich der Hersteller (bzw. Pflichtige) in der Regel auf ein Mitverschulden des Geschädigten berufen kann, wenn dieser einen Patch nicht verwandt hat. Allerdings kann dies nicht uneingeschränkt gelten, da manche Pat-

610 BGHZ 5, 378 (384) = NJW 1952, 1050; BGH LM Nr. 10 zu § 823 (Db) BGB; *v. Bar*, Verkehrspflichten, S. 126 mwN.; s. auch *Raab*, JuS 2002, 1041 (1044 f.).

611 BGH NJW 2004, 1590 (1592) = JZ 2004, 1124 (1127) m. Anm. *Spindler*; s. auch die parallelen Erwägungen des BGH im Fall der R-Gespräche, BGH NJW 2006, 1971 Tz. 22 ff. = MMR 2006, 453, 456, in concreto Zumutbarkeit von Eigenschutzmaßnahmen abgelehnt.

612 Zust.: *Spindler*, JZ 2004, 1128 (1128 ff.); *Rösler*, NJW 2004, 2566 (2566 ff.); *Mankowski*, MMR 2004, 312 (312 f.); *ders.* CR 2004, 185 (188).

613 S. o. Rn. 275 ff.

614 *Bartsch*, Software und das Jahr 2000, S. 86.

ches einen derartigen Umfang haben, das sie selbst bei breitbandigen Internet-Zugängen kaum herunterladbar sind, etwa das Service Pack 2 für Windows XP. Stellt hier der Hersteller aber kostenlos eine CD zur Verfügung, greifen die entsprechenden Beschränkungen für die Pflichten des Herstellers ebenfalls.

c) Schadensabwendungspflichten

323 Eher die Ausnahme sind Pflichten des Softwarenutzers, insbesondere gewerblicher, etwaigen Schäden durch eine eigenständige Bearbeitung des Programms zuvorzukommen, da ihnen oftmals nicht der Quellcode bekannt ist, und sie zudem das Risiko eingehen, mit urheberrechtlichen Beschränkungen durch den Softwarehersteller konfrontiert zu sein. Zwar darf nach § 69d I UrhG der Nutzungsberechtigte Bearbeitungen am Programm im Rahmen einer bestimmungsgemäßen Nutzung vornehmen, worunter auch die Fehlerbeseitigung fällt.[615] Doch kann aus dieser Erwägung nicht generell die Pflicht des Softwarebenutzers abgeleitet werden, auf eigenes Risiko hin Fehler im Programm zu beheben. Eine Ausnahme wäre nur dann gegeben, wenn die drohenden Schäden in keinem Verhältnis mehr zu den möglichen Risiken einer Urheberrechtsverletzung stehen, der Geschädigte über dem Hersteller gleichwertige Kenntnisse verfügt und das Programm nicht ohne Weiteres ausgetauscht werden kann.

324 **Ebensowenig** ist dem Softwarenutzer zuzumuten, zur Schadensabwendung die **neueste Version einer Software zu kaufen**, die keine IT-Sicherheitslücken mehr aufweist. Eine solche Pflicht zum Update-Kauf würde letztlich die Verantwortung für einen Schaden von der Entscheidung des Herstellers abhängig machen, ein neues, verbessertes Produkt auf den Markt zu bringen.[616] Anders ist dies nur zu beurteilen, sofern eine starke Gefährdungslage besteht und dem Nutzer keine andere Möglichkeit verbleibt, als die Software zu ersetzen.

325 Ein in der Praxis offenbar weit verbreitetes Phänomen ist die **zeitliche Verzögerung,** mit der Firmennetzwerke durch das Einspielen **von Patches** gesichert werden, und die Dritten in der Zwischenzeit entsprechende Angriffe ermöglichen. Auch hier ist zu berücksichtigen, dass gerade Unternehmen eine Organisationspflicht trifft, auftretende Si-

---

615 OLG Karlsruhe NJW 1996, 2583 (2584); Schricker-*Loewenheim*, § 69d UrhG, Rn. 9; *Schneider*, Handbuch des EDV-Rechts, C Rn. 200 ff.; *Haberstumpf*, in: Lehmann, Rechtsschutz und Verwertung von Computerprogrammen, Kap. II Rz. 159, 169; für das schweizerische Recht *Rigamonti*, SJZ 1998, 430 (433).

616 Zum Vorteilsausgleich, wenn der Hersteller dem Nutzer ein verbessertes Paket mit erweiterter Funktionalität zur Verfügung stellt, um den Fehler zu beheben, s. näher *Spindler*, NJW 1999, 3737 (3744) mwN.

cherheitsprobleme möglichst schnell zu bewältigen, um den Schaden gering zu halten. Natürlich können Sicherheitspatches nicht in jedem Fall unbesehen einfach auf alle PCs eines Netzwerkes aufgespielt werden; dennoch muss der unternehmerische Nutzer von Software seinerseits alles Zumutbare veranlassen, um Sicherheitslücken mit Hilfe von Sicherheitsupdates zu stopfen. Dies umfasst auch die durch den Einsatz von ungesicherten Laptops drohende Gefahr für Netzwerke; hier sind Netzwerkbetreiber gehalten, entsprechende Vorkehrungen gegen den Anschluss nicht gesicherter Notebooks zu treffen, sei es durch Kontrollen oder Sicherung solcher Geräte oder des Netzwerks.

d) Schadensminderung

326 IT-Sicherheitslücken und dadurch bedingte Angriffe durch Hacker mit der Folge von Datenverlusten werfen die Frage auf, zu welchen Schadensminderungsmaßnahmen der Nutzer verpflichtet ist. Dies lässt sich pauschal kaum beantworten, hängt es doch wiederum vom Gefahrenpotential, dessen Wahrscheinlichkeit und dem Rang der betroffenen Rechtsgüter ab,[617] ob etwa der Nutzer, z.B. ein Krankenhaus, gehalten ist, Reservesysteme vorzuhalten. Oftmals entsteht aber auch bei diesen Systemen das Problem, dass sie dieselben Programme verwenden (müssen), so dass auch hier die IT-Sicherheitslücke fortbesteht. In der Regel wird der Hersteller daher nicht den Nutzer auf den Einsatz von Reservesystemen bei IT-Sicherheitsproblemen[618] verweisen können. Für Daten ist indes inzwischen anerkannt, dass eine regelmäßige Datensicherung der gebotenen Pflicht zur Schadensminderung entspricht, bei deren Verletzung ein Schadensersatzanspruch vollständig entfallen kann.[619]

4. Beweisfragen

327 Nach allgemeinen Grundsätzen trägt der Geschädigte die Darlegungs- und Beweislast für die haftungsbegründenden Voraussetzungen, im Rahmen des § 823 Abs. 1 BGB also

---

617 Für den Jahr-2000-Fehler: *Wohlgemuth*, MMR 1999, 59 (65); allg. und zu den sich in der Rechtsprechung herausgebildeten Fallgruppen: MünchKommBGB-*Oetker*, § 254 BGB Rn. 76 ff.; Bamberger/Roth-*Unberath*, § 254 Rn. 30 ff., jeweils mwN.

618 Anders natürlich bei Hardware-Problemen, s. etwa OLG Hamm NJW-RR 1998, 380 (381) für einen ausgefallenen Drucker.

619 OLG Hamm JurPC Web-Dok. 165/2004 Abs. 2, 14; OLG Karlsruhe NJW 1996, 200 (201); OLG Karlsruhe NJW-RR 1997, 554 (554 f.); *Erben/Zahrnt*, CR 2000, 88 f.; *Günther*, Produkthaftung für Informationsgüter, 303 f.; *Meier/Wehlau*, NJW 1998, 1585 (1590) mwN; zur Frage, ob Vertrauensschutz entsprechende Pflichten aufgrund vorherigen Handelns begründen kann, die dann auch Stillstandskosten umfassen würden, BGH NJW 1998, 456 (458), übertragen auf Datensicherung im IT-Bereich könnte also bei entsprechendem Vertrauen aufgrund vorhergegangener ständiger Datensicherungen ein entsprechendes Mitverschulden wegen Unterlassung der Schadensminderung in Form der Datensicherung angebracht sein. Da bei der Haftung nach § 823 Abs. 1 BGB jedoch regelmäßig kein vorheriger Kontakt besteht, kann auch kein solches Vertrauen vorliegen.

insbesondere für Verkehrspflichtverletzung und Verschulden.[620] Die Rechtsdurchsetzung im Schadensfall hängt zunächst davon ab, die **Person des Schädigers** eindeutig zu identifizieren, was im Internet indessen unter Umständen auf erhebliche Schwierigkeiten stößt.[621] Auch wenn der Schädiger bekannt sein sollte, wird dieser seinen Wohnsitz oftmals im Ausland haben, so dass eine Rechtsverfolgung in der Praxis häufig unterbleiben wird. Bei Weiterverbreitung von Viren im E-Mail-Anhang eines Bekannten, Freundes oder Geschäftspartners mag der Nachweis gelingen. Der Absender von Spam-E-Mails oder die Initiatoren von Denial-of-Service-Attacken können demgegenüber im Regelfall nicht ohne weiteres ermittelt werden, da fremde E-Mail-Adressen und Rechner benutzt werden. Allgemeine Auskunftsansprüche privater Nutzer oder Unternehmen gegen Telekommunikationsunternehmen oder Internet-Provider zur Ermittlung des Absenders bestehen derzeit nicht.[622] Auskunftsberechtigt sind die Strafermittlungsbehörden, so dass bei strafbaren Handlungen im Einzelfall eine Akteneinsicht durch den Anwalt des Geschädigten und eine Beiziehung staatsanwaltlicher Ermittlungsakten im Zivilprozess in Betracht kommt. Oftmals wird die Inanspruchnahme privater Nutzer jedoch schon an der Identifikation der Person des Schädigers scheitern.

328 Auch wenn ein privater Nutzer eindeutig als Verursacher des Schadens identifiziert ist, hat der Geschädigte den Beweis einer **Pflichtverletzung** durch den Nutzer zu führen. Hierbei handelt es sich um Vorgänge, welche sich in der Sphäre des privaten Nutzers abspielen, in welche der Geschädigte keinen Einblick hat. Der Nachweis, dass ein privater Nutzer unter Verletzung von Sorgfaltspflichten einen E-Mail-Anhang geöffnet und so die Installation eines Virus oder Trojaners ermöglicht hat, wird daher nur schwer zu führen sein. Möglich wäre hier aber eine Untersuchung des Computers des Schädigers auf dem sich die E-Mail noch befindet. Hierzu kann das Gericht die Vorlage des Computers zur Einnahme des Augenscheins und sowie zur Begutachtung durch einen Sachverständigen anordnen (§§ 144 Abs. 1 Satz 2, 371 Abs. 2 ZPO). Ebenso kann so im Einzelfall das Vorhandensein und die regelmäßige Aktualisierung des Virenschutzes überprüft werden. Dies hilft aber dann nicht weiter, wenn der Rechner neu aufgesetzt wurde oder gar keine Protokolle über die Aktualisierung des Betriebssystems oder des Virenschutzes geführt wurden. Nur in Fällen der Beweisvereitelung kann die Behaup-

620 Palandt-*Sprau*, § 823 BGB Rn. 80; Bamberger/Roth-*Spindler*, § 823 BGB Rn. 280.
621 S. dazu auch *Mankowski* in: Ernst, Hacker, Cracker & Computerviren, Rn. 510, 513.
622 Für die Verletzung von Immaterialgüterrechten enthält § 14 Abs. 2 TMG eine Sonderregelung.

tung des Geschädigten gemäß § 371 Abs. 3 ZPO als bewiesen angesehen werden.[623] Beim Beweis des **Mitschuldens des Geschädigten** stellen sich spiegelbildlich dieselben Probleme, denn die hM und ständige Rechtsprechung bürden dem Schädiger die Beweislast für das Mitverschulden auf.[624]

5. Ergebnis

329 Für private Nutzer lassen sich zwar Pflichten hinsichtlich der Ergreifung von Sicherungsmaßnahmen herleiten. Diese sind mangels der Bekanntheit von Problem und Lösung allerdings stark bzw. auf die Einhaltung allseits bekannter Schutzmaßnahmen eingeschränkt. Standards oder Regelwerke, anhand derer für private IT-Nutzer diese Pflichten konkretisiert werden könnten, sind – soweit ersichtlich – nicht vorhanden. Auch wenn sich begrenzte Verkehrspflichten privater Nutzer entwickeln lassen, ergeben sich in der Praxis zum Teil erhebliche Probleme die Person des Schädigers zu identifizieren und die Pflichtverletzung zu beweisen.

330 Insbesondere mit den aufgezeigten Durchsetzungsproblemen mag zusammenhängen, dass bislang keine Fälle der Inanspruchnahme privater Nutzer bekannt geworden sind. Zu Recht wird daher darauf hingewiesen, dass die Ansprüche des Geschädigten oftmals nur auf dem Papier bestehen.[625] Für geschädigte Private gehen die Beweisschwierigkeiten mit dem Prozesskostenrisiko (insbesondere Sachverständigenkosten) einher, welche oftmals zudem in keinem vernünftigen Verhältnis zum Schaden stehen werden. Im Zusammenhang mit Viren usw. dürfte hinzukommen, dass private Nutzer diese Erscheinungen als letztlich nicht vollständig vermeidbares Risiko der Internetnutzung hinnehmen, ohne gegen den Verursacher vorzugehen. Bei geschädigten Unternehmen drohen regelmäßig hohe Schadenssummen, jedoch wird dann neben den Schwierigkeiten der prozessualen Rechtsdurchsetzung die mangelnde Beitreibbarkeit der Schadenssumme eine Rechtsverfolgung häufig nicht lohnen.[626] Gleichfalls werden Unternehmen die mit der Rechtsverfolgung verbundene Offenbarung von Sicherheitslücken scheuen.[627] Umgekehrt wäre eine Belastung der Nutzer mit praktisch kaum vorhersehbaren – und damit auch kaum versicherbaren Haftungsrisiken – wenig effizient. Eine Haftung privater

623 Dazu Zöller-*Greger*, § 371 ZPO Rn. 5; Musielak-*Huber*, § 371 ZPO Rn. 20.

624 BGH NJW-RR 2001, 1542 (1543); BGH NJW 2000, 664 (667); BGH NJW 1998, 3706 (3707); BGHZ 90, 17 (32 f.); BGHZ 91, 243 (260); RGZ 159, 257 (261); *Lange/Schiemann*, Schadensersatz, § 10 XIX; MünchKommBGB-*Oetker*, § 254 BGB Rn. 145.

625 *Mankowski*, in: Ernst, Hacker, Cracker & Computerviren, Rn. 510.

626 So auch *Mankowski*, in: Ernst, Hacker, Cracker & Computerviren, Rn. 510.

627 *Mankowski*, in: Ernst, Hacker, Cracker & Computerviren, Rn. 513.

Nutzer wegen Verletzung von Sorgfaltspflichten erscheint gegenwärtig im Rahmen von Vertragsverhältnissen im Bereich des E-Commerce am wahrscheinlichsten. Siehe dazu ausführlich unten zum Online-Banking Rn. 522 ff.

III. Einsatz von IT bei kommerziellen Unternehmen als Nutzer

1. Überblick

331 Bei kommerziellen Nutzern von Ist-Anlagen stellt sich die Lage anders dar. Als kommerzielle Nutzer können – negativ abgegrenzt – alle diejenigen gelten, die nicht privater Nutzer sind, wobei auch hier eine rollenspezifische bzw. funktionale Betrachtungsweise maßgeblich ist. Für bestimmte Bereiche existieren ausdrückliche Regelungen bzw. Regelungen, die die IT-Nutzung unter Auslegung der Norm erfassen könnten. Hinzu können deliktische Ansprüche bei Nichtergreifung der geregelten Pflichten kommen, sofern sie als Schutzgesetz i.S.d. § 823 Abs. 2 BGB einzuordnen sind. Weiter können auch im Rahmen der Haftung nach § 823 Abs. 1 BGB bei kommerziellen Nutzern allgemeine Verkehrssicherungspflichten bestehen, wobei sich der Pflichtenmaßstab von demjenigen bei privaten IT-Nutzern durchaus unterscheiden kann. Diese Pflichten gelten wiederum spiegelbildlich im Bereich der nach § 254 BGB den kommerziellen IT-Nutzern abzuverlangenden Selbstschutzpflichten, die oftmals im Bereich der Organisation besonders konkretisiert sind.

2. Gefahrenpotential und Gegenmaßnahmen

332 In der Regel liegen bei kommerziellen Nutzern unternehmenswichtige Daten vor, die entweder den Betrieb selbst bzw. dessen Organisation oder Umstände der Beziehungen zu den Kunden betreffen. Verlust oder Manipulation dieser Daten können demnach auch das gesamte Unternehmen bedrohen. Hinzu kommt, dass mit der zunehmenden Vernetzung gerade in größeren Unternehmen viele Akteure die Kommunikation bestimmen. Die Angriffsfläche ist damit häufig größer als bei einzelnen Privaten. Dementsprechend aufwändiger ist dann auch die Ergreifung von Gegenmaßnahmen.

3. Anforderungen an die kommerziellen Unternehmen

333 IT-Riskmanagementpflichten können sich sowohl aus allgemeinen gesellschafts- und wirtschafts- wie zivilrechtlichen Vorschriften als auch aus datenschutzrechtlichen Regelungen ergeben. Im Folgenden werden zunächst die relevanten Einzelvorschriften dargestellt. Dabei sind der Hintergrund der Regelung, die daraus resultierenden Pflichten und der Adressat, die möglichen Rechtsfolgen und die Anhaltspunkte für IT-

Konkretisierung von Interesse. Anschließend erfolgt eine Gesamtbetrachtung der Vorschriften.

a) Gesellschafts-, wirtschafts- und allgemein zivilrechtliche Anforderungen

334 Praktisch für (fast) alle kommerziellen IT-Nutzer können Pflichten verallgemeinert werden, die aus allgemeinen handels- und gesellschaftsrechtlichen Pflichten abgeleitet werden. Allerdings gelten diese Pflichten zunächst allein im Innenverhältnis zwischen den Organen und der juristischen Person; sie können nicht ohne weiteres auf das Außenverhältnis übertragen werden (sei es für Schädigungen Dritter, sei es für die Konkretisierung von § 254 BGB). Dennoch geben sie wichtige Anhaltspunkte auch für entsprechende Selbstschutzpflichten, da oftmals organisatorische Anforderungen in Rede stehen, die quasi vom Innen- auf das Außenverhältnis übertragen werden. Als Reaktionen auf verschiedene Firmenzusammenbrüche sowohl in den USA als auch in Deutschland sind zudem seit 1998 die Anforderungen an das unternehmensinterne Management gesetzlich verankert, teilweise auch verschärft worden – was auch Auswirkungen auf das IT-Management im Unternehmen hat. Neben den deutschen Vorschriften zum Riskmanagement sind hier in erster Linie der von den beiden US-Kongressabgeordneten Paul Sarbanes und Michael Oxley angeregte amerikanische Sarbanes-Oxley-Act (SOX) ebenso wie die Regelwerke zur Prüfung von Fremdkapital (Basel II) zu nennen. Demgemäß werden zunächst die im Rahmen der Corporate Governance entwickelten IT-Riskmanagementpflichten betrachtet (Rn. 335 ff.), einschließlich der mittelbar aus den neuen Fremdkapitalvergabevorschriften (Basel II) folgenden Vorgaben (Rn. 357 ff.), anschließend dann die jeweiligen Selbstschutz- bzw. Verkehrssicherungspflichten (Rn. 375 ff.).

(1) IT-Riskmanagement als Geschäftsleiterpflicht

(a) Hintergrund

335 Die Steuerung von Risiken beim Softwareeinkauf und -einsatz war seit jeher ein Thema überwiegend der Betriebswirtschaft. Softwarepflege, gemeinsame Projektrealisierung[628] und -implementierung dominier(t)en die Themenpalette.[629] Erst mit Einführung des § 91 Abs. 2 AktG durch das KonTraG 1998 ist die rechtlich verbindliche Pflicht der

628 S. etwa *Müller-Hengstenberg*, CR 2005, 385 ff., *Schneider*, CR 2000, 27 ff., *Karger*, ITRB 2004, 208 ff. zu entsprechenden Vertragsgestaltungen bei der Projektsteuerung und Projektrisiken.

629 Vgl. hierzu *Schneider*, Handbuch des EDV-Rechts, Kap. E Rn. 29 ff.; sowie im Zusammenhang mit AGB Kap. E II.

Geschäftsleitung – auch der GmbH[630] – zur Einrichtung eines Risikomanagements für alle Geschäftsfelder deutlicher in das Bewusstsein gerückt,[631] teilweise noch durch eine – dem deutschen Recht bislang fremde und nur in § 130 OWiG verankerte – Unternehmensstrafbarkeit für Organisationsmängel. Damit gehören im Prinzip auch der Einkauf und die Implementation von Software zu dem Bereich, dessen Risikopotentiale abgeschätzt und gesteuert werden müssen.

(b) Pflichten und Adressat

336 Die allgemeinen Anforderungen des § 91 Abs. 2 AktG verpflichten den Vorstand dazu, für eine Organisation und ein Managementsystem zu sorgen, das möglichst frühzeitig Risiken zu erkennen vermag, die die Existenz des Unternehmens bedrohen können.[632] Entsprechende Vorkehrungen müssen sowohl durch Festlegung von Zuständigkeiten als auch durch Verfahren getroffen werden. So müssen eindeutig Verantwortlichkeiten und Berichtswege bestimmt werden, um zu verhindern, dass keiner sich für bestimmte Risiken zuständig fühlt; ebenso muss klargestellt werden, wann und wie die Geschäftsleitung von bedeutsamen Vorfällen erfährt, um rechtzeitig darauf reagieren zu können.[633] Verfahrensmäßige Vorkehrungen bestehen oftmals aus Checklisten, die einzuhalten sind, um typische Risiken aufzufangen und um sich ihrer bewusst zu werden, oder aus Abstimmungsverfahren mit anderen Abteilungen, damit nach einem Vier-Augen-Prinzip eine gegenseitige Kontrolle gewährleistet wird.[634]

337 Der Bereich der IT-Sicherheit ist nicht ausdrücklich vom Wortlaut des § 91 Abs. 2 AktG erfasst. Insofern kommt der Auslegung der Norm entscheidende Bedeutung zu. Um die inhaltlichen Anforderungen richtig zu erfassen, ist insbesondere auch der Hintergrund der Herausbildung von Risk-Management-Systemen im Bereich des Kreditwe-

---

630 Zwar fehlt es hier an einer entsprechenden Regelung in §§ 35, 43 GmbHG, doch ist es allg. M., dass § 91 Abs. 2 AktG jedenfalls sinngemäß darauf angewandt werden kann, s. dazu *Drygala/Drygala*, ZIP 2000, 297 (301); *Hommelhoff*, in: FS Sandrock, 373 ff.; *Altmeppen*, ZGR 1999, 291 (300 ff.); *Bockslaff*, NVersZ 1999, 104 (109).

631 Schon zuvor bestanden in zahlreichen Einzelgebieten Pflichten zur ordnungsgemäßen Organisation und zum Risikomanagement, umfassend dazu *Spindler*, Unternehmensorganisationspflichten, 2001, passim.

632 *Spindler*, in: Fleischer, Handbuch des Vorstandsrechts, § 19 Rn. 8 ff.; *Seibert*, in: FS Bezzenberger, 427 (437); *Fleischer*, AG 2003, 291 (298); *Zimmer/Sonneborn*, in: Lange/Wall, § 1 Rn. 180 f.; *Becker/Janker/Müller*, DStR 2004, 1578 (1579); *Hauschka*, AG 2004, 461 (467 f.); *Becker/Janker/Müller*, DStR 2004, 1578 (1579); *Schwintowski*, NZG 2005, 200 (201); *Roth/Schneider*, ITRB 2005, 19; MünchKommAktG-*Hefermehl/Spindler*, § 91 AktG Rn. 14 ff. mwN.

633 Begr. RegE BT-Drucks. 13/9712, 15; *Zimmer/Sonneborn*, in: Lange/Wall, § 1 Rn. 181; *Hüffer*, § 91 AktG Rn. 7; *Stober*, DÖV 2005, 333 (334).

634 Ausführlicher dazu *Spindler*, in: Fleischer, Handbuch des Vorstandsrechts, § 19 Rn. 25, 47; *Spindler*, Unternehmensorganisationspflichten, 2001.

sens (§ 25a KWG) zu beachten.[635] Insbesondere beinhaltet § 91 Abs. 2 AktG demnach eine einfache Organisationsanforderung und schreibt nicht etwa ein allgemeines Risikomanagement vor.[636] Zu überwachen sind etwa risikoträchtige Zustände oder Entwicklungen und die Einhaltung der eingeleiteten Maßnahmen, ob also das Veranlasste umgesetzt wird und Innenrevision und Controlling die von ihnen gewonnenen Kenntnisse zeitnah dem Vorstand weiterleiten. Die Vorstandsmitglieder der AG haften insofern gesamtschuldnerisch gem. § 93 Abs. 2 S. 1 AktG für die Einrichtung geeigneter Maßnahmen, „insbesondere" eines Überwachungssystems, zur Früherkennung bestandsgefährdender Entwicklungen.

338 **Entwicklungen** sind hier Veränderungen und Prozesse,[637] wobei zur Erkennung von Veränderungen die Erfassung des Ist-Zustandes und eine **Risikoabschätzung** unerlässlich sind. Nicht jede nachteilige Entwicklung muss frühzeitig erkannt werden. Vielmehr bezieht sich § 91 Abs. 2 AktG lediglich auf besondere, bestandsgefährdende Entwicklungen, also auf solche Veränderungen, die sich auf die Vermögens-, Ertrags- oder Finanzlage der Gesellschaft wesentlich auswirken können.[638] Schließlich bedeutet „frühzeitiges Erkennen", dass nachteilige Entwicklungen noch verhindert werden können und der Bestandsgefährdung noch effektiv entgegengewirkt werden kann.[639] Insgesamt ist somit dafür Sorge zu tragen, dass sowohl bestehende, als auch zukünftige, d.h. potenzielle Risiken kontrollierbar und kalkulierbar sind, was die möglichst vollständige Identifizierung von Ursachen und Ausmaß der Risiken impliziert.[640]

339 In diesem Zusammenhang sind ergänzend die auf europäischer Ebene unterbreiteten Vorschläge zur Stärkung der Überwachung der Directors bzw. des Vorstands zu erwähnen,[641] insbesondere der Vorschlag der Europäischen Kommission zur Modernisierung der Achten Gesellschaftsrechtlichen Richtlinie („Prüferrichtlinie")[642], der insbesondere die Einrichtung eines **Audit Committees** vorsieht. Das Audit Committee soll insbesondere zuständig sein für die Überwachung des Risikomanagements, sowie der Innenrevi-

635 MünchKommAktG-*Hefermehl/Spindler*, AktG, 2. Aufl. 2004, § 91 AktG Rn. 14 ff.

636 Zur Unterscheidung eingehend: *Hüffer*, AktG, 6. Aufl. 2004, § 91 AktG Rn. 9; MünchKommAktG-*Hefermehl/Spindler*, AktG, § 91 AktG Rn. 23 f.

637 MünchKommAktG-*Hefermehl/Spindler*, § 91 AktG Rn. 14 ff.

638 BegrRegE BT-Drucks. 13/9712, 7.

639 BegrRegE BT-Drucks. 13/9712, 15.

640 *Terlau*, CR 1999, 284 (286).

641 KOM (2003) 286: Mitteilung der Kommission an den Rat und das Europäische Parlament: Stärkung der Abschlussprüfung in der EU.

642 KOM/2004/0177 endg. Vom 16.3.2004, abrufbar unter: http://www.europarl.eu.int/oeil/file.jsp?id=241922.

sion und des internen Kontrollsystems. In Deutschland verfügen bereits fast alle börsennotierten Gesellschaften über Audit Committees in Form von Ausschüssen des Aufsichtsrates. Allerdings bezieht sich der Richtlinienvorschlag darüberhinaus auch auf sonstige Unternehmen des öffentlichen Interesses wie Banken und Versicherungen[643], so dass auch in diesen Branchen die Einrichtung eines solchen Gremiums vonnöten wäre. Der im Vorschlag der Kommission verankerte Aufgabenkatalog stimmt ansonsten im Wesentlichen mit den Vorgaben des Abschnittes 5.3.2 DCGK überein, geht aber in Art. 39 mit der Statuierung der Überwachung des internen Kontrollsystems und der Innenrevision darüber hinaus. Zudem konkretisiert der Richtlinienvorschlag die Vorgaben des § 91 Abs. 2 AktG. Explizit ergibt sich daraus als IT-relevanten Anknüpfungspunkt allein die Pflicht des Vorstandes zur Einrichtung eines Risikomanagementsystems, so dass dem Aufsichtsrat im Rahmen seiner allgemeinen Überwachungstätigkeit auch die Kontrolle des Risk-Managements obliegt. Die Einrichtung eines internen Kontrollsystems kommt ihm hingegen nach deutschem Recht nur aus allgemeinen Pflichten zu, weshalb der europäische Richtlinienvorschlag diese allgemeinen Sorgfaltspflichten konkretisieren würde.[644] Allerdings steht die Annahme des Vorschlags der Kommission weiterhin aus, weshalb auch Art. 39 des Richtlinienvorschlags zur Modernisierung der Prüferrichtlinie gegenwärtig noch nicht zur Konkretisierung der Aufgaben des Aufsichtsrates herangezogen werden kann. Es bleibt insofern vorerst bei der zu § 91 Abs. 2 AktG dargelegten Gesetzesauslegung.

(c) Rechtsfolgen

340 Bei Verstoß gegen die Pflichten aus § 91 Abs. 2 AktG greift zum einen die bereits erwähnte gesamtschuldnerische Haftung der Vorstandsmitglieder gem. § 93 Abs. 2 S. 1 AktG ein. Sorgen die einzelnen Vorstandsmitglieder nicht für die Einrichtung eines Risk-Managements, das auch die IT-Risiken umfasst[645], kann eine entsprechende Haftung auf Schadensersatz gegenüber der Gesellschaft sie persönlich treffen gemäß §§ 93 I AktG. Eine persönliche Haftung gegenüber Dritten ist jedoch selbst unter Zugrundelegung der Rechtsprechung[646] eher die Ausnahme[647]. Zudem kann ein wichtiger Grund zur Abberufung und fristlosen Kündigung vorliegen.[648]

---

643 *Maul/Lanfermann*, BB 2004, 1861 (1865).

644 *Maul/Lanfermann*, BB 2004, 1861 (1866).

645 *Schultze-Melling*, CR 2005, 73 (76); *Roth/Schneider*, ITRB 2005, 19 (19).

646 BGHZ 109, 297, 302 (VI. Zivilsenat) = NJW 1990, 976 – Baustoff II = JZ 1990, 486 m. Anm. *Wagner*; zust. *Brüggemeier*, AcP 191 (1991), 33 (63 ff.); *Foerste*, VersR 2002, 1 ff.; mit anderer, rechtsgeschicht-

341 Nicht abschließend geklärt ist, ob bei Verstoß gegen die Pflicht aus § 91 Abs. 2 AktG bzw. die Pflicht zur ordnungsgemäßen Buchhaltung gem. § 91 Abs. 1 AktG auch eine deliktische Haftung der Vorstandsmitglieder im Rahmen einer Schutzgesetzverletzung bei § 823 Abs. 2 BGB in Betracht kommt. Dies setzt voraus, dass ein Vorstandsmitglied gegen ein den Schutz eines anderen bezweckendes Gesetz verstoßen hat. Die Einordnung des § 91 Abs. 1 und 2 als Schutzgesetz ist aber abzulehnen. Zum einen ist anerkannt, dass § 93 Abs. 1 und 2 kein Schutzgesetz im Sinne des § 823 Abs. 2 darstellt[649]. Es ist nicht ersichtlich weshalb die Organisationspflichten des § 91 Abs. 2 in haftungsrechtlicher Sicht über die Sorgfaltspflichten des § 93 hinausgehen sollten, zumal schon vor Einführung des §91 Abs.2 AktG nach §§ 76, 93 AktG die Pflicht bestand, für eine angemessene Organisation zu sorgen und gefährdende Entwicklung zu erkennen[650]. Zum anderen geht die hM auch im Rahmen des § 91 Abs. 1 davon aus, dass kein Schutzgesetz begründet wird[651], obwohl die Nähe des Regelungsbereichs zu den Vorschriften und Grundsätzen des Kapitalerhaltungsrechts die Annahme eher begründen könnte.

(d) Anhaltspunkte für IT-Konkretisierung

342 Zu den vom Riskmanagement abzudeckenden Bereichen gehören unter anderem auch der Einkauf, die Implementierung und die regelmäßige Kontrolle von Software, deren Risikopotentiale abgeschätzt und gesteuert werden müssen. Versagt die Software, oder darf sie nicht eingesetzt werden, können einem Unternehmen (aber auch anderen Verwendern, wie Behörden) erhebliche Schäden drohen, die bis hin zur fast völligen Lahmlegung eines Unternehmens gehen können. Unter diesen Umständen droht mithin eine Bestandsgefährdung und der Vorstand hat die Risiken, die sich aus dem IT-Einsatz ergeben, in die Risikoabschätzung zur Erkennung von Veränderungen einfließen zu lassen. Insbesondere der Ausfall von IT-gestützten Steuerungs- oder Buchführungssystemen kann bereits innerhalb weniger Tage zu einem größeren Schaden für das Unternehmen führen.

---

licher Begründung *Altmeppen*, ZIP 1995, 881 (886 f.); zusammenfassend *Gross*, ZGR 1998, 551 (562 ff.).

647 Zur Kritik an der Rechtsprechung bzgl. des Vorliegens von Verkehrssicherungspflichten bei mittelbarer Verletzungshandlung MünchKommAktG-*Hefermehl/Spindler*, § 93 AktG Rn. 188; MünchKommBGB-*Wagner*, § 823 BGB Rn. 394 mwN.; eingehend *Spindler*, Unternehmensorganisationspflichten, 2001, 844 ff.

648 KG, NZG 2004, 1165; s. auch VG Frankfurt/M WM 2004, 2157; MünchKommAktG-*Hefermehl/Spindler*, § 91 AktG Rn. 28 mwN.

649 *Spindler*, in: Fleischer, Handbuch des Vorstandsrechts, § 13 Rn. 41; MünchKommAktG-*Hefermehl/Spindler*, § 91 AktG Rn. 12 mwN.

650 *Spindler*, in: Fleischer, Handbuch des Vorstandsrechts, § 19 Rn. 6.

651 *Spindler*, in: Fleischer, Handbuch des Vorstandsrechts, § 13 Rn. 51 ff.

343 Neben der Pflicht zu einem ausreichenden Risikomanagement aus § 91 Abs. 2 AktG greift hinsichtlich der Buchführungssoftware auch die Pflicht des Vorstands zu ordnungsgemäßer Buchführung aus § 91 Abs.1 AktG, bzw. parallel hierzu aus § 41 Abs. 1 GmbHG, und verpflichtet die Geschäftsleitung dazu, angemessene organisatorische Maßnahmen zur Risikominimierung zu treffen. Hierzu gehört nicht allein die Datensicherung, sondern auch die Berücksichtigung alternativer Buchführungssysteme im Falle des EDV-Ausfalls.[652]

344 Eine genaue Zahl der Datensicherungs- und Kontrollabstände lässt sich allerdings nur individuell für jede AG und den jeweils verwendeten IT-Baustein einzeln bestimmen, da ansonsten dem Leitungsermessen des Vorstandes widersprochen würde. Die Unternehmensleitung hat insofern unter den zur Beseitigung des Risikos verfügbaren Maßnahmen im Rahmen des von der Rechtsprechung anerkannten zulässigen Risikos eine Auswahl zu treffen. Exemplarisch führt der BGH in einem obiter dictum zum ARAG/Garmenbeck-Urteil grundlegend aus[653]:

> "[...] Eine Schadensersatzpflicht kann erst in Betracht kommen, wenn die Grenzen, in denen sich ein von Verantwortungsbewusstsein getragenes, ausschließlich am Unternehmenswohl orientiertes, auf sorgfältiger Ermittlung der Entscheidungsgrundlagen beruhendes unternehmerisches Handeln bewegen muss, deutlich überschritten sind, die Bereitschaft, unternehmerische Risiken einzugehen, in unverantwortlicher Weise überspannt worden ist oder das Verhalten des Vorstandes aus anderen Gründen als pflichtwidrig gelten muss."

345 Als Anhaltspunkte für die Erforschung der Gefahren im Unternehmen können die folgenden Punkte dienen:

- die Bedeutung des EDV-Systems für die Geschäftstätigkeit des Unternehmens,
- die Beschaffenheit und Stabilität der eingesetzten EDV-Systeme,
- die Komplexität der Geschäftsprozesse,
- die Abhängigkeit der Funktionsfähigkeit der EDV-Systeme von Dritten (Software-Lieferanten),
- die Gefährdung der Geschäftsabläufe durch den Ausfall einzelner Softwarekomponenten bis hin zum Ausfall des kompletten IT-Systems mit der Aufteilung in Steuerungs- und Datenverarbeitungssoftware, sowie Hardware,
- die Abhängigkeit des Geschäftsbetriebs von EDV-Dienstleistern im Falle ausgelagerter Systeme,

652 *Terlau*, CR 1999, 284 (286); *Streitz*, in: v.Westphalen/Langheit/Streitz, Jahr-2000-Fehler, Rn. 238 ff.
653 BGH ZIP 1997, 883 (885).

- die Abhängigkeit des Geschäftsbetriebs von der Ordnungsmäßigkeit des Geschäftsbetriebes Dritter (Zulieferer, Kunden etc.).

346 Insbesondere in Bereichen sogenannter „kritischer Infrastrukturen", wie Verkehr, Logistik, Gesundheit, Finanzbereichen, um nur einige zu nennen, spielt die Sicherheit der Informationstechnologie eine entscheidende Rolle.[654] Der befürchtete Jahr-2000-Fehler hatte deutlich vor Augen geführt, wie abhängig Unternehmen und eine ganze Volkswirtschaft von IT-Produkten inzwischen sind.[655] Zu den Pflichten der Geschäftsleitung können dementsprechend auch der Abschluss von Pflegeverträgen und die Schaffung von redundanten Sicherheitssystemen gehören, um dem Ausfall der IT-Steuerungssoftware vorzubeugen.

(e) Riskmanagementpflichten in anderen Rechtsformen

347 Nicht nur in Aktiengesellschaften, sondern auch in anderen Rechtsformen gehört ein Riskmanagement zu den Geschäftsführerpflichten. Dies ergibt sich schon daraus, dass schon bei der Einführung des § 91 Abs. 2 AktG der Gesetzgeber selbst davon ausgegangen ist, dass damit nur allgemeine, aus den Sorgfaltspflichten der Geschäftsführung resultierende Anforderungen kodifiziert werden. Damit ergeben sich aber auch für andere Rechtsformen vergleichbare Pflichten, etwa für die GmbH nach § 43 GmbHG,[656] die indes nach dem Zuschnitt der jeweiligen Gesellschaft (kleine und mittlere Unternehmen) selbstverständlich zu modifizieren sind.

(f) Das IT-Riskmanagementsystem nach ISO 27001

348 Ähnlich den Qualitätsmanagementsystemen liegen inzwischen auch Normungen für das **IT-Riskmanagement** in Gestalt der Ende 2005 verabschiedeten ISO 27001[657] vor. Diese Normung folgt weitgehend dem britischen Ansatz im Qualitätsmanagementsektor, der auf die Steuerung von Geschäftsprozessen abzielt und weniger materielle Vorgaben

---

654 Eingehend dazu die Studien des Bundesamtes für Sicherheit in der Informationstechnologie, „Kritische Infrastrukturen", abrufbar unter: http://www.bsi.bund.de/fachthem/kritis/ (zuletzt abgerufen am 05.06. 2007).

655 Aus der damaligen Literatur statt vieler: *Bartsch*, CR 1998, 193 ff.; *Spindler*, NJW 1999, 3737 ff.; *v. Westphalen*, DStR 1998, 1722 ff.

656 Zur Frage der analogen Anwendung des § 91 Abs. 2 AktG auf den Geschäftsführer einer GmbH Baumbach/Hueck-*Schulze-Osterloh*, § 41 GmbHG Rn. 1; Lutter/Hommelhoff-*Hommelhoff/Kleindiek*, § 43 GmbHG Rn. 19 jeweils mwN.

657 ISO/IEC 27001, v. 15.10.2005, "Information technology - Security techniques - Information security management systems - Requirements".

trifft. In Deutschland wird neben der Zertifizierung nach ISO 27001[658] vor allem die Prüfung nach dieser Norm zuzüglich des vom BSI standardisierten Grundschutzes im IT-Sektor durchgeführt;[659] nur durch letztere wird die Einhaltung materieller Standards gewährleistet, da ein reines Managementsystem ohne jegliche Sicherheitsvorgaben nicht den Anforderungen an die Früherkennung von Risiken im IT-Bereich gerecht werden dürfte.

349 Die Norm ISO 27001 spezifiziert Anforderungen für Erstellung, Einführung, Betrieb, Überwachung und Überprüfung, Wartung und Verbesserung eines dokumentierten Informationssicherheits-Managementsystems.[660] In die Anforderungen werden alle möglichen Risiken in der gesamten Organisation einbezogen, wobei zwischen verschiedenen Organisationsformen differenziert wird. Hierbei werden sämtliche Arten von Organisationen (z.B. Handelsunternehmen, staatliche Organisationen, Non-Profitorganisationen)[661] berücksichtigt.

350 Grundsätzlich wird das Modell des "Plan-Do-Check-Act" (PDCA), also Planung, Implementierung, Überprüfung und Handlung für die Strukturierung des IT-Riskmanagementsystems verwendet.[662] Anders formuliert bedarf das IT-Managementsystem einer initialen Planung und Implementierung und einer anschließenden ständigen Überwachung und Verbesserung.

351 Ein Unternehmen, das ISO 27001 konform arbeitet, muss danach zunächst Zweck und Reichweite des IT-Riskmanagementsystems festlegen, indem wichtige Informationen über das Unternehmen, die wichtigen Einheiten und Technologien zusammengetragen werden. Anschließend müssen diese in einem Rahmenwerk, das auch wirtschaftliche, rechtliche und technische Erfordernisse einbezieht und in das generelle Riskmanagement des Unternehmen eingebettet ist, einbezogen werden, wobei auch Handlungen und Notwendigkeiten mit Hinblick auf IT-Sicherheit benannt werden müssen. Anschließend wird die Methode der Risikobestimmung gewählt und die vorhandenen Risiken sind zu identifizieren, analysieren und zu evaluieren. Für diese Risiken sind anschließend ge-

---

658 Zertifizierung nach ISO 27001 auf der Basis von IT-Grundschutz, Prüfschema für ISO 27001 – Audits, Stand 1.02.2006, abrufbar im Internet unter abrufbar unter: http://www.bsi.de/gshb/zert/ISO27001/Pruefschema06.pdf (zuletzt abgerufen am 05.06.2007).

659 *Capellaro/Füser*, Die Bank 2005, 68 (70 f.); *Roth/Schneider*, ITRB 2005, 19.

660 ISO 27001:2005, 4.1.

661 ISO 27001:2005, 1.1.

662 ISO 27001:2005, 0.2.

eignete Gegenmaßnahmen bzw. Vermeidungsstrategien zu definieren und zu bewerten. Dazu gehört z.B. auch die Versicherung gegen den Eintritt solcher Risiken.[663]

352 Schließlich muss ein Risikobehandlungsplan erstellt werden, der für alle Risiken die im Eintrittsfall zu ergreifenden Maßnahmen enthält. Dieser soll durchgesetzt werden, indem zusätzlich Kontrolleinrichtungen geschaffen werden. Dazu gehören auch Schulungen und Informationsprogramme. Die Überwachung und Überprüfung soll des Weiteren schnell Fehler im IT-Riskmanagement entdecken bzw. ineffektive Maßnahmen identifizieren und die entsprechenden Schlussfolgerungen ziehen und einarbeiten.

353 Zur ISO 27001 gehört auch eine entsprechende Verantwortungsverteilung. So sollen Nachweise für die Einbindung bzw. Verantwortlichkeit des Managements bezüglich des IT-Riskmanagements, z.B. einer entsprechenden Rollenverteilung, erbracht werden. Die verantwortlichen Mitarbeiter sind entsprechend zu informieren und bei Bedarf zu schulen. Zudem müssen notwendige Ressourcen für die verschiedenen Aufgaben des IT-Riskmanagements benannt und zur Verfügung gestellt werden.

354 Zu festgelegten Daten sollte schließlich eine interne unabhängige Überprüfung stattfinden. Zusätzlich soll eine regelmäßige Prüfung durch das Management stattfinden.

355 Es zeigt sich, dass Riskmanagement durch die ISO 27001 spezialisiert auf IT-Risiken übertragen wird. Im Anhang werden spezifische Aufgaben bezüglich wichtiger Risiken für verschiedene Einsatzbereiche, z.B. den Online-Handel oder Telearbeit, im IT-Sektor benannt. Dabei stellen die Anforderungen der ISO 27001 nur einen Teil des Gesamtriskmanagements dar und sind in dieses einzubetten.

356 Die möglichen Rechtsfolgen liegen auf der Hand: Ähnlich wie im Deliktsrecht (oder auch in anderen Rechtsbereichen wie dem Vertragsrecht) sind diese Standards geeignet, als allgemein anerkannte Regeln der Technik die nötige Sorgfalt im Sinne der objektiven Pflicht zu konkretisieren – wenn auch nicht abschließend, sondern nur in dem Sinne, dass vermutet wird, dass sie die vom Gesetz gestellten Anforderungen erfüllen.[664]

663 ISO 27001:2005, 4.2.1.f)4).

664 Ausführlich. dazu oben Rn. 174 ff.

(2) Mittelbare Wirkung von Basel II (Kreditwesenaufsichtsrecht)

(a) Hintergrund

357 Diese im Wesentlichen aus dem Gesellschaftsrecht stammenden Pflichten werden in absehbarer Zeit nochmals mittelbar durch das Kreditaufsichtsrecht verschärft – was breitflächige Auswirkungen auch auf kleinere oder mittlere Unternehmen gleich welcher Rechtsform haben wird, da die Fremdkapitalquote in Deutschland nach wie vor beachtlich ist. Denn aufgrund der sogenannten Basel II-Anforderungen müssen die Banken in qualifizierter Weise das Risiko jeder Gesellschaft per Rating vor jeglicher Fremdmittelvergabe einschätzen.[665] Mit der Neufassung der Richtlinie 2000/12/EG[666] und der Richtlinie 93/6/EWG[667] wird die auf der Grundlage der Baseler Eigenkapitalvereinbarung von 1988 (sog. Basel I) überarbeitete Baseler Eigenkapitalvereinbarung von 2004 (Basel II)[668] auf europäischer Ebene umgesetzt.[669] Im deutschen Recht erfolgte die Umsetzung im Kreditwesengesetz,[670] den „Mindestanforderungen an das Risikomanagement (MaRisk) und der Solvabilitätsverordnung (SolvV)[671]. Ziel der Regelungen ist es, die Eigenkapitalanforderungen stärker als bisher vom eingegangenen Risiko abhängig zu machen und die allgemeinen und besonderen Entwicklungen an den Finanzmärkten sowie im Riskmanagement der Institute zu berücksichtigen.[672]

---

665 *Kümpel*, Bank- und Kapitalmarktrecht, Rn. 19.91; *Fritz-Aßmus/Tuchtfeldt*, ORDO 54 (2003), 267 (270 f.); *Polke*, Die darlehensvertragliche Umsetzung der Eigenkapitalgrundsätze nach Basel II, 73 ff.

666 Richtlinie 2000/12/EG des Europäischen Parlaments vom 20.03.2000 über die Aufnahme und Ausübung der Tätigkeit der Kreditinstitute – sog. Bankenrichtlinie, ABl. EG L 126, 1 ff.

667 Richtlinie 93/6/EWG des Rates vom 15.03.1993 über die angemessene Eigenkapitalausstattung von Wertpapierfirmen und Kreditinstituten - sog. Kapitaladäquanzrichtlinie, ABl. EG L 141, 1 ff.

668 Basel Committee on Banking Supervision (2004), International Convergence of Capital Measurement and Capital Standards, A Revised Framework, Basel, Juni 2004. Die Baseler Dokumente können von der Website der Bank für Internationalen Zahlungsausgleich heruntergeladen werden unter abrufbar unter: http://www.bis.org.

669 BegrRegE zum Entwurf eines Gesetzes zur Umsetzung der neu gefassten Bankenrichtlinie und der neu gefassten Kapitaladäquanz-Richtlinie vom 15.02.2006, 1; abrufbar unter: http://www.bundesfinanzministerium.de/lang_de/DE/Geld__und__Kredit/Aktuelle__Gesetze/Entwurf__eines__Gesetzes__zur__Umsetzung__Bankenrichtlinie__anl,templateId=raw,property=publicationFile.pdf (zuletzt abgerufen am 05.06.2007). Zu Basel II s. zuletzt *Blöcker/Spielberg*, Die Bank 2005, 56 ff.; *Gaumert/Zattler*, Die Bank 2005, 55 ff.; *Hofmann/Lesko/Vorgrimler*, Die Bank 2005, 48 ff.; *Schöning/Weber*, Die Bank 2005, 47 ff.; *Schubert/Grießmann*, VW 2004, 1399 ff.; *Schulte-Mattler/von Kenne*, Die Bank 2004, 37 ff.; *Capellaro/Füser*, Die Bank 2005, 68 ff.; ausführlich Boos/Fischer/Schulte-Mattler-*Schulte-Mattler*, Basel II Rn. 1 ff.

670 BGBl. I vom 5.01.2007, S. 10, 31, inkraftgetreten am 20.01.2007.

671 BGBl. I vom 14.12.2006, S. 2926, inkraftgetreten am 1.01.2007.

672 BegrRegE zum Entwurf eines Gesetzes zur Umsetzung der neu gefassten Bankenrichtlinie und der neu gefassten Kapitaladäquanz-Richtlinie vom 15.02.2006, 1 (2); s. auch *Schulte-Mattler/von Kenne*, Die Bank 2004, 37 f.; Boos/Fischer/Schulte-Mattler/*Schulte-Mattler*, Basel II Rn. 11.

(b) Pflichten und Adressat

358 Die genannten Ziele sollen durch einen auf drei Säulen beruhenden Regelungsansatz erreicht werden, wobei die Säule I die Mindestkapitalanforderungen regelt und die bankenaufsichtliche Risikomessung stärker an die Risikosteuerungsmethoden der Banken annähert, während Säule II sich mit der qualitativen Bankenaufsicht und Säule III mit den Offenlegungspflichten befasst.[673] Durch Basel II bzw. die entsprechenden Gesetzesvorschriften zur Umsetzung werden die kreditgewährenden Finanzinstitute verpflichtet, eine individuelle Einschätzung der Bonität bei Unternehmen vor jeder Kreditentscheidung eines Kreditgebers vorzunehmen, welche auf Basis der internen Rating-Systeme der Institute oder durch externes Rating erfolgt.[674] Hierbei sind auch die operationellen Risiken des kreditnehmenden Unternehmens zu beachten, wozu auch die Risiken gehören, die sich aus dem Einsatz von Informationstechnologie in den Unternehmensprozessen ergeben.[675]

(c) Rechtsfolgen

359 Diese Pflichten richten sich allein an die Finanzinstitute, so dass Basel II und die entsprechende Gesetzgebung zur Umsetzung weder eine Pflicht noch eine Obliegenheit für die kreditnehmenden Unternehmen begründen und damit auch keine Rechtsfolgen in Form von Sanktionen oder in Form eines Rechtsverlustes haben können. Allerdings entsteht eine mittelbare Wirkung, da Unternehmen bei fehlendem oder nicht ausreichendem Riskmanagement bei der internen oder externen Risikoeinschätzung der Finanzinstitute schlechter abschneiden und jene zum Ausgleich der höheren Eigenmittelanforderungen schlechtere Kreditkonditionen bieten werden.

(d) Anhaltspunkte für IT-Konkretisierung

360 Für Zwecke des Ratings eines Unternehmens arbeiten die Banken heute mit branchenspezifischen Risikoprofilen, wobei im IT-Bereich wie in anderen Risikobereichen eine branchentypische Risikodisposition unterstellt wird. Unter dem Gesichtspunkt der IT-Sicherheit kann ein Unternehmen, für das im Ausgangspunkt eine branchentypische Risikodisposition angenommen wird, ein günstigeres Rating, also eine positivere Risiko-

673 Hierzu ausführlich *Schubert/Grießmann*, VW 2004, 1399 ff.; *Fischer*, VW 2002, 237 ff.; *Schulte-Mattler/von Kenne*, Die Bank 2004, 37 ff.; Boos/Fischer/Schulte-Mattler/*Schulte-Mattler*, Basel II Rn. 10 ff.

674 *Müller-Reichart/Dura/Fischer/Nosty*, VW 2002, 625; *Capellaro/Füser*, Die Bank 2005, 68 (68 f.).

675 Vgl. BegrRegE zum Entwurf eines Gesetzes zur Umsetzung der neu gefassten Bankenrichtlinie und der neu gefassten Kapitaladäquanz-Richtlinie vom 15.02.2006, 1 (2); s. auch *Capellaro/Füser*, Die Bank 2005, 68 (68 f.); *Schultze-Melling*, CR 2005, 73 (78); *Roth/Schneider*, ITRB 2005, 19 f.; Boos/Fischer/Schulte-Mattler/*Schulte-Mattler*, Basel II Rn. 134.

einschätzung bezüglich des Unternehmens als hinsichtlich der Branche insgesamt, und damit verbunden günstigere Kreditkonditionen nur erreichen, wenn es gegenüber der Bank nachweist, dass es effektivere IT-Sicherheitsmaßnahmen als der Durchschnitt besitzt.[676] Je mehr das Unternehmen bei seinen Geschäftsabläufen auf eine funktionierende IT angewiesen ist, desto größeres Gewicht haben IT-Sicherheitsrisiken demzufolge bei der Risikovorsorge des Unternehmens. Gefordert ist ein IT-Riskmanagement, welches sich mit allen Aspekten der IT-Sicherheit für das jeweilige Unternehmen befasst; es müssen wichtige IT-Systeme vorhanden und verfügbar sein sowie Angriffe auf diese Systeme wirksam abgewehrt werden können und Notfallpläne vorliegen. Missbrauch der IT durch externe oder interne Mitarbeiter, insbesondere durch Weitergabe von vertraulichen Firmendaten an externe Stellen, Geschäftsunterbrechungen durch IT-Systemausfälle oder Schadensersatzforderungen auf Grund unsicherer IT werden sich daher negativ auf das Risikoprofil des Unternehmens auswirken.[677] Die Relevanz der IT-Risiken als Teil des Geschäftsrisikos sind z.T. aber auch branchenspezifisch; so wird ein Unternehmen, dessen Geschäft ausschließlich auf Online-Handel basiert, ein sehr hohes IT-Risiko besitzen, während bei Finanzdienstleistern die finanziellen Risiken z.B. in Form von Wertberichtigungen überwiegen.[678] Insgesamt werden von der Bonitätsprüfung im Unternehmenskreditgeschäft bezogen auf die Anfälligkeit der IT-Systeme gerade mittelständische Unternehmen betroffen sein.[679]

361 Damit besteht aber indirekt ein breitflächiger **Zwang für diese Unternehmen, ein adäquates Riskmanagement** vorzuweisen, das die für das Controlling essentiellen Elemente des EDV-Einsatzes einschließlich des Rechtemanagements umfasst. Eine Darlehensvergabe ohne jegliche Prüfung der Risikovorsorge, deren Bestandteil auch die Absicherung der IT-Risiken einschließlich der Rechtssituation ist, wird daher nicht mehr möglich sein. Denn als Folge der Relevanz der dargestellten Faktoren kann ein darauf vorbereitetes Unternehmen mit gut dokumentiertem IT-Riskmanagement bei der Kreditvergabe einer Bank für günstigere Konditionen sorgen und umgekehrt können die Kreditbedingungen für einen Kreditnehmer eher schlechter sein, wenn dieser eine anfällige IT-Infrastruktur besitzt. Eine Investition in ein IT-lastiges Unternehmen wird für die Bank dann rentabel sein, wenn das Unternehmen neben den betriebswirtschaftlichen

676 *Capellaro/Füser,* Die Bank 2005, 68 f.
677 Beispiele nach *Capellaro/Füser,* Die Bank 2005, 68.
678 *Capellaro/Füser,* Die Bank 2005, 68 f.
679 Für die Auswirkungen der Kreditkosten auf den Mittelstand s. *Paul/Stein/Kaltofen,* Die Bank 2004, 342 f.; *Schulte-Mattler/Manns,* Die Bank 2004, 376 ff. mwN.

Voraussetzungen insbesondere die IT-relevanten Kriterien erfüllt. Von Vorteil ist es insofern, wenn die Prozesse des Kerngeschäfts durch die eingesetzten Applikationen optimal unterstützt werden. Diese sollten den entsprechenden branchenüblichen Standards entsprechen und auf dem Stand der Technik sein; die Prozesse im IT-Betrieb müssen wirksam sowie kosteneffizient und die wesentlichen IT-Risiken sollten identifiziert sein sowie geeignete Maßnahmen zu deren Reduktion umgesetzt werden. Zu einem effektiven Risikomanagement gehören auch Schulungen der Mitarbeiter und Aufklärungsmaßnahmen sowie eine im Unternehmen kommunizierte, schriftlich fixierte Sicherheits-Policy.[680] Die Maßnahmen müssen in regelmäßigen Abständen wiederholt werden, um Effektivität zu garantieren. Außerdem muss die IT-Infrastruktur insgesamt robust und geeignet ausgelegt sein, um das aktuelle Transaktionsvolumen zu bewältigen. Hilfreich ist eine flexible Konzeption, so dass durch akzeptable Erweiterungsmaßnahmen auch das zukünftig zu erwartende Transaktionsvolumen bewältigt werden kann. Zudem müssen die Verantwortlichkeiten in der IT klar geregelt sein, der Mitarbeitereinsatz ist insofern an den Erfordernissen auszurichten.[681]

362 In das Rating können durchaus auch andere IT-Zertifikate einbezogen werden.[682] So kann das Zertifikat als Nachweis dienen, dass ein IT-Sicherheitsmanagementsystem vorhanden ist und ein BS 7799-Zertifikat bzw. ein ISO 27001 Einfluss auch auf die Bewertung nach Basel II haben. Allerdings ist im Rahmen eines Ratings darauf zu achten, ob der für die Zertifizierung gewählte Gültigkeitsbereich sich auch mit den Unternehmensbereichen deckt, die wesentlich die Werthaftigkeit oder die Wertschöpfung des Unternehmens widerspiegeln.[683] Die für das BSI 7799-2 bzw. ISO 27001 erstellte Risikoanalyse kann hierfür nur bedingt herangezogen werden, da sich diese definitionsgemäß auf den Gültigkeitsbereich der entsprechenden Zertifizierung und nicht auf das Gesamtunternehmen bezieht.[684] Eine direkte Übertragbarkeit und damit ein unmittelbarer Nachweis im Sinne von Basel II lässt sich hierin folglich nicht sehen.

363 Beispiel: Hat ein Unternehmen keinerlei Kontrolle im Bereich des Einkaufs von Software bzw. IT-Produkten, und sind diese Produkte kritisch für die Erbringung der Leistungen des Unternehmens, können sich existentielle Risiken für das Unternehmen im

680 *Haar/Schädler*, Verbaselt, abrufbar unter: http://www.heise.de/ix/artikel/2004/12/099/ (zuletzt abgerufen am 05.06.2007).
681 Beispiele nach *Capellaro/Füser*, Die Bank 2005, 68 (69 f.).
682 *Capellaro/Füser*, Die Bank 2005, 68 (69 f.).
683 *Capellaro/Füser*, Die Bank 2005, 68 (70).
684 *Capellaro/Füser*, Die Bank 2005, 68 (70).

Falle des Versagens der Software ergeben. Ein Kreditunternehmen wäre daher u.U. schon von Rechts wegen gehalten, zusätzliche Sicherheiten oder einen höheren Kreditzins zu verlangen. Ein schlechtes IT-Riskmanagement kann sich daher auf die Finanzierungskonditionen eines Unternehmens unmittelbar auswirken.

364 Jedenfalls bezüglich des von dem Zertifikat erfassten Risikobereichs sollte sich das Finanzinstitut aber auf die Vorlage eines Zertifikats berufen können, um den Nachweis zu erbringen, dass im Bereich des IT-Managements des Unternehmens eine ausreichende Risikoeinschätzung stattgefunden hat. Für die Annahme, dass ein Zertifikat eine eigene Risikoeinschätzung durch das Finanzinstitut ersetzt, spricht, dass die Erteilung der genannten Zertifikate an hohe Anforderungen geknüpft ist und jene Anforderungen umfassend sind, so dass kein Raum für zusätzliche Anforderungen seitens der Finanzinstitute besteht. Zwar ist zu bedenken, dass das Verfahren und die Entscheidung zur Zuteilung der Zertifikate fehlerbehaftet sein können, doch ist es nicht praktikabel und nicht zu erwarten, dass das Finanzinstitut eine Überprüfung des Verfahrens vornimmt. Außerdem würde der Effizienzgewinn durch die Standardisierung stark gemindert, wenn sie keinen Nutzen im Rahmen von Ratingverfahren bringen könnte. Dies gilt vor allem für KMUs, für die Basel II eine besonders hohe Hürde bei der Kreditfinanzierung darstellt. Eine klare Rechtsgrundlage zu diesen Prüfungsverfahren und der Rolle von Zertifikaten ist allerdings bislang im Rahmen des Basel II-Verfahrens nicht ersichtlich.

(3) Anforderungen durch den Sarbanes-Oxley-Act (SOX)

(a) Hintergrund

365 Mit dem US-amerikanischen Sarbanes-Oxley-Act vom 30.07.2002, 15 U.S.C. 7201,[685] werden die Anforderungen an bestimmte Unternehmen bezüglich der Einrichtung eines IT-Riskmanagements und dessen rechtliche Implikationen zukünftig noch erheblich komplexer. Das Gesetz bezweckt nach der Gesetzesbegründung den Schutz von Anlegern durch genauere und verlässlichere wertpapierrechtliche Publizitätspflichten der börsennotierten Unternehmen.[686] Zu diesem Zweck werden die Verantwortlichkeiten der Unternehmensführung und der Wirtschaftsprüfer geregelt und strenge Maßstäbe für die Zusammenarbeit aufgestellt. Das Artikelgesetz, das vor allem Änderungen im Securities und Exchange Act of 1934 („Exchange Act“) vorsieht, ist insofern als Reaktion

685 Abrufbar unter: http://www.law.uc.edu/CCL/SOact/soact.pdf.

686 Dem Gesetzestext geht folgender Einleitungssatz voraus: „An Act to protect investors by improving the accuracy and reliability of corporate disclosures made pursuant to the securities laws, and for other purposes“.

auf die zahlreichen und schwerwiegenden Bilanzskandale mit sich anschließenden Unternehmenszusammenbrüchen, wie z.B. von Enron und WorldCom, zu werten.[687] Es dient nicht zuletzt auch der Wiederherstellung des Vertrauens der Anleger in die Richtigkeit der veröffentlichten Finanzdaten von Unternehmen, die den amerikanischen Rechtsvorschriften hinsichtlich periodischer Berichtspflichten und einzureichender Adhoc Mitteilungen unterliegen.[688] Nach § 13(a) bzw. 15(d) Exchange Act sind dies solche Unternehmen, deren Wertpapiere an einer US-amerikanischen Börse notiert und die insofern gem. § 12 Exchange Act bei der Wertpapieraufsichtsbehörde SEC (Securities and Exchange Commission) registriert sind, oder die Wertpapiere öffentlich in den USA angeboten haben, ohne diese an einer US-amerikanischen Börse notiert zu haben. Die Regelungen betreffen insofern auch eine Vielzahl deutscher Unternehmen, die in den USA Wertpapiere öffentlich anbieten. Damit kommen auch auf viele deutsche Unternehmen spezielle Handlungs- und Sorgfaltspflichten zu, die insbesondere auch im Bereich der IT-Sicherheit berücksichtigt werden müssen.

(b) Pflichten und Adressat

366 Um sicherzustellen, dass Unternehmen richtige und verlässliche Angaben machen, sieht der Sarbanes-Oxley Act in Zusammenhang mit den Ausführungsregeln der SEC[689] eine Vielzahl von Maßnahmen vor, die sich in erster Linie an Mitglieder der Leitungsorgane der registrierten Unternehmen und deren Abschlussprüfer richten. In Bezug auf das interne Kontrollsystem werden zwei Ziele verfolgt[690], deren Umsetzung konkrete Auswirkungen auf Vorstand, interne Revision, Aufsichtsrat und Abschlussprüfung hat[691].

---

687 Zum Fall Enron vgl. etwa United Bancruptcy Court Southern District of New York, In re: Enron Corp. et al., First Interim Report of Neal Batson, Court-Appointed Examiner, Sept. 21, 2002; Eine umfassende Dokumentenzusammenstellung zum Fall Enron ist auch abrufbar unter http://news.findlaw.com/legalnews/lit/enron/; zum Fall WorldCom vgl. abrufbar unter: http://lawcrawler.findlaw.com/scripts/lc.pl?entry=WorldCom&sites=news; krit. über den Erfolg des SOX Act *Schwarz/Holland*, ZIP 2002, 1661 ff.; s. auch *Schiessl*, AG 2002, 593 (593 ff.).

688 *Gruson/Kubicek*, Der Sarbanes-Oxley Act, 1 f., abrufbar unter: http://www.jura.unifrankfurt.de/ifawz1/baums/Bilder_und_Daten/Arbeitspapiere/paper113.pdf; auch AG 2003, 337 (338); Arbeitskreis „Externe und Interne Überwachung der Unternehmen" der Schmalenbach-Gesellschaft für Betriebswirtschaft e.V., BB 2004, 2399 (2399); *Schultze-Melling*, CR 2005, 73 (79).

689 Z.B. Auditing standards Nos. 1-3 des Public Company Accounting Oversight Board (PCAOB).

690 PricewaterhouseCoopers, Sarbanes-Oxley Act – Professionelles Management interner Kontrollen, 2004, passim; *Bülow*, Datenschutz-Berater 10/2005, 13; vgl. auch *Hütten/Stromann*, BB 2003, 2223 (2223 ff.).

691 Hierzu *Luttermann*, BB 2003, 745 (745 f.); *Gruson/Kubicek*, AG 2003, 337 (337 ff.) und AG 2003, 393 (393 ff.); Arbeitskreis „Externe und Interne Überwachung der Unternehmen" der Schmalenbach-Gesellschaft für Betriebswirtschaft e.V., BB 2004, 2399 (2399 ff.), zu den Auswirkungen auf den Berufsstand der Wirtschaftsprüfer ausführlich *Hilber/Hartung*, BB 2003, 1054 (1054 ff.); *Lenz*, BB 2002, 2270 (2270 ff.); *Keller/Schlüter*, BB 2003, 2166 (2166 ff.).

367 Zum einen müssen die CEO und CFO eines Unternehmens nach Section 302 (Disclosure Controls and Procedures) durch die Einrichtung eines internen Kontrollsystems sicherstellen, dass alle relevanten Informationen korrekt erfasst, verarbeitet und fristgerecht veröffentlicht werden und in einer eidesstattlichen Erklärung die korrekte und vollständige Darstellung der finanziellen Situation testieren.[692] Auf diese Weise wird die Verantwortlichkeit des Vorstands für Unternehmensberichte verstärkt und die Einrichtung von Offenlegungskontrollen und Offenlegungsverfahren verlangt.[693]

368 Zum anderen verpflichtet Section 404 (Internal Control over Financial Reporting) das Management, ein internes Kontrollsystem zur Sicherstellung einer effektiven Finanzberichterstattung zu etablieren. DEO und DFO müssen einen Prozess einrichten, der die Ordnungsmäßigkeit der Finanzberichterstattung und somit eine den Rechnungslegungsvorschriften entsprechende Erstellung von Abschlüssen sicherstellt[694], wobei insbesondere die Korrektheit, Nachvollziehbarkeit und Sicherheit der Prozesse geregelt wird.[695] Das so implementierte Überwachungssystem soll dafür sorgen, dass den Mitgliedern der Unternehmensorgane alle relevanten Informationen bezüglich der für den Unternehmensbericht bedeutsamen Teilprozesse und damit auch und gerade hinsichtlich des verwendeten IT-Systems jederzeit zur Verfügung stehen.[696] Die Verantwortlichkeit des Geschäftsführungsorgans für die Wirksamkeit interner Überwachungsmaßnahmen ist in einem jährlichen Bericht gesondert festzustellen und das Verfahren sowie jede Veränderung der internen Überwachung ist vom Management zu bewerten. Die Mitglieder des Leitungsorgans stehen durch Gewinnabschöpfung persönlich für die Korrektheit von Finanzberichtsabschlüssen ein, indem bei fehlerhaftem Abschluss erhaltene Boni zurückgezahlt und Gewinne aus dem Verkauf von erlangten Aktienoptionen herausgegeben werden müssen.

369 Nach mehrmonatigen Diskussionen hat die SEC nunmehr eine Fristverlängerung für ausländische Unternehmen hinsichtlich der Umsetzung der Regelungen in Section 404

---

692 Bzgl. der inhaltlichen Anforderungen der Bestätigungen eingehend *Gruson/Kubicek*, Der Sarbanes-Oxley Act, 46 ff., abrufbar unter: http://www.jura.uni-frankfurt.de/ifawz1/baums/Bilder_und_Daten/Arbeitspapiere/paper113.pdf.

693 Arbeitskreis „Externe und Interne Überwachung der Unternehmen“ der Schmalenbach-Gesellschaft für Betriebswirtschaft e.V., BB 2004, 2399 (2400).

694 *Büssow/Taetzner*, BB 2005, 2437 (3438 f.).

695 Ausführlich. *Hütten/Stromann*, BB 2003, 2223 (2224 f.); *Taetzner*, BB 2005, 2437 (2437 ff.); *Gruson/Kubicek*, Der Sarbanes-Oxley Act, 37 ff., abrufbar unter: http://www.jura.unifrankfurt.de/ifawz1/baums/Bilder_und_Daten/Arbeitspapiere/paper113.pdf.

696 *Pellens*, DBW 2003, 473; *Bülow*, Datenschutz-Berater 10/2005, 13; ausführlich zu Sec. 404 SOX auch *Büssow/Taetzner*, BB 2005, 2437 ff.

SOX verfügt, wonach die Anforderungen erst für die Geschäftsjahre zu erfüllen sind, die nach dem 15.07.2006 enden.[697] Insofern haben auch die betroffenen deutschen Unternehmen eine letzte Gnadenfrist erhalten, das interne Kontrollsystem den Anforderungen des Sarbanes-Oxley Act anzupassen und ihr IT-Sicherheitsmanagement entsprechend einzurichten.

370 Schließlich verdient auch die Einrichtung eines **Audit Committees** als Überwachungsorgan gemäß Section 301 SOX besondere Beachtung im Zusammenhang mit den vom Sarbanes-Oxley Act geforderten Überwachungsmaßnahmen.[698] Ihm kommt die Aufgabe zu, das Rechnungs- und das Finanzberichtswesen zu überwachen und Unternehmensabschlüsse zu überprüfen.[699] Das Audit Committee ist zudem für die Einrichtung eines **Whistleblowing-Verfahrens** verantwortlich, dass für Emittenten durch Section 301 SOX verbindlich vorgeschrieben ist, um die Gefahr deliktischer Handlungen, die mitunter auch die Existenz der Gesellschaft bedrohen können, zu verringern.[700] Kennzeichnend für den Begriff des Whistleblowings sind drei Merkmale: Ein Organisationsinsider erkennt illegale, illegitime oder unmoralische Praktiken von gleichfalls der Organisation angehörenden Personen und meldet diese einer speziellen geeigneten Stelle.[701] Das Merkmal der illegalen Praktiken wird dabei sehr weit verstanden und umfasst insbesondere auch Nachlässigkeiten und Organisationsmängel von Verantwortlichen.[702] Dementsprechend stellt das Whistleblowing-Verfahren auch und gerade hinsichtlich IT-Anwendungen besondere Anforderungen im Rahmen eines Sicherheits-Managements. Die Unternehmen trifft konkret die Pflicht zur Einrichtung interner oder externer Whistleblowing-Stellen, die prinzipiell dazu in der Lage sein müssen, den Hinweisen nachzugehen und ein festgestelltes haftungsrelevantes Verhalten zu unterbinden. Da sich zunächst nicht aufgedeckte deliktische Handlungen von Tochtergesellschaften auch

---

697 SEC Press Release 2005-25 vom 2. 3. 2005; Die Fristverlängerung wird angeordnet durch die SEC Final Rule, Release No. 33-8545, abrufbar unter http www.sec.gov.

698 Arbeitskreis „Externe und Interne Überwachung der Unternehmen“ der Schmalenbach-Gesellschaft für Betriebswirtschaft e.V., BB 2004, 2399 (2402 f.); *Gruson/Kubicek*, Der Sarbanes-Oxley Act, 6 ff., abrufbar unter http: abrufbar unter: http://www.jura.uni-frankfurt.de/ifawz1/baums/Bilder_und_Daten/Arbeitspapiere/paper113.pdf; auch AG 2003, 337 (340 ff.); *Schiessl*, AG 2002, 593 (600); *Hütten/Stromann*, BB 2003, 2223 (2223 f.); *Schwalbach*, AG 2004, 186 (188); zur Stellung des Audit Commitee Financial Experts eingehend *Luttermann*, BB 2003, 745 ff.

699 Festgelegt in Sec. 3 (a)(58)(A) Exchange Act, eingefügt durch Sec. 205 SOX.

700 Ausführlich. zum Whistleblowing-Verfahren *Berndt/Hoppler*, BB 2005, 2623; s. auch *Hütten/Stromann*, BB 2003, 2223 (2224).

701 *Near/Miceli*, Journal of Business Ethics 1985, 4; *Keenan*, Employee Responsibilities and Rights Journal 2000, 200; *Berndt/Hoppler*, BB 2005, 2623 (2624 f.) mwN.

702 *Grant*, Journal of Business Ethics 2002, 391 f.; *Johnson*, Whistleblowing – When it works and why, 31 ff.; *Leisinger*, Whistleblowing und Coporate Reputation Management, 259 ff.

als Gefährdung der Unternehmensfortführung der Muttergesellschaft auswirken können, empfiehlt sich die Einrichtung eines einheitlich geregelten Whistleblowing-Verfahrens für alle Konzernteile, um sich nicht straf- oder zivilrechtlichen Sanktionen ausgesetzt zu sehen.[703]

371 Im Gegensatz zu den besonderen Anforderungen an die Ausgestaltung des internen Überwachungssystems ist schließlich festzuhalten, dass die **interne Revision** nicht explizit im Sarbanes-Oxley Act erwähnt ist. Dennoch ergeben sich Konsequenzen für die Tätigkeit der internen Revision aus den geänderten Regelungen für Vorstand, Aufsichtsrat und Abschlussprüfer.[704] Da die Unternehmensleitung stärker für die Vollständigkeit und Richtigkeit der Finanzberichterstattung einstehen muss, verlagert sich auch für die interne Revision der Schwerpunkt der Prüfung auf die Aspekte der Funktionsfähigkeit und Ordnungsmäßigkeit der Finanzberichterstattung und des internen Kontrollsystems.[705] Um Kontrollschwächen aufzudecken, muss die interne Revision naturgemäß eigene Funktionstests durchführen, von denen auch die IT-Prozesse erfasst sind.

(c) Rechtsfolgen

372 Der SOA schreibt neben zivil- und strafrechtlichen Sanktionen, die das Gesetz selbst anordnet und im Falle von vorsätzlicher Abgabe einer falschen Erklärung Geldbußen bis zu einer Höhe von 5 Mio. US-Dollar sowie Freiheitsstrafen von bis zu 20 Jahren vorsieht, in Section 3 (b)(1) SOX vor, dass jeder Verstoß gegen den Sarbanes-Oxley Act auch als Verstoß gegen den Securities Act 1934 (15 U.S.C. § 78 (a) ff.) zu werten ist; es drohen mitunter zusätzlich durch die SEC erlassene Sanktionen.

(d) Anhaltspunkte für IT-Konkretisierung

373 Im Hinblick auf regulatorische Anforderungen im IT-Bereich sind die Regelungen über strafrechtliche und zivilrechtliche Sanktionen für Sicherheitsverstöße, die Unabhängigkeit der internen und externen Unternehmensprüfungen[706] und die erhöhten Publizitätspflichten bezüglich zu veröffentlichender Unternehmensinformationen von Bedeu-

---

703 *Berndt/Hoppler*, BB 2005, 2623 (2625).

704 Eingehend Arbeitskreis „Externe und Interne Überwachung der Unternehmen“ der Schmalenbach-Gesellschaft für Betriebswirtschaft e.V., BB 2004, 2399 (2399 ff.) mwN.

705 Arbeitskreis „Externe und Interne Überwachung der Unternehmen“ der Schmalenbach-Gesellschaft für Betriebswirtschaft e.V., BB 2004, 2399 (2401).

706 Ausführlich: Arbeitskreis „Externe und Interne Überwachung der Unternehmen“ der Schmalenbach-Gesellschaft für Betriebswirtschaft e.V., BB 2004, 2399 (2399 ff.) mwN.

tung.[707] Da es nur noch selten Geschäftsvorgänge gibt, die ohne die Verwendung von IT-Applikationen stattfinden, kommt insofern unter Verlässlichkeitsgesichtspunkten dem IT-Riskmanagement erhöhte Bedeutung zu.

374 So verpflichtet Section 302 SOX die Unternehmensleitung im Hinblick auf den Einsatz von IT-Systemen dazu, die Sicherheit und die Verfügbarkeit der im Zusammenhang mit der Rechnungslegung verwendeten Technik nachzuweisen und zu kontrollieren.[708] Auch im Hinblick auf Section 404 verschärfen die Anforderungen an die Sicherheit der Prozesse und der Wirksamkeit interner Überwachungsmaßnahmen nicht zuletzt die Anforderungen, die an das IT-Riskmanagement im Unternehmen zu stellen sind. Dabei sollen sogenannte „Control Frameworks", wie die von COSO oder COBIT, dazu dienen, dass Gefahren für die Rechnungslegung eliminiert oder wenigstens gemindert werden[709].

b) Allgemeine zivilrechtliche Pflichten

375 Wechselt man die Perspektive und betrachtet die Pflichtenlage der kommerziellen IT-Nutzer im Hinblick auf ihre Sicherungspflichten gegenüber Dritten, ergeben sich erhebliche Unterschiede in den geschuldeten Verkehrspflichten:

376 Ausgangspunkt ist zunächst wiederum, dass derjenige, der eine Gefahrenquelle schafft oder beherrscht, nach § 823 Abs. 1 BGB grundsätzlich verpflichtet ist, die notwendigen und zumutbaren Vorkehrungen zu treffen, um eine Schädigung anderer zu vermeiden,[710] wobei – wie bereits dargelegt – zur genaueren Konkretisierung des Inhalts und Umfangs der Verkehrssicherungspflicht in erster Linie auf die berechtigten Sicherheitserwartungen der betroffenen Verkehrskreise abzustellen ist,[711] ferner auf die Möglichkeit und Zumutbarkeit der Gefahrenvermeidung einerseits auf der Versenderseite, andererseits auf der Empfängerseite.[712]

---

707 *Bülow*, Datenschutz-Berater 10/2005, 13 (13); vgl. auch *Gruson/Kubicek*, AG 2003, 337 (337 ff.) und AG 2003, 393 (393 ff.).

708 *Knolmayer/Wermelinger*, Der Sarbanes-Oxley Act und seine Auswirkungen auf die Gestaltung von Informationssystemen, abrufbar unter: http://www.ie.iwi.unibe.ch/publikationen/berichte/resource/WP-179.pdf, 1.

709 *Knolmeyer/Wermelinger*, Der Sarbanes-Oxley Act und seine Auswirkungen auf die Gestaltung von Informationssystemen, abrufbar unter: http://www.ie.iwi.unibe.ch/publikationen/berichte/resource/WP-179.pdf, 7 f.

710 BGH NJW-RR 2003, 1459; NJW 1990, 1236; NJW-RR 2002, 525 mwN.

711 BGH NJW-RR 2002, 525 (526); BGH NJW 1978, 1629; BGH NJW 1990, 906 (907); Bamberger/Roth-*Spindler*, § 823 BGB Rn. 234; Schwarz/Peschel-*Mehner-Schwerdtfeger/Gottschalck*, Kap. 2 Rn. 246.

712 *Koch*, NJW 2004, 801 (804); *Libertus*, MMR 2005, 507 (509); Bamberger/Roth-*Spindler*, § 823 BGB Rn. 234.

377 Keine Unterschiede ergeben sich hinsichtlich der potenziell bedrohten Rechtsgüter Dritter, von geschützten Daten, Urheberrechten bis hin zum Recht am eingerichteten und ausgeübten Gewerbebetrieb. Auch lässt sich der Angriff des IT-Nutzers auf den Geschädigten jedenfalls mittelbar auf das vorsätzliche Handeln des ursprünglichen Angreifers, z.B. des Virenerstellers bzw. –verbreiters, zurückführen, so dass die Pflicht des Nutzers bestehen bleibt.[713] Die Unterschiede liegen vielmehr in den zumutbaren Verkehrssicherungspflichten für kommerzielle IT-Nutzer:

(1) Herleitung von Pflichten im IT-Bereich

378 Änderungen gegenüber den privaten IT-Nutzern ergeben sich vor allem hinsichtlich des zumutbaren für den Schutz einzusetzenden Aufwandes, den Sicherheitserwartungen des betroffenen Kreises gegenüber kommerziellen IT-Nutzern sowie der Bekanntheit der Problemlage und möglichen Gegenmaßnahmen. Im Gegensatz zu privaten Nutzern, für die der III. Zivilsenat des BGH den Einwand aus § 254 BGB nur bei weitgehender Bekanntheit eines Problems zulässt, kann eine solche Privilegierung für den kommerziellen IT-Nutzer nicht angenommen werden. Zwar ist ihm nicht wie einem IT-Hersteller zuzumuten, jedes Problem umgehend zu erkennen und sich ständig durch Fachzeitschriften oder Expertenberatung zu informieren, es ist jedoch zu verlangen, dass er regelmäßig auch Probleme beim Einsatz von Computern beachtet und, sofern er von Gefahren erfährt, diesbezüglich über die üblichen Informationskanäle, wie eben Fachzeitschriften oder Internetquellen, Erkundungen einholt. Je höherrangiger die Rechtsgüter sind, die in Kontakt mit IT-Produkten des kommerziellen IT-Nutzers kommen, je größer das Vertrauen Dritter in den Einsatz der IT-Produkte durch den IT-Nutzer ist, desto intensiver werden diese Kontrollen und diese Pflicht zur Erkundigung ausfallen. So wird etwa eine Bank, die Online-Banking einsetzt, verpflichtet sein, sich wesentlich schneller und regelmäßiger einen Überblick über Gefahrenlagen aus IT-Produkten zu verschaffen als ein Wertpapierdienstleister, der IT-Produkte lediglich intern oder gar nur sporadisch einsetzt.

379 Diese Maßstäbe entscheiden auch darüber, ob dem IT-Nutzer gar noch weitergehende Pflichten aufzubürden sind, etwa zur **eigenständigen Bewältigung von bekannt gewordenen Sicherheitslücken**. Allerdings kann dies nur besondere Fälle betreffen, da dem IT-Nutzer oftmals enge Grenzen zur Selbsthilfe gesetzt sind, zum einen durch rechtliche Grenzen im Rahmen von §§ 69c, d UrhG, zum anderen durch technische

713 *Koch*, NJW 2004, 801 (803).

Grenzen der Aufarbeitung komplexer Software. Grundsätzlich ist nach § 69c Nr. 2 UrhG die Bearbeitung oder Umarbeitung von Computerprogrammen nur mit Gestattung des Rechteinhabers möglich. Davon erfasst sind Abänderungen des geschützten Computerprogramms.[714] § 69c Rn 17. § 69d I UrhG stellt klar, dass auch die Fehlerbeseitigung eine Umarbeitung darstellt. Fehler können Bugs, Funktionsstörungen, Programmabstürze, Viren, trojanische Pferde oder ähnliches sein, nicht davon erfasst ist dagegen das Entfernen von Kopierschutzvorrichtungen wie ein Dongle.[715] Fehlerbeseitigungen sind nach § 69d I UrhG aber grds. von der Gestattungspflicht ausgenommen. Allerdings hängt diese Ausnahme wiederum von dem Willen des Rechteinhabers ab.[716] Denn dieser hat nach § 69d I 1. Hs. UrhG („Soweit keine besonderen vertraglichen Bestimmungen vorliegen,[...]“) die Möglichkeit, Ausnahmeregelung des § 69d I UrhG vertraglich abzubedingen oder ihren Umfang einzuschränken, wobei allerdings die Fehlerbeseitigung einen sogenannten „abredefesten Kern“ darstellt, der nicht abbedungen werden kann.[717] Schon vom Wortlaut aus sind Wartungen und Programmverbesserungen dagegen nicht von der Ausnahme des § 69d I UrhG erfasst.[718] Insofern bedürfen diese einer Gestattung des Rechteinhabers nach § 69c Nr. 2 UrhG. Daher kann etwa einem kommerziellen IT-Nutzer kein Vorwurf gemacht werden, wenn noch keine Lösung für ein Problem besteht, wie es z.B. häufig bei bekannten Systemlücken ohne entsprechendes Update des Herstellers der Fall ist.

380 Im Rahmen der Zumutbarkeitsprüfung sind allerdings die technischen Grenzen weniger relevant als die wirtschaftlichen Einschränkungen: Denn der kommerzielle IT-Nutzer kann immer darauf verwiesen werden, technischen Sachverstand einzukaufen, so dass im Wesentlichen die wirtschaftliche Seite ausschlaggebend ist.

381 Wie schon für private IT-Nutzer, finden sich diese Pflichten quasi spiegelbildlich sowohl hinsichtlich des Schutzes Dritter als auch der zumutbaren Eigenschutzpflichten (§ 254 BGB) wieder – wenngleich für den Schutz Dritter bestimmte besondere Verkehrserwartungen eine andere Rolle spielen mögen, so dass in diesen Situationen die Pflichtenstandards unterschiedlich ausfallen können. Anders formuliert wird der Ver-

714 Dreier/Schulze-*Dreier*, § 69c Rn. 15.
715 Schricker-*Loewenheim*, § 69d Rn. 9 f.; Dreier/Schulze-*Dreier*, § 69d Rn. 9.
716 Dreier/Schulze-*Dreier*, § 69d Rn. 2.
717 Schricker-*Loewenheim*, § 69d Rn. 13; Dreier/Schulze-*Dreier*, § 69d Rn. 12.
718 Dreier/Schulze-*Dreier*, § 69d Rn. 9; ferner Schricker-*Loewenheim*, § 69d Rn. 14.

kehr generell (nicht nur die Vertragspartner) von einem professionellen IT-Nutzer (Onlinebank) wesentlich höhere Sicherheitsmaßnahmen erwarten.

382 Bislang praktisch kaum geklärt sind etwa die sog. Vorsorgekosten für Schadensfälle im Rahmen von §§ 249, 254 BGB für IT-Systeme. Grundsätzlich können Vorhaltekosten, d.h. solche Kosten, die für eine eigene Betriebsreserve entstehen, vom Schädiger ersetzt werden, wenn diese zur Schadensminderung beitragen.[719] Im IT-Bereich wäre es denkbar, dass die Vorhaltung redundanter Systeme oder die Installation besonderer Sicherheitsmaßnahmen der Schadensminderung beiträgt, insbesondere wenn es sich um umsatzintensive Unternehmen handelt, die auf funktionierende Technik angewiesen sind. Als Beispiel käme der Bereich des Brokering in Frage: steht im Falle eines Ausfalles kein System bereit, können enorme Ausfälle und Schäden entstehen, die durch das Bereitstehen weiterer Systeme wesentlich geringer gehalten werden können. Daher erscheint es in diesen Fällen angemessen, auch Vorhaltekosten geltend machen zu können. Denkbar wäre auch das Geltendmachen von angemessenen „Kopfgeldern“, vergleichbar mit den Fangprämien bei Kaufhausdiebstählen,[720] wenn Unternehmen auf das Finden von Systemcrackern derartige Prämien aussetzen, da dies der Vermeidung von konkreten Schadensfällen entgegenwirkt und das Kopfgeld auch erst im Fall der Aufdeckung fällig wird bzw. die Forderung erst entsteht.[721]

383 Es ist somit für die zu ergreifenden Maßnahmen zu ermitteln,

- ob die Tatsache, dass ein Problem besteht, bekannt ist bzw. bekannt sein muss,
- ferner ob die Ergreifung der Sicherungsmaßnahme wirtschaftlich zumutbar ist, wobei einzubeziehen ist, inwiefern bereits der Eigenschutz derart stark wiegt, dass auch an sich unzumutbare Maßnahme über den kumulativen Effekt des Eigeninteresses doch als zumutbar anzusehen ist,
- sowie wie häufig der Nutzer Aktualisierungen vornehmen muss.

(2) Einzelfragen

384 Diese Punkte sind nun, wie bereits bei den privaten IT-Nutzern, bei den jeweiligen Sicherungsmaßnahmen zu überprüfen.

(a) Virenscanner

719 BGH NJW 1976, 286; Erman-*Kuckuk*, § 249 BGB Rn. 71; Bamberger/Roth-*Schubert*, § 249 BGB Rn. 99; MünchKommBGB-*Oetker*, § 249 BGB Rn. 195.

720 BGH NJW 1980, 119.

721 S. dazu Bamberger/Roth-*Schubert*, § 249 BGB Rn. 101.

385 Der Einsatz von Virenscannern ist bereits Privaten zumutbar. Als Grund, warum den kommerziellen Nutzern von Computersystemen hier geringere Pflichten obliegen sollen, kommen die erhöhten Kosten in Betracht. So sind die Programmlizenzen häufig pro genutzten Computer zu erwerben, so dass bei einer Vielzahl von Rechnern durchaus merkbare Kosten entstehen können. Allerdings ist das Gefahrenpotential durch Viren sehr hoch,[722] auch Leben und Gesundheit können betroffen sein, zudem besteht ein starkes Eigeninteresse hinsichtlich des Schutzes der eigenen Daten und Anlagen. In diesem Rahmen überwiegen die eigenen Schutzinteressen sowie diejenigen Dritter den wirtschaftlichen Aufwand. Eine wirtschaftliche Zumutbarkeit liegt demnach vor. Der Einsatz von Virenscannern ist Teil der Verkehrssicherungspflichten der Nutzer. Nach dem BSI-Grundschutz ist eine permanente Überwachung als Schutz vor Viren absolut notwendig.[723]

386 Eine Änderung könnte sich auch in der notwendigen Aktualisierungsfrequenz ergeben. Allerdings ist eine ständige Aktualisierung auch dem kommerziellen Nutzer nicht zumutbar,[724] solange auch gebräuchliche Standardvirenscanner nur wöchentlich automatische Aktualisierungen anbieten. Sollte sich jedoch das ständige Angebot von Updates durchsetzen, so kann zumindest an Arbeitstagen von einer täglichen Updatepflicht ausgegangen werden.[725]

(b) Firewall

387 Der Einsatz von Firewalls kann von privaten IT-Nutzern nicht generell verlangt werden. Grund hierfür ist einerseits, dass zwar die abstrakte Gefahr „Internet“, aber nicht die Lösung über eine Firewall bekannt ist. Hinzu kommt der nur unzureichende Schutz sowie als Hauptargument die technische Unzumutbarkeit des Einsatzes. Im Bereich der Haftung der kommerziellen Nutzer besteht dieses letzte Erfordernis jedoch nicht, sondern ist vielmehr nur Teil der wirtschaftlichen Erwägungen.

388 In Firmennetzen werden häufig zentrale Firewalls eingesetzt, die dann auch zentral eingerichtet oder gewartet werden. Aufgrund der Komplexität der Aufgabe[726] wird regelmäßig besonders geschultes Personal oder die Herbeiziehung externen Experten not-

---

722 Vgl. zum Beispiel heise-online v. 25.4.2006, abrufbar unter: http://www.heise.de/newsticker/meldung/72366.

723 BSI, IT-Grundschutzhandbuch 2005, B 1.6.

724 So aber *Schmidbauer*, abrufbar unter: http://www.i4j.at/news/aktuell36.htm.

725 „Kurze“ Abstände *Tita*, VW 2001, 1781 (1784).

726 Vgl. BSI, IT-Grundschutzhandbuch 2005, M 2.76.

wendig sein. Für die Wartung und Überwachung, aber auch für die lokale Einrichtung, ist es dem Unternehmen durchaus zuzumuten, Experten heranzuziehen. Diese können z.B. das eigene Personal unterweisen und schulen. Zudem können häufig die elementarsten Sicherungen bereits durch den kostengünstigen Einsatz einer Hardwarefirewall bzw. eines entsprechenden Routers ergriffen werden. Aufgrund der hohen Gefährdung der eigenen und fremden Daten ist die wirtschaftliche Zumutbarkeit des Einsatzes von Firewalls jedenfalls gegeben.

389 Es besteht somit die Pflicht zum Einsatz von Firewalls.[727]

(c) System- und Programmupdates

390 Bereits dem privaten Nutzer ist das Einspielen von Systemupdates zuzumuten, sofern diese automatisch oder halb-automatisch installiert werden. Begründung hierfür ist einerseits die notwendige Bekanntheit, andererseits die leichte technische Umsetzung. Diese Pflichten lassen sich als Mindeststandard ohne Weiteres auch auf den Einsatz bei kommerziellen Nutzern übertragen. Nicht verpflichtend für Private sind manuelle Systemupdates sowie Aktualisierungen der installierten Programme. Fraglich ist, ob diese weitergehenden Pflichten aber dem kommerziellen Nutzer obliegen.

391 Hierfür ist auch die Zweckrichtung der Verwendung von Programmen in kommerziellen Unternehmen zu beachten. Im Idealfall wird ein Softwareprodukt auf einem kommerziell verwendeten Rechnersystem nur dann installiert, wenn es auch tatsächlich für den Betrieb des Unternehmens benötigt wird.[728] Der Unternehmer ist darauf angewiesen, dass diese Programme auch durchgehend funktionieren. Nicht nur durch Systeme entstehen Sicherheitslücken, sondern auch durch Programmfehler. Es besteht also grundsätzlich auch durch sie eine hohe Gefährdung sowohl des eigenen Betriebs als auch mittelbar der Rechtsgüter Dritter. Die Gefährdung durch Viren ist damit auch hier immanent gegeben, was ebenfalls die Möglichkeit des Eintritts der bekannten hohen Schäden impliziert. Der Aufwand für die Aktualisierung der Programme ist jedoch nicht zu unterschätzen. So muss der Unternehmer zunächst Kapazitäten für die ständige oder regelmäßige Überprüfung bereitstellen, die Aktualisierungen vornehmen und dabei auch Behinderungen im Betrieb hinnehmen. Es werden immer wieder neue Sicherheitslücken entdeckt und bekannt gegeben, Programmaktualisierungen folgen ebenso häufig. Die Folge wäre, dass der Unternehmer ständig und immer wieder produktive Einheiten frei-

727 Ebenso und sogar für zweistufige Anlage der Firewall *Behnke/Schäffter*, DSB 2002, Heft 7-8, S. 10.

728 Ähnl. Empfehlung zum „minimalen Betriebssystem“ BSI, IT-Grundschutzhandbuch 2005, M 4.95.

stellen müsste, was einen enormen wirtschaftlichen Aufwand bedeutet. Dennoch ist er im Rahmen der Abwägung nicht vollständig frei von Pflichten zu stellen.

392 Sind ihm kritische Sicherheitslücken bekannt,[729] so kann davon ausgegangen werden, dass er diese baldmöglichst, z.B. innerhalb von einer Woche zu schließen versucht. Bei anderen Sicherheitsproblemen ist ihm jedenfalls eine regelmäßige Überprüfung und Aktualisierung, z.B. einmal im Monat, bei sensitiven Branchen, wie etwa im Online-Banking durchaus auch kürzer, zuzumuten.

393 Der Nutzer kann jedoch im Sinne einer **Selbstschutzpflicht** (nach § 254 BGB) **nicht gezwungen werden, ein Nachfolgeprodukt** zu erwerben, um den geforderten Sicherheitsstandard zu erreichen.[730] Ansonsten wäre die Pflicht von der Entscheidung des Herstellers, ein neues Produkt herauszubringen, abhängig. Sofern der Nutzer einen Softwarepflegevertrag geschlossen hat, dessen Laufzeit noch nicht beendet ist, stellt sich dieses Problem nicht.[731]

394 Allerdings ergibt sich hier ein **signifikanter Unterschied für die Haftung gegenüber Dritten**, wenn man die Perspektive wechselt und die Pflichten des kommerziellen IT-Nutzers aus Sicht potenziell geschädigter Dritter betrachtet (z.B. durch Versand verseuchter Daten durch Bot-Netze über den kommerziellen, „befallenen" IT-Nutzer). Denn das letztlich auf das Äquivalenzinteresse abstellende Argument im Verhältnis von IT-Hersteller zu Geschädigten, dass der Geschädigte nicht zu ständigem Neukauf eines Produktes verpflichtet sein kann, verfängt in diesen Konstellationen nicht. Zu berücksichtigen ist hier, dass der Hersteller innerhalb gewisser Grenzen rechtmäßig die Unterstützung des Produkts vollständig einstellen kann,[732] da er angesichts kurzer Produktzyklen den Support nicht ständig aufrechterhalten will.[733] Er ist zwar für eine gewisse Zeit nach Ablauf des Lebenszyklus zu Pflege- und Wartungsarbeiten am Programm verpflichtet; doch finden auch diese Pflichten eine zeitliche Grenze.[734] Es wäre jedoch nicht angebracht, den kommerziellen IT-Nutzer wegen des mangelnden Supports durch

729 Ebenso BSI, IT-Grundschutzhandbuch 2005, M 4.83.

730 *Spindler*, NJW 2004, 3145 (3150); *Spindler*, NJW 1999, 3737 (3744).

731 Zum Softwarepflegevertrag *Zahrnt*, CR 2000, 205 mwN.

732 Vgl. z.B. bezüglich der Unterstützung von Windows NT durch Microsoft heise-online, Meldung v. 09.03.2001, abrufbar unter: http://www.heise.de/newsticker/meldung/15958; *Lier*, VW 2004, 554 (556).

733 *Zahrnt*, CR 2000, 205 f., wobei die Frage, ob ein Softwarepflegevertrag vor Ablauf von 5 Jahren gekündigt werden darf, verneint wird; ebenso LG Köln CR 1999, 218; dazu im Bereich Produktsicherheit AG München NJW 1970, 1852; anders OLG Koblenz CR 2005, 482.

734 Ca. 5 Jahre, LG Köln CR 1999, 218; eher länger *Jaeger*, CR 1999, 209 (211); 10 Jahre *Bartsch*, CR 1998, 193.

den IT-Hersteller im Verhältnis zu geschädigten Dritten zu entlasten. Denn er verfügt über die Möglichkeiten, die Software entweder zu ersetzen oder die potenziellen Gefahrenquellen zu isolieren („vom Netz nehmen“) und dadurch die Gefahren zu minimieren.[735] Sind die Supportzyklen des Herstellers ausreichend lang,[736] so können dem IT-Nutzer anschließend in entsprechenden Abständen aus dem Blickwinkel des Haftungsrechts durchaus wiederkehrende Kosten auch in Form des Neukaufs aktueller Software, alternativ der Abschluss eines entsprechenden Softwarepflegevertrags,[737] zugemutet werden, sofern dies die einzige Möglichkeit zur Ergreifung notwendiger Sicherungsmaßnahmen ist.

(d) Nutzung von Nutzerkonten mit eingeschränkten Rechten

395 Im Normalbetrieb eines kommerziellen Nutzers werden lediglich die vorhandenen Programme genutzt, Eingriffe in das System durch die Nutzer sind meist sogar unerwünscht. Von daher ist eine organisatorische Aufteilung von Zugriffsrechten, also insbesondere die Vergabe geringer Eingriffsmöglichkeiten an die Nutzer und die Erstellung eines Administratorkontos, durchaus sinnvoll und schützt auch den Betrieb des Unternehmens.[738] Der wirtschaftliche Aufwand ist hierbei gering und damit zumutbar. In sehr kleinen Unternehmen, bei denen allerdings die Nutzer auch die Pflege der IT-Infrastruktur übernehmen, sind somit auch weitgehende Rechte der Nutzer erforderlich. Hier kann diese Pflicht nicht greifen.

(e) Intrusion Detection-Systeme

396 Intrusion Detection-Systeme werden insbesondere in größeren Netzwerken eingerichtet.[739] Der Aufwand zu ihrer Einrichtung ist relativ hoch.[740] So muss eine zentrale Komponente des Netzwerks alle durchgeleiteten Pakete analysieren können. Häufig werden auf den einzelnen Rechnern zusätzlich host-basierte Intrusion Detection-Systeme eingerichtet. Ins Gewicht fällt vor allem der Einrichtungs- und Wartungsaufwand, Lizenzkosten fallen hingegen nicht zwangsläufig an.[741] Der Betrieb erfordert je-

---

735 Zur Risikoverteilung bei Angriffen auf Computersysteme (hier DDoS) AG Gelnhausen CR 2006, 208.

736 Hier ist, unter Verweis auf LG Köln CR 1999, 218, auf 5-10 Jahre abzustellen.

737 Dazu *Zahrnt*, CR 2000, 205 mwN.

738 Für Windows NT z.B. IT-Grundschutzhandbuch 2005, M 4.51, M 4.53, allgemein *Bohne,* VW 2004, 1583.

739 Zum Erfolg des Einsatzes *Behnke/Schäffter,* DSB 2002, Heft 7-8, 10.

740 Ebenso *anonymus*, VW 2002, 1050; zur Komplexität solcher Systeme und der Anforderungen BSI, IT-Grundschutzhandbuch 2005, M 5.71.

741 Als Open Source-Projekt existiert z.B. Snort, abrufbar unter: http://www.snort.org/.

doch tiefe Kenntnisse von Netzwerken und Netzwerkverkehr, weshalb regelmäßig Experten notwendig sind.

397 Tritt ein Angriff auf, z.B. dadurch, dass ein Virus oder Wurm einen Teil des Systems befallen hat, so kann das Programm einen entsprechenden Alarm auslösen. In der Folge kann die Weiterverbreitung verhindert werden. Ein Großteil der Gefahren kann allerdings schon durch den Einsatz von Firewalls und Virenscanner abgewehrt werden. Intrusion Detection-Systeme sind folglich nachgelagert und dienen der Erkennung, falls die primären Abwehrmechanismen versagt haben.

398 Der hohe Aufwand rechtfertigt den Einsatz nur in Unternehmen mit größeren Netzwerken und entsprechendem Know-how.[742] Eine generelle Pflicht zum Einsatz solcher Systeme besteht nicht.

(f) Malware-Entfernungsprogramme

399 Es besteht weiter die Frage, ob nicht nur Abwehr- sondern auch Vorsorgemaßnahmen im Sinne einer beständigen Beobachtung bzw. Überprüfung durch den Nutzer verlangt werden können. So können Malware-Entfernungsprogramme zur Erkennung und teilweise auch zur Abwehr von Programmen dienen, die trotz der Ergreifung der Sicherungsmaßnahmen erfolgreich Zugang zum Computer gefunden haben.

400 Häufig sind diese Programme kostenlos verfügbar. Ihr Einsatz kann bei intensiver Beschäftigung damit auch programmiert und wiederholt ablaufen, so dass das Programm so gesteuert wird, dass es die tägliche Arbeit nicht direkt stört. Der wirtschaftliche Aufwand ist damit relativ gering, so dass der Einsatz dieser Programme verlangt werden kann.

401 Die nachträgliche Kontrolle als zweite Stufe ist nicht so häufig notwendig wie die Aktualisierung der primären Sicherungsprogramme. Ein regelmäßiger Einsatz alle zwei bis vier Wochen dürfte hier ausreichen.

(g) Ergebnis

402 Kommerzielle Nutzer müssen, abhängig auch von der Größe ihrer IT-Infrastruktur, Maßnahmen zur Sicherung ihrer IT-Systeme ergreifen. Dazu gehören die primäre Abwehr, die sekundäre Überprüfung durch Suchprogramme sowie die notwendige Aktualisierung der Programme.

---

742 Ebenso *Tita*, VW 2001, 1781 (1784); *Behnke/Schäffter*, DSB 2002 Heft 7-8, 10.

c) Zwischenergebnis: Allg. Verantwortlichkeit kommerzieller Unternehmen als Nutzer

403 Im Ergebnis zeigt sich, dass kommerziellen IT-Nutzern weitgehende Pflichten obliegen. Diese sind jedoch meist mit der einmaligen Einrichtung und entsprechender Konfiguration auch für die Zukunft sicher einzurichten. So kann das Update von Virenscannern, Firewall, Intrusion Detection-Systemen und Malware-Entfernungsprogrammen automatisiert erfolgen. Andere Pflege erfordert durchaus auch personellen Aufwand. Im Rahmen der Abwägung der betroffenen Güter unter Einbeziehung des hohen Eigeninteresses ist jedoch auch dieser angemessen.

4. Der Einfluss des Datenschutzrechts auf die Pflichten von IT-Nutzern (Datensicherheit und Datenschutz)

a) BDSG

(1) Hintergrund

404 Aus öffentlich-rechtlicher Sicht enthält vor allem das Datenschutzrecht allgemeine Vorgaben für kommerzielle IT-Nutzer: Denn die Sicherheit von IT-Systemen bedingt immer auch die Sicherheit der in diesen Systemen kursierenden Daten.[743] Regelmäßig werden die in einem System verarbeiteten Daten in irgendeiner Form personenbezogen i.S.d. § 3 Abs. 1 BDSG sein.[744] Zwar bezieht sich der Datenschutz primär auf den Schutz des durch die Daten Betroffenen in seinen persönlichen Belangen, wohingegen der Begriff der Datensicherung die Sicherheit der Daten an sich betrifft.[745] Allerdings sind einerseits die Bemühungen um Datensicherheit weitgehend mit denen um Datenschutz deckungsgleich;[746] andererseits betrifft das von der Datensicherheit erfasste Gefährdungspotential in der Folge immer auch den persönlichkeitsorientierten Bereich des Datenschutzes. Sofern sich also datenschutzrechtlich Pflichten zum Schutz der Daten ergeben, umfassen diese regelmäßig auch Pflichten zum Schutz der IT-Systeme.

(2) Kommerzieller IT-Nutzer als Adressat

405 Bezogen auf kommerzielle IT-Nutzer muss zunächst geklärt werden, ob und inwiefern sie dem Anwendungsbereich des BDSG unterfallen. Aufgrund der Verwendung von IT-

743 *Weichert*, in: Killian/Heussen, Kap. 135 Rn. 1; *Reiländer/Weck*, DuD 2003, 692 ff.; *Heibey*, in: Roßnagel, Handbuch Datenschutzrecht, Kap. 4.5 Rn. 2; *Opaschowski*, in: Roßnagel, Handbuch Datenschutzrecht, Kap. 2.1, Rn. 7 f.

744 Vgl. dazu BVerfG NJW 1984, 419 (422), wonach es „kein belangloses Datum“ mehr gebe.

745 Hierunter fallen Maßnahmen zum Schutz von Daten, Programmen und Datenverarbeitungssystemen vor möglichen Gefahren, dazu *Tinnefeld/Ehmann/Gerling*, Einführung in das Datenschutzrecht, S. 384.

746 *Schneider*, Handbuch des EDV-Rechts, Kap. B Rn. 487; s ferner die Abbildung bei *Tinnefeld/Ehmann/Gerling*, Einführung in das Datenschutzrecht, S. 386.

Systemen greifen Ausnahmen für nicht automatisierte vorliegende Daten wie z.B. Akten vorliegend generell nicht. Das BDSG unterscheidet zunächst zwischen nicht-öffentlichen und öffentlichen Stellen:

(a) Nicht-öffentliche gegenüber öffentlichen Stellen

406 Bei der Einordnung als nicht-öffentliche Stelle kommt es lediglich auf die privatrechtliche Organisationsform an.[747] Der persönliche Anwendungsbereich umfasst sowohl natürliche als auch juristische Personen,[748] aber auch Personenvereinigungen und Personengesellschaften des privaten Rechts, auch wenn ihnen keine eigene Rechtspersönlichkeit zukommt, also z.B. nicht rechtsfähige Vereine.[749]

407 Demgegenüber gehören zu den öffentlichen Stellen i.S.d. BDSG Behörden, Organe der Rechtspflege und andere öffentlich organisierte Einrichtungen, sofern sie nicht als öffentlich-rechtlich organisierte Einrichtungen am Wettbewerb teilnehmen. Ferner sind diejenigen Stellen erfasst, die zwar privatrechtlich organisiert sind, aber hoheitliche Aufgaben wahrnehmen. Öffentlich-rechtlich organisierte Unternehmen, die am Wettbewerb teilnehmen, werden dagegen nach §§ 12, 27 BDSG ebenfalls als nicht-öffentliche Stellen behandelt.[750]

(b) Persönliche Tätigkeiten

408 Weiter eingegrenzt wird der Anwendungsbereich durch sachliche Kriterien. Werden Daten nur für persönliche oder familiäre Tätigkeiten erhoben, so findet das BDSG keine Anwendung.[751] Damit verwendet das BDSG zur Abgrenzung letztlich ein ähnliches Kriterium, wie es oben (Rn 259 ff.) im Hinblick auf die rollenspezifische Abgrenzung von IT-Nutzern entwickelt wurde. Ein und dieselbe Person kann daher je nach Tätigkeit dem BDSG unterfallen oder aufgrund rein persönlicher Tätigkeiten aus dessen Anwendungsbereich ausscheiden.

(3) Datenschutzrechtliche Pflichten und IT-Konkretisierung

747 *Gola/Schomerus*, § 2 BDSG Rn. 19; *Wedde*, in: Roßnagel, Handbuch Datenschutzrecht, Kap. 4.3 Rn. 32. f.
748 *Gola/Schomerus*, § 2 BDSG Rn. 19; *Wedde*, in: Roßnagel, Handbuch Datenschutzrecht, Kap. 4.3 Rn. 38 f.
749 *Tinnefeld/Ehmann/Gerling*, Einführung in das Datenschutzrecht, S. 169 f.
750 *Gola/Schomerus*, § 2 BDSG Rn. 4.
751 Simitis-*Dammann*, § 1 Rn. 228.

(a) Die Pflichten zur Organisation und technischen Schutzmaßnahmen (§ 9 BDSG)

(i) Überblick

409 Zentrale Norm für die datenschutzrechtliche Pflicht, Sicherheitsmaßnahmen zu ergreifen, ist § 9 BDSG. Er ist auch deshalb wichtig für alle Stellen, die Daten verarbeiten, weil er fast immer Anwendung findet, sei es kraft einer expliziten Verweisung oder bei fehlenden bereichsspezifischen Regelungen zur Sicherheit von Daten.[752] Durch § 9 BDSG wird IT-Sicherheit „in den Dienst" des Datenschutzes gestellt.[753]

410 Nach § 9 BDSG sind „technische und organisatorische" Maßnahmen zu treffen, um die gesetzlichen Anforderungen zu gewährleisten.[754] Ziel der Norm ist, den ordnungsgemäßen Ablauf der Datenverarbeitung durch Sicherung von Hard- und Software sowie von Daten vor Verlust, Beschädigung, aber eben auch Missbrauch, Diebstahl und Verfälschung zu treffen.[755] Hierzu gehören insbesondere regelmäßige Datensicherungen, auch Maßnahmen zur Abwehr von Viren.[756] Grundsätzlich dürfen keine Verfahren oder Techniken eingesetzt werden, die zu einer erheblichen Gefährdung der grundrechtlich geschützten Rechte des Betroffenen führen,[757] die Maßnahmen müssen sich zusätzlich am aktuellen Stand der Technik orientieren.[758] Die zu ergreifenden Sicherungsmaßnahmen müssen der Sensitivität der Daten vielmehr angemessen sein.[759] Nach § 9 Satz 2 BDSG orientiert sich der notwendige Aufwand auch an der Erforderlichkeit vor dem Hintergrund von wirtschaftlichen Erwägungen als Ausprägung des Verhältnismäßigkeitsgrundsatzes.[760] § 9 Satz 2 BDSG erlaubt jedoch nicht das Unterlassen von Sicherungsmaßnahmen, sondern regelt nur die Schutzintensität.[761] Wichtig ist hier ein angemessenes Verhältnis zum Schutzzweck. Dies zeigt sich auch an der Anlage zu § 9 BDSG, nach der „auf die Art der zu schützenden [...] Daten" eingegangen werden muss.

---

752 *Tinnefeld/Ehmann/Gerling*, Einführung in das Datenschutzrecht, S. 388; Simitis-*Ernestus*, § 9 Rn. 4 ff.

753 *Tinnefeld/Ehmann/Gerling*, Einführung in das Datenschutzrecht, S. 644.

754 Dazu auch *Schöttle*, Anwaltliche Rechtsberatung via Internet, S. 39 ff.; *Kersten*, CR 2001, 576; *Heibey*, in: Roßnagel, Handbuch Datenschutzrecht, Kap. 4.5 Rn. 21.

755 Simitis-*Ernestus*, § 9 Rn. 2; *Gola/Schomerus*, § 9 BDSG Rn. 2 f.

756 *Gola/Schomerus*, § 9 BDSG Rn. 19.

757 *Tinnefeld/Ehmann/Gerling*, Einführung in das Datenschutzrecht, S. 384; *Heibey*, in: Roßnagel, Handbuch Datenschutzrecht, Kap. 4.5 Rn. 25 ff; Simitis-*Ernestus*, § 9 Rn. 27.

758 *Weichert*, in: Killian/Heussen, Computerrechts-Handbuch Kap. 135 Rn. 2; *Hermeler*, Rechtliche Rahmenbedingungen der Telemedizin S. 83.

759 *Tinnefeld/Ehmann/Gerling*, Einführung in das Datenschutzrecht, S. 389; Simitis-*Ernestus*, § 9 Rn. 28; *Aufhauser/Hindinger-Back*, 117; *Heibey*, in: Roßnagel Handbuch Datenschutzrecht, Kap. 4.5 Rn. 32.

760 *Tinnefeld/Ehmann/Gerling*, Einführung in das Datenschutzrecht, S. 389; *Heibey*, in: Roßnagel, Handbuch Datenschutzrecht, Kap. 4.5 Rn. 25 ff.; Simitis-*Ernestus*, § 9 Rn. 23.

761 *Wohlgemuth/Gerloff*, Datenschutzrecht, S. 158; *Gola/Schomerus*, § 9 BDSG Rn. 8.

Art. 17 Abs. 1 UAbs. 2 der Datenschutz-Richtlinie 95/46/EG (DRL) stellt sogar generell auf den aktuellen Stand der Technik ab.[762]

411 Notwendig ist also jeweils eine Analyse des Gefahrenpotentials, insbesondere konkreter Missbrauchsgefahren.[763] Die Analyse ist kein einmaliger, sondern vielmehr ein dauerhafter Prozess, da eine ständige Beobachtung der Risiken erforderlich ist.[764]

412 Die Anknüpfung des Schutzes an die personenbezogenen Daten bewirkt aber auch, dass Rechensysteme, die nicht zur Verarbeitung personenbezogener Daten verwendet werden, diesem Schutz nicht automatisch unterliegen. Wenn allerdings bei einem erfolgreichen Angriff auf diese Systeme auch andere, vom BDSG wiederum erfasste Systeme bedroht werden, liegt natürlich auch der Schutz des zunächst nicht datenrelevanten Systems im Pflichtenbereich des BDSG, wenn die anderen Systeme nicht anders geschützt werden können.

413 § 9 BDSG wird durch eine Anlage bereits im Rahmen des BDSG konkretisiert. Diese enthält allgemeingültige Beschreibungen professioneller Standards, insbesondere zu Zutritts-, Zugangs-, Zugriffs-, Weitergabe-, Eingabe-, Auftrags- und Verfügbarkeitskontrollen,[765] wobei die Aufzählung jedoch nur beispielhaft ist.[766] § 9 BDSG und seine Anlage regeln zwar grundsätzlich das „Ob“ der Ergreifung von Sicherungsmaßnahmen. Sie bieten auch Anhaltspunkte für die zu ergreifenden Maßnahmen, indem sie bestimmte Sicherheitsbereiche aufstellen. Die konkrete Ausfüllung ist jedoch eine Frage des Einzelfalls, wobei allerdings die Sensitivität der vorhandenen personenbezogenen und durch das BDSG geschützten Daten und die Gefährdungslage zu berücksichtigen sind.

414 Um den Anforderungen von § 9 BDSG nachzukommen, sind grundsätzlich mehrere wichtige Punkte zu beachten bzw. einzuhalten:

(ii) IT-Sicherheitskonzept

415 Am Anfang jeder Sicherheitsmaßnahme steht die Aufstellung eines gewissen IT-Sicherheitskonzepts. Durch die Erfassung auch organisatorischer Maßnahmen ist grund-

---

762 Ebenso § 5 Abs. 1 Satz 2 BerlinDSG.

763 *Schneider*, Handbuch des EDV-Rechts, Kap. B Rn. 492; eingehend dazu *Ernestus*, in: Roßnagel, Handbuch Datenschutzrecht, Kap. 3.2 Rn. 29 ff.

764 *Schneider*, Handbuch des EDV-Rechts, Kap. B Rn. 504; *Tinnefeld/Ehmann/Gerling*, Einführung in das Datenschutzrecht, S. 629 f.

765 Eingehend dazu Spindler, Unternehmensorganisationspflichten, 269 ff.

766 *Schneider*, Handbuch des EDV-Rechts, Kap. B Rn. 490.

sätzlich ein solches erforderlich.[767] Neben der Analyse der Sensitivität der Daten im Rahmen des § 9 Satz 2 BDSG werden die konkreten Risiken beleuchtet sowie deren Minimierung oder Ausschaltung.[768] Hierbei können formalisierte Methoden und Dokumente wie das IT-Grundschutzhandbuch des BSI angewandt werden.[769] Zur Erstellung des Sicherheitskonzepts gehört jedenfalls auch die entsprechende Dokumentation bereits im Rahmen der Planung.[770]

(iii) Datensicherung (Backup)

416 Bereits aus der Anforderung der Verfügbarkeitskontrolle ergibt sich, dass eine bestimmte Form der Datensicherung in Form von Kopien (Backup) oder ähnlich zu erfolgen hat – was von der zivilrechtlichen Rechtsprechung als „Selbstverständlichkeit" bezeichnet wird.[771] Hierbei kann eine regelmäßige Sicherung auf externen Datenträgern, Sicherungen auf anderen Rechnern oder auch die jederzeitige Verdopplung von Daten (sog. RAID-Systeme) verwendet werden.[772] Grundsätzlich empfiehlt sich insbesondere bei hochsensitiven Daten eine Kombination dieser Methoden.

(iv) Erkennung und Abwehr externer Angriffe

417 Insbesondere die unter den Begriffen Zugangs-, Zugriffs- und Weitergabekontrolle erfassten Sicherungsmaßnahmen können bei Angriffen von außen relevant sein. Danach soll gewährleistet werden, dass Dritte nicht auf Daten zugreifen, diese manipulieren oder zerstören können,[773] wovon auch der externe Zugriff durch unbefugte Dritte erfasst ist.[774]

418 Die Pflicht kann hier die Verwendung sicherer Authentifizierungsmethoden, also insbesondere Passwörter, aber auch den Schutz vor dem Zugang von außen durch eine Firewall umfassen.[775] Auch der Einsatz von Virenscannern zählt zum Stand der Technik

---

767 *Wohlgemuth/Gerloff*, Datenschutzrecht, S. 158; *Heibey*, in: Roßnagel, Handbuch Datenschutzrecht, Kap. 4.5 Rn. 135 ff.; *Schneider*, Handbuch des EDV-Rechts, Kap. B Rn. 499; *Bizer*, DuD 2006, 5; *Spindler*, Unternehmensorganisationspflichten, S. 273.

768 *Heibey*, in: Roßnagel, Handbuch Datenschutzrecht, Kap. 4.5 Rn. 135; *Spindler*, Unternehmensorganisationspflichten, S. 270.

769 *Wohlgemuth/Gerloff*, Datenschutzrecht, S. 162.

770 LG Köln CR 2003, 724 (725) = JurPC 62/2004, Rn. 38.

771 BGH NJW 1996, 2924 (2926); OLG Karlsruhe NJW-RR 1997, 554; krit. zur teilweise widersprüchlichen Rechtsprechung bei der vertraglichen Risikoverteilung *Erben/Zahrnt*, CR 2000, 88.

772 *Heibey*, in: Roßnagel, Handbuch Datenschutzrecht, Kap. 4.5 Rn. 123 ff.

773 *Ernestus*, in: Roßnagel, Handbuch Datenschutzrecht, Kap. 3.2 Rn. 25.

774 *Heibey*, in: Roßnagel, Handbuch Datenschutzrecht, Kap. 4.5 Rn. 42, 68.

775 *Tinnefeld/Ehmann/Gerling*, Einführung in das Datenschutzrecht, S. 662; *Heibey*, in: Roßnagel, Handbuch Datenschutzrecht, Kap. 4.5 Rn. 131.

und wird daher von § 9 BDSG gefordert.[776] Ob auch bereits Intrusion Detection Systeme[777] zum Stand der (Sicherheits-) Technik gehören, lässt sich nicht ohne weiteres entscheiden.[778] Je gebräuchlicher und je leichter handhabbar diese Systeme jedoch werden, desto eher wird eine Pflicht zum Einsatz bestehen.

(v) Schaffung verbindlicher Regelungen

419 Um den Anforderungen des § 9 BDSG sinnvoll nachkommen zu können, müssen die Vorgaben unternehmensintern insgesamt und überall eingeführt sowie eingehalten werden. Der Datenschutzpflichtige kann sich nicht auf reine Empfehlungen beschränken; auch muss den Unternehmensangehörigen verdeutlicht werden, dass an die Verletzung derartiger Regeln Sanktionen geknüpft werden können.

(vi) Dokumentation

420 Bereits als Teil der Risikoanalyse, aber auch, um die Durchsetzung zu ermöglichen bzw. zu erleichtern, empfiehlt sich die Dokumentation der vorgenommenen Maßnahmen sowie der dazu führenden Gründe. Hierzu gehört, die Art der Daten, Speicherung, Speicherort, Gefährdungspotentiale und technisch-organisatorische Maßnahmen. Für öffentliche Stellen bestehen durch die Rechnungshöfe des Bundes und der Länder festgelegte Mindestanforderungen.[779]

(vii) Datenschutzbeauftragter

421 Ein weiteres Instrument der unternehmensinternen Kontrolle ist die Pflicht zu Bestellung eines Datenschutzbeauftragten: Nach § 4f BDSG ist sowohl in öffentlichen als auch in nicht-öffentlichen Stellen ein Datenschutzbeauftragter zu bestellen.[780] Im öffentlichen Bereich gibt es auch entsprechende Regelungen der Länder.[781] Mit der Wahl der Verpflichtung zur Bestellung wurde eine Regelung geschaffen, die zwischen staatlicher Aufsicht und wirtschaftlicher Eigenkontrolle liegt.[782] Entsprechend § 4g BDSG wirkt der Beauftrage auf die Einhaltung des BDSG sowie anderer datenschutzrechtlicher Bestimmungen hin. Er ist somit auch verantwortlich für die durch § 9 BDSG sowie

776 *Heibey*, in: Roßnagel, Handbuch Datenschutzrecht, Kap. 4.5 Rn. 131.
777 Vgl. *Tinnefeld/Ehmann/Gerling*, Einführung in das Datenschutzrecht, S. 650.
778 Dafür *Heibey*, in: Roßnagel, Handbuch Datenschutzrecht, Kap. 4.5 Rn. 133 f.
779 IuK-Mindestanforderungen 2001, abrufbar unter http://www.bsi.de/gshb/deutsch/hilfmi/extern/IuKMindestanforderungen.pdf.
780 Ausführlich *Spindler*, Unternehmensorganisationspflichten, S. 283 ff.
781 *Abel*, in: Roßnagel, Handbuch Datenschutzrecht, Kap 5.6 Rn. 5.
782 *Königshofen*, in: Roßnagel, Handbuch Datenschutzrecht, Kap 5.5 Rn. 3 f.

die zugehörige Anlage normierten Pflichten.[783] Mittelbar übernimmt er folglich für alle Anlagen und Daten, für die das BDSG Anwendung findet, auch die Aufgabe des IT-Sicherheitsbeauftragten. Zu beachten gilt, dass der Datenschutzbeauftragte weder als betrieblicher Beauftragter noch als Unternehmensbeauftragter einzuordnen ist, was bedeutet, dass GmbH & Co., KG, OHG und AG nicht für jeden ihrer Betriebe einen gesonderten Datenschutzbeauftragten bestellen müssen, sondern nur für jede rechtlich selbstständige Einheit.[784]

422 Sofern der Datenschutzbeauftragte nicht selbst fahrlässig oder vorsätzlich seinen Pflichten nicht nachgekommen ist, ist vertragsrechtlich nicht er, sondern der Rechtsträger des Unternehmens verantwortlich. Der Datenschutzbeauftragte haftet somit grundsätzlich nicht persönlich, sondern ist nur intern verantwortlich gegenüber der nach außen verpflichteten Stelle.[785] Denkbar sind Schadensersatzansprüche der verantwortlichen Stelle gegen den Datenschutzbeauftragten bei Pflichtverletzungen.[786] Eine Haftung nach § 823 Abs. 1 oder Abs. 2 BGB i.V.m. den §§ 4f, g BDSG gegenüber Dritten dagegen kommt grds. nicht in Betracht, da der Beauftragte selbst keine Maßnahmen durchführen und veranlassen kann, weil er weder Entscheidungs- noch Anordnungsbefugnisse besitzt,[787] und sich weiter der schützenswerte Personenkreis nicht derart abgrenzen lässt, wie es für ein Schutzgesetz nach § 823 Abs. 2 BGB erforderlich ist.[788] Eine Haftung des Datenschutzbeauftragten selbst nach §Handbuch Datenschutzrecht 823 BGB wäre daher nur denkbar, wenn die verantwortliche Stelle ihm derartige Kompetenzen zum Treffen von Maßnahmen erteilt hätte, so das eine persönliche Haftung des Datenschutzbeauftragen einen absoluten Ausnahmefall darstellt.[789] Denkbar sind auch Ansprüche der Betroffenen nach §§ 824 826 BGB, wenn der Datenschutzbeauftragte seine Verschwiegenheitspflichten verletzt.[790] Allerdings bestehen gerade hinsichtlich der Haftung der Beauftragten nach wie vor Unsicherheiten. Seine organisatorische Stellung sowie die Aufgabenwahrnehmung unterliegen jedenfalls indirekt der behördlichen Aufsicht. So kann die Aufsichtsbehörde bei Fehlen entsprechender Fachkunde oder wegen anderer

783 *Gliss*, DSB 1996, Heft 5, 1; *Königshofen*, in: Roßnagel, Handbuch Datenschutzrecht; Kap 5.5 Rn. 27; *Spindler*, Unternehmensorganisationspflichten, S. 286; *Breinlinger*, RDV 1995, 7 (8).

784 Simitis-*Simitis*, § 4f BDSG Rn. 34 f.

785 *Königshofen*, in: Roßnagel, Handbuch Datenschutzrecht, Kap 5.5 Rn. 17.

786 Näher dazu Simitis-*Simitis*, § 4g BDSG Rn. 97 ff.

787 Simitis-*Simitis*, § 4f BDSG Rn. 127 f.; *Gola/Schomerus*, § 4f Rn. 48.

788 Simitis-*Simitis*, § 4g BDSG Rn. 103 ff.; allgemeinen zur Haftung des Beauftragten *Spindler*, Unternehmensorganisationspflichten, S. 940.

789 S. dazu Simitis-*Simitis*, § 4g BDSG Rn. 104.

790 Simitis-*Simitis*, § 4g BDSG Rn. 107.

wichtiger Gründe nach § 38 Abs. 5 Satz 3 BDSG bzw. § 36 Abs. 3 Satz 4 BDSG, § 626 BGB den Widerruf seiner Bestellung verlangen.[791]

(viii) Datenschutzaudit, § 9a BDSG

423 Noch relativ neu ist die Einführung eines Datenschutzaudits in § 9a BDSG. Das Vorbild hierzu entstammt dem Bereich des Umweltrechts[792] und dessen Umweltauditvorgaben im BImSchG bzw. der EG-Öko-Audit-VO. Ziel des Audits ist die Verbesserung des Datenschutzes in einem kontinuierlichen und auch wirtschaftlich motivierten Prozess. Die Norm wendet sich an öffentliche wie nicht-öffentliche Stellen, welche personenbezogene Daten unter Einsatz von IT-Systemen verarbeiten.[793] Regelungen zum Datenschutzaudit finden sich mit jeweils unterschiedlichem Normadressat auch an anderer Stelle, so z.B. in § 78c SGB X. Einige **Landesdatenschutzgesetze** enthalten ebenfalls entsprechende Regelungen zu Datenschutzaudits[794] für die öffentlichen Stellen des Landes, die ihr Datenschutzkonzept und ihre technischen Einrichtungen einer Prüfung unterziehen können.

424 Durch ein Audit wird eine externe und neutrale Begutachtung des vorhandenen Datenschutzkonzepts durchgeführt.[795] Das Audit ist nach der Fassung des § 9a BDSG nicht obligatorisch.[796] Entsprechende Zertifikate sollen insbesondere wirtschaftliche Vorteile hervorrufen. Allerdings ist die Zertifizierung finanziell aufwändig und damit vor allem für kleinere Unternehmen praktisch nicht finanzierbar.[797] Das Verfahren der Prüfung umfasst die Prüfung und Bewertung der Vorgaben, die die Prüfung veranlassende Stelle, also das Unternehmen, vorgibt.[798] Das Unternehmen wählt hierfür Produkt oder Verfahren aus,[799] erarbeitet hierzu ein Datenschutzkonzept und legt dem Gutachter die entsprechenden Unterlagen zur Prüfung und Bewertung vor.[800] Dabei umfasst die Prüfung auch eine Rechtmäßigkeitskontrolle, also die Bewertung der Erfüllung der allgemeinen

---

791 *Spindler*, Unternehmensorganisationspflichten, S. 287 f. mwN.
792 *Roßnagel*, in: Roßnagel, Handbuch Datenschutzrecht, Kap. 3.7 Rn. 83.
793 *Voßbein*, DuD 2004, 92 (93).
794 § 11c BdgDSG, § 10a DSG NW, § 4 Abs. 2, 43 Abs. 2 LDSG SH, s. dazu *Bäumler*, DuD 2004, 80; Simitis-*Bizer*, § 9a BDSG Rn. 32.
795 Zur Datenschutzzertifizierung *Reiländer/Weck*, DuD 2003, 692; *Rösser*, DuD 2003, 401.
796 *Tinnefeld/Ehmann/Gerling*, Einführung in das Datenschutzrecht, S. 455.
797 *Gola/Schomerus*, § 9a BDSG Rn. 4.
798 Simitis-*Bizer*, § 9a BDSG Rn. 69; *Roßnagel*, in: Roßnagel, Handbuch Datenschutzrecht, Kap. 3.7 Rn. 93.
799 *Roßnagel*, in: Roßnagel, Handbuch Datenschutzrecht, Kap. 3.7 Rn. 92.
800 Simitis-*Bizer*, § 9a BDSG Rn. 70; ähnl. *Roßnagel*, in: Roßnagel, Handbuch Datenschutzrecht, Kap. 3.7 Rn. 100, 106 f.

objektiven Vorgaben des BDSG.[801] Zusätzlich werden auch die technischen Einrichtungen und Verfahren durch den Auditor überprüft.[802] Die näheren Anforderungen ergeben sich aus dem nach § 9a Satz 2 BDSG zu erlassenden Ausführungsgesetz, für das allerdings bislang hinsichtlich der Durchführung des fakultativen Audits gemäß § 9a BDSG keinerlei bundeseinheitliche Regelungen bestehen, die die Rahmenbedingungen hinsichtlich der Akkreditierung der Gutachter, die Registrierung und deren Widerruf sowie die Verwendung des Datenschutzauditzeichens abstecken. Maßstab der Bewertung ist die Verbesserung von Datenschutz und Datensicherheit. § 9a BDSG bezieht ausdrücklich nicht nur den Datenschutz, sondern auch die Datensicherheit in das Audit ein.[803] Begutachtet werden können demnach auch Konzepte und Umsetzung der Pflichten aus § 9 BDSG sowie der zugehörigen Anlage. Allerdings verlangt § 9a S. 2 BDSG, dass die näheren Anforderungen an das Audit-Verfahren sowie die Auswahl und Zulassung der Gutachter in einem besonderen Gesetz geregelt werden müssen. Ein solches Ausführungsgesetz existiert aber bislang nicht.[804] Praktisch angewandt wird die Auditierung bislang daher lediglich in Schleswig-Holstein, die in § 43 Abs. 2 LDSG Schleswig-Holstein das Unabhängige Landeszentrum für Datenschutz (ULD) als Begutachter benennen, bei denen öffentliche Stellen ihr Datenschutzkonzept prüfen und beurteilen können. Dabei wird unterschieden zwischen einem Behördenaudit nach § 43 Abs. 2 LDSG SH und einem Produktaudit nach § 4 Abs. 2 LDSG SH. Die zum Datenschutzkonzept verwendeten Produkte können danach dem ULD vorgelegt werden. Das ULD überprüft dann die Produkte und verleiht ihnen gegebenenfalls ein Zertifikat (Gütesiegel).[805] Materielle Standards sind allerdings – soweit ersichtlich – nicht publiziert, nach denen die Auditierungen vorgenommen werden.

425 Die Common Criteria selbst beziehen solche Audits als mögliche Einsatzszenarien entsprechender Zertifikate ein. So sollen nach Nr. 6.3.4 der Common Criteria Teil 1 Auditoren von nach den Common Criteria erteilten Zertifikaten profitieren können. Sofern sich solche Querbezüge durchsetzen, könnte sich dies natürlich auch auf den finanziellen Aufwand für Datenschutzaudits auswirken, sofern die Prüfung nach den Common

801 *Münch*, RDV 2003, 223 (225); *Roßnagel*, in: Roßnagel, Handbuch Datenschutzrecht, Kap. 3.7 Rn. 96.
802 Simitis-*Bizer*, § 9a BDSG Rn. 70, 58.
803 Zum Audit nach § 9a BDSG s. auch *Schläger*, DuD 2004, 459; *Bäumler*, DuD 2004, 80; *Bizer*, DuD 2006, 5; *Roßnagel*, Datenschutzaudit, 2000.
804 Simitis-*Bizer*, § 9a BDSG Rn. 76.
805 Mehr dazu unter: https://www.datenschutzzentrum.de/material/recht/audit/audit.htm.

Criteria tatsächlich auch die Datenschutzanforderungen einbezogen hat.[806] So enthalten die Funktionsklassen der Common Criteria durchaus auch den Schutz von Daten.[807] Das Verfahren der Prüfung regeln die Common Criteria jedoch nicht.[808]

426 Eine staatlich geregelte **Datenschutz-Zertifizierung für IT-Produkte** (Hard- und Softwareprodukte sowie Datenverarbeitungsverfahren) ist derzeit nur im Bundesland Schleswig-Holstein möglich, soweit die Produkte zur Nutzung für öffentliche Stellen geeignet sind.[809] Das Unabhängige Landeszentrum für Datenschutz Schleswig Holstein (ULD)[810] bietet hierzu ein **Datenschutz-Gütesiegel** an, welches nachweist, dass die Vereinbarkeit eines Produktes mit den Vorschriften über Datenschutz und Datensicherheit in einem förmlichen Verfahren festgestellt worden ist.[811] Die Zertifizierung soll vorrangig Behörden die Auswahl datenschutzgerechter Produkte zu erleichtern (s. § 4 Abs. 2 LDSG SH), das ULD empfiehlt die Verwendung des Datenschutz-Gütesiegels aber auch als Wettbewerbsvorteil im Privatkundensektor. Es kann auch von Anbietern und Herstellern außerhalb Schleswig-Holsteins erworben werden.[812]

(4) Aufsicht und Durchsetzung

427 Relevant für die weiträumige Verbreitung von sicherer IT-Sicherheitsinfrastruktur sind nicht nur die positiv vorhandenen Pflichten, sondern insbesondere die Durchsetzung in Form von Aufsicht und Sanktionen. Nur anhand dieser lässt sich auch die Effektivität der vorhandenen Regelungen beurteilen (Enforcement).

(a) Aufsicht

428 Die Durchsetzung der datenschutzrechtlichen Pflichten erfolgt grundsätzlich im Rahmen der staatlichen Aufsicht, die ergänzend neben die Selbstkontrolle tritt.[813] Dabei ist wiederum zwischen den öffentlichen und den nicht-öffentlichen Stellen zu unterscheiden:

---

806 Ähnl. Überlegungen stellt *Münch*, RDV 2003, 223 (224 f.) an.

807 Common Criteria Teil 2 Nr. 8.1.

808 Common Criteria v3.0 Rev. 2 Teil 1, abrufbar unter: http://www.bsi.bund.de/cc/CCMB2005V3T1.pdf, Rn. 6.

809 Landesverordnung über ein Datenschutzaudit (Datenschutzauditverordnung – DSAVO) vom 3.4.2001, GVOBl. Schleswig-Holstein 4/2001, S. 51. abrufbar unter: http://www.datenschutzzentrum.de/guetesiegel/index.htm. Dazu auch Simitis-*Bizer*, § 9a BDSG Rn. 33 ff.

810 Abrufbar unter: http://www.datenschutzzentrum.de.

811 Zum Anforderungskatalog siehe abrufbar unter: http://www.datenschutzzentrum.de/download/anford.pdf.

812 Simitis-*Bizer*, § 9a BDSG Rn. 33.

813 *Hillenbrand-Beck*, in: Roßnagel, Handbuch Datenschutzrecht, Kap. 5.4 Rn. 4.

(i) Nicht-öffentliche Stellen

429 § 38 BDSG enthält eine explizite Aufsichtsregelung nicht-öffentlicher Stellen für den Bereich Datenschutz. Nach den Landesregelungen werden öffentlich-rechtliche Wettbewerbsunternehmen zwar den Pflichten der nicht-öffentlichen Stellen, aber der Aufsicht wie für öffentliche Stellen unterworfen.[814] In den Aufgabenbereich fallen auch die technischen und organisatorischen Maßnahmen nach § 9 BDSG.[815] Die Kompetenzen der Aufsichtsbehörde reichen vom Auskunftsrecht über die Betretung und Besichtigung von Räumen bis hin zur Anordnung von technischen oder organisatorischen Maßnahmen im Rahmen des § 9 BDSG. Die Kontrolle ist gemäß § 38 Abs. 1 Satz 1 BDSG anlassunabhängig. Nach § 38 Abs. 5 Satz 2 BDSG können bei schwerwiegenden Verstößen auch einzelne Verfahren untersagt werden. Im Wege des Verwaltungszwangs können die einzuhaltenden Pflichten auch durchgesetzt werden.[816] Zudem dient sie auch der Kontrolle des Datenschutzbeauftragten. An die Aufsichtsbehörde können sich auch betroffene Dritte wenden, die sich über die Verletzung eigener Rechte durch datenschutzrechtlich nicht erlaubtes Handeln beschweren.

(ii) Öffentliche Stellen

Für die Kontrolle der öffentlichen Stellen des Bundes ist nach § 24 Abs. 1 BDSG der Bundesbeauftragte für den Datenschutz zuständig, für die öffentlichen Stellen der Länder liegt die Zuständigkeit bei den Landesdatenschutzbeauftragten. Er nimmt hauptsächlich eine Beraterrolle ein.[817] Dementsprechend beschränken sich seine Kontrollkompetenzen auf ein Auskunfts- und Betretungsrecht, er teilt seine Ansicht bzw. Beanstandungen der öffentlichen Stelle mit. Er kann keine verbindlichen Weisungen erteilen,[818] die Beanstandung ist auch nicht als solche aufzufassen.[819] Zusätzlich kann er Rechtsverletzungen bei der jeweiligen höchsten Aufsichtsbehörde beanstanden, die anschließend im Rahmen ihrer Fach- oder Rechtsaufsicht entsprechende Schritte einleiten kann.[820] Dies gilt ebenso für die Landesdatenschutzbeauftragten, für die das Instrument der Beanstandung insgesamt durch die Länder übernommen wurde. Vom Aufga-

814 Simitis-*Dammann*, § 27 BDSG Rn. 16; *Hillenbrand-Beck*, in: Roßnagel, Handbuch Datenschutzrecht, Kap. 5.4 Rn. 44.
815 *Schneider*, Handbuch des EDV-Rechts, Kap. B Rn. 513.
816 *Auernhammer*, § 38 BDSG Rn. 14; Simitis-*Petri*, § 38 BDSG Rn. 64.
817 *Tinnefeld/Ehmann/Gerling*, Einführung in das Datenschutzrecht, S. 427.
818 *Heil*, in: Roßnagel, Handbuch Datenschutzrecht, Kap. 5.1 Rn. 57; *Gola/Schomerus*, § 25 BDSG Rn. 4.
819 BVerwG CR 1993, 242.
820 *Gola/Schomerus*, § 24 BDSG Rn. 7.

benbereich des Bundesdatenschutzbeauftragten sind auch die Sicherungsmaßnahmen des § 9 BDSG erfasst.[821]Sanktionen

Neben dem verwaltungsrechtlichen Zwang enthält das BDSG in §§ 43 f. BDSG Bußgeld- und **Strafvorschriften**. Jedoch werden die Pflichten nach § 9 BDSG nicht von diesen Sanktionen mangels Verweis in § 43 BDSG erfasst.

Neben die Strafvorschriften treten **Haftungsinstrumente**,[822] etwa in Gestalt von § 7 BDSG, der für den Betroffenen einen eigenständigen[823] Schadensersatzanspruch für die unzulässige Erhebung, Verarbeitung oder Nutzung von Daten vorsieht. Nach der Legaldefinition in § 3 Abs. 4 Nr. 1 BDSG erfasst das Verarbeiten von Daten auch das Speichern im Sinne von Erfassen, Aufnehmen oder Aufbewahren personenbezogener Daten auf einem Datenträger zum Zweck ihrer weiteren Verarbeitung oder Nutzung. Demnach ist jedenfalls auch ein Backup von der Haftungsregelung erfasst.

Im unternehmerischen Bereich wurde aufgrund des **Wettbewerberschutzes** nach § 1 UWG i.V.m. § 9 BDSG ein Anspruch der Wettbewerber sowie der Verbraucherschutzverbände auf Einhaltung der Pflichten aus § 9 BDSG angenommen. Denn bei Verletzung der datenschutzrechtlichen Pflichten verschafft sich ein Unternehmer einen Wettbewerbsvorteil gegenüber anderen Wettbewerbern.[824] Ob diese Annahme indes auch nach der Novellierung des UWG noch Gültigkeit beanspruchen kann, erscheint mehr als zweifelhaft: Denn schon unter dem alten UWG hatte der BGH einem allgemeinen Anspruch auf Einhaltung der Rechtsnormen (Vorsprung durch Rechtsbruch[825]) eine Absage erteilt und nur solche Normen sanktioniert, die einen Markt- bzw. Wettbewerbsbezug vorsahen[826] – zu denen das BDSG nicht gehören dürfe.[827] Der Gesetzgeber hat diese Rechtsprechung nunmehr in § 4 Nr. 7 UWG kodifiziert.

Mittelbare Wirkung kann § 9 BDSG sowohl für vertragliche als auch deliktische Ansprüche entfalten, in dem die Anforderungen nach § 9 BDSG den geschuldeten Sorgfaltsstandard bzw. die Verkehrspflichten konkretisieren.[828] Wer die nach § 9 BDSG erforderli-

---

821 *Gola/Schomerus*, § 24 BDSG Rn. 3.

822 Auf Auskunfts- und Berichtigungsansprüche wird in diesem Rahmen nicht eingegangen.

823 *Schneider*, Handbuch des EDV-Rechts, Kap. B Rn. 518 f.

824 LG Hamburg NJW-RR 1997, 1407; LG Stuttgart CR 1997, 83; *Weichert*, in: Killian/Heussen, Kap. 134 Rn. 69; *Kahlert*, DuD 2003, 412 (415).

825 BGHZ 110, 278 (289); BGH GRUR 1973, 146 (147).

826 BGHZ 110, 278 (289); BGH VersR 1999, 987; BGH WRP 2002, 684; BGH NJW-RR 2002, 1193; dazu auch *Hoeren*, VersR 2005, 1014; *v. Gamm*, GRUR 1996, 574 (577 f.).

827 *v. Gamm*, GRUR 1996, 574 (578); *Kahlert*, DuD 2003, 412 (415 f.).

828 *Abel*, in: Roßnagel, Handbuch Datenschutzrecht, Kap. 7.11 Rn. 28; *Gorny*, CR 1986, 673; *Schneider*,

chen Sicherungsmaßnahmen nicht ergreift, unterliegt der Haftung.[829] Außerdem kann § 9 BDSG ein Schutzgesetz im Sinne von § 823 Abs. 2 BGB sein.[830]

b) TMG

430 Auch das TMG enthält für Daten, die im Rahmen von Telediensten anfallen, Regelungen zur Datensicherheit, die mit § 9 BDSG vergleichbar sind. § 13 Abs. 4 TMG enthält eine Aufzählung von bestimmten Schutzzielen, die erreicht werden sollen. Ziel ist auch hier der Systemdatenschutz.[831] Nach § 13 Abs. 4 TMG muss der Diensteanbieter durch technische und organisatorische Vorkehrungen dafür sorgen, dass der Nutzer Teledienste geschützt gegen die Kenntnisnahme Dritter wahrnehmen kann. Wie die Schutzziele zu erreichen sind, regelt das TMG nicht, es sind jedoch die erforderlichen Maßnahmen zu ergreifen.

431 § 13 Abs. 4 TMG schützt allerdings nicht die Übertragung der Informationen, die bereits durch das TKG erfasst wird, sondern die **interne Datenverarbeitung**, was schon § 11 III TMG klarstellt.[832] § 13 Abs. 4 TMG enthält für bestimmte Teilbereiche das Erfordernis der Ergreifung von Maßnahmen. In diesen Bereichen liegt somit eine bereichsspezifische Spezialregelung vor, die das BDSG verdrängt.[833] Außerhalb dieser Teilbereiche gelten das BDSG und damit die Anforderungen des § 9 BDSG weiter. Insgesamt sind die Anforderungen des § 9 BDSG inklusive der zugehörigen Anlage auch im Rahmen des § 13 TMG anzuwenden, soweit sie nicht den speziellen Regelungen bezüglich der Nutzungsdaten nach § 13 Abs. 4 i.V.m. § 15 TMG widersprechen.[834]

c) TKG

432 Vorgaben für die Datensicherheit werden schließlich auch durch das Telekommunikationsrecht getroffen: Denn durch das Fernmeldegeheimnis werden Inhalt und Umstände der Kommunikation geschützt, so dass die individuelle Nachricht ebenso wie die Verbindungsdaten erfasst werden.[835] Diensteanbieter i.S.d. TKG müssen nach § 109 Abs. 1 TKG **angemessene technische Vorkehrungen** zum Schutz der im Rahmen des Tele-

---

Handbuch des EDV-Rechts, Rn. 498; zur vertraglichen Haftung *Gola/Schomerus*, § 7 BDSG Rn. 16 ff.

829 *Horns*, in: Abel, Datenschutz in Anwaltschaft, Notariat und Justiz, § 14 Rn. 73; *Holznagel*, Recht der IT-Sicherheit, S. 176.

830 Palandt-*Sprau*, § 823 BGB Rn. 85.

831 Spindler/Schmitz/Geis-*Schmitz*, § 4 TDDSG Rn. 1, 24.

832 Spindler/Schmitz/Geis-*Schmitz*, § 4 TDDSG Rn. 34.

833 BT-Drucks. 14/6098, 14; Roßnagel-*Bizer*, § 4 TDDSG Rn. 78; *Holznagel*, Recht der IT-Sicherheit, S. 188.

834 Roßnagel-*Bizer*, § 4 TDDSG Rn. 80.

835 *Weichert*, in: Killian/Heussen, Kap. 136 Rn. 2.

kommunikationsvorgangs anfallenden Daten treffen. Damit trägt § 109 TKG dem Rang des Fernmeldegeheimnisses sowie des Datenschutzes Rechnung.[836] Normadressat des § 109 Abs. 1 TKG sind auch diejenigen, die an der Telekommunikation lediglich mitwirken, also auch Wiederverkäufer, die für ihren Betrieb Daten erheben.[837] § 109 Abs. 1 Nr. 2 TKG enthält hierbei auch die Verpflichtung zum Schutz vor unbefugten Zugriffen. Allerdings werden die Anforderungen des TKG regelmäßig nur für solche kommerziellen IT-Nutzer relevant werden, die als IT-Intermediäre einzustufen sind, da sie gleichzeitig IT-Dienstleistungen erbringen, etwa als Access-Provider, die die Nutzung von elektronischen Kommunikationsnetzen erst ermöglichen.

d) Ergebnis

433 Wie dargelegt, findet das Datenschutzrecht in allen kommerziellen Bereichen Anwendung. Es enthält zudem Regelungen, die insbesondere auch die IT-Sicherheit öffentlich-rechtlich erfassen können. Der Konkretisierungsgrad ist weitaus höher als in anderen relevanten öffentlich-rechtlichen Bereichen, etwa im Produktsicherheitsrecht. Indes besteht auch hier die Notwendigkeit einer Standardisierung, um den sich rasch ändernden Gefahrenpotentialen Rechnung zu tragen.

IV. Besondere Sicherheitsanforderungen im Banken- und Finanzsektor

1. Vorbemerkung

434 Der Banken- und Finanzsektor eignet sich in besonderer Weise für eine Untersuchung der Pflichten der kommerziellen IT-Nutzer, da einerseits inzwischen fast alle Geschäftsvorgänge mittels Informationstechnik abgewickelt werden, andererseits Fehler oder Systemausfälle schnell zu hohen Schadenssummen und schwerwiegenden Folgen für die gesamte Volkswirtschaft führen können. Daher ist es nicht verwunderlich, dass gerade für diesen Sektor spezielle Regelungen existieren, insbesondere im Hinblick auf ein Risikomanagement. Der Finanzsektor kann in drei Sektoren untergliedert werden: den Bankenbereich (KWG, Rn. 435 ff.), den Wertpapierhandel (WpHG, Rn. 453 ff.) sowie schließlich den Versicherungsbereich, wobei die ersten beiden Sektoren einer genaueren Untersuchung unterzogen werden sollen.

---

836 Säcker-*Klesczewski*, § 109 TKG Rn. 1; Scheurle/Mayen-*Zerres*, § 87 TKG aF Rn. 1; Beck'scher TKG-Kommentar-*Ehmer*, § 87 TKG aF Rn. 1.

837 Säcker-*Klesczewski*, § 109 TKG Rn. 6.

2. Anforderungen nach dem KWG

a) Hintergrund

435 Für den Bereich der Bankenaufsicht regelt § 25a KWG als Teil der qualitativen Bankenaufsicht spezielle Organisationspflichten für die beaufsichtigten Kredit- und Finanzdienstleitungsinstitute. Eine ordnungsgemäße Organisation umfasst gemäß § 25a Abs. 1 Satz 3 Nr. 4 KWG ausdrücklich auch angemessene Sicherheitsvorkehrungen für den Einsatz der elektronischen Datenverarbeitung.

436 Zweck des KWG ist es, durch vorbeugende Überwachung allgemein das Entstehen von Schäden im Kreditwesen zu verhindern.[838] Aufgabe der zuständigen Bundesanstalt für Finanzdienstleistung (BaFin) ist es, Missständen im Kredit- und Finanzdienstleistungswesen entgegenzuwirken, welche die Sicherheit der den Instituten anvertrauten Vermögenswerte gefährden, die ordnungsmäßige Durchführung der Bankgeschäfte oder Finanzdienstleistungen beeinträchtigen oder erhebliche Nachteile für die Gesamtwirtschaft herbeiführen können (§ 6 Abs. 2 KWG). Das KWG dient damit der Schaffung von Vertrauen bei Anlegern und Marktteilnehmern, der Sicherstellung der Solvenz der Unternehmen und dem Schutz der Kunden und leistet einen Beitrag zur Stabilisierung des nationalen und internationalen Finanzsystems.[839] Das aufsichtsrechtliche Handlungsinstrumentarium der BaFin zur Erreichung dieser Ziele reicht von informellem Handeln (z.B. Anforderung von Informationen, Mitteilung der BaFin zu Vorgängen in den Instituten), Rundschreiben, Anordnungen im Einzelfall bis hin zum Erlass von Rechtsverordnungen.

437 § 25a KWG wurde 1997 durch die 6. Novelle des KWG eingeführt und setzt Art. 10 der Wertpapierdienstleistungs-Richtlinie 1993[840] und Art. 4 Abs. 4 der Kapitaladäquanz-Richtlinie 1993[841] in deutsches Recht um. Durch das Finanzkonglomeraterichtlinie-Umsetzungsgesetz vom 21.12.2004[842] wurde die Vorschrift ohne relevante Auswirkungen auf das Riskmanagement in ihrer gegenwärtigen Form neu gefasst.[843]

b) Pflichten und Adressat

838 Boos/Fischer/Schulte-Mattler-*Braun*, Einf. KWG Rn. 61.
839 Boos/Fischer/Schulte-Mattler-*Braun*, Einf. KWG Rn. 61.
840 Richtlinie 93/22/EWG des Rates vom 10. Mai 1993, ABl. Nr. L 141 vom 11. Juni 1993, 27.
841 Richtlinie 93/6/EWG des Rates vom 15. März 1993, ABl. Nr. L 141 vom 11. Juni 1993, 1.
842 BGBl. I, 3610.
843 *Spindler*, in: Fleischer, Handbuch des Vorstandsrechts, § 19 Rn. 22.

438 § 25 a KWG regelt organisatorische Mindeststandards, welche eine gesetzliche Konkretisierung der allgemeinen Anforderungen an eine ordnungsgemäße Geschäftsführung darstellen.[844] Nach § 25a Abs. 1 Satz 2 KWG sind die Geschäftsleiter (vgl. § 1 Abs. 2 Satz 1 KWG) für die ordnungsgemäße Geschäftsorganisation des Instituts verantwortlich. Die Vorschrift entspricht in ihrer Bedeutung § 91 Abs. 2 AktG und nimmt im Verhältnis zum Aktienrecht eine gewisse „Schrittmacherrolle" ein.[845] Weitergehend wird nunmehr sogar eine einheitliche Auslegung und Anwendung von § 25a Abs. 1 KWG und § 91 Abs. 2 AktG vertreten.[846]

439 § 25a Abs. 2 KWG regelt die Anforderungen an die Auslagerung von Bereichen des Instituts auf andere Unternehmen (Outsourcing). Da es sich bei dieser Regelung um einen Bestandteil der allgemeinen organisatorischen Pflichten handelt, orientiert sich die Auslegung nicht nur an den speziellen Risiken eines Outsourcing, sondern auch an den allgemeinen aufsichtsrechtlichen Zielen.[847] Das Institut hat den auszulagernden Bereich klar zu definieren, das Auslagerungsunternehmen mit der erforderlichen Sorgfalt auszuwählen und die erforderlichen Weisungsbefugnisse vertraglich zu sichern. Vor allem aber muss der ausgelagerte Bereich in das interne Kontrollsystem des auslagernden Instituts integriert bleiben, als ob die Dienstleistung intern vom Institut selbst erbracht würde[848].

c) Rechtsfolgen

440 Bei Verstößen gegen die Organisationspflichten des § 25a Abs. 1 Satz 3 Nr. 4 KWG kann die BaFin aufsichtsrechtliche Maßnahmen ergreifen. Hierzu gehören informelle, unverbindliche Maßnahmen ebenso wie Anordnungen im Einzelfall (Verwaltungsakte). § 6 Abs. 3 KWG ermächtigt die BaFin gegenüber den Instituten und ihren Geschäftsleitern Anordnungen zu treffen, die geeignet und erforderlich sind, um Verstöße gegen aufsichtsrechtliche Bestimmungen zu unterbinden, oder um Missstände in einem Institut zu verhindern oder zu beseitigen, welche die Sicherheit der dem Institut anvertrauten Vermögenswerte gefährden können oder die ordnungsgemäße Durchführung der Bankgeschäfte oder Finanzdienstleistungen beeinträchtigen. Darüber hinausgehend findet

844 Boos/Fischer/Schulte-Mattler-*Braun*, § 25a KWG Rn. 2.
845 *Fleischer*, ZIP 2003, 1 (10); *Spindler*, in: Fleischer, Handbuch des Vorstandsrechts, § 19 Rn. 19.
846 *VG Frankfurt/M* WM 2004, 2157 (2160); *Preußner*, NZG 2004, 303 (305), NZG 2004, 57 (59); *Bürkle*, WM 2005, 1496 (1497); *Witte/Hrubesch*, BB 2004, 725 (730); vorsichtiger *Spindler*, in: Fleischer, Handbuch des Vorstandsrechts, § 19 Rn. 19.
847 Boos/Fischer/Schulte-Mattler-*Braun*, § 25a KWG Rn. 550.
848 Boos/Fischer/Schulte-Mattler-*Braun*, § 25a KWG Rn. 613 ff.

sich in § 25a Abs. 1 Satz 4 KWG nunmehr eine besondere Anordnungsbefugnis für die BaFin gegenüber den Instituten (nicht auch den Geschäftsleitern), wenn diese im Einzelfall nicht die adäquaten, internen Maßnahmen zur Erfüllung der Organisationspflichten des § 25a Abs. 1 KWG ergreifen. Die Anordnungsbefugnis dient damit der Gefahrenprävention.[849] Der BaFin stehen zur Durchsetzung der Vorgaben des KWG Zwangsmittel zur Verfügung. Im Extremfall kann dies bis zur Abberufung des Geschäftsleiters (§ 36 Abs. 2 KWG) oder dem Widerruf der Erlaubnis (§ 35 KWG) reichen.[850]

441 Das KWG hat **keine drittschützende Wirkung** zugunsten individueller Gläubiger. Es dient ausschließlich dem Schutz der Allgemeinheit und der Funktionsfähigkeit des Kreditgewerbes.[851] Dies folgt aus § 4 Abs. 4 FinDAG, welcher der BaFin ausdrücklich nur „Aufgaben im öffentlichen Interesse“ zuweist. Bei Verletzung der Aufsichtspflicht durch die BaFin bestehen daher keine Amtshaftungsansprüche nach § 839 BGB i.V.m. Art. 34 GG.[852] Grundsätzlich sind die Vorschriften des KWG auch keine Schutzgesetze im Sinne von § 823 II BGB zugunsten der einzelnen Bankkunden.[853] Aus der Verletzung der IT-spezifischen Organisationspflichten nach § 25a Abs. 1 KWG können daher grundsätzlich keine Schadensersatzansprüche abgeleitet werden. Bei Verletzung eines Rechtsguts oder absoluten Rechts im Sinne von § 823 Abs. 1 BGB kommen Schadensersatzansprüche nach dieser Vorschrift in Betracht. Primäre Vermögensschäden sind danach jedoch nicht ersatzfähig. Zur Konkretisierung der Verkehrspflichten im Rahmen des § 823 Abs. 1 BGB kann auf die Anforderungen des § 25a Abs. 1 KWG zurückgegriffen werden, da sich die Verkehrserwartungen daran ausrichten.[854] Daneben kommt für den Vorstand eines als Aktiengesellschaft organisierten Instituts eine Haftung nach §§ 93, 91 Abs. 2 AktG in Betracht.

d) Anhaltspunkte für IT-Konkretisierungen

442 Gemäß § 25a Abs. 1 3 Nr. 4 KWG sind angemessene Sicherheitsvorkehrungen für den Einsatz der elektronischen Datenverarbeitung zu treffen. Hintergrund dieser Regelung ist die Dominanz von IT-Produkten in allen Geschäftsbereichen der Kredit- und Finanz-

849 Boos/Fischer/Schulte-Mattler-*Braun*, § 25a KWG Rn. 25.
850 Boos/Fischer/Schulte-Mattler-*Braun*, § 25a KWG Rn. 7.
851 Boos/Fischer/Schulte-Mattler-*Braun*, Einf. KWG Rn. 63.
852 Boos/Fischer/Schulte-Mattler-*Braun*, Einf. KWG Rn. 63; anders die frühere Rechtsprechung des BGH s. BGH WM 1979, 482; WM 1979, 482; allgemein *Schenke/Ruthig*, NJW 1994, 2324.
853 Boos/Fischer/Schulte-Mattler-*Braun*, Einf. KWG Rn. 67 mwN.
854 Für den Bereich der Haftung für die Weiterverbreitung von Viren *Koch*, NJW 2004, 801 (805).

dienstleistungsinstitute. Die wachsende Arbeitsteilung und Vernetzung mit Geschäftspartnern, Kunden, Börsen und anderen Institutionen, wie beispielsweise Aufsichtsbehörden, führen zu einer immer stärkeren Abhängigkeit von der Betriebsbereitschaft der IT-Systeme der Institute und der IT-Systeme Dritter.

443 Die **Angemessenheit der erforderlichen Sicherheitsvorkehrungen** ist ein unbestimmter Rechtsbegriff, welcher anhand der Ziele des § 6 Abs. 2 KWG zu konkretisieren ist.[855] Für den IT-Bereich bilden den Beurteilungsmaßstab insbesondere die Sicherung der anvertrauten Vermögenswerte, die Sicherung der ordnungsgemäßen Durchführung der Bankgeschäfte und Finanzdienstleistungen, sowie die Vermeidung von Nachteilen für die Gesamtwirtschaft durch Missstände im Kredit- und Finanzdienstleistungswesen.[856]

444 **Maßgebliche Kriterien** sind Art und Umfang des Einsatzes von EDV, die eingesetzte Hardware, die Organisation der Datenverarbeitung (zentrale Datenverarbeitung, dezentrale Datenverarbeitung, Datenverarbeitung außer Haus) und die Verarbeitungsform (Stapelverarbeitung, Dialogverarbeitung, Datenbanksystem, Kommunikationssystem).[857] Norminterpretierende und -konkretisierende Wirkung kommt hierbei den Rundschreiben der BaFin zu.[858]

445 **IT-spezifische Vorgaben** enthalten die Mindestanforderungen an das Risikomanagement (MaRisk)[859], wobei die Erläuterungen der BaFin als gängige Standards beispielsweise die BSI-Standards für den IT-Grundschutz und die Norm ISO 17799 der International Standards Organisation einstufen (unten Rn. 451). Darüber hinaus sind von der BaFin für die Auslegung des § 25a KWG und die Verwaltungspraxis die Empfehlungen des Basle Committee on Banking Supervision zu beachten.[860] Nach Principle 8 des Rahmenkonzepts zu „Internal Control Systems“ ist ein sicheres Management Informationssystem einzurichten. Wegen der mit elektronischen Informationssystemen und dem Einsatz der Informationstechnologie verbundenen Risiken sind hierbei allgemeine Kon-

---

855 Boos/Fischer/Schulte-Mattler-*Braun*, § 25a KWG Rn. 12, 143.

856 Boos/Fischer/Schulte-Mattler-*Braun*, § 25a KWG Rn. 143.

857 Boos/Fischer/Schulte-Mattler-*Braun*, § 25a KWG Rn. 144.

858 Boos/Fischer/Schulte-Mattler-*Braun*, § 25a KWG Rn. 19; *Spindler*, in: Fleischer, Handbuch des Vorstandsrechts, § 19 Rn. 27 ff.

859 Rundschreiben BaFin Nr. 18/2005 über „Mindestanforderungen an das Risikomanagement“ vom 20.12.2005, - sog. MaRisk-Rundschreiben, abrufbar unter http://www.bafin.de/rundschreiben/89_2005/051220.htm (zuletzt abgerufen am 20.02.2006). Ausführlich *Spindler,* in: Fleischer, Handbuch des Vorstandsrechts, 2006, § 19 Rn. 27 ff.

860 *Spindler*, in: Fleischer, Handbuch des Vorstandsrechts, § 19 Rn. 32.

trollen und Anwendungskontrollen einzuführen sowie Vorsorge für den Fall des Verlusts oder längeren Ausfalls von Systemen zu treffen.[861] Für den Bereich der IT-Sicherheit finden sich zudem Vorgaben zum Riskmanagement in den Empfehlungen „Riskmanagement for Electronic Banking" vom März 1998[862] und „Risk Management Principles for Electronic Banking" vom Juli 2003.[863]

446 Die **Sicherheitsvorkehrungen** müssen alle IT-spezifischen Sicherheitsrisiken abdecken. Es muss insbesondere sichergestellt sein, dass eingesetzte Programme nachvollziehbar und fehlerfrei arbeiten und Dokumentationen der Programme vorgehalten sind. Die Software muss geprüft sein. Bei Ausfall der eigenen EDV-Anlage muss die Geschäftstätigkeit fortgesetzt werden können; hierzu sind Notfallpläne zu erstellen.[864] Im Einzelnen lassen sich vier Fehlerkategorien unterscheiden: materielles Fehlerrisiko, Formalfehlerrisiko, technisches Ausfallrisiko und Fremdnutzungsrisiko.[865] Materielle Fehler beruhen auf sachlich falschen gespeicherten Daten oder ermittelten Verarbeitungsergebnissen. Formalfehler entstehen durch Nichtbeachtung von Formalvorschriften im Zusammenhang mit der Datenverarbeitung, was regelmäßig auf organisatorische Schwächen zurückzuführen ist. Das technische Ausfallrisiko realisiert sich, wenn Hard- oder Software bzw. Daten nicht oder nicht unversehrt vorhanden sind, oder Softwarefehler zu unkontrollierten Programmabstürzen führen. Nutzen Dritte unberechtigt die Hard- oder Software, oder greifen sie unerlaubt auf Daten zu (Fremdnutzungsrisiko), kann es zu einem Bruch der Vertraulichkeit, Urheberrechtsverletzungen, aber auch zu einem Verlust von Daten oder ganzen Systemen kommen.

447 Die notwendigen Sicherheitsvorkehrungen[866] zur Vermeidung dieser Risiken umfassen Vorkehrungen, um Fehler und Schäden aufzudecken und zu verhindern, Vorsorgemaßnahmen sowie Eventualplanungen. Der Schadensverhinderung und -aufdeckung dienen organisatorische Maßnahmen, wie beispielsweise die Kontrolle der Datenerfassung, Programmfreigabeverfahren und die Kontrolle des Systembetriebs. Daneben sind tech-

---

861 Framework for Internal Control Systems in Banking Organisations, Basle Committee on Banking Supervision, Basel 1998, abrufbar unter http://www.bis.org/pupl/bcbs40de.pdf (zuletzt abgerufen am 10.05.2006); Basel Committee Publication No. 33, S. 19, Rn. 32, 33.

862 Abrufbar unter http://www.bis.org/publ/bcbs35.pdf (zuletzt abgerufen am 10.05.2006).

863 Abrufbar unter http://www.bis.org/publ/bcbs82.pdf (zuletzt abgerufen am 10.05.2006).

864 *Spindler*, in: Fleischer, Handbuch des Vorstandsrechts, § 19 Rn. 26; C & L Deutsche Revision 6. KWG-Novelle, 246.

865 Boos/Fischer/Schulte-Mattler-*Braun*, § 25a KWG Rn. 145.

866 Ausführlich Boos/Fischer/Schulte-Mattler-*Braun*, § 25a KWG Rn. 152 ff.; *Tappert*, EDV-System-Prüfung, 1994.

nische Sicherheitsvorkehrungen zum Schutz des Rechenzentrums (z.B. technische Zugangskontrollen, Feuerschutz usw.) und bezüglich der Hardware (Wartung, Betriebsschloss am Terminal usw.) vorzusehen. Bei der Software sind Ansatzpunkte für technische Sicherheitsvorkehrungen beispielsweise Kennwortverfahren, programmierte Kontrollen sowie systemtechnische Zwangsläufigkeiten. Zu letzteren gehören Zweiterfassungen, Zwangsprotokollierungen u.ä. Vorsorgemaßnahmen dienen der Vorbereitung von Schadensfällen und umfassen Backup-Vereinbarungen bei Rechnerausfall, Datenauslagerung für den Fall der Zerstörung des Originaldatenspeichers und Datensicherung für den Fall des Verlustes von Originaldaten. Ebenso sind Eventualplanungen zu erstellen, welche im Schadensfall konkrete Anwendung finden. Hierzu gehören u. a. Datenrekonstruktionsverfahren für gesicherte Daten, Wiederanlaufverfahren nach Systemabbrüchen und Backup-Betrieb. Diese Anforderungen entsprechen weitgehend den von Principle 8 des Rahmenkonzepts zu „Internal Control Systems“ geforderten Kontroll- und Vorsorgemaßnahmen.[867]

448 Im Hinblick auf ein Outsourcing nach § 25a Abs. 2 KWG ist zu beachten, dass die Sicherheitsanforderungen vertraglich eindeutig festzulegen sind und das auslagernde Institut die Einhaltung dieser Pflichten zu überwachen hat[868]. Außerdem müssen je nach Bedeutung der ausgelagerten Bereiche Notfallpläne für den Ausfall oder die Schlechtleistung des externen Dienstleisters bestehen.[869]

e) Die MaRisk[870]

449 Durch die Überführung der existierenden Rahmenvorgaben der Mindestanforderungen an die Interne Revision (MaIR),[871] der Mindestanforderungen an das Kreditgeschäft (MaK)[872] und der Mindestanforderungen an das Betreiben von Handelsgeschäften

867 Framework for Internal Control Systems in Banking Organisations, Basle Committee on Banking Supervision, Basel 1998, abrufbar unter http://www.bis.org/publ/bcbs40.pdf (zuletzt abgerufen am 06.06.2007); Basel Committee Publication No. 33, S. 19, Rn. 32, 33.

868 Boos/Fischer/Schulte-Mattler-*Braun*, § 25a KWG Rn. 635.

869 Boos/Fischer/Schulte-Mattler-*Braun*, § 25a KWG Rn. 637.

870 Rundschreiben BaFin Nr. 18/2005 über „Mindestanforderungen an das Risikomanagement“ vom 20.12.2005, sog. MaRisk-Rundschreiben, abrufbar unter http://www.bafin.de/rundschreiben/89_2005/051220.htm (zuletzt abgerufen am 06.06.2007).

871 Rundschreiben BaFin Nr. 1/2000 (BA) zu „Mindestanforderungen an die Ausgestaltung der Internen Revision der Kreditinstitute“ vom 17.01.2000 – sog. MaIR-Rundschreiben, (ehemals BaKred)., abrufbar unter http://3a-strategy.de/about/glossary/innenrevision-rundschreiben2000/document_view (zuletzt abgerufen am 06.06.2007).

872 Rundschreiben BaFin 34/2002 (BA) über "Mindestanforderungen an das Kreditgeschäft der Kreditinstitute", vom 20.12.2002, Az.: I 4 - 44 - 5/2001 – sog. MaK-Rundschreiben, abrufbar unter http://www.bundesbank.de/download/bankenaufsicht/pdf/mak_rs34_2002.pdf (zuletzt abgerufen am 06.06.2007).

(MaH)[873] in die Mindestanforderungen an das Risikomanagement (MaRisk)[874] wird dem Konzept einer einheitlichen Risikobetrachtung Rechnung getragen.[875] In den neuen Rahmenvorgaben werden detailliert Pflichten bezüglich der Ausgestaltung der Leitungs-, Steuerungs- und Kontrollprozesse als elementare Bestandteile des institutsinternen Risikomanagements festgelegt,[876] wobei § 25 Abs. 1 Nr. 1 und 2 KWG als zentraler Anknüpfungspunkt dient[877]. Mit den MaRisk sollen zugleich die an die Kreditinstitute gerichteten qualitativen Anforderungen der zweiten Säule („Qualitative Bankenaufsicht") von Basel II abgedeckt werden.[878]

450 Die modular aufgebaute MaRisk, bestehend aus einem Allgemeinen und Besonderen Teil,[879] greift zum Teil die dargestellten Grundsätze der bestehenden Rahmenvorgaben auf.[880] Insbesondere die allgemeinen Anforderungen an das Risikomanagement wurden

---

873 BaKred-Verlautbarung über „Mindestanforderungen an das Betreiben von Handelsgeschäften" vom 25.10.1995 – sog. MaH-Rundschreiben, abrufbar im Internet unter abrufbar unter: http://www.bafin.de/verlautbarungen/minanfhg.htm (zuletzt abgerufen am 06.06.2007). Zur Auslegung der MaH sind insbesondere das Rundschreiben 4/98, abrufbar unter http://www.bafin.de/rundschreiben/96_1998/va_rs4_98.pdf#search=%22R%204/98%20%22 (zuletzt abgerufen am 06.06.2007) und das Rundschreiben 5/2001 vom 12.09.2001, Geschäftszeichen I 4-42-2/2001 zu berücksichtigen, abrufbar unter http://www.bafin.de/rundschreiben/93_2001/rs05_01.htm (zuletzt abgerufen am 06.06.2007).

874 Rundschreiben BaFin Nr. 18/2005 über „Mindestanforderungen an das Risikomanagement" vom 20.12.2005, - sog. MaRisk-Rundschreiben, abrufbar unter http://www.bafin.de/rundschreiben/89_2005/051220.htm (zuletzt abgerufen am 06.06.2007). Ausführlich hierzu und auch zu den Vorgängerrahmenvorgaben, s. *Spindler*, in: Fleischer, Handbuch des Vorstandsrechts, § 19 Rn. 27 ff.

875 Vgl. *Angermüller/Eichhorn/Ramke*, Kreditwesen 2005, 396; *dies.*, Kreditwesen 2004, 833; *Pfingsten/Maifarth/Rieso*, Die Bank 2005, 34 (34 f.); *Grabau/Schlee*, Kreditwesen 2005, 392; *Schwirten /Zattler*, Die Bank 2005, 52; *Zimmermann*, BKR 2005, 208 (209).

876 Vgl. Rundschreiben BaFin Nr. 18/2005 über „Mindestanforderungen an das Risikomanagement" vom 20.12.2005, AT 4, abrufbar unter http://www.bafin.de/rundschreiben/89_2005/051220.htm (zuletzt abgerufen am 06.06.2007); s. auch *Zimmermann* BKR 2005, 208 (210); *Angermüller/Eichhorn/Ramke*, Kreditwesen 2005, 396, beide allerdings noch zum zweiten Entwurf der MaRisk vom 22.09.2005, abrufbar unter http://www.bafin.de/marisk/marisk2_entwurf.pdf (zuletzt abgerufen am 06.06.2007).

877 *Wimmer*, BKR 2006, 146.

878 Vgl. Anschreiben zum Rundschreiben BaFin Nr. 18/2005 vom 20.12.2005 „Veröffentlichung der Endfassung der MaRisk", abrufbar unter http://www.bafin.de/schreiben/89_2005/051220.htm (zuletzt abgerufen am 06.06.2007); *Angermüller/Eichhorn/Ramke*, Kreditwesen 2004, 833; *Zimmermann*, BKR 2005, 208 (209); *Grabau/Schlee*, Kreditwesen 2005, 392. Zu den Anforderungen der Säule II s. Boos/Fischer/Schulte-Mattler-*Schulte-Mattler*, KWG, Basel II Rn. 159 ff.

879 Zur Gliederung der MaRisk näher *Schwirten/Zattler*, Die Bank 2005, 52 (52 f.); *Angermüller/Eichhorn/Ramke*, Kreditwesen 2005, 396; *Grabau/Schlee*, Kreditwesen 2005, 392.

880 *Angermüller/Eichhorn/Ramke*, Kreditwesen 2005, 396; zust. *Grabau/Schlee*, Kreditwesen 2005, 392; vgl. auch *Schwirten/Zattler*, Die Bank 2005, 52; ausdrücklich *Pfingsten/Maifarth/Rieso*, Die Bank 2005, 34: „diese Bausteine werden in die MaRisk bewusst und explizit aufgenommen." S. auch das Anschreiben der BaFin an die Verbände zum ersten Entwurf vom 02.02.2005, in dem es heißt, dass „der integrierte Ansatz die große Chance zur Entwicklung eines konsistenten und umfassenden Gesamtwerks auf der Basis des § 25a Abs. 1 KWG" eröffnet, abrufbar unter http://www.bafin.de/marisk/050202.htm (zuletzt abgerufen am 06.06.2007); bzgl. der Implementierung der „Mindestanforderungen an das Betreiben von Handelsgeschäften" (MaH) aus dem Jahr 1995 s. auch das Anschreiben der BaFin an die Verbände vom 22.09.2005; abrufbar unter http://www.bafin.de/marisk/marisk2_anschreiben.htm (zuletzt abgerufen am

jedoch erheblich erweitert. Das Risikomanagement wird verstanden als Teil einer ordnungsgemäßen Geschäftsorganisation und umfasst eine angemessene Strategie und ein angemessenes internes Kontrollverfahren, wobei letzteres aus dem Internen Kontrollsystem und der Internen Revision besteht.[881] Die Geschäftsleitung ist – unabhängig von einer internen Zuständigkeitsregelung – für die ordnungsgemäße Geschäftsorganisation und Weiterentwicklung verantwortlich.[882] Sie hat auf Grundlage einer Risikotragfähigkeit und der Analyse der geschäftspolitischen Ausgangssituation eine Strategie festzulegen, in der Ziele und die entsprechenden Maßnahmen zu definieren sind.[883] Die Festlegung des Inhalts der Strategie liegt allein in der Verantwortung der Geschäftsleitung, d.h. ist nicht Gegenstand von Prüfungshandlungen durch externe Prüfer oder die interne Revision.[884] Im Rahmen eines internen Kontrollsystems sind die Regelungen zur Aufbau- und Ablauforganisation zu treffen sowie Risikosteuerungs- und -controllingprozesse einzurichten.[885] Schließlich ist über eine Interne Revision die Prüfung und Beurteilung sämtlicher Aktivitäten und Prozesse sicherzustellen.[886] Sowohl die besonderen Anforderungen an das interne Kontrollsystem als auch die an die Ausgestaltung der Internen Revision werden in dem Besonderen Teil näher spezifiziert.[887] Die Pflicht, Organisationsrichtlinien, deren Inhalt detailliert geregelt ist,[888] aufzustellen

---

06.06.2007).

881 Rundschreiben BaFin Nr. 18/2005 über „Mindestanforderungen an das Risikomanagement“ vom 20.12.2005, Vorbemerkung, AT 1, 3 Rn. 1, abrufbar unter http://www.bafin.de/rundschreiben/89_2005/051220.htm (zuletzt abgerufen am 06.06.2007); vgl. auch *Grabau/Schlee*, Kreditwesen 2005, 392; *Zimmermann*, BKR 2005, 208 (210).

882 Rundschreiben BaFin Nr. 18/2005 über „Mindestanforderungen an das Risikomanagement“, vom 20.12.2005, AT 3, 5 Rn. 1, abrufbar unter: http://www.bafin.de/rundschreiben/89_2005/051220.htm (zuletzt abgerufen am 06.06.2007); s. zur Gesamtverantwortung der Geschäftsleitung ausführlich *Zimmermann*, BKR 2005, 208 (209); *Pfingsten/Maifarth/Rieso*, Die Bank 2005, 34 (35).

883 Vgl. Rundschreiben BaFin Nr. 18/2005 über „Mindestanforderungen an das Risikomanagement“ vom 20.12.2005, AT 4.2, 6 Rn.1, abrufbar unter: http://www.bafin.de/rundschreiben/89_2005/051220.htm (zuletzt abgerufen am 06.06.2007); *Pfinsten/Maifarth/Rieson*, Die Bank 2005, 34 (35).

884 Anlage 1: MaRisk – Regelungstext mit Erläuterungen vom 20.12.2005, AT 4.2, 8 Rn. 1, abrufbar unter: http://www.bafin.de/rundschreiben/89_2005/051220_anl1.pdf (zuletzt abgerufen am 06.06.2007).

885 Rundschreiben BaFin Nr. 18/2005 über „Mindestanforderungen an das Risikomanagement“ vom 20.12.2005, AT 4.3, 6 ff.; abrufbar unter: http://www.bafin.de/rundschreiben/89_2005/051220.htm (zuletzt abgerufen am 6.06.2007) s. hierbei insbesondere auch die genauen Vorgaben in AT 4.3.1 zur Aufbau- und Ablauforganisation und AT 4.3.2 zu den Risikosteuerungs- und –controllingprozessen; s. hierzu *Zimmermann*, BKR 2005, 208 (210).

886 Vgl. Rundschreiben BaFin Nr. 18/2005 über „Mindestanforderungen an das Risikomanagement“ vom 20.12.2005, AT 4.4, 7 Rn. 1-3, abrufbar unter: http://www.bafin.de/rundschreiben/89_2005/051220.htm (zuletzt abgerufen am 6.06.2007).

887 Rundschreiben BaFin Nr. 18/2005 über „Mindestanforderungen an das Risikomanagement“ vom 20.12.2005, BT 1 und BT 2, abrufbar unter: http://www.bafin.de/rundschreiben/89_2005/051220.htm (zuletzt abgerufen am 6.06.2007). Näher zur Internen Revision *Pfingsten/Maifarth/Rieso*, Die Bank 2005, 34 (35); *Grabau/Schlee*, Kreditwesen 2005, 392.

888 Vgl. Rundschreiben BaFin Nr. 18/2005 über „Mindestanforderungen an das Risikomanagement“ vom 20.12.2005, AT 5, 8 Rn. 3 a) bis d), abrufbar unter:

sowie eine Dokumentationspflicht aller Geschäfts-, Kontroll- und Überwachungsmaßnahmen[889] sollen die Einhaltung der genannten Vorgaben sichern.

451 Nach AT 4.3.2 der MaRisk hat ein Kreditinstitut bei der Einrichtung eines angemessenen Risikosteuerungs- und -controllingprozesses zunächst die Identifizierung, Beurteilung, Steuerung sowie die Überwachung und Kommunikation der wesentlichen Risiken zu gewährleisten, d.h. die wesentlichen Risiken müssen frühzeitig erkannt, vollständig erfasst und in angemessener Weise dargestellt werden können.[890] Operationelle Risiken werden im Modul BTR 4 behandelt, in welchem es um angemessene Risikosteuerungs- und –controllingprozesse geht.[891] Darunter sind Verlustrisiken zu verstehen, die ihre Ursache in inadäquaten und fehlerhaften internen Prozessen, Personen und Systemen oder externen Ereignissen haben.[892] In BTR 4 der MaRisk ist vorgesehen, dass wesentliche operationelle Risiken zumindest jährlich identifiziert und beurteilt werden; bedeutende Schadensfälle sind hingegen unverzüglich hinsichtlich ihrer Ursachen zu analysieren. Es ist zudem jährlich hierüber an die Geschäftsleitung detailliert Bericht zu erstatten, woraufhin entschieden werden muss, welche Maßnahmen zu ergreifen sind. Daneben spielt auch die Interne Revision eine erhebliche Rolle. Ihr ist nach AT 4.4 der MaRisk zur Wahrnehmung der Aufgaben ein vollständiges und uneingeschränktes Informationsrecht einzuräumen; hierfür erhält sie auch das Recht, Einblick in die Aktivitäten und Prozesse sowie in die IT-Systeme des Kreditinstituts zu nehmen.[893] Zwar sind die weiteren besonderen Anforderungen an die

---

http://www.bafin.de/rundschreiben/89_2005/051220.htm (zuletzt abgerufen am 6.06.2007); näher hierzu *Zimmermann*, BKR 2005, 208 (215).

889 In dem zweiten Entwurf wurden alle Dokumentationsanforderungen des ersten Entwurf zugunsten einer „Generalklausel" gestrichen, um den Kreditinstituten breite Spielräume im Hinblick auf erforderliche Dokumentationen zu eröffnen, s. hierzu das Anschreiben der BaFin an die Verbände vom 22.09.2005, abrufbar unter: http://www.bafin.de/marisk/marisk2_anschreiben.htm (zuletzt abgerufen am 6.06.2007). Zu der Regelung im ersten Entwurf s. den ersten Entwurf über die „Mindestanforderungen an das Risikomanagement", AT 6, 8 Rn. 1 f., abrufbar unter: http://www.bafin.de/marisk/marisk_entwurf.pdf (zuletzt abgerufen am 6.06.2007); krit. hierzu *Grabau/Schlee*, Kreditwesen 2005, 392. Zu der neuen, allgemeiner gefassten Regelung, die auch in der verabschiedeten Endfassung beibehalten wurde und lediglich in dem zweiten Absatz bezogen auf die Begründung konkretisiert wurde s. Rundschreiben BaFin Nr. 18/2005 über „Mindestanforderungen an das Risikomanagement" vom 20.12.2005, AT 6, 8 Rn. 1 f., abrufbar unter: http://www.bafin.de/rundschreiben/89_2005/051220.htm (zuletzt abgerufen am 6.06.2007).

890 Rundschreiben BaFin Nr. 18/2005 über „Mindestanforderungen an das Risikomanagement", vom 20.12.2005, AT 4.3.2, 7 Rn. 2, abrufbar unter: http://www.bafin.de/rundschreiben/89_2005/051220_anl1.pdf (zuletzt abgerufen am 6.06.2007).

891 *Zimmermann*, BKR 2005, 208 (210); s. zum ersten Entwurf der MaRisk *Angermüller/Eichhorn/Ramke*, Kreditwesen 2005, 396.

892 *Zimmermann*, BKR 2005, 208 (210); Boos/Fischer/Schulte-Mattler-*Schulte-Mattler*, KWG, Basel II Rn. 133.

893 Rundschreiben BaFin Nr. 18/2005 über „Mindestanforderungen an das Risikomanagement" vom 20.12.2005, AT 4.4, 8 Rn. 4, abrufbar unter:

Interne Revision in dem besonderen Teil in Abschnitt BT 2 der MaRisk konkretisiert, nähere Regelungen speziell zum IT-Grundschutz sind dort jedoch nicht aufgelistet. Einzelne detaillierte Regelungen zur technisch-organisatorischen Ausstattung finden sich aber in dem allgemeinen Teil der MaRisk,[894] wobei jedoch keine konkreten Anforderungen an bestimmte Systeme gestellt werden, sondern vielmehr die Ziele für ein IT-System vorgegeben werden, um eine möglichst flexible Regelung zu schaffen. Hiernach hat sich gemäß AT 7.2 der MaRisk der Umfang und die Qualität der technisch-organisatorischen Ausstattung insbesondere an betriebsinternen Erfordernissen, den Geschäftsaktivitäten sowie der Risikosituation zu orientieren. Abzustellen ist grundsätzlich nach AT 7.2 der MaRisk auf „gängige Standards", wozu die Erläuterungen der BaFin z. B. das IT-Grundschutzhandbuch (seit der Version 2005 umbenannt in IT-Grundschutzkataloge) des BSI und den internationalen Standard ISO 17799 der International Standards Organisation zählen. Die Eignung der Standards ist regelmäßig vom fachlich und technisch zuständigen Personal zu überprüfen. Die IT-Systeme, d.h. Hardware- und Software-Komponenten sowie die zugehörigen IT-Prozesse müssen die Integrität, die Verfügbarkeit, die Authentizität sowie die Vertraulichkeit der Daten sicherstellen.[895] Außerdem sind die IT-Systeme nach AT 7.2 der MaRisk vor ihrem erstmaligen Einsatz und auch nach wesentlichen Veränderungen zu testen und von den fachlichen sowie von den technisch zuständigen Mitarbeitern abzunehmen. Für Notfälle in kritischen Aktivitäten und Prozessen ist gemäß AT 7.3 der MaRisk ein Notfallkonzept zu treffen, welches geeignet sein muss, das Ausmaß möglicher Schäden zu reduzieren und Geschäftsführungs- sowie Wiederanlaufpläne zu umfassen hat. Die Wirksamkeit und Angemessenheit ist regelmäßig durch Notfalltests zu überprüfen. Innerhalb eines angemessenen Zeitraums müssen die Wiederanlaufpläne die Rückkehr zum Normalbetrieb ermöglichen und die im Notfall zu verwendenden Kommunikationswege sind festzulegen.[896]

---

http://www.bafin.de/rundschreiben/89_2005/051220_anl1.pdf (zuletzt abgerufen am 06.06.2007).

894 *Pfingsten/Maifarth/Rieso,* Die Bank 2005, 34 (36); *Angermüller/Eichhorn/Ramke*, Kreditwesen 2005, 396; s. auch *Zimmermann,* BKR 2005, 208 (216), der insbesondere auf die finanziellen Herausforderungen des IT-Sektors hinweist.

895 Rundschreiben BaFin Nr. 18/2005 über „Mindestanforderungen an das Risikomanagement" vom 20.12.2005, AT 7.2, 9 Rn. 2, abrufbar unter http://www.bafin.de/rundschreiben/89_2005/051220_anl1.pdf (zuletzt abgerufen am 06.06.2007).

896 Rundschreiben BaFin Nr. 18/2005 über „Mindestanforderungen an das Risikomanagement" vom 20.12.2005, AT 7.3, 10 Rn. 1 f., abrufbar unter http://www.bafin.de/rundschreiben/89_2005/051220_anl1.pdf (zuletzt abgerufen am 06.06.2007).

452 Demgegenüber verweist das **britische Recht** in seinem FSA (Financial Services Authority) Handbook in der Sektion ***Senior Management Arrangements, Systems and Controls*** **(SYSC**) neben einer Reihe von einzelnen Pflichten vor allem auf die Einhaltung der ISO 17799.[897]

3. Anforderungen nach dem WpHG

a) Hintergrund

453 Das WpHG ist die zentrale Regelung des deutschen vertriebs- und marktbezogenen Kapitalmarktrechts. Es handelt sich hierbei um öffentliches Aufsichtsrecht. Die Marktaufsicht nach dem WpHG steht in engem Zusammenhang mit der Bankenaufsicht nach dem KWG, da Kreditinstitute und Finanzdienstleitungsinstitute sowohl dem KWG, als auch dem WpHG unterfallen. Die Bundesanstalt für Finanzdienstleitungsaufsicht (BaFin) ist neben der Bankenaufsicht nach KWG auch für die Überwachung und Durchsetzung der Vorgaben des WpHG zuständig (§ 4 Abs. 1 Satz 1 WpHG).[898]

b) Pflichten und Adressat

454 Die Vorschriften der §§ 31 ff. WpHG verpflichten die Kreditinstitute und Wertpapierhandelsunternehmen zu anlegerschutz-orientierter Organisation.[899] Nach § 33 Abs. 1 Nr. 1 WpHG sind die Wertpapierdienstleistungsunternehmen verpflichtet, die für eine ordnungsmäßige Durchführung der Wertpapierdienstleistung und Wertpapiernebendienstleistung notwendigen Mittel und Verfahren vorzuhalten und wirksam einzusetzen. Bei der Auslegung dieser Norm kann auf § 25a Abs. 1 KWG zurückgegriffen werden.[900] Wie § 25a Abs. 1 KWG stellt auch § 33 Abs. 1 WpHG eine Umsetzung des Art. 10 der Wertpapierdienstleistungs-Richtlinie von 1993 dar.[901] Die Auslegung orientiert sich daher an den Zielen der Richtlinie, die Anleger zu schützen sowie die Stabilität und das reibungslose Funktionieren der Wertpapiermärkte bzw. des Finanzsystems zu gewährleisten.[902] So müssen die Unternehmen die Risiken und die Art ihrer Bewältigung ständig im Auge behalten und angemessene Vorsorge betreiben[903].

c) Rechtsfolgen

---

897 SYSC 3A.7.8.

898 Zur Abgrenzung von Bank- und Marktaufsicht Schwark-*Schwark*, § 1 WpHG Rn. 6.

899 *Spindler*, in: Fleischer, Handbuch des Vorstandsrechts, § 19 Rn. 41.

900 Schwark-*Schwark*, § 33 WpHG Rn. 6.

901 *Spindler*, in: Fleischer, Handbuch des Vorstandsrechts, § 19 Rn. 42.

902 Erwägungsgründe 37 und 38 der Richtlinie 93/22/EWG des Rates vom 10. Mai 1993, ABl. Nr. L 141 vom 11. Juni 1993, 27.

903 Assmann/Schneider-*Koller*, § 33 WpHG Rn. 6.

455 Ein Verstoß gegen die Organisationspflichten des § 33 Abs. 1 Nr. 1 WpHG zieht weder straf- noch ordnungswidrigkeitsrechtliche Folgen nach sich.[904] Da es sich um öffentliches Aufsichtsrecht handelt, kann ein Verstoß jedoch aufsichtsrechtliche Konsequenzen haben.[905]

456 Bei der Organisationsvorschrift des § 33 WpHG handelt es sich nicht um ein Schutzgesetz im Sinne von § 823 Abs. 2 BGB906, da die dort geregelten Pflichten zu unbestimmt sind, um aus ihrer Verletzung Individualansprüche ableiten zu können, und es sich lediglich um Hilfspflichten handelt, die der betriebsinternen Durchsetzung der Verhaltenspflichten der §§ 31, 32 WpHG dienen.[907] Deliktische Ansprüche sind allenfalls bei Verletzung eines der Rechtsgüter oder Rechte des § 823 Abs. 1 BGB oder bei vorsätzlich sittenwidriger Schädigung (§ 826 BGB) denkbar.[908] In Betracht kommen im Einzelfall zudem vertragliche Schadensersatzansprüche gegenüber dem Kunden wegen verschuldeter Nichterreichbarkeit des Wertpapierdienstleistungsunternehmens im Falle eines Systemausfalls[909]; allerdings strahlt § 33 WpHG nicht unmittelbar auf die schuldrechtliche Beziehung zwischen Anleger und Wertpapierdienstleistungsunternehmen aus[910].

d) Anhaltspunkte für IT-Konkretisierungen

457 Im Einzelnen verlangt § 33 Abs. 1 Nr. 1 WpHG das Vorhalten von persönlichen und sachlichen Mitteln, soweit diese für die richtige Ordnung des Geschäftsbetriebes erforderlich sind.[911] Die erforderlichen sachlichen Mittel beziehen sich auf die technische Ausstattung, insbesondere somit auch auf EDV-Systeme. Hinsichtlich der notwendigen Verfahren müssen die Wertpapierdienstleistungsunternehmen ausreichende Maßnahmen in Bezug auf die elektronische Datenverarbeitung treffen, so dass Unbefugten der Zugriff auf die Daten des Unternehmens verwehrt wird.[912] Die wertpapierhandelsrechtlichen Organisationsvorschriften verlangen außerdem

---

904 Schwark-*Schwark*, § 33 WpHG Rn. 4; Assmann/Schneider-*Koller*, § 33 WpHG Rn. 50.

905 *Balzer*, WM 2001, 1533 (1539); Assmann/Schneider-*Koller*, vor § 31 WpHG Rn. 17.

906 BGH v. 8.5.2001 – XI ZR 192/00, BB 2001, 1865, 1867; *Kümpel*, Wertpapierhandelsgesetz, S. 162; Schwark-*Schwark*, vor § 31 WpHG Rn. 9; *Lang*, WM 2000, 451 (456); *Balzer*, WM 2001, 1533 (1540); *Hopt*, ZHR 159 (1995), 135 (161); *Spindler*, Unternehmensorganisationspflichten, S. 828; *Arendts*, ÖBA 1996, 775 (780); Assmann/Schneider-*Koller*, § 33 WpHG Rz. 1.

907 *Balzer*, WM 2001, 1533 (1540); Schwark-*Schwark*, § 33 WpHG Rn. 4; Assmann/Schneider-*Koller*, § 33 WpHG Rn. 1.

908 Assmann/Schneider-*Koller*, § 33 WpHG Rn. 1.

909 Für Direktbanken *Balzer*, WM 2001, 1533 (1540 f.); *Balzer*, ZBB 2000, 259 (264).

910 Assmann/Schneider-*Koller*, § 33 WpHG Rn. 1.

911 *Balzer*, WM 2001, 1533 (1539).

912 Assmann/Schneider-*Koller*, § 33 WpHG Rn. 9.

Vorkehrungen im Hinblick auf Systemausfälle und -störungen.[913] Die Wertpapierdienstleistungsunternehmen haben hierzu Vorkehrungen zu treffen, die eine rasche Behebung technischer Fehler ermöglichen sowie ggf. Ersatzkapazitäten zu reservieren.[914] Auch die **Richtlinie gemäß § 35 Abs. 6 WpHG** zur Konkretisierung der Organisationspflichten von Wertpapierhandelsunternehmen gemäß § 33 Abs. 1 WpHG[915] fordert ausdrücklich Vorkehrungen, um bei Systemausfällen und -störungen Verzögerungen bei der Auftragsausführung oder -weiterleitung möglichst gering zu halten (Nr. 2.2).

4. Die MiFID

a) Hintergrund

458 Mit der Richtlinie über Märkte für Finanzinstrumente[916] und die konkretisierende Durchführungsrichtlinie bzw. -verordnung[917] werden vor allem zwei Ziele verfolgt: die Verbesserung des Anlegerschutzes und die Förderung der Marktintegrität im Sinne von Fairness, Effizienz und Transparenz. Der Erreichung dieser Ziele dienen vor allem Organisationspflichten[918], die in Art. 13 MiFID, Art. 6, 7 DVO und Art. 5-20 DRL geregelt sind und die Bereiche Compliance, Risikomanagement und Innenrevision betreffen.[919]

---

913 Assmann/Schneider-*Koller*, § 33 WpHG Rn. 11a.

914 *Balzer*, ZBB 2000, 258 (260); *Balzer*, WM, 2001, 1533 (1539); Assmann/Schneider-*Koller*, § 33 WpHG Rn. 11a.

915 Assmann/Schneider-*Koller*, § 35 WpHG Rn. 8.

916 Richtlinie 2004/39/EG des Rates und des Europäischen Parlamentes vom 21.4.2004 über Märkte für Finanzinstrumente, zur Änderung der Richtlinien 85/611/EWG und 93/6/EWG und der Richtlinie 2000/12/EG des Europäischen Parlaments und des Rates und zur Aufhebung der Richtlinie 93/22/EWG, ABl. EG Nr. L 141 v. 30.4.2004, 1.

917 Richtlinie 2006/73/EG der Kommission vom 10.8.2006 zur Durchführung der Richtlinie 2004/39/EG des Europäischen Parlaments und des Rates in Bezug auf die organisatorischen Anforderungen an Wertpapierfirmen und die Bedingungen für die Ausübung ihrer Tätigkeit sowie in Bezug auf die Definition bestimmter Begriffe für die Zwecke der genannten Richtlinie, ABl. EG Nr. L 241 v. 2.9.2006, 26; Verordnung (EG) Nr. 1287/2006 der Kommission v. 10.8.2006 zur Durchführung der Richtlinie 2004/39/EG des Europäischen Parlaments und des Rates betreffend die Aufzeichnungspflichten für Wertpapierfirmen, die Meldung von Geschäften, die Markttransparenz, die Zulassung von Finanzinstrumenten zum Handel und bestimmter Begriffe im Sinne dieser Richtlinie, ABl. EG Nr. L 241 v. 2.9.2006, 1.

918 *Spindler/Kasten*, AG 2006, 785; EuGH v. 11.8.1995 – Rs. C-433/93 – Kommission/Deutschland, Slg. 1995, I-2303 Rz. 18 ff.; v. 30.5.1991 – Rs. C-361/88 – Kommission/Deutschland, Slg. 1991, I-2567 Rz. 15 ff. – TA-Luft; *Ruffert* in: Callies/Ruffert, § 249 EGV Rz. 51; EUV/EGV-*Schroeder*, Art. 249 EGV Rz. 93 ff., 95.

919 Zu allen Aspekten ausführlich *Spindler/Kasten*, AG 2006, 785 ff.

459 Der Referentenentwurf zur Umsetzung der MiFID vom 27.9.2006[920] sieht hinsichtlich der Ausführung von Wertpapiergeschäften Änderungen unter anderem am KWG und am WpHG vor, wobei hier nur die neuen Organisationsanforderungen von Interesse sind. Da die Anforderungen in § 33 WpHG und § 25a KWG zum Teil aber schon einen höheren Konkretisierungsgrad besitzen als die Vorgaben der MiFID, enthält der RefE keine bahnbrechenden Neuerungen[921]. Allerdings ist zu bedenken, dass sich die nationale Umsetzung nicht mit dem Verweis auf die Verwaltungspraxis, wie z.B. durch die MaRisk beeinflusst, begnügen kann, da dies nicht die nötige rechtliche Verbindlichkeit garantiert[922].

b) Pflichten und Adressat

460 Hinsichtlich des ersten Themenbereichs der Compliance enthält Art. 13 Abs. 2 MiFID die generalklauselartige Verpflichtung, angemessene Strategien und Verfahren anzuwenden, die sicherstellen, dass die Anforderungen der Richtlinie eingehalten werden. Eine Konkretisierung erfolgt in Art. 6 DRL in der Form, dass z.B. die Verpflichtung zur Aufspürung und Minimierung von Fehlerrisiken und zur Bestellung eines Compliance-Beauftragten zur Überwachung der Geschäftsprozesse festgeschrieben wird.[923.]

461 Des Weiteren werden effiziente Riskmanagementsysteme vorgeschrieben;
Art. 7 Abs. 1a DRL konkretisiert diese Anforderungen durch das Gebot, Risiken zu identifizieren und einer individuellen Bewertung mit Hilfe von sogenannten Risikotoleranzschwellen zu unterziehen.

462 Zuletzt umfassen die Organisationspflichten auch eine Pflicht zur internen Revision (Art. 8 DRL), die unabhängig die Wirksamkeit der Systeme überprüfen und bewerten und auf dieser Grundlage Empfehlungen aussprechen soll.

463 Wie bereits dargelegt, werden sich die Änderungen an WpHG und KWG in Grenzen halten. Die neuen organisatorischen Anforderungen an die Wertpapierfirmen werden sich aus einem Verweis in § 33 WpHG auf den erweiterten § 25a KWG-RefE und aus spezifischen Vorschriften ergeben.

---

920 Abrufbar unter: http://www.bundesfinanzministerium.de/lang_de/DE/Geld__und__Kredit/Aktuelle__Gesetze/005__c,templateId=raw,property=publicationFile.pdf (zuletzt abgerufen am 06.06.2007.

921 *Spindler/Kasten*, AG 2006, 785 (786).

922 *Spindler/Kasten*, AG 2006, 785 (787).

923 Zur weiteren Konkretisierung siehe *CESR*, CESR/05-24c, s. 13 ff.

464 Im Hinblick auf das Outsourcing von Geschäftsprozessen enthält die MiFID kein Verbot, allerdings muss die Auslagerung wichtiger betrieblicher Aufgaben, also des Kernmanagements i.S.d. Art. 13 DRL, im Unterschied zu untergeordneten Bereichen den besonderen Anforderungen des Art. 13 Abs. 5 1. Unterabs. Satz 2 MiFID genügen, wonach eine Auslagerung die Qualität der internen Kontrolle oder die Möglichkeit einer aufsichtsrechtlichen Überprüfung nicht beeinträchtigen darf. Der RefE zeichnet diese Unterscheidung nicht nach, sondern unterstellt sämtliche Auslagerungen, ob kritische Arbeitsbereiche betreffend oder nicht, den höheren Anforderungen. Die Möglichkeit der Auslagerung hängt von der Ordnungsmäßigkeit der Geschäftsorganisation, des angemessenen und wirksamen Risikomanagements und der Erhaltung der Verantwortung der Geschäftsleitung ab; im Rahmen des WpHG darf außerdem das Rechtverhältnis zum Kunden nicht verändert werden (Art. 14 Abs. 1 Ziff b) DRL).

465 Nach Art. 13 Abs. 6 MiFID sind Aufzeichnungen über alle Dienstleistungen und Geschäfte der Wertpapierfirmen anzufertigen, um die Aufsichtsbehörde in die Lage zu versetzen, die Erfüllung der Verpflichtungen der Wertpapierfirma gegenüber ihren Kunden überprüfen zu können. Art. 51 DRL sieht eine Archivierung dieser Aufzeichnung für fünf Jahre vor. Der RefE sieht in § 34 Abs. 1 und 2 die Umsetzung dieser Vorgaben vor; dabei sollen sämtliche Wertpapierdienstleistungen und -nebendienstleistungen, also auch die bloße Anlageberatung, erfasst werden.

466 Die MiFID regelt in Art. 18, 13 Abs. 3 explizit die Interessenkonflikte. Wertpapierfirmen haben alle angemessenen organisatorischen Vorkehrungen zu treffen, um Interessenkonflikte zwischen ihnen und ihren Kunden oder zwischen ihren Kunden untereinander zu erkennen und zu verhindern. Nach § 33 Abs. 1 Nr. 3 WpHG-RefE müssen Interessenkonflikte durch eine wirksame Organisation vermieden werden. Nur bei Unmöglichkeit müssen sind sie dem Kunden zu offenbaren[924].

924 Zum gesamten Problemkomplex ausführlich *Spindler/Kasten*, AG 2006, 785 (789 ff.); s. auch zu Interessenkonflikten allgemein Enriques, Conflicts of Interest in Investment Services: the Price and uncertain impact of MiFID's Regulatory Framework, University of Bologna, abrufbar unter http abrufbar unter: http://papers.ssrn.com/sol3/papers.cfm?abstract_id= 782828 (zuletzt abgerufen am 06.06.2007); dem Problem von Interessenkonflikten und Vermögensverwaltung widmet sich Kruithof, Conflicts of Interest in Institutional Asset Management: Is the EU Regulatory Approach adequate?, Financial Law Institute – Universiteit Gent, Working Paper Series, WP 2005, 07, Dec 2005; *Bolton/Freixas/Shapiro*, NBER, working paper series, No. 10571, abzurufen unter http://www2.law.columbia.edu/contracteconomics/papers/Bolton/Conflicts_Interest_Info.pdf (zuletzt abgerufen am 06.06.2007); Cain/Loewenstein/Moore, J.Leg.Studies, 34 (2005), 1, abzurufen unter www.journals.uchicago.edu/JLS/journal/issues/v34n1/340105/340105.web.pdf (zuletzt abgerufen am 06.06.2007).

c) Rechtsfolgen

467 Da die MiFID keine eigenen Regelungen zur Sanktionierung der genannten Pflichten enthält und auch die nach dem Referentenentwurf geplanten Änderungen des KWG und WpHG nicht die Rechtsfolgen betreffen, bleibt die oben dargestellte Rechtslage von der neueren Entwicklung unberührt.

d) Anhaltspunkte für IT-Konkretisierung

468 Konkrete Anhaltspunkte für die Umsetzung der Organisationspflichten im IT-Bereich sind nur vereinzelt vorhanden. So werden die Wertpapierfirmen etwa in Art. 13 Abs. 5 2. Unterabs. MiFID, das Risikomanagement betreffend, dazu verpflichtet, wirksame Kontroll- und Sicherheitsmechanismen für Datenverarbeitungssysteme einzurichten. Art. 5 Abs. 3 DRL enthält nur die Generalverpflichtung zur Überwachung und Sicherstellung der EDV-Systemsicherheit. Im Vergleich hierzu sind die Vorschriften in § 25a Abs. 1 Nr. 2 KWG zur Sicherheit von IT-Systemen deutlich präziser[925].

469 Die Einführung einer Aufzeichnung- und Archivierungspflicht hat auch für den IT-Bereich Bedeutung. Nach Art. 51 Abs. 2 sind Aufzeichnungen so auf einem Datenträger zu speichern, dass sie der Behörde leicht zugänglich gemacht werden können, wobei diese Aufzeichnungen insbesondere nicht anderweitig manipulierbar oder veränderbar sein dürfen.

5. Zwischenergebnis: besondere Verantwortlichkeit im Banken- und Finanzsektor

470 Im Banken-, Versicherungs- und Finanzsektor ist durch KWG, WpHG, VAG und die entsprechenden Mindestanforderungen, wie z.B. MaRisk, eine starke Aufsicht vorhanden. Die Pflichten sind auch hinsichtlich der Verwendung von Informationstechnik geregelt. Die Aufsichtsbehörde hat zusätzlich auch entsprechende Mittel, um diese Anforderungen durchzusetzen. Zwar sind die Normen nicht als Schutzgesetze i.S.d. § 823 Abs. 2 BGB zu qualifizieren, durch die Möglichkeit, sie zur Konkretisierung der Verkehrssicherungspflichten im Rahmen des § 823 Abs. 1 BGB heranzuziehen, besteht aber dennoch ein enger Zusammenhang auch zur deliktischen Haftung.

6. Die Verteilung der Risiken bei Online-Bankgeschäften

471 In den letzten Jahren konnte ein stetig ansteigendes Auftreten neuartiger Bedrohungen des E-Commerce durch den Missbrauch im Internetverkehr verwendeter Legitimati-

925 *Spindler/Kasten*, AG 2006, 785 (786).

onsmedien beobachtet werden. Waren Angriffe auf die Sicherheit der Informationssysteme bislang meist von dem Wunsch getrieben, Störungen um ihrer selbst Willen zu verursachen (z.B. Denial-of-Service-Attacken), verlagert sich die Motivation zunehmend hin zu bloßem Gewinnstreben.[926] Besonders betroffen waren hierbei bislang die Kunden des Online-Banking,[927] insbesondere der Deutschen Bank, der Postbank sowie der Volks- und Raiffeisenbanken, aber auch die Kunden des Internet-Auktionshauses eBay. Angesichts der fortschreitenden Verlagerung des Wareneinkaufs im Internet und der vermehrten Online-Abwicklung von Bankgeschäften dürfte künftig eine Zunahme dieser Fälle zu verzeichnen sein, was – neben hier nicht zu behandelnden strafrechtlichen Konsequenzen[928] – verstärkt Fragen der zivilrechtlichen Haftung aufwirft. Entscheidend sind hierbei die Fragen der Risikoverteilung und Risikobeherrschung im Verhältnis von Unternehmer (hier: Bank) und Kunde beim Geschäftsverkehr im Internet (s. zum Online-Banking Rn. 503 ff.). Probleme bereiten im Haftungsfall vor allem die Beweisführung hinsichtlich einer Identitätstäuschung oder einer Pflichtverletzung des Nutzers.

472 Im Folgenden wird für das Online-Banking zunächst das Gefahrenpotential anhand dreier beispielhafter Szenarien (a)) dargestellt. Darauf folgt eine Untersuchung der Haftungsverteilung zwischen den Beteiligten (b)), welche sich in einem ersten Teil der materiellen Rechtslage (b)(1) bis b)(3)) und in einem zweiten der prozessualen Rechtslage widmet (b)(4)).

a) Gefahrenpotential

(1) Szenario 1: Phishing[929], ohne Trojaner, mit Visual Spoofing

926 Vgl. die Einschätzung der Mitteilung der EU-Kommission „Eine Strategie für eine sichere Informationsgesellschaft – ‚Dialog, Partnerschaft und Delegation der Verantwortung'" vom 31.5.2006, KOM(2006) 251 endgültig (abrufbar unter: http://eur-lex.europa.eu/LexUriServ/site/de/com/2006/com2006_0251de01.pdf, zuletzt abgerufen am 06.06.2007). Ebenso der Symantec Internet Threat Report für das erste Halbjahr 2006 (abrufbar unter: http://www.symantec.com/specprog/threatreport/entwhitepaper_symantec_internet_security_threat_report_x_09_2006.en-us.pdf).

927 Frankfurter Allgemeine Zeitung vom 11.7.2005: „Trickbetrüger nehmen Internet-Banking ins Visier" und vom 10.3.2006: „Angriffe auf Online-Bankkunden nehmen sprunghaft zu"; Süddeutsche Zeitung vom 2.8.2006: „Surfen am Abgrund"; Spiegel-Online vom 24.9.2006: „Phishing und Pharming – Die Bedrohung wächst", abrufbar unter: http://www.spiegel.de/netzwelt/technologie/0,1518,438677,00.html (zuletzt abgerufen am 06.06.2007).

928 Dazu *Popp*, NJW 2004, 3517.

929 Der Begriff leitet sich aus dem englischen „Password-Fishing" ab. Zur steigenden Anzahl von Phishing-E-Mails weltweit vgl. BSI, Die Lage der IT-Sicherheit in Deutschland 2005, S. 22 ff. (abrufbar unter: http://www.bsi.de/literat/lagebericht/lagebericht2005.pdf, zuletzt abgerufen am 06.06.2007). Dem Sy-

473 Angreifer A schickt dem Nutzer N eine E-Mail mit vorgetäuschter („gespoofter“) Absender-Adresse der Hausbank B von N. Es handelt sich um eine HTML-Mail, die dem Layout einer typischen Mail von B entspricht und N auffordert, aus benannten Gründen PIN und TAN einzugeben. Die E-Mail enthält einen Link zum Webserver von A, auf dem das Online-Portal von B nachgebildet wurde. N ist halbwegs versiert und überprüft die einschlägigen Sicherheitsmerkmale der Online-Verbindung: URL im Adress-Feld, Schloss-Symbol und Zertifikatsinformationen (Fingerprint). Alle diese Merkmale werden jedoch mithilfe Aktiver Inhalte dem Original nachgebildet (Visual Spoofing), so dass N die Fälschung nicht bemerkt und seine Zugangsdaten arglos preisgibt. N ist die Freischaltung Aktiver Inhalte gewohnt, da auch das reguläre Portal von B nur mit Aktiven Inhalten nutzbar ist. A nutzt die Zugangsdaten, um eigene Transaktionen auszulösen.

(2) Szenario 2: Man-in-the-middle-Angriff mittels DNS-Spoofing/Pharming i. w. S.

474 Die kriminelle Organisation KO hat eine Schwachstelle in der BIND-Software (die am weitesten verbreitete DNS-Server-Software) entdeckt, bevor sie von den BIND-Entwicklern aufgedeckt wurde. Die Schwachstelle erlaubt, DNS-Server zu korrumpieren, indem der Angreifer DNS-Datensätze mit falschen Zuordnungen zwischen Domain-Namen und IP-Adressen einspielt. Nach erfolgtem Angriff liefert der DNS-Server falsche IP-Adressen als Antwort auf DNS-Anfragen aus.

475 KO gelingt es, den DNS-Server des Providers P so zu manipulieren, dass anstelle der korrekten IP-Adresse die IP-Adresse eines KO-Servers ausgeliefert wird, wenn DNS-Anfragen nach dem Online-Banking-Portal der Bank B eingehen. Auf diese Weise gelangt der Nutzer N des Online-Portals von B nicht auf den Bank-Server, sondern auf den Server von KO, auf dem das Online-Portal von B nachgebildet wurde. B setzt ausschließlich auf das PIN-TAN-Verfahren. N übersendet in bestem Glauben alle Zugangsdaten. Da das Portal die Eigenschaft hat, unmittelbar nach dem Zugang den Konto-Stand an den Kunden zu übermitteln, muss KO mit den Zugangsdaten von N Kontakt zum echten Portal aufnehmen, um die entsprechenden Daten an N übersenden zu können. KO übernimmt also die Rolle eines Man-in-the-middle.

---

mantec Internet Threat Report zufolge, wurde im ersten Halbjahr 2006 ein Anstieg der Varianten von Phishing-E-Mails um 81 Prozent auf fast 160.000 Varianten registriert (S. 82 ff., abrufbar unter: http://www.symantec.com/content/en/us/about/media/ISTR_XI_Global_FINAL.pdf, zuletzt abgerufen am 06.06.2007).

476 Die von N initiierte Transaktion wird von KO manipuliert, d.h. vor allem Höhe und Empfänger der Transaktion werden verändert. An B wird die manipulierte Transaktion übermittelt, an N jedoch eine Bestätigung über die Ausführung der beabsichtigten Transaktion mit dem vermeintlich richtigen Kontostand. N beendet die Verbindung.

477 Der Angriff von KO beginnt Freitag abend in der Hoffnung, dass bei B signifikante Abweichungen möglichst spät entdeckt werden. Z.B. soll B möglichst spät erkennen, dass sich die Verbindungen zu einigen IP-Adressen häufen – nämlich zu den KO-Servern.

478 Dem Angriff lässt sich leicht begegnen, indem die Banken ihren Kunden die festen IP-Adressen der Online-Banking-Portale mitteilen und nicht die URL. Unter dieser Voraussetzung müsste der Angreifer Routing-Tabellen im Internet manipulieren oder Trojanische Pferde einsetzen, um den Online-Kunden auf seinen Server zu lotsen. DNS-Spoofing und die Manipulation des IP-Routing gelten als die Achillesfersen des Internets.

(3) Szenario 3: Pharming i. e. S., mit Trojaner

479 Mithilfe eines Interesse erweckenden E-Mail-Anhangs gelingt es dem Angreifer A, ein Trojanisches Pferd auf dem Rechner des Nutzers N zu platzieren. Der Trojaner ergänzt die „host"-Datei auf dem Rechner um den manipulierten Eintrag für das Online-Banking-Portal der Bank B. Daraufhin werden Aufrufe des Bank-Portals auf den Webserver von A geleitet. A übernimmt die Rolle eines Man-in-the-middle. Ansonsten entspricht der Angriff dem Szenario „Pharming im weiteren Sinne".

b) Haftungsverteilung zwischen den am Online-Banking Beteiligten

480 Nachdem die Bankpraxis nach Auftreten der ersten Schadensfälle durch Phishing und Pharming noch dahin ging, Schäden der Kunden (aus Kulanz) vollumfänglich zu ersetzen, stellen sich die Banken zunehmend auf den Standpunkt, der Kunde sei durch die Berichterstattung in den Medien und die Informationsarbeit der Banken hinreichend über die Risiken des Online-Banking informiert. Schäden seien daher regelmäßig auf mangelnde Sorgfalt des Kunden zurückzuführen. Bislang sind – soweit ersichtlich – zwar noch keine Haftungsfälle vor Gericht gelangt, angesichts der Erfahrungen im Zusammenhang mit ec-Kartenmissbrauch ist jedoch zu erwarten, dass sich diese Linie durchsetzen wird und die Banken dem Kunden das Risiko des Phishing und Pharming zuweisen.

(1) Rechtliche Grundlagen des Online-Banking

481 Die Online-Bankgeschäfte bilden einen Ausschnitt aus dem Bereich des Direktbanking,[930] welcher neben der Abwicklung von Bankgeschäften über die herkömmlichen Kommunikationswege wie Brief, Telefon und Fax auch Online- und Homebanking umfasst.[931] Der Begriff des Online-Banking kann als Überbegriff für alle online abgewickelten Bankgeschäfte verwendet werden (Online-Banking i.w.S.). Von **Online-Banking i. e. S.** (früher: Btx) spricht man, wenn Bankgeschäfte über ein geschlossenes Netz, d.h. eine von einem Telekommunikationsunternehmen (z.B. T-Online, AOL) vermittelte, geschlossene Kunde-zu-Bank-Verbindung abgewickelt werden, für deren Nutzung eine Registrierung und Zulassung des Kunden durch den Netzbetreiber erforderlich ist.[932] **Homebanking** ist dem gegenüber nach gängiger Unterscheidung die Abwicklung von Bankgeschäften über ein offenes Netz wie das Internet.[933]

482 Der Zentrale Kreditausschuss (ZKA) hat für Online-Banking i.e.S. und Homebanking Musterbedingungen entwickelt,[934] welche sich im verwendeten **Sicherungsverfahren** unterscheiden,[935] im Übrigen aber nicht wesentlich von einander abweichen[936]. Die Sonderbedingungen für die konto-/depotbezogene Nutzung des Online-Banking mit PIN und TAN („**Online-Bedingungen**“) knüpfen an die Verwendung des PIN-/TAN-Verfahrens an und entsprechend weitgehend den alten Btx-Bedingungen. Daneben wurden für die Verwendung des HBCI-Verfahrens die Bedingungen für die konto-/depotbezogene Nutzung des Online-Banking mit elektronischer Signatur[937] („**Homebanking-Bedingungen**“) entwickelt.[938] Die Verwendung des einen oder anderen Sicherungsverfahrens ist gesetzlich nicht vorgeschrieben und folglich auch nicht an den Zugang über ein geschlossenes oder offenes Netz geknüpft. Das PIN-

930 *Kümpel*, Bank- und Kapitalmarktrecht, 4.733.

931 Ausführlich zu diesen Unterscheidungen *Bock* in: Bräutigam/Leupold, Kap. VII Rn. 3 ff.

932 *Bock* in: Bräutigam/Leupold, Kap. VII Rn. 4; *Gößmann*, in: Bankrechts-Handbuch, Band I, § 55 Rn. 1; *Hellner/Escher-Weingart*, in: Hellner/Steuer, Band 3, Teil 6/96; *Koch*, Versicherbarkeit von IT-Risiken, Rn. 806.

933 Vgl. das Homebanking-Abkommen vom 1.10.1997; *Bock* in: Bräutigam/Leupold, Kap. VII Rn. 4; *Gößmann*, in: Bankrechts-Handbuch, Band I, § 55 Rn. 1, 27; *Koch*, Versicherbarkeit von IT-Risiken, Rn. 806; *Hellner/Escher-Weingart*, in: Hellner/Steuer, Band 3, Teil 6/96.

934 *Neumann/Bock*, Zahlungsverkehr im Internet, Rn. 109.

935 *Borges*, in: Derleder/Knops/Bamberger, Handbuch zum deutschen und europäischen Bankrecht, § 8 Rn. 1.

936 *Gößmann*, in: Bankrechts-Handbuch, Band I, § 55 Rn. 27.

937 Das Homebanking-Computer-Interface-Verfahren (HBCI) auf Grundlage des Homebanking-Abkommens von 1997 soll gegenüber dem PIN-/TAN-Verfahren eine höhere Sicherheit gewährleisten. Ausführlich dazu *Stockhausen*, WM 2001, 605 ff.

938 Die Online-Bedingungen und Homebanking-Bedingungen sind abgedruckt in WM 2001, 650 ff. und *Gößmann*, in: Bankrechts-Handbuch, Band I, Anh. 6 und 7 zu §§ 52- 55, S. 1147 ff.

/TAN-Verfahren findet daher gegenwärtig auch im Internet Anwendung.[939] Das Homebanking-Abkommen verpflichtet die Banken jedoch, Online-Banking zumindest auch im HBCI-Dialog durchzuführen.[940] In der Praxis dürfte gegenwärtig das PIN-/TAN-Verfahren noch am weitesten verbreitet sein.[941]

483 Dem Online-Banking liegt im Verhältnis des Kunden zur Bank ein neben dem eigentlichen Girovertrag (und den Allgemeinen Bankenbedingungen) bestehender **Online-Bankingvertrag** zugrunde, welcher durch die Online-Bedingungen bzw. Homebanking-Bedingungen der Banken näher ausgestaltet wird.[942] Hierbei handelt es sich im Grundsatz um einen Geschäftsbesorgungsvertrag nach § 675 BGB.[943] Weist der Kunde die Bank beispielsweise an, einen bestimmten Betrag von seinem Konto auf ein anderes Konto zu überweisen, liegt der einzelnen Transaktion ein **Überweisungsvertrag** (§§ 676a ff. BGB) zugrunde. Ein solcher wird bei einer Online-Überweisung mittels elektronischer Willenserklärung[944] des Kunden durch Eingabe von PIN und TAN und konkludenter Annahme durch die Bank (§ 362 HGB) geschlossen.[945] Die Bank erwirbt aufgrund der Überweisung einen Aufwendungsersatzanspruch (§§ 670, 675 BGB) in Höhe des Überweisungsbetrages und belastet das Konto des überweisenden Kunden.[946]

(2) Vorschlag der EU-Kommission für eine Zahlungsdiensterichtlinie („SEPA“)

484 Die künftige Rechtslage im Bereich des Online-Banking wird maßgeblich durch den europäischen Gesetzgeber mitbestimmt werden. Nachdem die EU-Kommission bereits 1997 in der – rechtlich nicht verbindlichen – **Empfehlung vom 30. Juli 1997** zu den Geschäften, die mit elektronischen Zahlungsinstrumenten getätigt werden[947] eine gewisse Hilfestellung bei der Ausformung der Rechte und Pflichten der Parteien im Onli-

939 *Bock*, in: Bräutigam/Leupold, Kap. VII Rn. 16; *Koch*, Versicherbarkeit von IT-Risiken, Rn. 806.

940 *Stockhausen*, WM 2001, 605 (611).

941 *Bock*, in: Bräutigam/Leupold, Kap. VII Rn. 7; *Recknagel*, Vertrag und Haftung beim Internet-Banking, S. 14.

942 *Bock*, in: Bräutigam/Leupold, Kap. VII Rn. 30; *Neumann/Bock*, Zahlungsverkehr im Internet, Rn. 106; *Borges*, in: Derleder/Knops/Bamberger, Handbuch zum deutschen und europäischen Bankrecht, § 8 Rn. 14; *Gößmann*, in: Bankrechts-Handbuch, Band I, § 55 Rn. 15.

943 *Karper*, DuD 2006, 215 (216); *Werner*, in: Hoeren/Sieber, Kap. 13.5 Rn. 37.

944 Zum Begriff *Bock*, in: Bräutigam/Leupold, Kap. VII Rn. 43.

945 Palandt-*Sprau*, § 676a BGB Rn. 11.

946 *Kind/Werner*, CR 2006, 353; *Borges*, NJW 2005, 3313 (3315); *Karper*, DuD 2006, 215 (216); *Neumann/Bock*, Zahlungsverkehr im Internet, Rn. 179; MünchKommBGB-*Casper*, § 676a BGB Rn. 33.

947 97/489/EG: Empfehlung der Kommission vom 30. Juli 1997 zu den Geschäften, die mit elektronischen Zahlungsinstrumenten getätigt werden (besonders zu den Beziehungen zwischen Emittenten und Inhabern solcher Instrumente) (Text von Bedeutung für den EWR), ABl. Nr. L 208 vom 2. August 1997, S. 52 ff.

ne-Banking gegeben hatte, legte die Kommission Ende 2005 den Vorschlag für eine **Zahlungsdiensterichtlinie** vor.[948]

485 Im Interesse der Rechtssicherheit und eines hohen Verbraucherschutzniveaus strebt die EU eine europaweite **Harmonisierung der Hauptrechte und -pflichten** der Nutzer und Anbieter von Zahlungsdiensten an. Der Anwendungsbereich der Richtlinie erstreckt sich auf alle Zahlungsdienste gemäß Art. 2 Abs. 1 i.V.m. Anhang „Zahlungsdienste" unabhängig von der Art und Weise technischen Durchführung. Erfasst werden demnach ec-Kartensysteme ebenso wie Online-Banking. Gemäß ihrer Zielsetzung bezweckt die Richtlinie zwar die Verbesserung des **grenzüberschreitenden** Zahlungsverkehrs, im Interesse einer einheitlichen Rechtslage wird die auf europäischer Ebene gefundene Lösung jedoch wohl auch auf reine Inlandsfälle ausstrahlen.

486 Der Vorschlag regelt die wesentlichen **Sorgfaltspflichten** des Zahlungsdienstnutzers (Art. 46) und der Pflichten des Zahlungsdienstleisters (Art. 47) in Bezug auf Zahlungsverifikationsinstrumente. Der Nutzer ist danach verpflichtet, bei der Verwendung eines Zahlungsverifikationsinstruments die Bedingungen für dessen Ausgabe und Benutzung einzuhalten (Art. 46 lit. a), sowie dem Zahlungsdienstleister unverzüglich nach Feststellung den Verlust, Diebstahl, die widerrechtliche Aneignung oder die sonstige nicht autorisierte Verwendung des Zahlungsverifikationsinstruments anzeigen (Art. 46 lit. b). Der Zahlungsdienstleister hat hierzu die erforderlichen organisatorischen Vorkehrungen zu treffen (Art. 47 Abs. 1 lit. c). Ebenso muss der Dienstleister sicherstellen, dass die personalisierten Sicherheitsmerkmale des Zahlungsverifikationsinstruments keiner anderen Person als dem Inhaber zugänglich sind (Art. 47 Abs. 1 lit. a). Detaillierte IT-spezifische Sorgfaltspflichten enthält der Vorschlag nicht.

487 Ebenso trifft der europäische Gesetzgeber eine ausdrückliche Regelung der **Beweislastverteilung** bei strittiger Autorisierung (Art. 48). Bestreitet der Zahlungsdienstnutzer einen abgeschlossenen Zahlungsvorgang, hat die Bank nachzuweisen, dass der Zahlungsvorgang authentifiziert war, ordnungsgemäß aufgezeichnet und verbucht und nicht durch eine technische Panne oder einen anderen Mangel beeinträchtigt worden ist (Abs. 1). Streitet der Nutzer die Autorisierung der Zahlung auch nach Vorlage dieser Nachweise noch ab, hat er seinerseits Fakten oder Umstände vorzutragen, die die Ver-

948 Vorschlag für eine Richtlinie des Europäischen Parlaments und des Rates über Zahlungsdienste im Binnenmarkt und zur Änderung der Richtlinien 97/7/EG, 2000/12/EG und 2002/65/EG vom 1. Dezember 2005, KOM (2005), 603 endg. (von der Kommission vorgelegt).

mutung zulassen, dass er die Zahlung nicht autorisiert und nicht in betrügerischer Absicht oder grob fahrlässig in Bezug auf die ihm nach Art. 46 lit. b obliegenden Pflichten (Rn. 486) gehandelt haben kann (Abs. 2). Im Fall des Online-Banking könnte hierzu unter Umständen schon die Anzeige eines Diebstahls der Legitimationsmedien oder Vorliegen einer Phishing-Mail bzw. eines Trojaners auf dem Rechner des Kunden ausreichen. Um diese Vermutung zu widerlegen und nachzuweisen, dass der Zahlungsdienstnutzer die Zahlung autorisiert bzw. in betrügerischer Absicht oder in Bezug auf die ihm gemäß Art. 46 obliegenden Pflichten grob fahrlässig gehandelt hat, reicht die vom Zahlungsdienstleister aufgezeichnete Nutzung eines Zahlungsverifikationsinstruments allein nicht aus (Abs. 3). Die bloße Verwendung von PIN und TAN könnte danach nicht mehr zur Begründung eines Anscheinsbeweises für Urheberschaft oder pflichtwidriges Handeln des Kunden herangezogen werden.[949]

488 Der Zentrale Kreditausschuss (ZKA) hat die Regelung des Art. 48 Abs. 3 des Entwurfs als unausgewogen kritisiert und hierbei insbesondere auf die Gefahr betrügerischer Handlungen von Kunden unter Ausnutzung der Beweisregel hingewiesen. Der ZKA fordert, die bisherigen Beweislastgrundsätze (im deutschen Recht damit den Anscheinsbeweis) beizubehalten, da andernfalls das Online-Banking-Angebot eingeschränkt oder erheblich verteuert werden müsste. Die vom BGH[950] zu ec-Karten bestätigen Grundsätze zum Anscheinsbeweis sollten durch gesetzgeberische Maßnahmen auf europäischer Ebene nicht angetastet werden.[951]

489 Die Bestimmungen über die **Haftung des Kunden** (Art. 50) sehen eine Haftungshöchstgrenze von € 150 für Schäden vor, die vor Erfüllung der Anzeigepflicht gemäß Art. 46 lit. b aus der Verwendung eines verlorenen oder gestohlenen Zahlungsverifikationsinstruments entstanden sind. Dagegen haftet der Nutzer ohne Haftungshöchstbetrag für alle Schäden, die durch nicht autorisierte Zahlungsvorgänge entstanden sind, wenn er sie in *betrügerischer Absicht* oder durch *grobe Fahrlässigkeit* gegenüber den ihm nach Artikel 46 obliegenden Pflichten herbeigeführt hat. Nach Anzeige des Verlusts,

---

949 Siehe zu dieser Einschätzung auch *Burgard*, WM 2006, 2065 (2069) zum Anscheinsbeweis beim ec-Kartenmissbrauch.

950 BGH NJW 2004, 3623 ff.

951 Anmerkungen des Zentralen Kreditausschusses zum Vorschlag der Europäischen Kommission für eine „Richtlinie des Europäischen Parlaments und des Rates über Zahlungsdienste im Binnenmarkt und zur Änderung der Richtlinien 97/7/EG, 2000/12/EG und 2002/65/EG“ vom 1. Dezember 2005 (KOM[2005] 603 endgültig), S. 5, 38 f., abrufbar unter http://www.bankenverband.de/pic/artikelpic/022006/sp0602_eu_NLF-ZKA_final_dt.pdf (zuletzt abgerufen am 06.06.2007).

des Diebstahls oder der widerrechtlichen Aneignung des Zahlungsverifikationsinstruments beim Zahlungsdienstleister trägt der Zahler keinerlei finanzielle Folgen aus der Verwendung des verlorenen, gestohlenen oder widerrechtlich angeeigneten Instruments, es sei denn, er hat in betrügerischer Absicht gehandelt.

(3) Materiell-rechtliche Rechtslage

490 Bei Fällen der Identitätstäuschung aufgrund Phishing und Pharming stellt sich nach derzeitiger Rechtslage die Frage, ob die Bank vom Kunden die Erstattung des Überweisungsbetrages verlangen kann. Als Anspruchsgrundlagen kommt ein Aufwendungsersatzanspruch (unten (a)) oder ein Schadensersatzanspruch (unten (b)) in Betracht. Eine verschuldensunabhängige Haftung des Bankkunden aufgrund von AGB-Klauseln kommt hingegen nicht in Betracht, dazu unten (c).

(a) Aufwendungsersatzanspruch der Bank

(i) Vertragsschluss

491 Ein Aufwendungsersatzanspruch der Bank gemäß §§ 670, 675, 676a BGB auf Erstattung des überwiesenen Betrages beruht auf vertraglicher Grundlage und setzt damit einen wirksam zustande gekommenen Überweisungsvertrag zwischen dem Kunden und der Bank in Bezug auf die konkret ausgeführte Transaktion voraus. Gelingt einem Angreifer aufgrund einer Phishing- oder Pharming-Attacke die Veranlassung einer Überweisung, so kommt zwischen Kunde und Bank **kein Vertragsschluss** zustande.[952] Die Problematik liegt hierbei in der Praxis im Bereich der Beweislast. Denn die Bank wird sich auf den Standpunkt stellen, dass die Erklärung, welche aufgrund der Verwendung des einschlägige Legitimationsmediums (z.B. PIN und TAN) dem Kunden (objektiv) zuzurechnen ist, auch tatsächlich von diesem oder einem autorisierten Dritten stammt.[953] Verlangt die überweisende Bank nun vom Kunden Aufwendungsersatz, steht sie – wenn der Kunde den Vertragsschluss bestreitet – vor dem Problem im Prozess die anspruchsbegründende Tatsache des Vertragsschlusses beweisen zu müssen (dazu ausführlich unten Rn. 552 ff.).[954] Das Risiko einer gefälschten Überweisung trägt grundsätzlich die Bank.[955] Denkbar wäre jedoch auch mit einem Teil der Literatur eine Rechtsscheinshaftung des Kunden anzunehmen (dazu sogleich).

---

952 *Bock*, in: Bräutigam/Leupold, Kap. VII Rn. 81; Palandt-*Sprau*, § 676a BGB Rn. 11.
953 So auch *Borges*, NJW 2005, 3313 (3316).
954 *Borges*, NJW 2005, 3313 (3316); *Karper*, DuD 2006, 215 (218).
955 BGH NJW 2001, 2968 (2969); BGH NJW 1994, 2357 (2358); BGH NJW 1994, 3344 (3345).

(ii) Bindung kraft Rechtsscheins

492 Aus Sicht der Bank unterscheidet sich ein gefälschter Online-Überweisungsauftrag, welcher unter Verwendung des Legitimationsmediums des Kunden (z.B. PIN/TAN, HBCI, elektronische Signatur) erstellt wurde, nicht von einem vom berechtigten Kontoinhaber stammenden Auftrag. Es entsteht mithin der **Schein einer ordnungsgemäßen Willenserklärung** des Bankkunden. Ein Teil der Literatur leitet eine Bindung des Bankkunden gegenüber der Bank folglich aus Rechtsscheinsgrundsätzen her.

493 Schon im Rahmen des **Btx-Systems** wurde für den missbräuchlich handelnden Dritten eine Anscheinsvollmacht angenommen und dem Inhaber des Btx-Anschlusses damit die Erklärung des Dritten zugerechnet, wenn er den Missbrauch von PIN und TAN ermöglich hatte.[956] In den meisten Verfahren, welche eine behauptete missbräuchliche Verwendung von ec-Karten zum Gegenstand hatten, wurde dagegen keine Rechtsscheinshaftung angenommen, sondern nur ein Anscheinsbeweis zugunsten der Tatsache, dass der Karteninhaber oder ein von ihm autorisierter Dritter gehandelt hat (näher Rn. 562).[957] Allerdings ist einzuräumen, dass die Rechtsprechung diese Frage kaum thematisiert hat. Allerdings hat sich der BGH im Rahmen von R-Gesprächen zum Thema der Anscheinsvollmacht geäußert und klargestellt, dass die entwickelten Grundsätze der Anscheinsvollmacht, also eine „gewisse Dauer und Häufigkeit", für ein Greifen unbedingt vorliegen müssen.[958] Für Internet-Auktionen haben Instanzgerichte in neueren Entscheidungen eine Anscheinsvollmacht zwar nicht grundsätzlich abgelehnt, aber die Zurechenbarkeit des Rechtsscheins und – im Hinblick auf den derzeitigen Sicherheitsstandard des Internet – ein schutzwürdiges Vertrauen des Klägers verneint.[959]

494 Soweit die Literatur zum Online-Banking eine Rechtsscheinshaftung bejaht, verweist sie auf die Grundsätze der Anscheinsvollmacht[960] oder nimmt in Fortbildung dieser

---

956 So für über Btx getätigte Rechtsgeschäfte: OLG Oldenburg NJW 1993, 1400 (1401); OLG Köln NJW-RR 1994, 177 (178); LG Ravensburg NJW-RR 1992, 111; LG Koblenz NJW 1991, 1360.

957 Vgl. etwa KG NJW 1992, 1051 (1052); LG Bonn NJW-RR 1995, 815; LG Darmstadt WM 2000, 911 (913 f.); LG Frankfurt WM 1999, 1930 (1932 f.); LG Hannover WM 1998, 1123 f.; LG Köln WM 1995, 976 (977 f.); AG Frankfurt NJW 1998, 687 f.; AG Osnabrück NJW 1998, 688 f.

958 BGH JZ 2006, 1073 (1074) mit Anm. *Lobinger*.

959 OLG Hamm NJW 2007, 611; OLG Köln MMR 2006, 321 (322); LG Bonn MMR 2004, 179 (180); LG Bonn MMR 2002, 255 (257) bestätigt von OLG Köln MMR 2002, 813 (814); dazu auch *Wiebe*, in: Spindler/Wiebe, Internet-Auktionen und Elektronische Marktplätze, Kap. 4 Rn. 65 ff.; ebenso *Borges*, NJW 2005, 3313 (3316).

960 So *Gößmann*, in: Bankrechts-Handbuch, Band I, § 55 Rn. 26; Baumbach/Hopt-*Hopt* (7) Bankgeschäfte F/35; allgemein zur Anscheinsvollmacht Palandt-*Heinrichs*, § 172 BGB Rn. 11 ff.; MünchKommBGB-*Schramm*, § 167 BGB Rn. 54 ff.

Grundsätze eine besondere Rechtsscheinsvollmacht an,[961] wobei sie den Rechtsschein jeweils mit dem hohen technischen Sicherheitsstandard der Online-Banking-Systeme begründet.[962]

(a) Anscheinsvollmacht

495 Eine Bindung des Kunden an eine gefälschte elektronische Willenserklärung kraft Anscheinsvollmacht ist mit der überwiegenden Meinung abzulehnen.[963] Ein „Normalfall" der Anscheinsvollmacht[964] liegt beim Online-Banking schon deshalb nicht vor, da der objektive Rechtsscheinstatbestand nicht auf dem (mehrfachen) Auftreten eines anderen als Vertreter beruht, sondern vielmehr von einem Handeln des Kunden selbst ausgegangen wird.[965]

496 Typisch für die Fälle der Anscheinsvollmacht ist überdies das Handeln eines Dritten, der aus der Sphäre des Vertretenen stammt, etwa aus dessen Unternehmen, und dessen Handlungen grundsätzlich vom Vertretenen kontrolliert werden können.[966] Demgegenüber kennzeichnen sich die Sachverhalte, in denen elektronische Legitimationsmedien missbräuchlich verwandt wurden, im Wesentlichen durch den (behaupteten) Eingriff Dritter, die nicht dem „Lager" des Kunden entstammen, sondern unbekannt agieren.

497 Weitere Voraussetzung für eine solche Zurechnung qua Anscheinsvollmacht ist aber nach wie vor, dass der Dritte für eine gewisse Dauer und wiederholt für den vermeintlich Vertretenen aufgetreten ist.[967] An beiden Merkmalen lässt sich aber für missbräuchliche Erklärungen im Internet im Bereich des Online-Banking mit Fug und Recht zweifeln: es fehlt bei einem einmaligen oder nur kurzzeitig andauernden Missbrauch an der

---

961 Zur „Btx-Rechtsscheinsvollmacht" *Lachmann*, NJW 1984, 405 (408); für Btx im Bankbereich unter Verwendung von PIN und TAN auch *Borsum/Hoffmeister*, NJW 1985, 1205 (1206).

962 *Gößmann*, in: Bankrechts-Handbuch, Band I, § 55 Rn. 26; zum Btx-System LG Ravensburg CR 1992, 472 (473); *Lachmann*, NJW 1984, 405 (408); *Borsum/Hoffmeister*, NJW 1985, 1205 (1206).

963 *Borges*, NJW 2005, 3313 (3315); *Kind/Werner*, CR 2006, 353; *Kunst*, MMR Beilage 9/2001, 23 (24); *Wiesgickl*, WM 2000, 1039 (1047); *Bock*, in: Bräutigam/Leupold, Kap. VII Rn. 82; *Langenbucher*, Die Risikozuordnung im bargeldlosen Zahlungsverkehr, S. 145 f.

964 Eine Anscheinsvollmacht liegt nach den anerkannten Grundsätzen der Rechtsprechung vor, wenn der Vertretene das Handeln des Vertreters nicht kennt, er es aber bei pflichtgemäßer Sorgfalt hätte erkennen können und der andere Teil annehmen durfte, der Vertretene dulde und billige das Handeln des Vertreters.

965 So auch *Bock*, in: Bräutigam/Leupold, Kap. VII Rn. 82.

966 Paradigmatisch etwa der Fall BGH NJW 1998, 1854; vgl. ferner die Auflistung der einschlägigen Rechtsprechungsfälle bei Soergel-*Leptien*, § 167 BGB Rn. 31 ff.; schließlich MünchKommBGB-*Schramm*, § 167 BGB Rn. 61 („Organisationsmangel") sowie Rn. 64 („Organisationsrisiko"); ausführlich *Recknagel*, Vertrag und Haftung beim Internet Banking, S. 137 f.

967 BGH NJW 1998, 1854 (1855); BGH NJW-RR 1986, 1169; OLG Dresden NJW-RR 1995, 803 (804); MünchKommBGB-*Schramm*, § 167 BGB Rn. 68; Palandt-*Heinrichs* § 172 BGB Rn. 12; Soergel-*Leptien*, § 167 BGB Rn. 21.

erforderlichen Dauer, um von einem entsprechend zurechenbaren, gesetzten Rechtsschein ausgehen zu können.[968] Dauert der Missbrauch längere Zeit an, so greifen im Übrigen bereits die entsprechenden Kontroll- und Meldepflichten des Kunden gegenüber der Bank ein, so dass die Bank Schadensersatzansprüche gegen den Kunden wegen Vertragspflichtverletzung geltend machen kann.[969]

498 Aus dogmatischer Sicht kann dieses Unbehagen gegenüber einer Anscheinsvollmacht schließlich damit begründet werden, dass hier statt einer Zurechnung einer Erklärung, die auf einer Handlung und einem Erklärungsbewußtsein beruhen müsste, letztlich eine Haftung auf das positive Interesse für die **fahrlässige Verletzung von rechtsverkehrsbezogenen Sorgfaltspflichten** eingeführt wird, ein Tatbestand, wie er für die Pflichtverletzungen im vorvertraglichen Stadium eher typisch ist.[970] Eine weit verbreitete Lehre möchte die Anscheinsvollmacht daher insgesamt auf den Handelsverkehr beschränken.[971]

(b) Allgemeine Haftung für fahrlässig gesetzte Rechtsscheinstatbestände?

499 Ein Teil der Literatur bejaht eine besondere Rechtsscheinsvollmacht in Fortbildung der Grundsätze zur Anscheinsvollmacht, wobei jedoch auf das Erfordernis der „gewissen Häufigkeit und Dauer“ verzichtet werden soll.[972] Bei R-Gesprächen lehnt der BGH in der Regel die herkömmliche Anscheinsvollmacht ab. Allerdings komme eine Rechtsscheinshaftung bei R-Gesprächen aber doch in Betracht, wenn ein Minderjähriger wiederholt und über gewisse Dauer R-Gespräche angenommen hat und der Anbieter durch das Begleichen der Rechnung durch den Anschlussinhaber davon ausgehen konnte, dass dieser die Inanspruchnahme dulde.[973] Das bedeutet, dass der BGH gerade nicht auf das anerkannte Merkmal der „gewissen Häufigkeit und Dauer“ verzichten will. Gegen die Annahme einer Rechtsscheinshaftung beim Online-Banking spricht indessen, dass die

968 Wie hier *Siebert*, Das Direktbankgeschäft, S. 133; *Langenbucher*; Die Risikozuordnung im bargeldlosen Zahlungsverkehr, S. 146; *Recknagel*, Vertrag und Haftung beim Internet-Banking, S. 138 f.

969 *Recknagel*, Vertrag und Haftung beim Internet-Banking, S. 139.

970 So insbesondere *Flume*, AT II, § 49, 3, 4; dem folgend *Medicus*, Bürgerliches Recht, Rn. 101; *Pawlowski*, Allgemeiner Teil des BGB, Rn. 720; Staudinger-*Schilken*, § 167 BGB Rn. 31; *Erfurth*, WM 2006, 2198 (2200); *Wiesgickl*, WM 2000, 1039 (1047); *Werner*, Bankrecht und Bankpraxis, Rn. 19/349; *Langenbucher*, Die Risikozuordnung im bargeldlosen Zahlungsverkehr, S. 25; *Recknagel*, Vertrag und Haftung beim Internet-Banking, S. 138.

971 *Canaris*, Die Vertrauenshaftung im deutschen Privatrecht, S. 48 ff.

972 Zur „Btx-Rechtsscheinsvollmacht“ *Lachmann*, NJW 1984, 405 (408); für Btx im Bankbereich unter Verwendung von PIN und TAN auch *Borsum/Hofmeister*, NJW 1985, 1205 (1206); im Ergebnis wohl ebenso *Dörner*, AcP 202 (2002), 363 (390 f.).

973 BGH JZ 2006, 1073 (1074) mit Anm. *Lobinger*.

gesetzlich geregelten Fälle der Rechtsscheinshaftung im nicht-kaufmännischen Verkehr[974] für die Zurechnung eines Rechtsscheins grundsätzlich die **bewusste Schaffung des Rechtsscheinstatbestandes** (z.B. §§ 170 ff., 405 BGB) verlangen.[975] Insbesondere im Verbraucherbereich dürften an die Zurechnung fahrlässig gesetzter Rechtsscheine daher hohe Anforderungen zu stellen sein.[976] Die Anscheinsvollmacht durchbricht den genannten Grundsatz insoweit, als sie Fahrlässigkeit als Zurechnungsgrund ausreichen lässt (zur rechtsdogmatischen Kritik oben Rn. 498). Dies lässt sich indessen nur unter Hinweis, wie auch vom BGH bei R-Gesprächen bekräftigt,[977] auf die Anforderungen des objektiven Rechtsscheinstatbestandes – mehrmaliges Auftreten des Vertreters von gewisser Dauer – rechtfertigen. Der Vertretene hat aufgrund der zeitlichen Streckung des Rechtsscheinstatbestandes insbesondere die Möglichkeit, das Handeln des Dritten (der noch dazu seiner Sphäre entstammt) zu erkennen und zu verhindern. Versäumt er dies, stellt die Rechtsprechung die fahrlässige Nichtverhinderung des Handelns des Vertreters dem bewussten Dulden gleich.[978]

500 Beim Online-Banking wird im Regelfall nur ein einmaliger Identitätsmissbrauch vorliegen. Der dadurch entstandene Rechtsschein kann dem Kunden auch dann nicht zugerechnet werden, wenn ihm im Einzelfall – etwa bei Beantwortung einer Phishing-E-Mail – eine Sorgfaltspflichtverletzung vorzuwerfen sein sollte, denn vor dem eigentlichen Missbrauch besteht zwar die abstrakte Gefahr eines Angriffs Dritter, anders als bei der Anscheinsvollmacht wird der Bankkunde jedoch nicht durch konkrete Anhaltspunkte für ein Missbrauchsverhalten Dritter für Schutzmaßnahmen sensibilisiert. Somit mag zwar ein punktuelles Fehlverhalten vorliegen (bspw. die sorglose Weitergabe von PIN und TAN im Zusammenhang mit Phishing-Mails), dieses genügt jedoch nicht, um es in der Rechtswirkung dem bewussten Dulden gleich zu stellen; es begründet vielmehr al-

974 Nach §§ 56, 362 HGB wird im kaufmännischen Verkehr ein Rechtsschein auch rein objektiv zugerechnet. Dazu *Langenbucher*, die Risikozuordnung im bargeldlosen Zahlungsverkehr, S. 25.

975 *Canaris*, Die Vertrauenshaftung im deutschen Privatrecht, S. 51, 477 ff.; *Langenbucher*, Die Risikozuordnung im bargeldlosen Zahlungsverkehr, S. 25, 146 mwN. Gleiches gilt für die Duldungsvollmacht und den Blankettmissbrauch (§ 172 BGB analog), BGH NJW 1996, 1469 ff.; *Canaris*, Die Vertrauenshaftung im deutschen Privatrecht, S. 62. Auch bei der abhanden gekommenen Vollmachtsurkunde genügt die bloße Fahrlässigkeit des Vertretenen nicht, siehe BGH NJW 1975, 2101 (2102).

976 In diese Richtung auch *Canaris*, Bankvertragsrecht, Rn. 527 ff. Zum Streit um die Anscheinsvollmacht im nicht-kaufmännischen Bereich *Canaris*, Die Vertrauenshaftung im deutschen Privatrecht, S. 48 ff.

977 BGH JZ 2006, 1073 (1074) mit Anm. *Lobinger*.

978 Die Anscheinsvollmacht entpuppt sich somit als abgeschwächte Duldungsvollmacht. Bei der Duldungsvollmacht begründet bereits das erstmalige Auftreten als Vertreter den Rechtsschein, jedoch nur deshalb, weil der Vertretene das Handeln bewusst duldet, Palandt-*Heinrichs*, § 172 BGB Rn. 8.

lenfalls eine zum Schadensersatz verpflichtende **Vertragspflichtverletzung**.[979] Eine Gleichstellung mit den Fällen der Anscheinsvollmacht müsste überdies die Beherrschbarkeit des eingesetzten Mediums und des Missbrauchs Dritter in gleichem Maße wie im Falle des Risikos des in der Organisationsphäre eingesetzten Gehilfen postulieren – woran erhebliche Zweifel bestehen.

501 Gegen eine Lösung nach Rechtsscheinsgrundsätzen spricht im Bereich des E-Commerce und des Online-Banking im Besonderen, dass ein Schadensersatzanspruch **flexiblere Lösungen** erlaubt als eine pauschale Zurechnung kraft Rechtsscheins. Der Vorteil einer Lösung über Schadensersatzregeln liegt hierbei insbesondere die Berücksichtigung eines **Mitverschuldens** der Bank (§ 254 BGB) bei der Bemessung der Schadenshöhe.

(b) Schadensersatzansprüche der Bank

502 Verletzt der Kunde schuldhaft seine Sorgfaltspflichten aus dem Online-Bankingvertrag, haftet er der Bank für entstandene Schäden gemäß **§§ 280 Abs. 1, 241 Abs. 2 BGB**. Die Online- und Homebanking-Bedingungen enthalten keine eigene Haftungsregelung (mehr), vielmehr kommt die Haftungsregelung der Ziffer 3 der AGB-Banken zur Anwendung, welche eine **verschuldensabhängige Haftung** vorsieht.[980] Diese Haftungsklausel entspricht dem gesetzlichen Leitbild und ist mit § 307 BGB vereinbar.[981] Wie nunmehr auch im österreichischen Recht anerkannt,[982] kann die Bank das Risiko für ein (von ihr nicht verschuldetes) Versagen der Sicherheitssysteme nicht im Wege einer verschuldensunabhängigen Risikohaftung auf den Kunden verlagern. Für die Haftung beim Online-Banking ist dabei entscheidend die Pflichtenverteilung zwischen Kunde und Bank, die gerade im IT-spezifischen Bereich bislang wenig geklärt ist. Gerichtliche Entscheidungen zu den Pflichten im Zusammenhang mit Online-Banking liegen soweit ersichtlich noch nicht vor.

(i) Interessenlage und Zurechnungskriterien

503 Der Bank obliegen als Initiator des Online-Banking Pflichten zur Sicherung der in diesem Verfahren getätigten Bankgeschäfte. Dahinter steht die Wertung, dass die Bank

---

979 Im Ergebnis ebenso *Langenbucher*, Die Risikozuordnung im bargeldlosen Zahlungsverkehr, S. 146.

980 *Borges*, NJW 2005, 3313 (3314); *Kind/Werner*, CR 2006, 353 (354); *Karper*, DuD 2006, 215 (216); *Bock*, in: Bräutigam/Leupold, Kap. VII Rn. 81; *Langenbucher*, Die Risikozuordnung im bargeldlosen Zahlungsverkehr, S. 146.

981 *Neumann/Bock*, Zahlungsverkehr im Internet, Rn. 178.

982 OGH 4 Ob 179/02f.

durch die Eröffnung des Online-Verkehrs ein Risiko veranlasst hat,[983] welches sie mit ihren personellen, finanziellen und technischen Ressourcen besser beherrschen kann als der Kunde.[984] Hinzu kommt die Möglichkeit der Banken, Sicherungsaufwand und Schäden auf durch entsprechende Preisgestaltung umzulegen.[985] Die Kreditinstitute entscheiden in eigener Verantwortung über das angebotene Sicherungssystem und steuern damit gerade im Hinblick auf neue Formen von Bedrohungen aus dem Internet das beim Kunden verbleibende Restrisiko und die von ihm zu treffenden Sicherungsmaßnahmen. So verwenden einige Banken noch immer Aktive Inhalte in ihren Webangeboten, welche auf der Kundenseite ein großes Angriffspotential eröffnen (näher Rn. 515). Hinzu kommt ein großer Informationsvorsprung der Banken gerade auch im Hinblick auf neu auftretende Bedrohungsformen.[986]

504 Die Banken ziehen aus dem Online-Banking beträchtliche eigene Vorteile. Diese liegen in der Einsparung von Personal, Filialen und – zeitgeistgerecht – jederzeitiger Erreichbarkeit der Bank für den Kunden und der Möglichkeit einer Marktexpansion ohne größeren Investitionsaufwand.[987] Man wird zwar zugeben müssen, dass Online-Banking – etwa in Form geringerer Überweisungsgebühren und Unabhängigkeit von Banköffnungszeiten – auch dem Bankkunden Vorteile bietet. Bei wertender Betrachtung liegen die Vorteile indessen überwiegend auf Seiten der Bank, die sich überdies an die breite Masse der Bankkunden wendet und nicht nur an den technisch versierten Internet-Nutzer.[988] Wegen höherer Transaktionskosten beim herkömmlichen Bankgeschäft schafft die Bank zudem selbst Anreize, durch den Abbau von Filialen – etwa in ländlichen Gebieten –, aber auch faktischen Zwang zur Inanspruchnahme ihres Online-Angebots.

505 Auch wenn Vorteile und Risiken somit vornehmlich bei der Bank liegen, wird man den Bankkunden nicht aus allen Sorgfaltspflichten entlassen können. Der Kunde verfügt mit seinem privaten Computer über eine **potenzielle Gefahrenquelle** (allgemein Rn.282). Hinzu kommt, dass bei Phishing und Pharming der PC des Kunden das primäre Angriffsziel bildet und Sicherheitsvorkehrungen somit notwendig auch beim Kunden (sei-

983 Zu ähnl. Erwägungen im Rahmen der Rechtsprechung zu Dialern s. BGH MMR 2004, 308 (311); LG Stralsund MMR 2006, 487 (488).
984 Ebenso *Erfurth*, WM 2006, 2198 (2206).
985 *Erfurth*, WM 2006, 2198 (2206).
986 Ebenso *Kind/Werner*, CR 2006, 353 (356).
987 So auch *Erfurth*, WM 2006, 2198 (2206).
988 *Spindler*, in: Hadding/Hopt/Schimansky, S. 179; *Recknagel*, Vertrag und Haftung beim Internet-Banking, S. 225 f.

nem PC) selbst ansetzen müssen. Ein maßgeblicher Gesichtspunkt ist hierbei die **Möglichkeit des Selbstschutzes** (allg. Rn. 294 ff.), d.h. inwieweit der Kunde mit einfachen und kostengünstigen Mitteln eigene Schutzvorkehrungen treffen kann, wobei aber insbesondere im technischen Bereich keine überzogenen Anforderungen an die Sorgfalt des Durchschnittsnutzers gestellt werden dürfen (näher unten Rn. 531 ff.).

506 Anders als in den ec-Karten-Fällen, in denen viele Sachverhalte sich dem gesunden Menschenverstand erschließen, etwa die Aufbewahrung einer ec-Karte zusammen mit der PIN in einem Jackett im Büro etc,[989] ist das Bewusstsein für IT-Risiken wesentlich geringer ausgeprägt, da die technischen Vorgänge komplex und für den überwiegenden Teil der Kunden schwer zu durchschauen sind. Dies trifft in besonderem Maße auf die neuen Bedrohungslagen des Phishing und Pharming zu, welche den meisten Online-Banking-Kunden nicht oder nur wenig bekannt sind.

507 Um entsprechende Sorgfaltspflichten im Umgang mit den Legitimationsmedien beim Online-Banking anzunehmen, die sich auch auf Risiken des EDV-Einsatzes beziehen, muss ein Mehr an Aufklärung und Information sowie an Sicherungsmaßnahmen seitens der das System einsetzenden Bank verlangt werden. Erst die Weitergabe des nötigen Wissens und die Schaffung eines Risikobewusstseins auf Seiten des Kunden versetzt diesen bei technisch komplexen Dienstleistungen in die Lage, die angemessenen Sicherheitsvorkehrungen zu ergreifen. Die vom Kunden verlangten Pflichten sind daher stets im Lichte der Pflichten, die der Bank obliegen, zu sehen. Ob mangels ausreichender Aufklärung und Instruktion bereits eine Pflichtverletzung des Bankkunden zu verneinen oder der Anspruch der Bank nach § 254 BGB zu kürzen ist, wird sich nur im Einzelfall beurteilen lassen.

(ii) Pflichten der Bank

508 Die Bestimmung der Pflichten der Bank erlangt in zweifacher Hinsicht Bedeutung: zum einen kann die Verletzung der die Bank treffenden Vertragspflichten nach §§ 280 Abs. 1, 241 Abs. 2 BGB eine **Schadensersatzhaftung** gegenüber dem Kunden begründen, zum anderen beeinflussen die Sorgfaltsanforderungen der Bank – quasi spiegelbildlich – die Obliegenheiten der Bank im Rahmen der Prüfung des **Mitverschuldens** (§ 254 BGB) (dazu unten Rn. 548).

---

989 S. etwa für den vergleichbaren Fall der gemeinsamen Aufbewahrung von ec-Karte und Scheckvordrucken in einem im Büro aufgehängten Jackett AG Hannover WM 1996, 2013 f.; s. auch LG Köln NJW-RR 2001, 1340 (1341).

(a) Technische Sicherheit

509 Die Bank unterliegt beim Online-Banking den für ein Unternehmen üblichen Sorgfaltsanforderungen.[990] Die allgemeinen Organisationspflichten im IT-Bereich ergeben sich hierbei aus § 25a KWG (oben Rn. 435 ff.). Als grundlegende Pflicht obliegt der Bank die Bereitstellung eines **technisch sicheren Online-Banking-Systems**.[991] Das System muss danach einerseits Schutz vor gegen die Bank selbst gerichteten Angriffen bieten. Genauso hat die Bank durch die technische Gestaltung des Online-Banking-Verfahrens aber auch die technischen Voraussetzungen für eine sichere Benutzung des Online-Banking durch den Kunden zu schaffen und – soweit technisch möglich – Missbräuchen durch Dritte bereits auf technischer Ebene zu begegnen. Schließlich ist durch regelmäßige Überprüfungen die Sicherheit des Systems auch während des Betriebs zu gewährleisten und auf Sicherheitslücken – insbesondere nach Hinweisen von außen[992] – durch erforderliche Anpassung des Systems zu reagieren.

510 Aus Sicht des Gesetzgebers bestand zumindest vor Auftreten der ersten Fälle von Phishing und Pharming keine Notwendigkeit, einen allgemeinen Sicherheitsstandard gesetzlich, untergesetzlich oder durch eine freiwillige Verpflichtung der Banken einzuführen.[993] Maßgeblich für die Sicherheitserwartungen des Verkehrs ist gegenwärtig der jeweilige **Stand der Technik**.[994] Hierbei ist anerkannt, dass normative Standards[995] wie der „Stand der Technik" den Pflichteninhalt nicht nur dort konkretisieren, wo eine Vorschrift des technischen Sicherheitsrechts eine ausdrückliche Regelung vorsieht. Vielmehr umschreiben technische Standards auch außerhalb dieses Bereichs die zur Gefahrsteuerung objektiv geeigneten Maßnahmen.[996] Der erforderliche Sicherheitsstandard bestimmt sich nach dem **Gefährdungspotential** des technischen Systems,[997] welches im

990 *Spindler*, in: Hadding/Hopt/Schimansky, S. 178; zust. *Erfurth*, WM 2006, 2198 (2201).

991 *Kind/Werner*, CR 2006, 353 (357 f.); *Karper*, DuD 2006, 215 (217); *Koch*, Versicherbarkeit von IT-Risiken, Rn. 812; *Recknagel*, Vertrag und Haftung beim Internet-Banking, S. 151, 206; *Gößmann*, in: Bankrechts-Handbuch, § 55 Rn. 19.

992 Vgl. etwa zu den Sicherheitsmängeln der Online-Banking-Portale der Sparda-Bank und der DAB-Bank durch sog. Cross-Site-Scripting-Lücken (XXS) abrufbar unter: http://www.heise.de/newsticker/meldung/76258.

993 Antwort der Bundesregierung vom 4.7.2000 auf die Kleine Anfrage der Abgeordneten Rainer Funke, Dr. Edzard Schmidt-Jortzig, Dr. Max Stadler, weiterer Abgeordneter und der Fraktion der F.D.P. – Drucksache 14/3603 –, BT-Drucks. 14/3757, S. 3.

994 So auch *Kind/Werner*, CR 2006, 353 (359); *Recknagel*, Vertrag und Haftung beim Internet-Banking, S. 207, 225.

995 Zur Unterscheidung zwischen anerkannten Regeln der Technik, Stand der Technik und Stand von Wissenschaft und Technik grundlegend *Marburger*, Die Regeln der Technik im Recht, S. 121 ff.

996 *Marburger*, Die Regeln der Technik im Recht, S. 439.

997 *Marburger*, Die Regeln der Technik im Recht, S. 126 f.

Online-Banking durch das Risiko beträchtlicher Vermögensschäden und die Offenbarung personenbezogener Daten des Kunden gekennzeichnet ist. Im Bereich des Online-Banking muss zudem berücksichtigt werden, dass sich die Online-Dienstleistung der Banken gerade auch an den **technisch nicht versierten Nutzer** wendet.

511 Die Unterhaltung und der Betrieb technischer Systeme stellen Dauertatbestände dar, die eine Pflicht zur **Anpassung der Systeme** an den jeweils verbesserten technischen Standard nach sich ziehen, wobei jedoch der mit einer Anpassung verbundene Sicherheitsgewinn mit dem wirtschaftlichen Aufwand in Relation zu setzen ist.[998] Hier lassen sich Parallelen zum Recht der Anlagensicherheit, aber auch zum Produkthaftungsrecht ziehen: Der Hersteller eines Produkts haftet zwar nicht für im Zeitpunkt des Inverkehrbringens nach dem Stand von Wissenschaft und Technik nicht erkennbare Fehler (Entwicklungsfehler), doch ist er verpflichtet seine künftige Produktion auf die neu aufgetretene Gefahrenlage einzustellen.[999] Diese Wertung ist auf die Bank als IT-Dienstleister übertragbar, so dass sie zur Behebung von Sicherheitslücken ihres Systems bzw. Umstellung des Online-Banking-Sicherungsverfahrens verpflichtet ist,[1000] wenn sich herausstellt, dass das verwendete PIN/TAN-Verfahren nach geltendem Stand der Technik nicht mehr sicher ist. Man wird der Bank für die Umstellung ihrer Systeme aber eine **Übergangszeit** einräumen müssen.

512 Gegenwärtig dürfte aufgrund der Erfahrungen mit Phishing und Pharming davon auszugehen sein, dass ein **konventionelles PIN-/TAN-Verfahren** nicht mehr dem Stand der Technik entspricht, da es für Angriffe Dritter aus dem Netz – insbesondere durch Schadprogramme, die den PC unbemerkt kontrollieren – eine erhöhte Anfälligkeit aufweist.[1001] Die - für Btx wohl noch gültige - Annahme, dass die TAN Sicherheit verspricht, da sie zwar ausgespäht werden kann, aber schon während des Ausspähens verbraucht ist,[1002] hilft nicht weiter. Denn die TAN, die eingesetzt wird, gelangt in den oben Rn. 473 ff. beschriebenen Angriffsszenarien überhaupt nicht bis zur Bank, sondern wird vorher quasi „abgesogen“ und gesammelt werden, so dass sie dann für einen Einsatz durch Dritte zusammen mit der PIN-Nummer zur Verfügung steht.

---

998 Dazu *Marburger*, Die Regeln der Technik im Recht, S. 162, 437 f.; allgemein dazu: MünchKommBGB-*Wagner*, § 823 BGB Rn. 271 ff.

999 BGH NJW 1990, 906 (907 f.); BGH NJW 1994, 517 (519 f.); BGH NJW 1994, 3349 (3350 f.); *Kullmann*, in: Kullmann/Pfister, Kz. 1520, Bl. 60 f.; MünchKommBGB-*Wagner*, § 823 BGB Rn. 580, 602.

1000 So auch *Kind/Werner*, CR 2006, 353 (359); *Recknagel*, Vertrag und Haftung beim Internet-Banking, S. 47 f.

1001 So wohl auch *Kind/Werner*, CR 2006, 353 (357).

1002 So für das Btx-Banking *Hellner*, FS Werner, S. 251, 270.

513 Ein Teil der Banken hat auf die neue Bedrohungslage bereits reagiert und neue Varianten des PIN-/TAN-Verfahrens eingeführt. Nach Einschätzung des BSI sind für das Online-Banking allein Verfahren geeignet, bei welchen ein **Medienbruch** durch den Einsatz zusätzlicher Hardware erfolgt. Von den gegenwärtig im Einsatz befindlichen PIN/TAN-Sicherungsverfahren entsprechen diesen Anforderungen einzig Verfahren mit **TAN-Generator** und Verfahren bei welchen eine Bestätigung der übermittelten Transaktionsdaten auf das Mobiltelefon des Kunden erfolgt (**mTAN**). Beide Verfahren ermöglichen es, dass Manipulationen der Transaktionsdaten durch ein Schadprogramm vom Kunden (mTAN) bzw. der Bank (TAN-Generator) sofort erkannt werden können.

514 Das **HBCI-Verfahren** mit Chipkarte und elektronischer Signatur gilt derzeit als das wohl sicherste Verfahren beim Online-Banking.[1003] Eine **Pflicht zum Systemwechsel** von PIN-/TAN auf ein Verfahren mit elektronischer Signatur (z.B. HBCI) – so die Forderung von Verbraucherschutzverbänden[1004] – wird man zum gegenwärtigen Zeitpunkt nicht annehmen können. Zwar ist ein Verfahren mit Chipkarte und elektronischer Signatur äußerst sicher gegenüber Missbräuchen. Neuere Varianten des PIN-/TAN-Verfahrens (z.B. mTAN der Postbank, Sm@rtTAN plus der Volksbanken) haben sich aber als durchaus leistungsfähig erwiesen, so dass gegenwärtig kein zwingendes sicherheitstechnisches Bedürfnis zum Umstieg auf HBCI erkennbar ist.[1005] Überdies ist zu bedenken, dass Verfahren mit Chipkarte vom Bankkunden – insbesondere wegen der höheren Kosten für die Anschaffung und die weniger komfortable Bedienung (z.B. keine Nutzungsmöglichkeit am Arbeitsplatz) – bislang nur zögerlich angenommen werden.

515 Die Sicherheit des Online-Bankings kann auf einfache Weise auch bei der Gestaltung des Web-Portals der Bank erhöht werden. Die **Verwendung Aktiver Inhalte** in sensiblen Webangeboten wie dem Online-Banking entspricht nicht dem Stand der Technik. Durch die Verwendung Aktiver Inhalte auf den Seiten der Bank wird der Kunde gezwungen Aktive Inhalte in seinem Browser freizuschalten um das Online-Banking-Angebot überhaupt nutzen zu können. Die Freischaltung Aktiver Inhalte führt auf der

---

1003 Selbst das HBCI-Verfahren hat sich bei einem gestellten Angriff durch den Chaos Computer Club in Zusammenarbeit mit dem Hessischen Rundfunk als nicht völlig sicher gegenüber Trojanern erwiesen, wenn der Bankkunde seine Chipkarte im Lesegerät stecken lässt, vgl. abrufbar unter: http://www.heise.de/newsticker/meldung/9349. Sofern der Kunde darüber instruiert war, die Chipkarte nach Beendigung des Online-Banking aus dem Lesegerät zu entfernen, wird man hier eine Pflichtverletzung des Kunden annehmen können.

1004 Vgl. *Stockhausen*, WM 2001, 605 (606).

1005 Im Ergebnis ebenso *Kind/Werner*, CR 2006, 353 (359). Dazu auch *Spindler*, in: Hadding/Hopt/Schimansky, S. 212 f.

Kundenseite jedoch zugleich zu einer deutlich erhöhten Gefährdung, da Aktive Inhalte wichtige Hilfsmittel für mehr oder weniger aufwändige Angriffe Dritter sind. Alternative Möglichkeiten zur ansprechenden Gestaltung von Webseiten ohne Aktive Inhalte sind verfügbar und mit nur geringem Aufwand auch noch nachträglich umsetzbar. Verwendet die Bank auf ihren Webseiten dennoch Aktive Inhalte, wird man im Schadensfall eine eigene Pflichtverletzung, zumindest aber ein Mitverschulden der Bank annehmen müssen.

(b) Beobachtungspflichten

516 Neben der fortlaufenden Überwachung der eigenen Systeme trifft die Bank auch die Pflicht die Sicherheit des Online-Bankings insoweit zu beobachten, als nicht die Bank selbst, sondern der Kunde Angriffsziel ist. Maßgebliche Wertung ist hierbei, dass die Bank als **überlegene Systembeherrscherin** über das spezifische Wissen um Risiken verfügt oder sich dieses zumindest leichter aneignen kann als der Kunde.[1006] Übertragen auf Phishing und Pharming bedeutet dies, dass die Bank Vorkehrungen treffen muss, um neu auftauchende Formen von Bedrohungen aus dem Internet zu erkennen und durch entsprechende Reaktionen zu beseitigen oder zumindest zu minimieren.

517 Entsprechend der Produktbeobachtungspflicht des Herstellers[1007] kann hierbei eine **passive** und **aktive** Beobachtungspflicht unterschieden werden. Die Bank hat daher Hinweisen auf Missbräuche aufgrund von bekannt gewordenen Missbrauchsfällen und Kundenbeschwerden nachzugehen. Ebenso ist die Bank aber auch gehalten, aktiv im Internet, einschlägigen Fachpublikationen usw. Informationen über neue Risiken zu beschaffen. Die Beobachtungspflichten der Bank dürfen hierbei nicht überspannt werden. Es genügt daher, wenn die Bank sich auf die Beobachtung marktüblicher und von Kunden üblicherweise eingesetzter Betriebssysteme und Software beschränkt. Organisatorisch ist sicherzustellen, dass diese Informationen an den Kunden (z.B. auf der Website der Bank, durch Informationsbriefe und Flyer) auch weiter gegeben werden (zur Warnpflicht unten Rn. 518).

1006 *Wiesgickl*, WM 2000, 1039 (1049); *Karper*, DuD 2006, 215 (217).
1007 Ausführlich dazu Bamberger/Roth-*Spindler*, § 823 BGB Rn. 511.

(c) Aufklärungs-, Instruktions- und Warnpflichten

518 Die Bank trifft gegenüber dem Kunden eine Aufklärungs- und Instruktionspflicht bereits im Vorfeld der erstmaligen Benutzung.[1008] Gerade für technisch unerfahrene Kunden besteht in dieser Situation der größte Informationsbedarf. Mit Abschluss des Online-Bankingvertrages ist der Kunde daher in die **Benutzung** des Systems[1009] und das **Missbrauchsrisiko**[1010] im Besonderen einzuweisen.[1011] Sofern verschiedene Sicherungsverfahren (z.B. PIN-/TAN und HBCI) angeboten werden, kann von der Bank auch erwartet werden, dass der Kunde vor die **Wahl zwischen den verschiedenen Systemen** gestellt wird. Dem Kunden sind hierzu die Vor- und Nachteile der einzelnen Systeme zu erläutern und – insbesondere im Fall von HBCI – die (höheren) Kosten dem Nutzen gegenüber zu stellen. In der Praxis der Banken erfolgt derzeit oftmals keinerlei Hinweis auf Verfahren mit Chipkarte und elektronischer Signatur – dies dürfte jedoch mit dem Umstand zusammenhängen, dass viele Kunden sich für das bequemere PIN-/TAN-Verfahren entscheiden und die Kosten für die Anschaffung von HBCI scheuen. Erlangt die Bank Kenntnis von neuen Risiken (zur Beobachtungspflicht oben Rn. 516), hat sie ihre Kunden unverzüglich zu **warnen**. Soweit aufgrund der neuen Risikolage erforderlich, hat die Bank ihre Benutzerinformation entsprechend **umzustellen**.[1012]

519 Die Information des Kunden kann in einem persönlichen Beratungsgespräch, einer gesonderten **schriftlichen Bedienungsanleitung** sowie den **Online- bzw. Homebanking-Bedingungen** (s. Rn. 482), einer **Benutzerführung auf dem Bildschirm** und durch eine auffällige Information auf der **Website** des Kreditinstituts (insbesondere in der Nähe des Login-Buttons) erfolgen.[1013] Nicht empfehlenswert ist hierbei die Verwendung von Pop-Up-Fenstern, da diese von vielen Browsern geblockt werden.[1014] Ob die Anord-

---

1008 *Kind/Werner*, CR 2006, 353 (356); *Karper*, DuD 2006, 215 (218); *Bock*, in: Bräutigam/Leupold, Kap. VII Rn. 65 ff.; *Neumann/Bock*, Zahlungsverkehr im Internet, Rn. 167; *Canaris*, Bankvertragsrecht, Rn. 527 ff; *Gößmann*, in: Bankrechts-Handbuch, Band I, § 55 Rn. 19 ff.; *Recknagel*, Vertrag und Haftung beim Internet-Banking, S. 220 ff.

1009 *Bock*, in: Bräutigam/Leupold, Kap. VII Rn. 66.

1010 *Recknagel*, Vertrag und Haftung beim Internet-Banking, S. 220 f.; *Bock*, in: Bräutigam/Leupold, Kap. VII Rn. 67; *Gößmann*, in: Bankrechts-Handbuch, Band I, § 55 Rn. 20.

1011 Ebenso für das Btx-System schon *Hellner*, FS Werner, S. 251, 260 f.; *Siebert*, Das Direktbankgeschäft, S. 125; allgemein für automatisierte Einrichtungen bereits *Köhler*, AcP 182 (1982), 126, 129 ff.

1012 Ebenso *Kind/Werner*, CR 2006, 353 (357). Zur Parallelproblematik der Umstellung der Instruktion durch den Hersteller MünchKommBGB-*Wagner*, § 823 BGB Rn. 602.

1013 *Kind/Werner*, CR 2006, 353 (357); *Bock*, in: Bräutigam/Leupold, Kap. VII Rn. 67 f.; *Recknagel*, Vertrag und Haftung beim Internet-Banking, S. 220; *Gößmann*, in: Bankrechts-Handbuch, Band I, § 55 Rn. 21.

1014 *Kind/Werner*, CR 2006, 353 (357).

nung von Sorgfaltspflichten in den AGB der Banken für sich alleine ausreicht,[1015] erscheint zweifelhaft, da das „Kleingedruckte“ vom Kunden erfahrungsgemäß kaum gelesen wird.[1016] Überdies taugen AGB kaum um den Kunden die Benutzung eines komplexen technischen Systems anschaulich zu erläutern.[1017] Erforderlich und empfehlenswert erscheint daher dem Kunden in jedem Fall eine gesonderte Benutzerinformation zukommen zu lassen und eine Benutzerführung am Bildschirm vorzusehen. Dagegen sollten die Banken von Informationen per **E-Mail** absehen. Empfehlenswert ist es als Schutz gegen Phishing gegenüber dem Kunden von vornherein ausdrücklich klarzustellen, dass die Bank mit ihm unter keinen Umständen per E-Mail in Kontakt treten wird (s. auch Rn. 538).[1018]

520 Die Informationen müssen jeweils auch für einen **Durchschnittskunden** ohne größere technische Fähigkeiten leicht verständlich sein.[1019] Die Anforderungen der Rechtsprechung zur Klarheit und Verständlichkeit von Produktinformationen können hier herangezogen werden.[1020] Im IT-Bereich stößt die Informationspflicht an die **Grenzen des technischen Verständnisses** des Durchschnittskunden. Unbedenklich sind in diesem Zusammenhang Hinweise zur Verwahrung und Geheimhaltung der Legitimationsmedien selbst (z.B. sichere Verwahrung von PIN und TAN oder der Chipkarte bei HBCI). Anders wäre dies zu beurteilen, wenn die Bank dem Kunden Informationen beispielsweise zu komplizierten Einstellungen von Browser oder Firewall zukommen lässt, die zwar erhöhte Sicherheit gewährleisten, einen Großteil der Bankkunden aber überfordern und für sie ohne fremde Hilfe nicht zu bewerkstelligen sind (ausführlich zu den Sorgfaltsanforderungen an private Nutzer im IT-Bereich oben Rn. 280 ff., zu Firewalls Rn. 298). Die Bank kann die Risiken des Online-Banking nicht durch Übererfüllung ihrer Aufklärungs- und Instruktionspflicht auf den Kunden abwälzen. Denn es würde ein Risiko auf den Kunden verlagert, welchem dieser durch eigene Maßnahmen nicht zu begegnen vermag.

1015 So aber *Bock*, in: Bräutigam/Leupold, Kap. VII Rn. 67; ebenso *Hellner*, FS Werner, S. 251, 260 f., allerdings für das Btx-Banking, das geringere Probleme als das Internet aufwies.

1016 So zutreffend *Canaris*, Bankvertragsrecht, Rn. 527 q; *Fervers*, WM 1988, 1037 (1041); aA *Recknagel*, Vertrag und Haftung beim Internet-Banking, S. 220 mit dem Argument, eine derartige Nachlässigkeit dürfte nicht zu Lasten der Bank gehen.

1017 *Neumann/Bock*, Zahlungsverkehr im Internet, Rn. 167.

1018 *Kind/Werner*, CR 2006, 353 (357).

1019 *Neumann/Bock*, Zahlungsverkehr im Internet, Rn. 167.

1020 Näher Bamberger/Roth-*Spindler*, § 823 BGB Rn. 502 ff.; MünchKommBGB-*Wagner*, § 823 BGB Rn. 588 ff.

(d) Organisationspflichten

521 Erlangt die Bank Kenntnis von missbräuchlichen Transaktionen, hat sie dafür Sorge zu tragen, dass keine weiteren unberechtigten Transaktionen erfolgen können.[1021] Daneben hat die Bank Vorkehrungen dahingehend zu treffen, dass der Kunde den Zugang zum Online-Banking bei Kenntnis oder Verdacht eines Missbrauchs jederzeit **sperren** lassen kann.[1022]

(iii) Pflichten des Kunden

522 Die **vertraglichen Schutzpflichten** nach §§ 280 Abs. 1, 241 Abs. 2 BGB entsprechen inhaltlich weitgehend den **deliktischen Verkehrspflichten**[1023] (zu den deliktischen Verkehrspflichten des privaten Nutzers ausführlich oben Rn. 275 ff.). Schutzmaßnahmen, welche vom privaten IT-Nutzer nach deliktsrechtlichen Grundsätzen verlangt werden können, bilden im vertraglichen Bereich grundsätzlich zugleich den Mindestgehalt der vertraglichen Schutzpflichten nach § 241 Abs. 2 BGB. Im Einzelfall können die vertraglichen Sorgfaltsanforderungen angesichts der bestehenden Sonderverbindung und der damit verbundenen verstärkten Einwirkungsmöglichkeit auf die Rechte und Rechtsgüter des Vertragspartners über die deliktischen Pflichten hinausgehen. Die Pflichten des Kunden werden konkretisiert durch die Online- und Homebanking-Bedingungen.

(c) Allgemeine Geschäftsbedingungen der Banken

523 Auch wenn die Online-Bedingungen und Homebanking-Bedingungen keine ausdrückliche Haftungsregelung vorsehen, sind sie insoweit für die Haftung des Kunden von Bedeutung, als sie die Pflichten des Kunden näher ausgestalten.

(i) Online-Banking-AGB in der Praxis

524 Die im Bereich des Online-Banking derzeit verwendeten Sonderbedingungen für Online- und Homebanking sehen ausdrückliche Regelungen der Pflichten des Kunden vor. So regeln die **Online-Bedingungen**[1024]:

> 7. Geheimhaltung der PIN und TAN
>
> Der Teilnehmer hat dafür Sorge zu tragen, dass keine andere Person Kenntnis von der PIN und den TAN erlangt. Jede Person, die die PIN und - falls erforderlich - eine TAN kennt, hat die Mög-

1021 *Karper*, DuD 2006, 215 (218).

1022 Vgl. auch Art. 47 des Vorschlags der EU-Kommission für eine Zahlungsdiensterichtlinie.

1023 Palandt-*Heinrichs*, § 280 BGB Rn. 28; MünchKommBGB-*Ernst*, § 280 BGB Rn. 104; Bamberger/Roth-*Grüneberg/Sutschet*, § 241 BGB Rn. 92.

1024 Abgedruckt in WM 2001, 650 f.

lichkeit, das Online-Banking-Leistungsangebot zu nutzen. Sie kann z.B. Aufträge zu Lasten des Kontos/Depots erteilen. Insbesondere Folgendes ist zur Geheimhaltung der PIN und TAN zu beachten:

PIN und TAN dürfen nicht elektronisch gespeichert oder in anderer Form notiert werden;

die dem Teilnehmer zur Verfügung gestellte TAN-Liste ist sicher zu verwahren;

bei Eingabe der PIN und TAN ist sicherzustellen, dass Dritte diese nicht ausspähen können.

Stellt der Teilnehmer fest, dass eine andere Person von seiner PIN oder von einer TAN oder von beidem Kenntnis erhalten hat oder besteht der Verdacht einer missbräuchlichen Nutzung, so ist der Teilnehmer verpflichtet, unverzüglich seine PIN zu ändern bzw. die noch nicht verbrauchten TAN zu sperren. Sofern ihm dies nicht möglich ist, hat er das Kreditinstitut unverzüglich zu unterrichten. In diesem Fall wird das Kreditinstitut den Online-Banking-Zugang zum Konto/Depot sperren. Das Kreditinstitut haftet ab dem Zugang der Sperrnachricht für alle Schäden, die aus ihrer Nichtbeachtung entstehen.

525 Ähnlich bestimmen die **Homebanking-Bedingungen**[1025]:

IV. Legitimationsverfahren/Geheimhaltung

(1) Der Nutzer ist verpflichtet, die mit dem Kreditinstitut vereinbarten Sicherungsmaßnahmen durchzuführen.

(2) Mit Hilfe der mit dem Kreditinstitut vereinbarten Medien identifiziert und legitimiert sich der Nutzer gegenüber dem Kreditinstitut. Der Nutzer hat dafür Sorge zu tragen, dass kein Dritter in den Besitz der Identifikations- und Legitimationsmedien kommt sowie Kenntnis von dem zu deren Schutz dienenden Passwort erlangt. Denn jede Person, die im Besitz der Medien ist und das Passwort kennt, kann die vereinbarten Dienstleistungen nutzen. Insbesondere Folgendes ist zur Geheimhaltung der Identifikations- und Legitimationsmedien zu beachten:

Die den Nutzer identifizierenden Daten dürfen nicht außerhalb der Sicherheitsmedien, z.B. auf der Festplatte des Rechners, gespeichert werden;

die Identifikations- und Legitimationsmedien sind nach Beendigung der Online-Banking-Nutzung aus dem Lesegerät zu entnehmen und sicher zu verwahren;

das zum Schutz der Identifikations- und Legitimationsmedien dienende Passwort darf nicht notiert oder elektronisch abgespeichert werden;

bei Eingabe des Passwortes ist sicherzustellen, dass Dritte dieses nicht ausspähen können.

526 Die Bedingungen stellen weitgehend allgemeine Pflichten hinsichtlich der Geheimhaltung der Legitimationsmedien auf, sehen jedoch keine IT-spezifischen Pflichten wie et-

1025 Abgedruckt in WM 2001, 650.

wa die Installation von Anti-Virensoftware, Firewalls usw. oder Verhaltenspflichten in Bezug auf Phishing-E-Mails vor.

527 Die deutschen Banken haben auf die neuartigen Bedrohungsszenarien durch Phishing und Pharming nunmehr mit einer **Anpassung der Allgemeinen Bankbedingungen** reagiert. So bestimmen nunmehr beispielsweise die AGB der Deutsche Bank AG.[1026]

- Anfragen außerhalb der bankseitig zur Verfügung gestellten originären Zugangswege, in denen nach vertraulichen Daten wie Geheimzahl oder Passwort/Online-TAN gefragt wird, dürfen nicht beantwortet werden.
- Der Aufforderung per elektronischer Nachricht (z.B. E-Mail), eine damit übersandte Verknüpfung zum (vermeintlichen) Online-Banking der Bank anzuwählen und darüber persönliche Zugangsdaten einzugeben, darf nicht gefolgt werden.
- Auf einer Login-Seite (Startseite) zum (vermeintlichen) Online-Banking der Bank darf keine TAN eingegeben werden.
- Der Kunde hat sich regelmäßig über aktuelle Sicherheitshinweise zum Online-Banking auf der Website der Deutschen Bank zu informieren.
- Der Kunde hat vor seinem jeweiligen Zugang zum Online-Banking sicherzustellen, dass auf seinem verwendeten System handelsübliche Sicherheitsvorkehrungen (wie Anti-Viren-Programm und Firewall) installiert sind und diese ebenso wie die verwendete Systemsoftware regelmäßig aktualisiert werden. Beispiele handelsüblicher Sicherheitsvorkehrungen kann der Kunde der Website der Deutschen Bank entnehmen.

528 Die AGB der comdirect Bank[1027] enthalten unter anderem die Regelung

> Die Sicherheitsvorkehrungen gem. Nr. 4 sollten nicht abgespeichert werden, insbesondere ist im Internet der Cache des verwendeten Browsers zu deaktivieren oder nach der Nutzung zu löschen (vgl. Sicherheitshinweise im Internet).

529 Die Vereinbarkeit vieler derzeit gebräuchlicher Bedingungen für die Online-Nutzung mit den Vorschriften der §§ 307 ff. BGB, war bislang noch nicht Gegenstand gerichtlicher Entscheidungen. Angesichts der oben entwickelten Kriterien für Sorgfaltspflichten

---

1026 Vgl. A II Nr. 8. der AGB der Deutsche Bank AG. Besondere Bestimmungen im Hinblick auf Angriffe aus dem Internet sehen auch die AGB der Citibank (C I Nr. 11) vor. Entsprechende Hinweise zur Sicherheit beim Online-Banking stellt auch der Bundesverband Deutscher Banken (BDB) in seinen Empfehlungen zur Verfügung, abrufbar unter: http://www.bankenverband.de/pic/artikelpic/072005/br0507_rb_phishing.pdf und abrufbar unter: http://www.bankenverband.de/pic/artikelpic/092006/06_09_OnlineBankingSicherheit.pdf (zuletzt abgerufen am 06.06.2007).

1027 Siehe A. II. Nr. 9, abrufbar unter: http://www.comdirect.de/static/pdf/corp0058.pdf (zuletzt abgerufen am 06.06.2007).

des privaten IT-Nutzers, sind die Grenzen des für den Kunden technisch und wirtschaftlich Zumutbaren zu beachten (allgemein Rn. 289 ff., zum Online-Banking unten Rn. 531 ff.). Hier könnten sich zumindest Teile der Sorgfaltsanforderungen an den Kunden im Online-Banking-Bereich als zu streng und mit dem Verbot den Kunden entgegen den Geboten von Treu und Glauben unangemessen zu benachteiligen (§ 307 Abs. 1, 2 BGB), unvereinbar erweisen.[1028]

(ii) Inhaltskontrolle

(a) Geheimhaltung und sichere Verwahrung der Legitimationsmedien

530 Die den Kunden treffenden Sorgfaltspflichten sind insoweit unproblematisch, als es um die **Geheimhaltung** und **sichere Verwahrung** von PIN und TAN bzw. der Chipkarte bei HBCI geht.[1029] Hier liegen Vergleiche zur ec-Karte nahe. Der Kunde darf die Legitimationsmedien nicht an Dritte weitergeben und die PIN nicht auf einem am Bildschirm befestigten Zettel zu notieren oder auf dem PC abspeichern. Bei der Eingabe von PIN und TAN muss sichergestellt sein, dass Dritte diese nicht ausspähen können. Hierbei handelt es sich um Vorgänge, die auch in der Laiensphäre leicht nachzuvollziehen sind und die jeder Kunde in ihrer Bedeutung für die Geheimhaltung und Funktionsfähigkeit des Gesamtsystems unschwer erkennen und befolgen kann. Die Bedeutung der Geheimhaltung der Legitimationsmedien ist überdies von der ec-Karte und Kreditkarte dem Bankkunden vertraut. Die von der Rechtsprechung zur ec-Karte entwickelten Grundsätze dürften insoweit auch übertragbar sein.[1030]

(b) IT-spezifische Pflichten des Bankkunden beim Online-Banking

(i) Grundsätze

531 Weitgehend ungeklärt ist, welche **IT-spezifischen** Sorgfaltspflichten (insbesondere Umgang mit Phishing-E-Mails, Installation von Virenschutz, Firewalls usw.) dem Kunden zumutbar auferlegt werden können. Auszugehen ist hierbei von den allgemeinen Pflichten privater IT-Nutzer (Rn. 275 ff.). Denn Pflichten, welche den privaten Nutzer aufgrund deliktischer Verkehrspflichten gegenüber Dritten treffen, sind grundsätzlich

---

1028 S. dazu auch *Erfurth*, WM 2006, 2198 (2201 f.).

1029 *Kind/Werner*, CR 2006, 353 (354).

1030 Vgl. etwa zu den Sorgfaltsanforderungen an die Verwahrung der ec-Karte und PIN in der Wohnung BGH NJW 2001, 286 ff.: keine grobe Fahrlässigkeit bei Aufbewahrung von ec-Karte und PIN in einer Wohnung; OLG Frankfurt NJW-RR 2001, 1341 (1342): keine grobe Fahrlässigkeit bei Aufbewahrung der PIN in einem anderen Stockwerk des Hauses. Ausführlich auch *Werner*, in: Hellner/Steuer, Band 3, 6/1386 ff.

auch im Rahmen einer vertraglichen Sonderverbindung zu beachten (§ 241 Abs. 2 BGB).[1031] Im Rahmen des Vertragsverhältnisses zwischen Bank und Kunde ist daher jedenfalls kein gegenüber den deliktischen Sorgfaltspflichten geringerer Maßstab anzusetzen.

532 Gewichtiger ist indes die Frage, ob den Bankkunden beim Online-Banking gegenüber den allgemeinen Grundsätzen **erhöhte Sorgfaltspflichten** treffen.[1032] Hierfür mag zwar sprechen, dass sich der Kunde der höheren Sensibilität von Online-Bankgeschäften bewusst sein dürfte und die Risiken durch Phishing-E-Mails und Trojaner aufgrund von Medienberichten und der Informationsarbeit der Banken einem breiten Publikum bekannt geworden sind (allg. Rn. 473).[1033] Die bloße Kenntnis von der Bedrohungslage darf indessen nicht darüber hinwegtäuschen, dass dem Großteil der Internet-Nutzer und Online-Bankkunden zum gegenwärtigen Stand spezielle Computer- und Internet-Kenntnisse fehlen, um allen diesen Phänomenen wirksam zu begegnen.

533 Anders als die Pflichten zur Geheimhaltung und sicheren Verwahrung der Legitimationsmedien, erschließen sich die im IT-spezifischen Bereich erforderlichen Maßnahmen dem Durchschnittskunden nicht ohne weiteres. Die Anpassung oder Änderung der Sicherheitseinstellungen des eigenen PC, werden normale Nutzer häufig überfordern. Die technischen Fähigkeiten des Durchschnittsnutzers müssen aber Grenze der zu fordernden Sorgfaltspflichten markieren, da sich daran die Sicherheitserwartungen des Verkehrs ausrichten (allg. Rn. 277 ff.).[1034] Realisiert sich eine Gefahr, welche nur für einen technisch versierten Nutzer beherrschbar ist, trägt dieses Risiko die Bank. Dies rechtfertigt sich aber aus der Erwägung, dass sich die Banken mit ihrem Online-Banking-Angebot nicht nur an technisch versierte Nutzer, sondern gerade auch an die breite Masse der Kunden wenden.[1035]

534 Bei der Bestimmung der Sorgfaltspflichten wird man ausgehend, vom Maßstab des Durchschnittskunden anhand des konkreten Bedrohungsszenarios, sowie der Bekannt-

---

1031 Palandt-*Heinrichs*, § 280 BGB Rn. 28; MünchKommBGB-*Ernst*, § 280 BGB Rn. 104; Bamberger/Roth-*Grüneberg/Sutschet*, § 241 BGB Rn. 92.

1032 So etwa *Karper*, DuD 2006, 215 (217). Nach *Kind/Werner* sollen die Sorgfaltanforderungen an den Kunden wegen der Gefahren des Online-Banking zwar besonders hoch anzusetzen sein. Dennoch verneinen die Autoren sogar eine Pflicht zur Einrichtung von Virenschutzprogrammen, s. CR 2006, 353 (355).

1033 *Karper*, DuD 2006, 215 (217).

1034 Ebenso *Spindler*, in: Hadding/Hopt/Schimansky, S. 178 f.; *Erfurth*, WM 2006, 2198 (2201); *Recknagel*, Vertrag und Haftung beim Internet-Banking, S. 225.

1035 *Spindler*, in: Hadding/Hopt/Schimansky, S. 179; *Recknagel*, Vertrag und Haftung beim Internet-Banking, S. 225 f.; im Ergebnis ebenso *Erfurth*, WM 2006, 2198 (2201).

heit des betreffenden Problems und der (wirtschaftlichen und technischen) Zumutbarkeit möglicher Schutzmaßnahmen, zu unterscheiden haben. Soweit es zur Abwehr von Phishing-Versuchen darum geht, keine verdächtigen E-Mails zu beantworten, keine in E-Mails eingebetteten Link anzuklicken, keine unbekannten Anhänge zu öffnen usw., wird man ein entsprechendes Nutzerverhalten nach gehöriger Aufklärung durch die Bank als zumutbar ansehen können (unten Rn. 538). Problematischer ist es dagegen den Kunden zu bestimmten Einstellungen des Browsers oder der Firewall zu verpflichten (unten Rn. 535). In der Praxis wird sich eine Pflichtverletzung des Kunden nur durch eine **Gesamtwürdigung aller Umstände im Einzelfall** feststellen lassen.

(ii) Pflicht zur Sicherung des privaten Computers

535 Hinsichtlich der Sicherung des privaten Computers wird man auch beim Online-Banking-Kunden gegenüber den oben Rn. 280 ff. entwickelten allgemeinen Pflichten zum Einsatz von **Virenscannern** und **Systemupdates** kein „Mehr“ verlangen können. Der BGH hatte in seiner **Dialer-Entscheidung** eine Pflicht des privaten Nutzers zur Verwendung eines Dialerschutzprogrammen noch verneint,[1036] was indessen auf das Vorhalten eines allgemeinen Virenschutzes nicht übertragbar ist (s. oben Rn. 295 ff.). Zu weitgehend ist es aber aus den dargelegten Gründen (Rn. 531 ff.), dem Online-Banking-Kunden darüber hinaus unter Berufung auf die Sensibilität des Bankgeschäfts beispielsweise eine Pflicht zur Konfiguration einer Firewall oder zur Vornahme bestimmter Browsereinstellungen aufzuerlegen.[1037]

536 Die Sicherung des privaten Computers läuft als Präventionsmaßnahme indessen leer, wenn – wie häufig – **Online-Bankgeschäfte vom Arbeitsplatz** aus getätigt werden und hierzu (erlaubt oder unerlaubt[1038]) die Hard- und Software des Arbeitgebers verwendet wird. Nutzt der Kunde das Online-Banking am Arbeitsplatz, bedarf es keiner großen Anstrengungen für einen einigermaßen versierten Computerspezialisten, ein Programm auf dem Rechner im Hintergrund zu installieren, das die Vorgänge auf dem Computer aufzeichnet, insbesondere die eingegebenen Kennwörter oder Internet-Adressen. Dem Kunden kann hier allenfalls vorgeworfen werden, seine Kennwörter auf dem Arbeits-

1036 BGH MMR 2004, 308 (311); ausführlich *Spindler*, JZ 2004, 1128 ff.; vgl. auch LG Stralsund MMR 2006, 487 (489) mit zu Recht krit. Anm. *Ernst*, CR 2006, 590 ff.

1037 So aber *Karper*, DuD 2006, 215 (217)

1038 Die arbeitsrechtliche Zulässigkeit der privaten Nutzung des Internet am Arbeitsplatz ist heute meist im Arbeitsvertrag oder Betriebsvereinbarungen geregelt. Ausführlich zur arbeitsrechtlichen Problematik, *Hanau/Hoeren*, Private Internetnutzung durch Arbeitnehmer.

platzrechner zu gebrauchen, wenn er davon ausgehen musste, dass dieser auch Dritten zugänglich ist und keine besonderen Sicherheitsvorkehrungen bestanden. Aber auch hier ist eine Aufklärung über die Risiken erforderlich, da vielen Kunden nicht bewusst ist, welche technischen Möglichkeiten des Ausspähens am Computer bestehen.

(iii) Pflichten bei der Teilnahme am E-Mail-Verkehr

537 Bei der Durchführung von Online-Bankgeschäften kann vom privaten Bankkunden die Einhaltung gewisser grundlegender Verhaltensstandards verlangt werden. Hierzu gehört etwa PIN und TAN nicht auf dem Computer **abzuspeichern**[1039] und bei der Verwendung von HBCI die Chipkarte nach Abschluss der Transaktion aus dem Lesegerät zu entfernen, um ein Ausspähen durch Trojaner zu verhindern.[1040] Ebenso gelten die unter Rn. 311 f. beschriebenen Pflichten im **Umgang mit unbekannten E-Mail-Anhängen**.

538 Nach gehöriger Aufklärung durch die Bank wird man von Teilnehmern am Online-Banking auch erwarten können, dass er **Phishing-E-Mails** mit (vermeintlichem) Bankabsender nicht beantwortet (Szenario 1). Insbesondere darf der Kunde auf E-Mail-Anfrage keine PIN und TAN auf vermeintlichen Login-Seiten eingeben.[1041] Hierbei handelt es sich um einfache und jedem Internet-Nutzer heute ohne weiteres verständliche Vorsorgemaßnahmen, welche keine speziellen IT-Kenntnisse erfordern. Bei der Feststellung der Pflichten des Bankkunden wird man zudem berücksichtigen müssen, dass Phishing-E-Mails mit Bankabsender aufgrund der Aufklärungsarbeit der Banken und Medienberichten in der Masse der Spam-E-Mails eine gewisse Bekanntheit auch unter privaten Nutzern erlangt haben. Besondere Vorsicht ist zudem geboten, wenn bereits der äußere Anschein oder die sprachliche Aufmachung der E-Mail (z.B. gebrochenes Deutsch) Zweifel an der Urheberschaft der Bank begründen.[1042] Eine Pflichtverletzung wird aber zu verneinen sein, wenn die Bank selbst E-Mails zur Kommunikation mit dem Kunden nutzt und der Kunde davon ausgehen durfte, es handele sich um eine Nachricht seiner Bank.[1043] Viele Banken stellen mittlerweile in ihren Informationsmaterialien klar, dass sie den Kunden unter keinen Umständen per E-Mail kontaktieren oder gar zur Preisgabe von PIN und TAN auffordern werden.

1039 *Recknagel*, Vertrag und Haftung beim Internet-Banking, S. 221.
1040 Vgl. abrufbar unter: http://www.heise.de/newsticker/meldung/9349.
1041 *Karper*, DuD 2006, 215 (217); *Recknagel*, Vertrag und Haftung beim Internet-Banking, S. 222 f.
1042 So auch *Erfurth*, WM 2006, 2198 (2202).
1043 *Borges*, NJW 2005, 3313 (3314 f.); jedenfalls stünde ein Mitverschulden der Bank im Raum.

(iv) Pflichten bei der Durchführung von Online-Bankgeschäften

539 Ob der Durchschnittskunde zur **Überprüfung der Sicherheitsmerkmale der Online-Verbindung** (URL im Adress-Feld, Schloss-Symbol und Zertifikatsinformationen[1044]) verpflichtet ist,[1045] erscheint fraglich.[1046] Zum gegenwärtigen Zeitpunkt stellt das Wissen um diese – eigentlich einfach zu bewerkstelligenden – Schutzmaßnahmen noch kein Allgemeingut des durchschnittlichen Internet-Nutzers dar. Jedenfalls wird man deshalb eine intensive Informationsarbeit der Banken verlangen müssen, um eine entsprechende Kundenpflicht bejahen zu können. Keine Pflichtverletzung des Bankkunden wird man zudem annehmen können, wenn die Bank wechselnde URLs verwendet.[1047] Wie Szenario 1 (Rn. 473) zeigt, versagen diese Sicherheitsmaßnahmen bei der Verwendung von Visual Spoofing (eine andere Frage ist dann, ob bereits das Öffnen und Beantworten der Phishing-E-Mail eine Pflichtverletzung begründet, s. Rn. 537).[1048]

(v) Verhaltenspflichten im Missbrauchsfall

540 Der Kunde ist verpflichtet, bei Kenntnis oder Verdacht von Unregelmäßigkeiten seiner Bank Mitteilung zu machen und den Online-Zugang seines Kontos **sperren** zu lassen.[1049] Unterlässt der Kunde eine ihm mögliche Mittelung und hätte die Bank die Transaktion bei unverzüglicher Meldung noch verhindern oder rückgängig machen können, haftet der Kunde gegenüber der Bank.

541 Zur Vermeidung einer Vergrößerung des Schadens ist der Kunde nach einem erkannten Missbrauch gehalten, seine **PIN zu ändern**.[1050] Eine weitergehende, verdachtsunabhängige Pflicht zur Änderung der PIN in regelmäßigen Abständen ist dagegen abzulehnen, da der Durchschnittskunde infolge der wachsenden Zahl von im Alltag verwendeten Identifikationsnummern und Passwörtern schnell überfordert wäre.[1051]

1044 Das Sicherheitszertifikat kann durch Doppelklick auf das Schlosssymbol eingesehen werden.

1045 So *Karper*, DuD 2006, 215 (216).

1046 So auch *Kind/Werner*, CR 2006, 353 (356); *Erfurth*, WM 2006, 2198 (2202).

1047 *Erfurth*, WM 2006, 2198 (2202).

1048 Ausführlich zu den Manipulationsmöglichkeiten *Erfurth*, WM 2006, 2198 (2202 f.).

1049 *Borges*, NJW 2005, 3313 (3314); *Werner*, MMR 1998, 338 (339); *Werner*, in: Hellner/Steuer, Band 6, 19/68; *Recknagel*, Vertrag und Haftung beim Internet-Banking, S. 223.

1050 *Werner*, in: Hellner/Steuer, Band 6, 19/68; *Recknagel*, Vertrag und Haftung beim Internet-Banking, S. 224.

1051 *Spindler*, in: Hadding/Hopt/Schimansky, S. 218; *Werner*, in: Hellner/Steuer, Band 6, 19/70; *Recknagel*,

(iii) Zusammenfassende Bewertung der Bedrohungsszenarien

(a) Szenario 1

542 Der Kunde hat (wenn man so weitgehende Sorgfaltspflichten überhaupt bejahen kann, s. Rn. 539) durch Überprüfung der Online-Verbindung sorgfaltsgemäß gehandelt. Die URL im Adress-Feld, das Schloss-Symbol und die Zertifikatsinformationen waren durch Visual Spoofing für den Kunden nachgebildet und als Täuschung nicht erkennbar. Die Verwendung von Aktiven Inhalten stellt eine Pflichtverletzung auf Seiten der Bank dar (Rn. 515). Da der Bankkunde schon zur Nutzung des regulären Online-Banking-Angebots Aktive Inhalte in seinem Browser freischalten musste, kann darin seinerseits keine Pflichtverletzung gesehen werden.

543 Davon zu trennen ist die Frage der Pflichtverletzung durch die bloße Antwort auf eine Phishing-E-Mail. Bei entsprechender Aufklärung des Kunden durch die Bank wird man hier eine Pflichtverletzung seitens des Kunden bejahen können, wenn keine besonderen Umstände vorliegen, auf Grund derer er auf eine E-Mail seiner Bank vertrauen durfte. Eine Pflichtverletzung scheidet regelmäßig aus, wenn die Bank selbst zum Kunden per E-Mail in Kontakt getreten ist.

(b) Szenario 2

544 Der Angriff mittels DNS-Spoofing richtet sich gegen den Server des Providers, nicht gegen den PC des Bankkunden. Der Kunde handelt unter keinem Gesichtspunkt sorgfaltswidrig, da der Angriff für ihn nicht erkennbar, noch verhinderbar ist.[1052] Das Risiko für den Kunden besteht hier darin, ob es ihm überhaupt gelingt den von der hM bejahten Anscheinsbeweis für seine Urheberschaft zu erschüttern (unten Rn. 579 ff.).

(c) Szenario 3

545 Beim Pharming i.e.S. kommt eine Pflichtverletzung des Bankkunden zunächst unter dem Gesichtspunkt des Öffnens des E-Mail-Anhangs in Betracht. Hierbei wird man darauf abstellen müssen, ob die E-Mail von einem bekannten und vertrauenswürdigen Absender stammte. Das Öffnen von Spam-E-Mails als solches begründet grundsätzlich zwar noch keine Pflichtverletzung, jedoch hat auch der private Nutzer beim Umgang mit Anhängen unbekannter Herkunft besondere Sorgfalt walten zu lassen. Kann dem

---

Vertrag und Haftung beim Internet-Banking, S. 224.

1052 So auch *Kind/Werner*, CR 2006, 353 (356); *Erfurth*, WM 2006, 2198 (2202); *Borges*, NJW 2005, 3313 (3315).

Kunden nicht vorgeworfen werden kann, er habe fahrlässig einen unbekannten E-Mail-Anhang geöffnet, kommt eine Pflichtverletzung wegen mangelnder Sicherung des eigenen PC mit Anti-Virus-Software und Systemupdates in Betracht. Die Sorgfaltsanforderungen an den privaten Nutzer und Bankkunden sind dabei in oben dargelegtem Umfang beschränkt.

(iv) Vertretenmüssen des Kunden, § 280 Abs. 1 Satz 2 BGB

546 Die von den Banken für das Online-Banking entwickelten AGB enthalten keine spezielle Haftungsregelung. Anders als nach den ec-Bedingungen[1053] haftet der Kunde somit nicht nur für grobe, sondern bereits für **einfache Fahrlässigkeit** (§ 276 Abs. 1, 2 BGB),[1054] wobei vermutetet wird, dass der Kunde ein pflichtwidriges Verhalten auch zu vertreten hat (§ 280 Abs. 1 Satz 2 BGB). Für die Reichweite der Haftung des Bankkunden kommt es daher ganz entscheidend darauf an, wie eng oder weit die Pflichten des Kunden gefasst werden.

(v) Schaden der Bank

547 Überweist die Bank einen Geldbetrag an einen Angreifer, welcher sich Zugang zum Legitimationsmedium des Kunden verschafft hat, so besteht ein Schaden der Bank grundsätzlich in Höhe des Überweisungsbetrages. Während bei einer Bargeldabhebung am Geldautomaten mittels EC-Kartenmissbrauchs der Täter im Regelfall nicht mehr ermittelt werden kann und der Abhebungsbetrag somit (vorbehaltlich eines etwaigen Mitverschuldens der Bank) meist identisch mit dem Schaden der Bank ist, liegt die Situation bei einer Online-Überweisung insoweit anders, als eine Rückverfolgung der Überweisung technisch möglich ist.[1055] Geht man davon aus, dass die Überweisung dem Kunden nicht zurechenbar ist und mithin keine wirksame Anweisung des Kunden gegenüber der Bank vorliegt,[1056] steht der Bank ein Anspruch aus § 812 Abs. 1 Satz 1 Fall 2 BGB (Direktkondiktion) gegen den Zahlungsempfänger[1057] und unter Umständen

---

1053 Vgl. III Nr. 1.4 der ec-Bedingungen der Privatbanken, abgedruckt bei *Werner*, in: Heller/Steuer, Band 3, 6/1763a.

1054 *Kind/Werner*, CR 2006, 353 (354).

1055 *Langenbucher*, Die Risikozuordnung im bargeldlosen Zahlungsverkehr, S. 148.

1056 Dazu *Langenbucher*, Die Risikozuordnung im bargeldlosen Zahlungsverkehr, S. 175. Liegt dagegen – etwa wegen Bejahung einer Rechtsscheinshaftung – eine wirksame Anweisung des Kunden vor, sind auch die Voraussetzungen für einen Aufwendungsersatzanspruch der Bank nach §§ 670, 675, 676a BGB erfüllt. Der Kunde kann in diesem Fall nur Bereicherungs- und Schadensersatzansprüche gegen den Täter geltend machen.

1057 OLG Hamburg WM 2006, 2078; *Langenbucher*, Die Risikozuordnung im bargeldlosen Zahlungsverkehr, S. 176; *Oechsler*, in: Derleder/Knops/Bamberger, Handbuch zum deutschen und europäischen Bank-

Schadensersatzansprüche gegen den Täter zu. Ein liquidationsfähiger Schaden entsteht demnach erst, wenn die Durchsetzung dieser Ansprüche scheitert oder von vornherein aussichtslos ist, weil der Täter beispielsweise vom Ausland aus gehandelt hat und nicht greifbar ist.[1058] Der Schaden wird in diesen Fällen dem Überweisungsbetrag entsprechen. Im Einzelfall wird eine Kürzung des Anspruchs wegen Mitverschuldens der Bank (§ 254 BGB) in Betracht kommen.

(vi) Mitverschulden der Bank, § 254 BGB

548 Im Schadensersatzprozess der Bank gegen den Kunden, könnte sich der Kunde auf ein **Mitverschulden** (§ 254 BGB) der Bank berufen, wenn die mangelnde Sicherheit des Online-Bankings *mitursächlich* für den Missbrauch wurde.[1059] Eine Obliegenheitsverletzung der Bank wird beispielsweise vorliegen, wenn sie dem Kunden das Erkennen manipulierter Websites durch häufig wechselnde Designs der Login-Seite oder unklare oder nicht nachvollziehbare URLs erschwert. Ebenso kann ein Mitverschulden der Bank in Betracht kommen, wenn das SSL-Zertifikat nicht auf den Namen der Bank ausgestellt ist und dem Kunden hierdurch die Überprüfung der Authentizität der Website erschwert wird. Die Beweislast für ein Mitverschulden der Bank liegt nach allgemeinen Grundsätzen beim Kunden.[1060]

(d) Verschuldensunabhängige Haftung des Kunden aufgrund AGB?

549 Da Internet-Banking trotz aller Sicherungsvorkehrungen Risiken aufweist, wäre es aus wirtschaftlicher Sicht verständlich, dass in Allgemeinen Geschäftsbedingungen das Risiko von trotzdem auftretenden Missbrauchsfällen dem Kunden zugewiesen wird. In den **Btx-Bedingungen** war in Ziffer 9 eine verschuldensunabhängige Haftung des Kunden für Schäden vorgesehen, welche durch sorgfaltswidrigen Umgang mit PIN und TAN entstehen[1061]; eine vergleichbare Regelung enthielten bis 1989 die **ec-Bedingungen**.[1062] Nach dem **Sphärengedanken**[1063] sollte das Missbrauchsrisiko bei

---

recht, § 37 Rn. 40; *Schimansky*, in: Bankrechts-Handbuch, Band I, § 50 Rn. 3 f.

1058 *Langenbucher*, Die Risikozuordnung im bargeldlosen Zahlungsverkehr, S. 148; wohl auch *Bock*, in: Bräutigam/Leupold, Kap. VII Rn. 81.

1059 *Karper*, DuD 2006, 215 (219); *Borges*, NJW 2005, 3313 (3315); *Bock*, in: Bräutigam/Leupold, Kap. VII Rn. 81.

1060 *Kind/Werner*, CR 2006, 353 (360); BGH NJW 1994, 3102 (3105); Bamberger/Roth-*Unberath*, § 254 BGB Rn. 68 mwN.

1061 Dazu *Canaris*, Bankvertragsrecht, Rn. 527 ff, 527 hh.

1062 Zur Unwirksamkeit dieser Klausel nach § 9 Abs. 2 Nr. 1 AGBG (jetzt § 307 Abs. 2 Nr. 1 BGB) s. BGHZ 135, 116 (121 ff.); ausführlich *Neumann/Bock*, Zahlungsverkehr im Internet, Rn. 171 ff.

1063 *Canaris*, Bankvertragsrecht, Rn. 527 ff; *Borsum/Hofmeister*, NJW 1985, 1205 ff.; *Werner*, in: Hell-

der Verwendung von PIN und TAN von demjenigen getragen werden, in dessen Verantwortungsbereich der sichere Umgang mit diesem Legitimationsmedium gehörte. Die Zulässigkeit solcher verschuldensunabhängig formulierter Klauseln ist umstritten,[1064] die Frage war jedoch nicht Gegenstand einer gerichtlichen Entscheidung. Für das Online-Banking wäre eine Übertragbarkeit des Sphärengedankens denkbar, da auch hier der Kunde nach Überlassung der Legitimationsmedien das Risiko eines Missbrauchs letztlich besser beherrschen kann. Dagegen spricht aber bereits, dass es sich beim Btx um ein geschlossenes System handelte und Bedrohungen wie Phishing und Pharming zur damaligen Zeit noch unbekannt waren; die Missbrauchsursachen beim Btx waren stets am Anschluss des Kunden zu suchen.[1065]

550 Für den Bereich des Online-Banking ist mit der heute wohl herrschenden Meinung die Anordnung einer verschuldensunabhängigen Haftung in AGB als gemäß § 307 BGB unwirksam anzusehen.[1066] Nach § 307 Abs. 2 Nr.1 BGB besteht eine gesetzliche Vermutung („im Zweifel“) der Unwirksamkeit einer Klausel bei Abweichung vom **Leitbild des dispositiven Gesetzesrechts** in AGB, die nur dann widerlegt ist, wenn eine Gesamtwürdigung aller Umstände unter Abwägung der beiderseitigen Interessen ergibt, dass die Klausel den Kunden nicht unangemessen benachteiligt.[1067] Maßgeblich ist hierbei zu berücksichtigen, dass das in § 280 Abs. 1 BGB zum Ausdruck kommende **Verschuldensprinzip** nicht nur auf Zweckmäßigkeitserwägungen beruht, sondern eine Ausprägung des Gerechtigkeitsgebots darstellt.[1068] Eine Abweichung vom Verschuldensprinzip kann nur dann wirksam vereinbart werden, wenn sie durch höhere Interessen des Verwenders der AGB gerechtfertigt oder durch Gewährung rechtlicher Vorteile ausgeglichen wird.[1069] Ein besonderes Interesse der Bank an der alleinigen Risikotragung durch den Kunden besteht beim Online-Banking indessen nicht, da die Bank durch

---

ner/Steuer, Band 6, Rn. 19/82; *Recknagel*, Vertrag und Haftung beim Internet-Banking, S. 141 f.

1064 Für zulässig hielten wegen unübersehbarer Schadensrisiken solche Klauseln: *Hellner*, FS Werner, S. 251, 273 ff.; *Reiser*/*Werner*, WM 1995, 1901 (1907); letztlich auch *Blaurock*, CR 1989, 561 (566), da der Kunde jederzeit die PIN-Nummern ändern könne; dagegen bereits *Borsum*/*Hoffmeister*, BB 1983, 1441 (1443); *Canaris*, Bankvertragsrecht, Rn. 527 ff.

1065 *Recknagel*, Vertrag und Haftung beim Internet-Banking, S. 142.

1066 *Kind/Werner*, CR 2006, 353 (354); *Erfurth*, WM 2006, 2198 (2200); *Wiesgickl*, WM 2000, 1039 (1050); *Bock*, in: Bräutigam/Leupold, Kap. VII Rn. 85; *Neumann/Bock*, Zahlungsverkehr im Internet, Rn. 176; *Spindler*, in: Hadding/Hopt/Schimansky, S. 216 f.; *Hartmann*, in: Hadding/Hopt/Schimansky, S. 319; *Recknagel*, Vertrag und Haftung beim Internet-Banking, S. 141 f.; *Werner*, in: Hellner/Steuer, Band 6, 19/82.

1067 BGH NJW 2003, 1447 (1448); Palandt-*Heinrichs*, § 307 BGB Rn. 25.

1068 BGHZ 135, 116 (121); BGHZ 114, 238 (242 f.).

1069 BGHZ 135, 116 (121); BGHZ 114, 238 (242 f.).

Eröffnung des Online-Banking-Verkehrs das Risiko geschaffen hat[1070] und sie die Sicherheit des Online-Banking entscheidend durch die Auswahl der technischen Systeme mitbestimmt.[1071] Eine alleinige Risikozuweisung an den Kunden ist auch deshalb abzulehnen, weil Möglichkeiten des Kunden zur Gefahrbeherrschung maßgeblich durch die Instruktion und Aufklärung seitens der Bank mitbestimmt werden. Da die Risikoabwälzung auch nicht durch Vorteile des Kunden ausgeglichen wird, ist eine Klausel, welche ohne Rücksicht auf schuldhafte Pflichtverletzungen das Missbrauchsrisiko dem Kunden zuweist, als nach Treu und Glauben unangemessene Benachteiligung zu werten (§ 307 Abs. 1, 2 Nr. 1 BGB).[1072]

(e) Zwischenergebnis

551 In materiell-rechtlicher Hinsicht kommen in den Fällen des Missbrauchs der Legitimationsmedien beim Online-Banking Ansprüche der Bank gegen den Kunden aus § 670 BGB bzw. §§ 280 Abs. 1, 241 Abs. 2 BGB in Betracht. Eine verschuldensunabhängige Haftung zu Lasten des Kunden kann in AGB nicht wirksam vereinbart werden. Sofern die Bank keinen Vertragsschluss beweisen kann (zum Anscheinsbeweis s. unten), kann sie ihre Forderung allein auf eine Sorgfaltspflichtverletzung des Kunden im Umgang mit den Legitimationsmedien stützen. Entscheidend ist hierbei die Pflichtenabgrenzung zwischen Bank und Kunde, wobei sich eine enge Wechselbeziehung zwischen den Pflichten der Bank (insbesondere Informations- und Warnpflichten) und den Pflichten des Kunden zeigt. Den Bankkunden treffen beim Online-Banking keine gegenüber dem normalen Internetverkehr erhöhten Sorgfaltsanforderungen. Die Sicherheitserwartungen des Verkehrs orientieren sich insbesondere im IT-spezifischen Bereich an den technischen Fähigkeiten des Durchschnittsnutzers. Sofern im Einzelfall ein Schadensersatzanspruch gegen den Kunden bejaht werden kann, kommt eine Kürzung wegen Mitverschuldens der Bank etwa wegen unzureichender Aufklärung in Betracht.

1070 *Recknagel*, Vertrag und Haftung beim Internet-Banking, S. 142.

1071 *Werner*, MMR 1998, 338 (340); *Wiesgickl*, WM 2000, 1039 (1050); *Janisch/Schartner*, DuD 2002, 162 (167); *Recknagel*, Vertrag und Haftung beim Internet-Banking, S. 142. Zu verschuldensunabhängigen Abwälzung des Fälschungsrisikos auf den Kunden in den ec-Bedingungen 1989 s. BGHZ 135, 116 (122) und ausführlich *Neumann/Bock*, Zahlungsverkehr im Internet, Rn. 171 ff.; zur Kundenkreditkarte BGHZ 114, 238 (245).

1072 *Kind/Werner*, CR 2006, 353 (354).

(4) Prozessuale Rechtslage, insbesondere Anscheinsbeweis

552 Nach allgemeinen Beweislastgrundsätzen trägt die **Bank die Darlegungs- und Beweislast** dafür, dass zwischen ihr und dem Kunden ein Überweisungsvertrag zustande gekommen ist oder – wenn ein Missbrauchsfall vorliegt – dass der Kunde die ihm obliegende Sorgfalt verletzt hat (die Beweislastumkehr des § 280 Abs. 1 Satz 2 BGB gilt nur hinsichtlich des Vertretenmüssens).[1073] Bestreitet der Kunde Urheber des elektronischen Überweisungsauftrages zu sein, wird die Bank im Regelfall nicht beweisen können, dass gerade der Kunde oder ein von ihm bevollmächtigter Dritter die für die Überweisung erforderlichen Eingaben getätigt und das Legitimationsmedium verwandt hat.[1074] Angesichts der Beweisnot der Bank kommen **Beweiserleichterungen** in Form entweder einer Umkehr der Beweislast ((a)) oder eines Anscheinsbeweises ((b)) zu Lasten des Kunden in Betracht.

(a) Umkehr der Beweislast

553 Eine Beweislastumkehr zugunsten der Bank, so dass der Kunde nachweisen müsste, dass er nicht die elektronische Willenserklärung abgegeben hat, findet keine Grundlage im Gesetz[1075] und wäre auch nicht sachgerecht, da sie dem Kunden den Vollbeweis aufbürden würde. Der Kunde ist selbst unter Zugrundelegung von Gedanken aus der **Gefahrenkreis- bzw. Sphärentheorie**[1076] nicht in der Lage, Risiken zu beherrschen, die nicht aus seinem Bereich stammen; gerade durch diese nicht auszuschließende Möglichkeit charakterisiert sich jedoch das Internet-Banking, da Kommunikationskanäle, die weder vom Kreditinstitut noch vom Kunden beherrschbar sind, benutzt werden.[1077]

1073 *Borges*, NJW 2005, 3313 (3316); *Erfurth*, WM 2006, 2198 (2203); *Karper*, DuD 2006, 215 (218); *Wiesgickl*, WM 2000, 1039 (1047); *Werner*, in: Schwarz/Peschel-Mehner, Recht des Internet, Teil 2, Kap. 2 A Rn. 2 f.

1074 *Kind/Werner*, CR 2006, 353 (359); *Karger*, DuD 2006, 215 (218); *Langenbucher*, Die Risikoverteilung im bargeldlosen Zahlungsverkehr, S. 147.

1075 Zur Beweislastumkehr als Rechtsfortbildung Musielak-*Foerste*, § 286 ZPO Rn. 37; MünchKommZPO-*Prütting*, § 286 ZPO Rn. 117, 119, 121; *Stodolkowitz*, VersR 1994, 11 (13 f.); für strenge Voraussetzungen *Prütting*, RdA 1999, 107 (110 f.); Zöller-*Greger*, Vor § 284 ZPO Rn. 17 f.

1076 Grundlegend *Prölss*, Beweiserleichterungen im Schadensersatzprozeß, S. 65 ff.; krit. *Musielak*, AcP 176 (1976), 465 (470 ff.).

1077 *Recknagel*, Vertrag und Haftung beim Internet-Banking, S. 145. Ebenso verneint die Rechtsprechung eine Beweislastumkehr bei Internet-Auktionen OLG Naumburg NOZ 2005, 2222 (2224); OLG Köln MMR 2002, 813; LG Bonn MMR 2004, 179 (180); LG Bonn MMR 2002, 255 (256); LG Konstanz MMR 2002, 835 (836).

554 Die oben beschriebene Bedrohungslage (Rn. 473 ff.) beim Online-Banking unterscheidet sich auch wesentlich von den **Btx-Fällen**,[1078] in denen Instanzgerichte wohl eine Beweislastumkehr zu Lasten des Anschlussinhaber bejaht haben.[1079] Dort war nur fraglich, ob der Anschlussinhaber selbst oder ein Familienangehöriger bzw. Dritter den häuslichen Btx-Anschluss benutzt hatte. Die missbräuchliche Nutzung hatte daher jedenfalls im Einflussbereich des Anschlussinhabers stattgefunden, was eine Beweislastverteilung nach Risikosphären nahe liegend erscheinen ließ. Überdies handelte es sich bei Btx um ein geschlossenes System.[1080] Auf die technischen Möglichkeiten des Phishing oder Pharming lässt sich dieser Gedanke nicht übertragen, da hierbei Angriffe aus dem Internet als einem offenen Netz erfolgen, welches der Kontrolle des Bankkunden entzogen ist.

555 Die Ablehnung einer Beweislastumkehr rechtfertigt sich auch im Hinblick auf **technische Weiterentwicklungen** oder Durchbrechungen des technischen Schutzes: Bei Annahme einer Beweislastumkehr würde dem vermeintlich Erklärenden stets der Vollbeweis aufgebürdet, dass die Erklärung nicht von ihm stammt. Der jeweilige technische Standard und sein Schutzniveau könnten nicht angemessen berücksichtigt werden.[1081] In vergleichbarer Weise und aus guten Gründen wendet die ständige Rechtsprechung bei technischen Regeln (z.B. DIN) stets nur einen Anscheinsbeweis bei Verletzung technischer Standards an.[1082] Eine Beweislastumkehr wäre der besonderen Situation beim Online-Banking nicht angemessen.[1083]

(b) Beweis des ersten Anscheins

(i) Voraussetzungen des Anscheinsbeweises

556 Die überwiegende Ansicht in der Literatur belässt es bei der Beweislast der Bank, spricht sich in Anlehnung an die Rechtsprechung und hM zur ec-Karte (dazu Rn. 562) jedoch für einen alternativen **Anscheinsbeweis**[1084] zugunsten der Bank aus.[1085] Der

---

1078 OLG Oldenburg NJW 1993, 1400 ff.; OLG Köln VersR 1993, 840 ff.; OLG Köln VersR 1998, 725 ff.

1079 Das OLG Oldenburg spricht bspw. von einer „tatsächlichen Vermutung“, was trotz Bezugnahme auf den Sphärengedanken auf einen bloßen Anscheinsbeweis hindeutet, s. OLG Oldenburg NJW 1993, 1400 (1401).

1080 *Trapp*, WM 2001, 1192 (1195).

1081 Ähnl. *Sieber/Nöding*, ZUM 2001, 199 (208 f.): Flexibilität für künftige technische Entwicklungen erforderlich.

1082 S. etwa BGH NJW 1991, 2021; Bamberger/Roth-*Spindler*, § 823 BGB Rn. 22 ff.

1083 Dies verkennt *Trapp*, WM 2001, 1192 (1200 f.), der hier eine gesetzliche Spezialregelung des Beweismaßes annehmen will; ähnl. wie hier aber *Melullis*, MDR 1994, 109 (111); *Recknagel*, Vertrag und Haftung beim Internet-Banking, S. 144 f.; s. auch *Roßnagel*, MMR 2000, 451 (459).

1084 So *Langenbucher*, Die Risikozuordnung im bargeldlosen Zahlungsverkehr, S. 146.

Beweis des ersten Anscheins spricht nach Ansicht des Schrifttums demnach für die Tatsache, dass

- derjenige, der das Legitimationszeichen verwandt hat, entweder der Kunde selbst ist oder zumindest von diesem autorisiert wurde, die Willenserklärung abzugeben,
- hilfsweise für die Tatsache, dass der Kunde den Missbrauch der Legitimationszeichen schuldhaft ermöglicht hat.

557 Gerichtliche Entscheidungen zur Beweislast beim Online-Banking stehen soweit ersichtlich noch aus.[1086]

558 Für das PIN-/TAN-Verfahren und das HBCI-Verfahren ist anders als in **§ 371a Abs. 1 Satz 2 ZPO/§ 292a ZPO aF** für die qualifizierte elektronische Signatur nach dem Signaturgesetz (SigG) kein Anscheinsbeweis für die Echtheit der Erklärung im Gesetz angeordnet. Dies schließt indessen nicht aus, aufgrund der allgemeinen Grundsätze des Beweisrechts einen Anscheinsbeweis auch für diese Sicherungsverfahren zu bejahen.[1087] Für Sicherungsverfahren auf Basis einer elektronischen Signatur wie beispielsweise HBCI liegt eine Parallele zu der gesetzlichen Regelung in § 371a Abs. 1 Satz 2 ZPO/§ 292a ZPO nahe.[1088]

559 Grundlage des Anscheinsbeweises ist, dass sich unter Berücksichtigung aller unstreitigen und festgestellten Einzelumstände und besonderen Merkmale des Sachverhalts ein für die zu beweisende Tatsache nach der Lebenserfahrung **typischer Geschehensablauf** ergibt.[1089] Ein typischer Geschehensablauf setzt voraus, dass ein bestimmter Sachverhalt feststeht, der nach der allgemeinen Lebenserfahrung auf eine bestimmte Ursache oder auf einen bestimmten Ablauf als maßgeblich für den Eintritt eines bestimmten Erfolgs

---

1085 *Borges*, NJW 2005, 3313 (3316); *Karper*, DuD 2006, 215 (218 f.); *Kunst*, MMR Beilage 9/2001, 23 (25); *Recknagel*, Vertrag und Haftung beim Internet-Banking, S. 149 ff.; *Werner*, MMR 1998, 232 (235); *Bock*, in: Bräutigam/Leupold, Kap. VII Rn. 83; *Neumann/Bock*, Zahlungsverkehr im Internet, Rn. 180; *Kümpel*, Bank- und Kapitalmarktrecht, 4.752; *Werner*, in: Hellner/Steuer, Band 6, 19/84; *Werner*, in: Schwarz/Peschel/Mehner, Recht des Internet, Teil 2, Kap. 2 A Rn. 24 f.; *Borges*, in: Derleder/Knops/Bamberger, Handbuch zum deutschen und europäischen Bankrecht, § 8 Rn. 79; einschränkend *Wiesgickl*, WM 2000, 1039 (1050).

1086 Das LG Bonn begründet seine Ablehnung des Anscheinsbeweises bei Internet-Auktionen jedoch ausdrücklich auch mit dem Unterschied zwischen dem bloßen Passwortschutz und der Verwendung von PIN und TAN, s. MMR 2004, 179 (181).

1087 Gegen einen Umkehrschluss zu § 292a ZPO (jetzt § 371a Abs. 1 Satz 2 ZPO nF) im Zusammenhang mit Internet-Auktionen auch *Mankowski*, CR 2003, 44 (47); *Ernst*, Vertragsgestaltung im Internet, Rn. 28.

1088 *Stockhausen*, WM 2001, 605 (618); *Wiesgickl*, WM 2000, 1039 (1050); *Bock*, in: Bräutigam/Leupold, Kap. VII Rn. 84; *Recknagel*, Vertrag und Haftung beim Internet-Banking, S. 150.

1089 BGH NJW 2004, 3623 - ec-Karte; BGH NJW 2001, 1140 (1141); BGH NJW 1987, 2876; Musielak-*Foerste*, § 286 ZPO Rn. 23.

hinweist.[1090] Die aus dem Sachverhalt zu ziehende Schlussfolgerung muss sich dem Betrachter gleichsam aufdrängen, so dass individuelle Kennzeichen des Einzelfalles zurücktreten und bedeutungslos erscheinen.[1091] Es handelt sich hierbei um keine Umkehr der Beweislast, sondern die Berücksichtigung von Erfahrungssätzen[1092] durch den Richter im Rahmen der freien Beweiswürdigung (§ 286 Abs. 1 ZPO),[1093] wobei die dem Erfahrungssatz zugrunde liegenden Tatsachen entweder unstreitig sein müssen oder ihrerseits des Vollbeweises bedürfen.[1094]

560 Die Typizität des Geschehensablaufs erfordert nicht, dass die Ursächlichkeit einer bestimmten Tatsache für einen bestimmten Erfolg bei allen Sachverhalten dieser Fallgruppe notwendig immer vorhanden ist. Die Ursächlichkeit einer bestimmten Tatsache für einen bestimmten Erfolg muss aber so häufig gegeben sein, dass die **Wahrscheinlichkeit**, einen solchen Fall vor sich zu haben, **sehr groß** ist.[1095] Die bloß abstrakte Möglichkeit eines anderen Geschehensablaufs steht der Annahme eines Erfahrungssatzes nicht entgegen.[1096]

561 Bei der Prüfung des Anscheinsbeweises sind zwei Fragen strikt zu trennen[1097]: Als Vermutungsgrundlage ist zunächst zu prüfen, ob beim Online-Banking überhaupt ein Erfahrungssatz bejaht werden kann. Wird ein Erfahrungssatz bejaht, stellt sich weiter die Frage, ob die **Vermutungsfolge** im Einzelfall dadurch erschüttert werden kann, dass die ernsthafte Möglichkeit eines Phishing- oder Pharming-Angriffs und damit ein atypischer Geschehensablauf dargelegt wird.

(ii) Rechtslage bei ec-Karten und Internet-Auktionen

(a) ec-Karten

562 Für den Einsatz von **ec-Karten** bejaht die obergerichtliche Rechtsprechung seit langem einen Anscheinsbeweis dafür, dass bei Einsatz der PIN tatsächlich auch der Verfügungsberechtigte die ec-Karte benützt oder jedenfalls grob fahrlässig den Missbrauch

---

1090 BGH NJW 2004, 3623 - ec-Karte; BGH NJW 2001, 1140 (1141); BGH WM 1997, 1493 (1496); BGHZ 100, 31 (33).

1091 S. BGHZ 100, 241 (216).

1092 Ausführlich MünchKommZPO-*Prütting*, § 286 ZPO Rn. 55 ff.; Stein/Jonas-*Leipold*, § 286 ZPO Rn. 90.

1093 MünchKommZPO-*Prütting*, § 286 ZPO Rn. 47; Zöller-*Greger*, Vor § 284 ZPO Rn. 29.

1094 Zöller-*Greger*, Vor § 284 ZPO Rn. 29.

1095 BGH NJW 2004, 3623 - ec-Karte; BGH VersR 1991, 460 (462); Zöller-*Greger*, Vor § 284 ZPO Rn. 29.

1096 BGH NJW 2004, 3623 (3624); Stein/Jonas-*Leipold*, § 286 ZPO Rn. 90.

1097 S. auch *Karger*, DuD 2006, 215 (219).

ermöglicht hat.[1098] Die hM nimmt hierbei an, dass die bei den Banken verwendeten Sicherheitssysteme für ec-Karten und Geldautomaten Manipulationen durch Dritte mit sehr hoher Wahrscheinlichkeit ausschließen oder zumindest nachträglich erkennbar machen.[1099] Im Einzelfall dürfte zwar nach wie vor Streit über die Verschlüsselungsgüte des Systems bestehen.[1100] Auch lässt die Rechtsprechung zunehmend die Möglichkeiten des Ausspähens oder Abfangens der PIN als Erschütterung des Anscheinsbeweises genügen.[1101] Sie fragt dann aber häufig nach Einhaltung der gebotenen Sorgfalt zur Abschirmung der PIN-Eingabe,[1102] denn es liegt weitgehend im Macht- und Einflussbereich des Kunden, ob Dritte Kenntnis von der PIN erhalten, etwa indem er bei der Eingabe der PIN diese verdeckt hält etc.[1103] Da beim Online-Banking ebenfalls mit PIN gearbeitet wird, liegt eine Übertragung dieser Grundsätze nahe. Der BGH hatte die Frage des Anscheinsbeweises beim ec-Kartenmissbrauch bislang offen gelassen.[1104] In der Entscheidung vom 5. Oktober 2004 hat das Gericht nunmehr die bisherige Rechtsprechungslinie der Instanzgerichte bestätigt.[1105]

(b) Internet-Auktionen

563 Ganz anders ist die Rechtslage im Bereich der Internet-Auktionen. Die Vergabe von Passwörtern begründet nach der Rechtsprechung der Instanzgerichte und dem wohl überwiegenden Teil der Literatur **keine Vermutung** für die Verwendung durch den Inhaber.[1106] Anders als bei ec-Karten und dem Online-Banking trägt somit bei Internet-Auktionen der Erklärungsempfänger die volle Beweislast für den Vertragsschluss. Die

---

1098 St. Rspr. der meisten Instanzgerichte: s. etwa KG NJW 1992, 1051 (1052); LG Bonn NJW-RR 1995, 815; LG Darmstadt WM 2000, 911 (913 f.); LG Frankfurt WM 1999, 1930 (1932 f.); LG Hannover WM 1998, 1123 f.; LG Köln WM 1995, 976, (977 f.); AG Frankfurt NJW 1998, 687 f.; AG Osnabrück NJW 1998, 688 f.; aA OLG Hamm NJW 1997, 1711 (1712 f.): wegen mangelnder Schlüsselsicherheit; LG Berlin WM 1999, 1920 f.: wegen Möglichkeit des Ausspähens.

1099 *Neumann/Bock*, Zahlungsverkehr im Internet, Rn. 181; *Werner*, MMR 1998, 338 (339) mwN. aus der Rechtsprechung der Instanzgerichte.

1100 Charakteristisch das Urteil des OLG Hamm NJW 1997, 1711 (1712 f.); dieses Urteil ist jedoch ein Einzelfall geblieben. Außerdem haben die Banken die Verschlüsselungstiefe der EC-Karten verbessert, so dass diese Rechtsprechung jedenfalls von ihrem Ausgangspunkt her nicht mehr anwendbar sein dürfte.

1101 So etwa AG München NJW-RR 2001, 1056 (1057).

1102 S. LG Halle WM 2001, 1298 (1299).

1103 Allerdings mag man darüber streiten, welches Ausmaß an Sorgfalt angesichts der Realität im Einsatz von PIN-Eingabegeräten dem Kunden abverlangt werden kann. Oftmals sind diese Geräte für jedermann einsehbar, so dass die Geheimhaltung durch verdeckte Eingabe an den Kunden in zahlreichen Situationen überspannte Anforderungen stellen würde.

1104 BGHZ 145, 337 (342).

1105 BGH NJW 2004, 3623 (3624).

1106 OLG Köln MMR 2002, 813 (814); LG Bonn MMR 2004, 179 (180); LG Bonn MMR 2002, 255 (256); LG Konstanz MMR 2002, 835 (837); ebenso *Borges*, NJW 2005, 3313 (3317); *Borges*, in: Derleder/Knops/Bamberger, Handbuch zum deutschen und europäischen Bankrecht, § 8 Rn. 80; *Mehrings*, in: Hoeren/Sieber, Kap. 13.1 Rn. 270 ff.; *Wiebe*, in: Spindler/Wiebe, Internet-Auktionen und Elektronische Marktplätze, Kap. 4 Rn. 61.

Durchsetzung vertraglicher Ansprüche wird mithin regelmäßig ausscheiden, wenn der registrierte Nutzer behauptet, er habe die Erklärung nicht abgegeben, was in der Literatur als „Widerrufsrecht kraft Beweislast“ kritisiert wird.[1107]

564 Die instanzgerichtliche Rechtsprechung verneint unter Hinweis auf den derzeitigen **Sicherheitsstandard** der im Internet verwendeten Passwörter und das Fehlen einheitlicher Maßstäbe für die Verschlüsselung den für die Annahme eines Anscheinsbeweises typischen Geschehensablauf. Der Sicherheitsstandard für Passwörter sei nicht ausreichend, um aus der Verwendung eines geheimen Passworts auf denjenigen als Verwender zu schließen, dem dieses Passwort ursprünglich zugeteilt worden ist.[1108] Die Tatsache, dass weltweit tagtäglich Millionen von Rechtsgeschäften per Internetauktion klaglos abgewickelt werden, lasse den Schluss auf die Verlässlichkeit des Mediums Internet im Allgemeinen und der Kommunikationsplattform Internet-Auktion im Besonderen nicht zu.[1109] Hervorgehoben wird dabei der Unterschied der Verwendung eines bloßen Passwortes – welches noch dazu online ohne Identitätsprüfung vergeben wird – gegenüber den Sicherungsverfahren bei ec-Karten mit PIN und Online-Banking mit PIN und TAN.[1110] Für die hM lässt sich hierbei die gesetzgeberische Wertung des § 371a Abs. 1 Satz 2 ZPO/§ 292a ZPO aF anführen, wonach erst eine qualifizierte elektronische Signatur den Anscheinsbeweis rechtfertigt (zur Bedeutung dieser gesetzlichen Wertung für das Online-Banking unten Rn. 558).[1111] Soweit diese Beweislastverteilung für den Käufer im Einzelfall ein Reuerecht begründen sollte, wird dies in der Rechtsprechung hingenommen, weil der Verkäufer dieses Risiko bei der Nutzung einer Internet-Auktion in Kenntnis der Missbrauchsmöglichkeiten eingehe.[1112]

565 Ein Teil der Literatur argumentiert dagegen, für die Authentizität einer unter einer E-Mail-Adresse abgegebenen und durch Passwort geschützten E-Mail spreche die **allge-**

1107 *Mankowski*, CR 2003, 44; *Ernst*, Vertragsgestaltung im Internet, Rn. 26.

1108 OLG Köln MMR 2002, 813 (814); LG Bonn MMR 2002, 255 (256); LG Bonn MMR 2004, 179 (180).

1109 LG Bonn MMR 2004, 179 (180).

1110 LG Bonn MMR 2002, 255 (257); LG Bonn MMR 2004, 179 (181); *Borges*, NJW 2005, 3313 (3317); *Wiebe*, MMR 2002, 257 (258); *Wiebe*, in: Spindler/Wiebe, Internet-Auktionen und Elektronische Marktplätze, Kap. 4 Rn. 61. Gegen die Zugrundelegung bestimmter technischer Sicherheitsstandards, weil es sich hierbei um eine „normative Überhöhung“ handele, s. *Mankowski*, CR 2003, 44 (45).

1111 *Mehrings*, in: Hoeren/Sieber, Kap. 13.1 Rn. 290; *Wiebe*, MMR 2002, 257 (258); *Wiebe*, in: Spindler/Wiebe, Internet-Auktionen und Elektronische Marktplätze, Kap. 4 Rn. 62.

1112 OLG Naumburg NJOZ 2005, 2222 (2224); LG Bonn MMR 2004, 179 (180). Abweichend davon möchte *Wiebe*, in: Spindler/Wiebe, Internet-Auktionen und Elektronische Marktplätze, Kap. 4 Rn. 68; die das Missbrauchsrisiko nicht einem der beiden Vertragspartner des Kaufvertrags, sondern als Betreiber des elektronischen Marktplatzes und Nutznießer des Geschäftsverkehrs dem (dritten) Auktionshaus auferlegen.

meine Lebenserfahrung, was bereits (unabhängig von einem technischen Sicherheitsstandard) einen Anscheinsbeweis rechtfertige.[1113] Das Ausspähen des Passwortes sei wegen der zu überwindenden technischen Hürden nicht jedermann möglich, sondern verlange besondere Fachkenntnisse.[1114] Die Wahrscheinlichkeit einer Manipulation sei folglich trotz der mangelnden Sicherheit des Passwortsystems im Verhältnis zum Gesamtumfang des E-Mail-Aufkommens denkbar gering.[1115] Wertungsmäßig wird überdies darauf hingewiesen, der Nutzer habe das Missbrauchsrisiko zu tragen, weil er sich des Internets in Kenntnis seiner Risiken bediene.[1116]

(iii) Bestehen eines Erfahrungssatzes beim Online Banking

(a) Ausgangspunkt der hM: Technische Sicherheit des Online-Banking

566 Grundlage für beide Formen des Anscheinsbeweises (Urheberschaft für die Erklärung und Sorgfaltspflichtverletzung) ist, dass für das Online-Banking überhaupt entsprechende Erfahrungssätze formuliert werden können. Als Vermutungsgrundlage des Anscheinsbeweises hat die **Bank** daher die technische Sicherheit ihres Online-Banking-Systems gegen Eingriffe Dritter zu **beweisen** (Rn. 559). Die **hM bejaht** für das Online-Banking einen Anscheinsbeweis mit dem mehr oder minder pauschalen Hinweis auf den **hohen technischen Sicherheitsstandard** der verwendeten PIN-/TAN-Sicherungssysteme. Diese könnten nur mit einem Aufwand überwunden werden, welcher unter technischen oder wirtschaftlichen Gesichtspunkten unwahrscheinlich erscheine.[1117] Die Annahme hinreichender technischer Sicherheit beim Online-Banking bildet somit die tatsächliche Basis für die erforderliche hohe Wahrscheinlichkeit, dass die Erklärung vom Kunden selbst oder einem autorisierten Dritten abgesandt wurde

---

1113 So *Mankowski*, CR 2003, 44 (45).

1114 *Mankowski*, CR 2003, 44 (45); *Hoffmann*, in: Leible/Sosnitza, Versteigerungen im Internet, Teil 3 Kap. B Rn. 176; *Ernst*, Vertragsgestaltung im Internet, Rn. 29.

1115 *Mankowski*, MMR 2004, 182 ff.; *Mankowski*, CR 2003, 44 (45); *Krüger/Büttner*, MDR 2003, 181 (186); *Hoffmann*, in: Leible/Sosnitza, Versteigerungen im Internet, Teil 3, Kap. B, Rn. 184; *Ernst*, Vertragsgestaltung im Internet, Rn. 26 ff.

1116 *Mankowski*, CR 2003, 44 (46).

1117 *Werner*, MMR 1998, 338 (339); *Wiesgickl*, WM 2000, 1039 (1047, 1050); *Trapp*, WM 2001, 1192 (1199); *Bock*, in: Bräutigam/Leupold, Kap. VII Rn. 83; *Kunst*, MMR Beilage 9/2001, 23 (24 f.); *Neumann/Bock*, Zahlungsverkehr im Internet, Rn. 183; *Werner*, in: Hoeren/Sieber, Kap. 13.5. Rn. 37; *Werner*, in: Hellner/Steuer, Band 6, 19/ 17, 84; *Werner*, in: Schwarz/Peschel-Mehner, Recht des Internet, Teil 2, Kap. 2 A Rn. 25; *Recknagel*, Vertrag und Haftung beim Internet-Banking, S. 150. Im Ergebnis wohl ebenfalls auf die technische Sicherheit abstellend *Karper*, DuD 2006, 215 (218 f.).

oder aber, dass sich ein unbefugter Dritter die Legitimationsmedien nur aufgrund einer Sorgfaltspflichtverletzung des Kunden zunutze machen konnte.

567 Der Anscheinsbeweis ist jedoch nur solange und nur insoweit gerechtfertigt, als ein technisches Sicherheitsniveau gewährleistet werden kann, welches auch im Hinblick auf die technische Fortentwicklung und aktuelle Bedrohungen noch als weitgehend unüberwindlich angesehen werden kann.[1118] In Bezug auf die Sicherheit des PIN-/TAN-Verfahrens ist der hM im Ausgangspunkt zumindest soweit zuzustimmen, als PIN und TAN durch **Ausrechnen** oder bloßes **Ausprobieren** nur unter völlig unwahrscheinlichen Umständen erlangt werden können.[1119] Genauso wird man den Anscheinsbeweis für die Urheberschaft des Bankkunden für einen Transaktionsauftrag nicht schon deshalb verneinen können, weil der Bankkunde – unter Verletzung seiner Pflichten aus dem Online-Bankingvertrag – die Verwendung der Legitimationsmedien durch Dritte ermöglichen kann.[1120] Denn während bei Internet-Auktionen die **Weitergabe des Passwortes** – etwa im Familienkreis – nicht unüblich sein dürfte,[1121] werden die Legitimationsmedien für das Online-Banking regelmäßig auch im Familienkreis (und erst recht im Bekanntenkreis) vertraulich behandelt.

568 Bei der Frage des Anscheinsbeweises vielfach unberücksichtigt bleiben indes die in neuerer Zeit aufgetretenen Möglichkeiten des **„Ausspähens“** der Legitimationsmedien durch Phishing-E-Mails und Trojaner. Für ec-Karten hat der BGH die Möglichkeit des Ausspähens der PIN mit Hilfe optischer oder technischer Hilfsmittel bzw. Manipulation des Geldautomaten zwar als Möglichkeit zur Kenntnis genommen. Das Gericht sah den Anscheinsbeweis aufgrund solcher Phänomene aber nicht generell in Frage gestellt.[1122] Diese Erwägungen können aufgrund der völlig anders gelagerten Möglichkeiten die Legitimationsmedien auszuspähen jedoch nicht unbesehen auf das Online-Banking übertragen werden. Zwar kann auch beim Online-Banking das Ausspähen „konventionell“

1118 *Werner*, in: Schwarz/Peschel-Mehner, Recht des Internet, Teil 2, Kap. 2 A Rn. 73.

1119 *Kind/Werner*, CR 2006, 353 (369); *Wiesgickl*, WM 2000, 1039 (1047). Ebenso die Antwort der Bundesregierung vom 4.7.2000 auf die Kleine Anfrage der Abgeordneten Rainer Funke, Dr. Edzard Schmidt-Jortzig, Dr. Max Stadler, weiterer Abgeordneter und der Fraktion der F.D.P. – Drucksache 14/3603 –, BT-Drucks. 14/3757, S. 2.

1120 *Wiesgickl*, WM 2000, 1039 (1047) verneint aus diesem Grund einen Anscheinsbeweis für die Urheberschaft.

1121 So auch *Hoffmann*, in: Leible/Sosnitza, Versteigerungen im Internet, Teil 3, Kap. B, Rn. 175, 185.

1122 Vgl. BGH NJW 2004, 3623 (3624). Im Fall verneinte der BGH eine Erschütterung des Anscheinsbeweises, da die Klägerin am Tag des Diebstahls der ec-Karte keine Abhebung vorgenommen hatte. Nach Auffassung des BGH bestand bei diesem Geschehensablauf keine Möglichkeit des „Ausspähens“ der PIN ohne Sorgfaltswidrigkeit der Kundin.

durch Verschaffung der auf einem Zettel notierten PIN und einer TAN-Karte erfolgen – die Situation unterscheidet sich dann nicht wesentlich von der ec-Kartenproblematik. Weitaus relevanter sind indessen die hier interessierenden neuen Erscheinungen der Phishing-E-Mails oder trojanischen Pferde. Gerade im Hinblick auf diese Gefahren bieten viele der derzeit verwendeten PIN-/TAN-Sicherungsverfahren nicht die erforderliche Sicherheit um von einer faktischen Unüberwindbarkeit sprechen zu können. Nach dem derzeitigen Stand der Technik wird man zwischen Verfahren mit Medienbruch (unten (b)) und solchen ohne Medienbruch (unten (c)) zu unterscheiden haben:

(b) Sicherungsverfahren ohne Medienbruch

569 Angesichts der neuen „elektronischen" Bedrohungsformen muss die vor einigen Jahren wohl noch zutreffende Annahme, die Überwindung der PIN-/TAN-Sicherungsverfahren sei nur mit unvertretbarem Aufwand möglich und liege daher außerhalb jeder Wahrscheinlichkeit, heute zumindest für **Systeme ohne Medienbruch** (Rn. 512) als obsolet angesehen werden. Wie oben beschrieben (Rn. 512) liegt der Nachteil dieser PIN-/TAN-Verfahren in der **Möglichkeit, PIN und TAN auf rein elektronischem Wege** (im Zweifel damit auch aus dem weit entfernten Ausland) beispielsweise durch Trojaner **auszuspähen**.

570 Für die unberechtigte Nutzung von Nutzer-Accounts bei Internet-Auktionen stellte das LG Konstanz auf der Grundlage eines Sachverständigengutachtens fest, das Ausspähen des Passworts durch Trojaner usw. sei eine „reale Gefahr".[1123] Die vielfältigen Manipulationsmöglichkeiten im Internet ließen damit keinen sicheren Rückschluss auf die Person des Erklärenden zu.[1124] Das OLG Köln verneinte für Internet-Auktionen trotz der Schwierigkeiten bei der Entschlüsselung des Passworts den für die Annahme eines Anscheinsbeweises typischen Geschehensablauf, weil ein Missbrauch auch ohne vorherige Entschlüsselung des Passwortes durch bloßes Ausspähen möglich sei.[1125]

1123 LG Konstanz MMR 2002, 835; dazu auch *Winter*, MMR 2002, 836.

1124 LG Konstanz MMR 2002, 835.

1125 Das OLG Köln MMR 2002, 813 (814) führt hierzu aus: „Auf die vom Kl. dargestellten Probleme einer „Entschlüsselung" des Passworts kommt es in diesem Zusammenhang nicht an. Ein Missbrauch setzt nämlich eine vorherige Entschlüsselung gar nicht voraus. Vielmehr kann jemand, der mit Abläufen im Netz ausreichend vertraut ist, was heute schon bei einer Vielzahl der Jugendlichen gegeben ist, ohne allzu großen Aufwand das Passwort „lesen". Von einer für einen Anscheinsbeweis ausreichenden Typizität wird man möglicherweise bei der Verwendung einer elektronischen Signatur ausgehen können, nicht aber bei einem ungeschützten Passwort."

571 Gegenüber dem bloßen Passwortschutz bei Internet-Auktionen bieten Verfahren mit PIN und TAN zwar einen deutlich höheren Schutz gegen Entschlüsselung. Auch dieses System hilft indessen nicht, wenn ein Angreifer aufgrund einer Phishing-E-Mail oder Pharming Zugriff auf PIN und TAN selbst erhält. Auf die von der hM angeführten technischen und finanziellen Hindernisse bei der Entschlüsselung kommt es aber nicht an, wenn PIN und TAN abgefangen und das **Sicherheitssystems des Internet-Banking** somit **umgangen** werden kann. Mit der Begründung des OLG Köln und des LG Koblenz lässt sich im Ergebnis auch der Anscheinsbeweis beim Online-Banking mit PIN-/TAN-Verfahren ohne Medienbruch in Zweifel ziehen.[1126] Angesichts der beschriebenen Anfälligkeit von Sicherungsverfahren ohne Medienbruch für Identitätsmissbrauch (vgl. die Bedrohungsszenarien und oben Rn. 512) und der Vielzahl der technischen Möglichkeiten des Ausspähens der Legitimationsmedien durch Phishing-E-Mails und Pharming lässt sich ein **Anscheinsbeweis für die Urheberschaft** bei Verwendung dieser Systeme **nicht** mehr begründen.[1127]

572 Ebenso wenig ist eine Vermutung für eine **Pflichtverletzung** des Kunden gerechtfertigt. Gegen Bedrohungen durch Phishing und Pharming ist ein wirksamer Schutz durch den Kunden selbst schon wegen mangelnder IT-Kenntnisse regelmäßig nur in sehr begrenztem Umfang möglich (zu den Pflichten des Kunden im Einzelnen oben Rn. 281 ff.). Insbesondere bei der zunehmend zu beobachtenden Verwendung von Trojanern kann selbst dann Zugriff auf die Zugangsdaten erlangt werden, wenn der Kunde alle zumutbaren Sicherheitsvorkehrungen getroffen hat.[1128] Zum Teil werden eigene Sicherheitsmaßnahmen des Kunden auch durch Maßnahmen der Bank konterkariert – so etwa bei Verwendung Aktiver Inhalte auf den Websites der Bank (Rn. 515). Keine Pflichtverletzung des Kunden ist beispielsweise auch dann anzunehmen, wenn der Identitätsmissbrauch durch eine lückenhafte Webanwendung ermöglicht wurde. Beispielhaft hierfür sind etwa Sicherheitslücken im Internet Explorer von Microsoft[1129] oder anderer Programme.[1130] Keineswegs kann gegenwärtig somit davon ausgegangen werden, die

---

1126 Ebenso *Erfurth*, WM 2006, 2198 (2205). Anders *Karper*, DuD 2006, 215 (219) der zufolge die Einschätzung des LG Koblenz auf das Verfahren unter Nutzung von PIN und TAN wegen dessen höheren Schutzniveau nicht übertragen werden könne. Dies lässt indes außer Betracht, dass die Verschlüsselungsgüte keinen Schutz gegen ein Ausspähen des Passworts bietet.

1127 Ebenso, jedoch ohne Ausnahme der Sicherungsverfahren mit Medienbruch *Kind/Werner*, CR 2006, 353 (359); *Erfurth*, WM 2006, 2198 (2205).

1128 *Kind/Werner*, CR 2006, 353 (359).

1129 Vgl. dazu abrufbar unter: http://www.heise.de/security/news/meldung/78372.

1130 Ebenso mit weiteren Beispielen *Erfurth*, WM 2006, 2198 (2202).

missbräuchliche Verwendung von PIN und TAN beruhe typischerweise auf einer Pflichtverletzung des Bankkunden.

573 In Zukunft ist zu erwarten, dass sich die Methode der „Online-Betrügereien“ zunehmend von einfachen Phishing-E-Mails weg, hin zur Verwendung von **immer ausgefeilteren Schadprogrammen** verlagern wird.[1131] Im selben Maße verringern sich damit aber zugleich die Möglichkeiten des Bankkunden diesen Bedrohungen durch eigene Sorgfalt wirksam zu begegnen und somit die Risiken des Online-Banking zu beherrschen. Gerade in den die Fällen des Pharming (Szenarien 2 und 3) sind schon nach gegenwärtigem Stand der Informatik eine Vielzahl von Fallgestaltungen denkbar, in denen dem Kunden keine Pflichtverletzung vorgeworfen werden kann. Daraus muss gefolgert werden, dass der dem Anscheinsbeweis zugrunde liegende **Erfahrungssatz**, ein Missbrauch durch Dritte beruhe typischerweise auf einer Sorgfaltspflichtverletzung des Bankkunden, jedenfalls **für PIN-/TAN-Verfahren ohne Medienbruch zu verneinen** ist, da die zu fordernde Typizität angesichts der neuen Bedrohungsformen nicht (mehr) gegeben ist.[1132] Beließe man es bei der gegenwärtigen hM, würden die Risiken der künftigen Entwicklung von Schadprogrammen letztlich in weiten Teilen beweisrechtlich einseitig dem Kunden aufgebürdet, obwohl die Banken durch den Einsatz besserer technischer Systeme schon heute Abhilfe schaffen können.

574 Der Anscheinsbeweis kann bei Verwendung von PIN-/TAN-Verfahren ohne Medienbruch auch nicht auf das häufig – insbesondere in Bankenkreisen – verwendete Argument gestützt werden, erfolgreiche Phishing und Pharming-Attacken stellten **nur Einzelfälle** dar, so dass die ordnungsgemäße Transaktion der typische Geschehensablauf sei.[1133] Diese Behauptung entbehrt angesichts sich häufender Meldungen über Missbräuche beim Online-Banking allerdings einer gesicherten tatsächlichen Grundlage.[1134] Die Banken dürften über aussagekräftiges Zahlenmaterial verfügen, halten sich diesbezüglich jedoch bedeckt. Im Hinblick auf die Rechtsprechung der Instanzgerichte zu Internet-Auktionen ist die Tragfähigkeit des Arguments insgesamt zweifelhaft. Denn die-

1131 *Erfurth*, WM 2006, 2198 (2206).

1132 So auch *Kind/Werner*, CR 2006, 353 (359); *Erfurth*, WM 2006, 2198 (2206); Zweifel auch bei *Borges*, NJW 2005, 3313 (3317).

1133 So im Ergebnis *Borges*, NJW 2005, 3313 (3317); *Karper*, DuD 2006, 215 (219).

1134 Frankfurter Allgemeine Zeitung vom 11.7.2005: „Trickbetrüger nehmen Internet-Banking ins Visier“ und vom 10.3.2006: „Angriffe auf Online-Bankkunden nehmen sprunghaft zu“; Süddeutsche Zeitung vom 2.8.2006, S. 2: „Surfen am Abgrund“; Spiegel-Online vom 24.9.2006: „Phishing und Pharming – Die Bedrohung wächst“, abrufbar unter: http://www.spiegel.de/netzwelt/technologie/0,1518,438677,00.html (zuletzt abgerufen am 06.06.2007).

se misst der weit überwiegenden Zahl der fehlerfrei durchgeführten Online-Geschäfte wegen der Unsicherheit des Passwortschutzes keine entscheidende Bedeutung bei.[1135] Da – wie ausgeführt – auch das PIN-TAN-Verfahren ohne Medienbruch in erheblichem Umfang anfällig für Ausspähen ist, dürften hier keine anderen Grundsätze gelten.

(c) Sicherungsverfahren mit Medienbruch

575 Gegenwärtig kann der erforderliche hohe Sicherheitsstandard zur Bejahung eines Anscheinsbeweises allenfalls dort bejaht werden, wo **Sicherungssysteme mit Medienbruch** (s. Rn. 513) Verwendung finden. Bei Verwendung eines TAN-Generators kann eine ausgespähte TAN wegen deren Verknüpfung mit der konkreten Transaktion des Bankkunden technisch nicht für eine andere (missbräuchliche) Transaktion verwendet werden. Bei Übermittlung der TAN und Bestätigung der übermittelten Transaktionsdaten durch eine SMS auf das Mobiltelefon des Bankkunden (mTAN) gelangt die gültige TAN stets nur auf das Mobiltelefon des Kunden. Ein Identitätsmissbrauch ist bei Verwendung von Systemen mit Medienbruch damit von vornherein nur dann denkbar, wenn neben der PIN auch die zugehörige Hardware (TAN-Generator, Mobiltelefon) in den Besitz des Täters gelangt, was dann aber die Vermutung einer unsorgfältigen Verwahrung dieser Geräte nahe legt (unten Rn. 576). Ein **Ausspähen der TAN auf *rein* elektronischem Wege** durch Trojaner u.ä. ist dagegen ***nicht* möglich**, was insbesondere ein Handeln vom Ausland aus praktisch unmöglich macht.

576 Da eine authentifizierte Transaktion durch unbefugte Dritte bei Verwendung von Sicherungsverfahren mit Medienbruch regelmäßig nur denkbar ist, wenn der Täter erstens die PIN kennt und zweitens auch in den Besitz der Hardware, d.h. des TAN-Generators oder des Mobiltelefons, gelangt ist, ist hier auch der **Anscheinsbeweis für ein pflichtwidriges Handeln** des Bankkunden gerechtfertigt. Selbst wenn die PIN auf elektronischem Wege „abgefischt“ werden konnte, müsste sich der Täter zusätzlich den TAN-Generator bzw. das Mobiltelefon des Bankkunden (nebst der PIN des Mobiltelefons) verschaffen. Hier ist dann aber – anders als bei Verfahren ohne zusätzliche Hardware – die **Parallele zur ec-Kartenproblematik** tatsächlich gerechtfertigt, da dem Kunden letztlich nichts anders abverlangt wird, als TAN-Generator bzw. Mobiltelefon – also körperliche Gegenstände – sicher und von der PIN getrennt zu verwahren. Dies ent-

1135 LG Bonn MMR 2004, 179 (180).

spricht weitgehend den Anforderungen, welche die Rechtsprechung für die sichere und getrennte Verwahrung von PIN und ec-Karte aufgestellt hat. Der Fall, dass die PIN auf elektronischem Wege (noch dazu wie häufig aus dem Ausland) durch einen Trojaner usw. ausgespäht, der Aufenthalt des Bankkunden ermittelt und dann noch die Hardware entwendet wird, dürfte bloß theoretische Relevanz besitzen. Entsprechend der Rechtsprechung zu ec-Karten (Rn. 562) erscheint daher eine tatsächliche Vermutung für die Weitergabe oder unsorgfältige Verwahrung der PIN und der Hardware gerechtfertigt.

(d) Zwischenergebnis

577 Nach derzeit **hM** im juristischen Schrifttum wird es der Bank regelmäßig gelingen, die technische Sicherheit der PIN-/TAN-Systeme als Grundlage des Anscheinsbeweises zu beweisen. Insbesondere die Gefahr des Ausspähens trifft damit beweisrechtlich den Kunden, da dieser die Legitimationsmedien geheim halten müsse und folglich eine tatsächliche Vermutung dafür spreche, dass der Kunde den Missbrauch von PIN und TAN zumindest fahrlässig ermöglicht habe.[1136] Wegen des vermeintlich hohen technischen Sicherheitsstandards wird angenommen, die Ursache eines Missbrauchs könne nur aus der Sphäre des Kunden kommen.[1137] Phishing und Pharming werden damit nicht als Frage der (mangelnden) Sicherheit des Online-Banking gesehen, sondern einseitig dem Verantwortungsbereich des „Unsicherheitsfaktors Benutzer“ zugewiesen, der nun seinerseits den Anscheinsbeweis erschüttern muss.

578 Verfahren **ohne Medienbruch** weisen indessen keine hinreichende technische Sicherheit gegenüber Manipulationen Dritter auf, welche die Vermutung zuließe, der Kunde selbst habe die Transaktion initiiert oder aber seine Pflichten verletzt (s. Rn. 512 ff.). Anders ist dies bei Sicherungsverfahren **mit Medienbruch bzw. einem zweiten unabhängigen Kommunikationskanal (Zwei-Kanal-Verfahren)**, da bei diesen Eingriffe von außen mit an Sicherheit grenzender Wahrscheinlichkeit auszuschließen sind. Nur bei diesen – bislang nur vereinzelt eingesetzten Verfahren – kommt daher ein Anscheinsbeweis in Betracht.

(iv) *Erschütterung des Anscheinsbeweises*

1136 *Karger*, DuD 2006, 215 (219); *Borges*, NJW 2005, 3313 (3316); *Recknagel*, Vertrag und Haftung beim Internet-Banking, S. 127.

1137 Dazu *Werner*, MMR 1998, 232 (235); *Wiesgickl*, WM 2000, 1039 (1050); *Gößmann*, in: Bankrechts-Handbuch, § 55 Rn. 26. Auch der Trojaner-Angriff auf das HBCI-Verfahren wurde nicht als Angriff auf die Sicherungssysteme des Online-Banking, sondern als Angriff auf den Computer des Kunden gewertet, s. *Neumann/Bock*, Zahlungsverkehr im Internet, Rn. 183.

(a) Grundsatz

579 Soweit man den Anscheinsbeweis bejaht, liegt es am Bankkunden, den Anscheinsbeweis zu erschüttern, voraussetzt, dass der Gegner (hier der Bankkunde) Tatsachen behauptet und beweist, aus denen sich die **ernsthafte Möglichkeit eines abweichenden (atypischen) Geschehensablaufs** im konkreten Einzelfall ergibt.[1138] Die Tatsachen aus denen die Möglichkeit eines abweichenden Ablaufs abgeleitet werden sollen, bedürfen des Vollbeweises.[1139] Die Erschütterung des Anscheinsbeweises ist nicht mit den strengeren Anforderungen des Beweises des Gegenteils gleich zu setzen.[1140]

580 Für den oben (Rn. 556) formulierten alternativen Anscheinsbeweis bedeutet dies, dass der Bankkunde den Anscheinsbeweis für die Urheberschaft erschüttern kann, indem er die ernsthafte Möglichkeit einer Veranlassung des Bankgeschäfts durch einen unbefugten Dritten darlegt und erforderlichenfalls beweist. Gelingt dem Kunden die Erschütterung des Anscheinsbeweises für die **Urheberschaft**, bedeutet dies indessen nicht notwendig, dass es der Bank nunmehr verwehrt ist, das Konto des Kunden zu belasten. Vielmehr wird angenommen, dass der Kunde die Transaktion des Unbefugten durch die Verletzung eigener **Sorgfaltspflichten** ermöglicht hat. Hier zeigt sich, dass die Festlegung der Sorgfaltspflichten des Kunden zugleich mitbestimmend für die Erschütterung des Anscheinsbeweises ist. Kann der Kunde diesen Anscheinsbeweis nicht erschüttern, haftet er nach §§ 280 Abs. 1, 241 Abs. 2 BGB gegenüber der Bank auf Schadensersatz.[1141]

581 Welche **Anforderungen** die Rechtsprechung an die Erschütterung des Anscheinsbeweises stellt, bleibt der freien richterlichen Beweiswürdigung im Einzelfall überlassen.[1142] Denkbar ist, dass die Rechtsprechung die Anforderungen an die Erschütterung des Anscheinsbeweises wegen der andauernden Diskussion über die Sicherheit des Online-Banking relativ niedrig ansetzen wird.[1143] Dies erscheint zumindest dann interessengerecht, wenn man entgegen der hier vertretenen Auffassung einen Anscheinsbeweis bei

---

1138 BGH NJW 1991, 230 (231); *Borges*, NJW 2005, 3313 (3317); *Karper*, DuD 2006, 215 (218); Musielak-*Foerste*, § 286 ZPO Rn. 23; MünchKommZPO-*Prütting*, § 286 ZPO Rn. 64; Thomas/Putzo-*Reichold*, § 286 ZPO Rn. 13; Zöller-*Greger*, Vor § 284 ZPO Rn. 29; *Neumann/Bock*, Zahlungsverkehr im Internet, Rn. 180, 184 ff.

1139 BGH NJW 1991, 230 (231); Zöller-*Greger*, Vor § 284 ZPO Rn. 29; Stein/Jonas-*Leipold*, § 286 ZPO Rn. 98.

1140 MünchKommZPO-*Prütting*, § 286 ZPO Rn. 64.

1141 *Neumann/Bock*, Zahlungsverkehr im Internet, Rn. 184 f.

1142 BGH NJW 1969, 277; Stein/Jonas-*Leipold*, § 286 ZPO Rn. 98.

1143 So auch die Einschätzung von *Neumann/Bock*, Zahlungsverkehr im Internet, Rn. 186; *Kind/Werner*, CR 2006, 353 (359).

Sicherungssystemen ohne Medienbruch befürwortet. Das LG Stralsund sah den Anscheinsbeweis für die Richtigkeit einer Telefonrechnung dadurch als erschüttert an, dass sich ein Virus mit Namen „Backdoor-Explorer 32-Trojan“ auf dem Rechner des Telefonkunden befunden hatte.[1144] Beim Phishing soll man zumindest den Anscheinsbeweis für die Urheberschaft durch eine noch vorhandene Phishing-E-Mail erschüttern können.[1145] In der Literatur wird darüber hinaus zum Teil die Ansicht vertreten, die ernsthafte Möglichkeit eines atypischen Geschehensablaufs könne bereits mit Hilfe von Medienberichten und einschlägiger Fachliteratur über Pharming-Angriffe bewiesen werden.[1146] Bejaht man jedoch den Erfahrungssatz, genügen allein abstrakte Berichte über mögliche Bedrohungen ohne Bezug zum konkreten Einzelfall nicht, um den Anscheinsbeweis zu entkräften. Gerade beim Pharming werden aber oftmals greifbare Anhaltspunkte für eine Manipulation durch Dritte fehlen, da diese Angriffe nachträglich kaum feststellbar sind.[1147] Ebenso kann dem Kunden entgegen gehalten werden, er habe die Installation eines Schadprogramms oder lückenhafter Software nachträglich in manipulatorischer Absicht bewirkt, was diesen zum Vollbeweis des atypischen Geschehensablaufs zwingt. Zu strenge Anforderungen an die Erschütterung des Anscheinsbeweises und tatsächliche Nachweisprobleme können im Ergebnis einer Beweislastumkehr oder gar einer (in AGB unzulässigen) verschuldensunabhängigen Haftung des Bankkunden gleichkommen.[1148]

582 Bei **PIN-/TAN-Verfahren mit Medienbruch** wird man dagegen in Anlehnung an die Rechtsprechung zu ec-Karten strengere Anforderungen anlegen können, da ein Missbrauch praktisch nur dann möglich ist, wenn der Täter Zugriff auf die Hardware (TAN-Generator, Mobiltelefon) und zugleich auf die PIN erlangt. Der Anscheinsbeweis wäre hier beispielsweise dann erschüttert, wenn beispielsweise die erforderliche Hardware und die Legitimationsdaten bei einem Diebstahl entwendet wurden ohne dass dem Inhaber Fahrlässigkeit vorgeworfen werden könnte.

(b) Erörterung der Beweislage bei den einzelnen Bedrohungsszenarien

1144 LG Stralsund MMR 2006, 487 (488 f.). Eine Pflichtverletzung wegen unterlassenen Virenschutzes verneinte das Gericht unter Berufung auf die Dialer-Rechtsprechung des BGH.

1145 *Borges*, NJW 2005, 3313 (3317); *Karper*, DuD 2006, 215 (219).

1146 So *Kind/Werner*, CR 2006, 353 (360).

1147 *Borges*, NJW 2005, 3313 (317); *Karper*, DuD 2006, 215 (219).

1148 So zutreffend *Erfurth*, WM 2006, 2198 (2206).

583 Bejaht man mit der bislang vorherrschenden Ansicht den Anscheinsbeweis auch bei Verwendung von PIN-/TAN-Verfahren ohne Medienbruch, ergeben sich im Einzelfall erhebliche Beweisschwierigkeiten und Prozessrisiken, die insbesondere beim Einsatz von Trojanern oftmals nicht überwindbar sein werden. Im Einzelnen stellt sich die Beweislage in den eingangs geschilderten Bedrohungsszenarien wie folgt dar:

(i) Szenario 1

584 Das Phishing per E-Mail und Visual Spoofing ist auf die aktive Mitwirkung des Bankkunden angewiesen, der die E-Mail öffnen, dem angegebenen Link folgen und schließlich PIN und TAN eingeben muss. Am Kunden ist es zunächst den Anscheinsbeweis für die Urheberschaft der Erklärung zu erschüttern, was beim Phishing wohl gelingen wird, sofern die Phishing-E-Mail noch nachweisbar vorhanden ist.[1149]

585 Auch wenn der Nachweis eines Angriffs Dritter erfolgreich geführt wird, steht der Kunde vor dem Problem, auch den Anscheinsbeweis einer Pflichtverletzung zu erschüttern. Er wird dann darzulegen haben, dass er gutgläubig auf die Absenderschaft der Bank für die (Phishing-)E-Mail vertraut hat und deshalb PIN und TAN übermittelt hat. Die Anforderungen an die Erschütterung des Anscheinsbeweises sind dabei abhängig davon, welche Sorgfaltsanforderungen dem Bankkunden auferlegt werden. Sofern bereits die bloße Beantwortung einer Phishing-E-Mail eine Pflichtverletzung begründet, wird die Erschütterung des Anscheinsbeweises in der Regel wohl ausscheiden.

(ii) Szenario 2

586 Der Bankkunde kann den Beweis des ersten Anscheins für seine Urheberschaft für eine Transaktion erschüttern, wenn er die ernsthafte Möglichkeit einer Manipulation darlegt. Hierbei wird es entscheidend darauf ankommen, ob die Rechtsprechung beispielsweise die gehäufte Verbindung zu einigen IP-Adressen als Erschütterung des Anscheinsbeweises ausreichen lässt. Gelingt dem Bankkunden schon der Nachweis einer Manipulation des Provider-Servers nicht, besteht der Anscheinsbeweis seiner Urheberschaft fort.

(iii) Szenario 3

587 Beim Pharming i.e.S. mit Trojaner obliegt dem Bankkunden als erste Hürde die Erschütterung des Anscheinsbeweises für seine Urheberschaft für die Transaktion. Diese wird gelingen, wenn sich der Trojaner auf dem PC des Kunden noch nachweisen

1149 *Karper*, DuD 2006, 215 (219).

lässt.[1150] Andernfalls kommt es auf die Frage der Pflichtverletzung nicht mehr an, da der Bankkunde als Urheber des Auftrags an die Bank gilt.

588 Für die Erschütterung des Anscheinsbeweises für eine Sorgfaltswidrigkeit wird man hinsichtlich einzelner Pflichtverletzungen unterscheiden müssen: Im Hinblick auf die Sicherung des eigenen PC kann sich der Bankkunde entlasten, wenn er die Durchführung der ihm zumutbaren Sicherungsmaßnahmen (Virenschutz, regelmäßige Systemupdates) nachweist. Dieser Nachweis lässt sich bei beim Betriebssystem Windows und den meisten Anti-Virus-Programmen durch eine automatisch protokollierte Liste der Updates führen. Konnte die Installation des Trojaners trotz dieser Sorgfaltsmaßnahmen nicht verhindert werden, ist der Anscheinsbeweis für eine Pflichtverletzung des Kunden dennoch erschüttert. Bejaht man eine Pflichtverletzung wegen des Öffnens eines E-Mail-Anhangs, kommt es darauf an, ob der Bankkunde darlegen kann, dass er auf die Seriosität des Inhalts vertrauen durfte.

(c) Zwischenergebnis

589 Entgegen der wohl hM kann beim – derzeit überwiegend im Einsatz befindlichen - Authentisierungsverfahren mittels PIN/TAN **ohne Medienbruch** kein Anscheinsbeweis dafür bejaht werden, dass entweder der Bankkunde selbst gehandelt oder aber den Missbrauch durch Dritte pflichtwidrig ermöglicht hat. Angesichts der neuen und nur schwer beherrschbaren Bedrohungen insbesondere durch Schadprogramme fehlt die hierfür erforderliche Typizität des Geschehensablaufs. Eine entsprechende Typizität ließe sich allein bei den nach dem – gegenwärtigen Stand der Technik – als sicher zu bewertenden Verfahren bejahen, die auf einem **Medienbruch** bzw. der Verwendung eines zweiten, unabhängigen Kommunikationskanals (Zwei-Kanal) beruhen.

Nach gegenwärtig hM hängt die Risikoverteilung beim Online-Banking dagegen – auch bei Einsatz des PIN/TAN-Verfahrens – davon ab, wie streng die Gerichte die Erschütterung des Anscheinsbeweises handhaben. Für den Bankkunden birgt die Annahme eines Anscheinsbeweises das beweisrechtliche Risiko selbst dann haften zu müssen, wenn alle Sorgfaltsanforderungen beachtet wurden, wenn die Erschütterung des Anscheinsbeweises (etwa bei Pharming-Angriffen) nicht gelingt.Haftung weiterer Akteure

[1150] Vgl. auch LG Stralsund MMR 2006, 487 (488) zur Erschütterung des Anscheinsbeweises für die Richtigkeit der Telefonrechnung bei bloßem Vorliegen eines Trojaners auf dem PC des Kunden. Kritisch zu dieser Entscheidung *Ernst*, CR 2006, 590 ff.

Die aufgezeigten Gefahren beim Online-Banking werfen die Frage nach den Rückgriffsmöglichkeiten des von seiner Bank in Anspruch genommenen Kunden auf. Da die eigentlichen Täter entweder nicht identifizierbar oder – etwa bei Wohnsitz im Ausland – nur schwer greifbar sind, kommen als mögliche Anspruchsgegner meist nur die Hersteller fehlerhafter IT-Produkte sowie Internet-Provider und private Nutzer in Betracht:

(5) IT-Hersteller

590 Nutzt ein Trojaner eine Sicherheitslücke in einer vom Bankkunden verwendeten Software (beispielsweise seinem Betriebssystem, Internet-Browser usw.), stellt sich im Schadensfall die Frage einer Haftung des IT-Herstellers gegenüber dem Kunden. Mangels Eigentumsverletzung (Rn. 108 ff.)) kommen gegen den IT-Hersteller regelmäßig nur vertragliche Ansprüche in Betracht. Wurde aber die Installation des Trojaners durch einen Fehler der Software ermöglicht, ist im Ausgangspunkt zunächst festzuhalten, dass kein Schadensersatzanspruch der Bank gegen den Kunden besteht, da dieser nicht pflichtwidrig gehandelt hat. Gleichfalls entfällt mangels Schaden ein produkthaftungsrechtlicher Regressanspruch des Kunden gegen den Hersteller.

591 *Soweit* man den Anscheinsbeweis bejaht (s. oben Rn. 556), lautet die praktisch relevante Frage in diesem Zusammenhang, ob es dem Kunden überhaupt gelingt, die Ursächlichkeit der Softwarelücke für die Installation des Trojaners zu beweisen. Schlägt die Erschütterung des Anscheinsbeweises (oben Rn. 579 ff.) fehl und haftet er gegenüber der Bank in Höhe des Überweisungsbetrages, dürfte die anschließende Inanspruchnahme des Herstellers der Software kaum größere Erfolgsaussichten haben. Wegen des Beweis- und Kostenrisikos wird die Bedeutung der Produkthaftung wird im vorliegenden Zusammenhang damit eher gering sein. Ansprüche der Bank gegen den IT-Hersteller scheitern bereits an der fehlenden Vertragsbeziehung und Rechtsgutsverletzung. Die engen Voraussetzungen einer Drittschadensliquidation werden im Verhältnis zwischen Bank und Kunde regelmäßig nicht vorliegen.[1151]

(6) Intermediäre

592 Eine Haftung von Intermediären gegenüber dem Bankkunden erscheint zumindest auf vertraglicher Grundlage möglich, wenn der Provider eine ihn selbst treffende Sicherungspflicht schuldhaft verletzt hat (ausführlich zu den Sicherungspflichten der Intermediäre unten Rn. 659 ff.). Sofern sich aber nachweisen lässt, dass die Identitätstäu-

[1151] Dazu Palandt-*Heinrichs*, Vorb v § 249 BGB Rn. 112 ff.; Bamberger/Roth-*Schubert*, § 249 BGB Rn. 153.

schung durch einen Angriff auf den Provider des Bankkunden verursacht wurde (vgl. beispielsweise Szenario 2 zu DNS-Spoofing, Rn. 474), haftet der Kunde mangels eigener Pflichtverletzung nicht gegenüber seiner Bank. Eine Inanspruchnahme des Providers durch den Kunden scheitert wiederum am fehlenden Schaden des Bankkunden. Konnte dagegen die Verantwortlichkeit des Intermediärs schon gegenüber der Bank nicht nachgewiesen (d.h. der Anscheinsbeweis erschüttert) werden, dürfte auch hier eine Inanspruchnahme des Intermediärs regelmäßig aus Beweisnot unterbleiben. Eigene vertragliche Ansprüche der Bank gegen den Provider des Kunden bestehen ebenso wie deliktische Ansprüche regelmäßig nicht.

(7) Private Nutzer

593 Hat ein privater Nutzer (etwa ein Freund oder Bekannter) den Trojaner in einem E-Mail-Anhang an den Bankkunden gesandt, stellen sich im Schadensfall die oben erwähnten Probleme zur Haftung privater Nutzer (s. Rn. 275 ff.). Mangels Vertragsverhältnis und Eigentumsverletzung infolge der Installation des Trojaners (Rn. 114), wird ein Schadensersatzanspruch gegen den Versender aber allenfalls bei Verstoß gegen ein Schutzgesetz (§ 823 Abs. 2 BGB) oder vorsätzlich sittenwidriger Schädigung zu bejahen sein (§ 826 BGB).

c) Ergebnis

594 Zum gegenwärtigen Zeitpunkt muss davon ausgegangen werden, dass das Online-Banking über Internet-Verbindung unter Verwendung eines normalen PC keine hinreichende Sicherheit zu bieten vermag. Primär obliegt es der das Online-Banking anbietenden Bank, ein dem Stand der Technik entsprechendes Sicherungsverfahren vorzuhalten. Die Schwachstellen des Online-Bankings bilden derzeit zum einen Sicherheitslücken in den Online-Banking-Systemen und die mangelnde Sicherung des privaten Computers. Eine strenge Risikoverteilung nach Gefahrenbereichen kommt hierbei jedoch nicht in Betracht. An den durchschnittlichen privaten Nutzer können beim Online-Banking insbesondere im technischen Bereich nur begrenzte Sorgfaltsanforderungen gestellt werden (z.B. Virenschutz, Systemupdates). Soweit ein Restrisiko im Bereich der privaten Nutzung verbleibt, ist dieses wertungsmäßig der Bank zuzurechnen. Wegen des von der hM angenommenen Anscheinsbeweises kann dieses Restrisiko aber nach gegenwärtiger Rechtslage im Einzelfall beweisrechtlich auf den Bankkunden verlagert werden, wenn eine Manipulation der Online-Transaktion – insbesondere im Falle eines Pharming-Angriffs – nicht nachweisbar ist.

7. Zwischenergebnis: besondere Verantwortlichkeit im Banken- und Finanzsektor

595 Im Banken-, Versicherungs- und Finanzsektor ist durch KWG, WpHG, VAG und die entsprechenden Mindestanforderungen, wie z.B. MaRisk, eine starke Aufsicht vorhanden. Die Pflichten sind auch hinsichtlich der Verwendung von Informationstechnik geregelt. Die Aufsichtsbehörde hat zusätzlich auch entsprechende Mittel, um diese Anforderungen durchzusetzen. Zwar sind die Normen nicht als Schutzgesetze i.S.d. § 823 Abs. 2 BGB zu qualifizieren, durch die Möglichkeit, sie zur Konkretisierung der Verkehrssicherungspflichten im Rahmen des § 823 Abs. 1 BGB heranzuziehen, besteht aber dennoch ein enger Zusammenhang auch zur deliktischen Haftung.

V. Besondere Risikopotentiale für Experten und beratende Berufe (Rechtsanwälte etc.)

1. Vorbemerkung

596 Bestimmte Berufsgruppen unterliegen weitergehenden Pflichten als andere, sei es aufgrund ihrer besonderen Vertrauensstellung im Rechtsverkehr oder sei es aufgrund bestimmter volkswirtschaftlich besonders wichtiger Funktionen, die sie übernehmen. Wenn sich solche berufsbezogenen Pflichten auf die Vorhaltung oder Behandlung von Daten beziehen, so können auch spezielle Pflichten im Hinblick auf IT-Sicherheit normiert oder den vorhandenen Regelungen zu entnehmen sein. Besonders betrachtet werden sollen hier insbesondere Rechtsanwälte und Ärzte, aber auch Steuerberater, für die spezielle Pflichten im Hinblick auf den Umgang mit Informationen bestehen.

2. Gefahrenpotential und Gegenmaßnahmen

597 Grundsätzlich unterscheidet sich das technische Gefahrenpotential nur wenig von den Gefahren bei anderen kommerziellen Nutzern – nicht indes das Schädigungspotential. Daten, die in einem besonderen Vertrauensverhältnis wie zwischen Anwalt und Mandant oder Arzt und Patient preisgegeben werden, sind häufig existenziell wichtig und/oder höchstpersönlich. Das Bekanntwerden bzw. die Einsicht Fremder in diese Informationen kann einen hohen vermögensrelevanten Schaden hervorrufen, ist aber auch geeignet, in so weitgehendem Maße in (höchst-)persönliche Rechtsgüter einzugreifen, dass eine Schädigung meist nicht vermögensrelevant einzuordnen bzw. aufzuwiegen ist, und die Daten bereits deshalb eines maximalen Schutzes bedürfen. Darüber hinaus können vermehrte Verstöße zu einer Erschütterung des Vertrauens des Rechtsverkehrs in diese spezifischen Berufe führen, was insgesamt zu Marktstörungen führen kann. Aus

diesem Grunde sind allgemein das Rechtsverhältnis zwischen Klienten und Berufsträger[1152] sowie spezifisch die hierbei offenbarten Informationen einem auch strafrechtlich abgesicherten strengen Schutzregime unterworfen.[1153]

3. Rechtsanwälte

598 Ein solches Vertrauensverhältnis besteht insbesondere für Rechtsanwälte in ihrer Beziehung zu Mandanten. Dementsprechend sind für Daten, die einem Anwalt anvertraut sind, neben den Vorschriften des BDSG und des StGB die Bundesrechtsanwaltsordnung (BRAO) und die Berufsordnung für Rechtsanwälte (BORA) zu beachten.

a) § 43a Abs. 2 BRAO (Verschwiegenheitspflicht)

599 Nach § 43a Abs. 2 BRAO ist der Anwalt zur Verschwiegenheit verpflichtet, wobei sich diese Pflicht auf „alles" bezieht, was ihm in Ausübung seines Berufs bekannt geworden ist. Verletzt der Anwalt vorsätzlich seine Pflicht aus § 43a Abs. 2 BRAO, so ist regelmäßig auch § 203 Abs. 1 Nr. 3 StGB verwirklicht.

600 In diesem Rahmen ist etwa fraglich, ob ein Anwalt verpflichtet ist, elektronische Informationen nur verschlüsselt zu übertragen.[1154] So wird die Frage aufgeworfen, ob das Versenden von unverschlüsselten **E-Mails** an den eigenen Mandanten der offenen Versendung von Postkarten gleichkommt und aus diesem Grunde eine Verletzung von § 43a Abs. 2 BRAO und § 203 Abs. 1 Nr. 3 StGB vorliegen kann.[1155] Dies wird man jedoch zu verneinen haben, da die E-Mails nur an den Mandanten gerichtet sind und E-Mailkonten regelmäßig durch Passwörter geschützt sind.[1156] Fraglich ist, ob dies auch dann gilt, wenn der **Kommunikationsverkehr** mittels Funktechniken unverschlüsselt oder nicht ausreichend gesichert übertragen wird. Während es relativ komplex ist, Daten eines kabelgebundenen Kommunikationsvorgangs abzufangen und auszulesen, stellt dies im Fall von drahtlosen Übertragungsformen, wie etwa WLAN kein Problem dar. Wird ein Funknetz ohne Verschlüsselung genutzt und werden hierbei E-Mails oder an-

---

1152 Für das anwaltliche Vertrauensverhältnis *Henssler*, NJW 1994, 1817 (1818); für das ärztliche Vertrauensverhältnis *Hermeler*, Rechtliche Rahmenbedingungen der Telemedizin, 45.

1153 Dazu BVerfG NJW 2005, 1917 (1919); *Henssler*, NJW 1994, 1817 (1818).

1154 Dazu *Härting*, NJW 2005, 1248 (1248 ff.) mwN.

1155 So mit guten Gründen *Backu*, ITRB 2003, 251 (251); *Jungk*, AnwBl 2001, 170 (172); *Lapp*, BRAK-Mitt 1997, 106 (107); *Streitz*, NJW-CoR 2000, 208 (209); *Wagner/Lerch*, NJW-CoR 1996, 380 (384); differenzierend *v. Lewinski*, BRAK-Mitt 2004, 12 (13).

1156 So *Härting*, NJW 2005, 1248 (1249); *Härting*, MDR 2001, 61 (62); *v. Lewinski*, BRAK-Mitt 2004, 12 (16).

dere Daten übertragen, so kann diese jeder in einem gewissen Umkreis ohne besondere technische Schwierigkeiten abfangen und einsehen.[1157]

601 Nach derzeit wohl hM geht eine Verpflichtung zu aktiven T-Sicherheitsmaßnahmen jedoch über den Wortlaut des § 43a Abs. 2 BRAO, der sich auf die Pflicht zur Verschwiegenheit beschränkt, und das tradierte Verständnis des Anwaltsgeheimnisses hinaus.[1158] Jedenfalls im Falle der Verwendung von drahtlosen Übermittlungsformen wird man jedoch die Verwendung gängiger Verschlüsselungsstandards – etwa dem Wired Equivalent Privacy (WEP)-Standard – fordern müssen, um eine Basissicherheit zu gewährleisten.

602 Weitere Konkretisierungen enthält **§ 2 BORA**,[1159] der in Abs. 4 alle Personen, die bei der Berufstätigkeit des Anwalts mitwirken, ebenfalls zur Verschwiegenheit verpflichtet, so dass etwa auch ausgelagerte Tätigkeiten des Anwalts, z.B. die externe Pflege der IT-Komponenten des Anwalts, erfasst werden können.

b) BDSG

(1) Rechtsanwälte als nicht-öffentliche Stellen

603 Rechtsanwälte erheben, speichern und verarbeiten Daten im Sinne des BDSG, wenn sie Daten ihrer Mandanten im Rahmen ihrer IT-Systeme verwenden. In diesem Rahmen sind sie als nicht-öffentliche Stellen zu qualifizieren, auch wenn sie nach § 1 BRAO als Organe der Rechtspflege gelten,[1160] da sie keine Stelle des Bundes oder der Länder sind.[1161]

(2) Verhältnis des BDSG zur BRAO

604 Da sowohl das BDSG als auch die BRAO Pflichten zum Datenschutz bzw. Verschwiegenheit regeln, liegt es auf der Hand, dass das Verhältnis zwischen beiden Regelungen Probleme bereitet. In Rede stehen sowohl die Verdrängung des BDSG durch die BRAO als lex specialis als auch die Subsidiarität des BDSG (§ 1 Abs. 3 BDSG),[1162] die aller-

---

1157 Dazu näher *Dornseif/Schumann/Klein*, DuD 2002, 1; zur strafrechtlichen Beurteilung *Ernst*, CR 2003, 898.

1158 *Härting*, NJW 2005, 1248 (1249); *Härting*, MDR 2001, 61 (62); *v. Lewinski*, BRAK-Mitt 2004, 12 (16); aA *Eylmann*, in Henssler/Prütting, BRAO, 2. Aufl. (2004), § 43a BRAO Rn. 64.

1159 *Eylmann*, in: Henssler/Prütting, § 43a BRAO Rn. 28 ff.; *Feuerich/Weyland*, § 43a BRAO Rn. 12 ff.; *Hartung*, in: Hartung/Holl, § 43a BRAO Rn. 25 ff. und § 2 BORA Rn. 1 ff.

1160 *Zuck*, in: Abel, Datenschutz in Anwaltschaft, Notariat und Justiz, § 2 Rn. 27; vgl. *Wedde*, in: Roßnagel, Handbuch Datenschutzrecht, Kap. 4.3 Rn. 34.

1161 *Gola/Schomerus*, § 2 BDSG Rn. 12.

1162 S. dazu Stellungnahme der Bundesrechtsanwaltskammer (BRAK) zu der Frage der Bestellung eines Beauftragten für Datenschutz in Rechtsanwaltskanzleien, abrufbar unter:

dings nur dann greifen würde, wenn die BRAO besondere Regelungen bereithält. Dieser grundsätzliche Streit kann hier nur ansatzweise gestreift werden, da er für hier interessierenden Fragen der IT-Sicherungspflichten letztlich nicht entscheidend ist: So decken sich die Ziele des § 9 BDSG weitgehend mit denen des Berufsrechts,[1163] ohne dass dies speziell kodifiziert wäre. Im Rahmen der Selbstverwaltung unterliegt der Anwalt nach § 73 Abs. 2 Nr. 4 BRAO einer gewissen Kontrolle durch die Rechtsanwaltskammern.[1164] Diese können auf die Einhaltung des Berufsrechts achten und im Verletzungsfall berufsrechtliche Schritte bis hin zum Entzug der Anwaltszulassung nach § 114 BRAO gerichtlich erwirken. Dem Anwalt obliegt demnach auch auf Basis des Berufsrechts der sorgsame Umgang mit den Daten; allerdings lassen sich diese Pflichten tatsächlich nicht konkret benennen. Sie dürften, zumindest was z.B. die regelmäßige Datensicherung sowie den Einsatz von allgemein bekannten Sicherungssystemen betrifft, ähnlich den durch § 9 BDSG und der zugehörigen Anlage geregelten Pflichten sein.[1165] Die Anlage zu § 9 Satz 1 BDSG enthält eine allgemeingültige Beschreibung professioneller Standards, deren Nichtbeachtung sowohl standes- als auch strafrechtlich relevant wäre.[1166] Durch das besondere Schadenspotential, das durch den Verlust oder die Entwendung von Daten aus dem Verhältnis zwischen Mandant und Anwalt verwirklicht werden kann, sind bei der Verwendung von Rechnersystemen in der anwaltlichen Tätigkeit dem Anwalt jedenfalls die Sicherungsmaßnahmen zuzumuten, deren Gefahr allgemein bekannt ist und die ohne spezielles Fachwissen eingesetzt werden können. Dies zeigt sich auch an der Anlage zu § 9 BDSG, nach der „auf die Art der zu schützenden [...] Daten“ eingegangen werden muss. Im Einzelfall, also z.B. bei Gefahren, die sich bereits im konkreten Fall gezeigt haben, wird dem Anwalt aber auch die Beiziehung von Fachpersonal zur Absicherung abverlangt werden können. Der Anwalt muss allerdings nicht „mit Kanonen auf Spatzen schießen“;[1167] für äußerst unwahrscheinliche Be-

---

http://www.brak.de/seiten/pdf/Stellungnahmen/2004/StnBDSinKanzleien.pdf, S. 3 unter Verweis auf BAG NJW 1998, 2466; ebenso *Rüpke*, AnwBl 2004, 552 (552 f.).

1163 *Abel*, in: Roßnagel, Handbuch Datenschutzrecht, 7.11 Rn. 28 f.; *Rüpke*, AnwBl 2004, 552, (555); die BRAK hat Vorschläge zur Konkretisierung des § 43a Abs. 2 BRAO zur Erweiterung auch auf technische Organisationspflichten gemacht.

1164 Stellungnahme der BRAK, abrufbar unter: http://www.brak.de/seiten/pdf/Stellungnahmen/2004/StnBDSinKanzleien.pdf, 6 (zuletzt abgerufen am 06.06.2007); Feuerich/Weyland-*Feuerich*, § 73 BRAO Rn. 42; *Abel*, in: Roßnagel, Handbuch Datenschutzrecht, Kap. 7.11 Rn. 38.

1165 Dazu auch *Schöttle*, Anwaltliche Rechtsberatung via Internet, S. 39 ff.

1166 *Abel*, in: Roßnagel, Handbuch Datenschutzrecht, Kap. 7.11 Rn. 28.

1167 *Gola/Schomerus*, § 9 BDSG Rn. 7.

drohungsszenarien müssen keine aufwändigen und dementsprechend kostspieligen Maßnahmen ergriffen werden.

605 Demgemäß sind die grundsätzlichen Pflichten des § 9 BDSG auch aus dem Berufsrecht herleitbar. Insofern ist bisher der einzige relevante Unterschied, was die Pflicht zur Ergreifung von Sicherungsmaßnahmen im Bereich der IT-Sicherheit angeht, dass im einen Fall die Aufsichtsbehörde nach § 38 BDSG die Einhaltung der Voraussetzungen des § 9 BDSG im speziellen, im anderen Fall die Rechtsanwaltskammern die Einhaltung der vermutlich kongruenten Pflichten nach Berufsrecht kontrollieren. Zwar enthält § 38 Abs. 3 Satz 2 BDSG ein Auskunftsverweigerungsrecht über alle diejenigen Daten, deren Herausgabe dem Auskunftspflichtigen unter Androhung von Strafe verboten ist. Gestützt auf diese Ausnahme kann der Anwalt somit jegliche inhaltlichen Daten zurückhalten. Hinzu kämen die Schranken der §§ 43a Abs. 2, 56 Abs. 1 BRAO.[1168] Diese würde natürlich nicht für Daten gelten, die schon von Anfang an voll dem BDSG unterfallen. Auskunft erteilen müsste der Anwalt aber z.B. über die grundsätzlichen Rahmenbedingungen seiner Datenverarbeitung wie die Umstände der regelmäßigen Datensicherung. Allerdings ist gerade die Auskunftspflicht im Rahmen der BRAO sehr differenziert ausgestaltet. Aus diesem Grunde tritt § 38 BDSG jedenfalls vollständig zurück.[1169]

(3) Ergebnis

606 Insofern kann offen bleiben, ob das BDSG insgesamt subsidiär ist oder nur im Einzelfall als allgemeineres Gesetz zurücktritt. Der Pflichtenmaßstab richtet sich an § 9 BDSG sowie der zugehörigen Anlage aus. Die Prüfung der jeweiligen Pflichtenerfüllung erfolgt nicht nach dem BDSG, sondern wird durch die Rechtsanwaltskammern durchgeführt.

c) Vertragliche Nebenpflichten

607 Unabhängig davon, ob gesetzliche Pflichten greifen, können auch aus der vertraglichen Beziehung (als Dienst- oder Geschäftsbesorgungsvertrag)[1170] spezielle Pflichten bezüglich der IT-Sicherheit bestehen. Die Verletzung von Nebenpflichten kann Schadensersatzansprüche aus §§ 280 ff. BGB nach sich ziehen. Dabei werden derartige IT-bezogene Nebenpflichten umso eher anzunehmen und umso weit reichender sein, je

1168 Quaas/Zuck-*Zuck*, § 2 Rn. 52, 54; *Abel*, in: Roßnagel, Handbuch Datenschutzrecht, Kap. 7.11 Rn. 38.
1169 *Abel*, in: Roßnagel, Handbuch Datenschutzrecht, Kap. 7.11 Rn. 38.
1170 Palandt-*Weidenkaff*, § 611 BGB Rn. 20.

mehr die Parteien auf eine vertrauensvolle Zusammenarbeit angewiesen sind, oder sich eine Partei auf die Fachkunde der anderen verlassen muss, einschließlich der IT-bezogenen Sachkunde und Ressourcen.[1171]

608 Selbstverständlich erwartet der Mandant einen **besonders sorgsamen Umgang** mit den offenbarten sensiblen Daten. Daraus ergeben sich eben auch Sorgfaltspflichten hinsichtlich der Daten und der Ergreifung von speziellen Sicherungsmaßnahmen gegen bekannte Gefahren. Wie bereits dargelegt (Rn. 0) kann die Verletzung der Pflichten aus § 9 BDSG mittelbar über die Konkretisierung der geschuldeten Sorgfalt vertragliche Ansprüche oder gar eine deliktische Haftung auslösen.[1172] Wer also schon Sicherungsmaßnahmen nach dem BDSG nicht ergreift, unterliegt der Haftung.[1173] Dem Anwalt können also jedenfalls mindestens die Pflichten eines kommerziellen Nutzers auferlegt werden. Die Verpflichtung zur Ergreifung von Sicherungsmaßnahmen endet auch nicht mit der Aufgabe oder Beendigung des Mandats. Soweit auch die Aufbewahrung von Akten über diesen Zeitraum hinaus notwendig ist, wirken die Pflichten als nachwirkende Vertragspflichten fort.[1174]

d) Deliktische Haftung

609 Sanktionen für die Verletzung entsprechender Pflichten können sich neben der vertraglichen Haftung auch aus § 823 Abs. 1 BGB ergeben, bei der vorsätzlichen Preisgabe zusätzlich aus § 823 Abs. 2 BGB i.V.m. § 203 StGB oder § 826 BGB. Schutzgut des § 823 Abs. 1 StGB ist dabei das Recht auf informationelle Selbstbestimmung. Wiederum sind die jeweiligen Verkehrssicherungspflichten des Anwalts maßgeblich, auch im Hinblick auf das geschützte Rechtsgut. Aufgrund der extrem hohen Sensibilität der Daten ist der Anwalt demnach einem besonders hohen Standard in Bezug auf die Sicherungspflichten unterworfen. Die dem kommerziellen Nutzer obliegenden Pflichten sind somit als absoluter Mindeststandard anzusehen. Auch hier kann der Anhang zu § 9 BDSG als Orientierungshilfe dienen.[1175]

e) Ergebnis

1171 Bamberger/Roth-*Grüneberg-Sutschet*, § 241 BGB Rn. 44.

1172 *Abel*, in: Roßnagel, Handbuch Datenschutzrecht, Kap. 7.11 Rn. 28.

1173 *Horns* in: Abel, Datenschutz in Anwaltschaft, Notariat und Justiz, § 14 Rn. 73.

1174 Die Pflicht zur Aufbewahrung der Handakten ergibt sich aus § 50 Abs. 2 S. 1 BRAO. Besteht diese Pflicht, so muss die Aufbewahrung natürlicherweise bei Mandatsende genauso ausgestaltet sein, wie bei Fortführung des Mandats.

1175 *Abel*, in: Roßnagel, Handbuch Datenschutzrecht, Kap. 7.11 Rn. 28.

610 Der Anwalt ist verpflichtet, diejenigen Pflichten zu ergreifen, die auch einem kommerziellen Nutzer obliegen würden. Durch das besondere Vertrauensverhältnis zwischen ihm und seinen Klienten besteht diesbezüglich auch eine besondere vertragliche Pflicht, die auch deliktsrechtlich untermauert wird.

4. Steuerberater

611 Das Verhältnis zwischen dem Steuerberater und seinem Klienten ist durch ein ähnliches Vertrauensverhältnis gekennzeichnet. Es ist deshalb für den Steuerberater anerkannt, dass das Vertrauensverhältnis mit dem zwischen Anwalt und Mandant vergleichbar ist.[1176] Der Steuerberater nimmt ebenfalls eine unabhängige Organstellung ein,[1177] die Steuerberatung ist nur ein Teil der Rechtsberatung.[1178]

612 Für Steuerberater enthält § 9 der Berufsordnung der Steuerberater (BOStB) die Verschwiegenheitspflicht. Sie ist ähnlich § 2 BORA angelegt, aber umfangreicher und deutlicher. So hält § 9 Abs. 6 BOStB ausdrücklich fest, dass der Steuerberater dafür Sorge zu tragen hat, dass Unbefugte keinen Einblick in die Unterlagen erhalten. Demgemäß hat der Steuerberater die Pflicht, die Daten ausreichend gegen den Zugriff von Dritten zu sichern, wobei auch hier die Pflichten mit denen des Anhangs von § 9 BDSG vergleichbar sein dürften. Da der rechtliche Status dem eines Anwalts ähnlich und auch der Schutz vor staatlichen Eingriffen ebenso zu gestalten ist,[1179] dürfte eine Kontrolle der Einhaltung bezüglich der geschützten Daten ebenfalls nur durch die Bundessteuerberaterkammer erfolgen.

613 Für die **vertraglichen Nebenpflichten und die deliktische Haftung** ergeben sich gegenüber den Ausführungen zum Verhältnis zwischen Anwalt und Mandant **keine Besonderheiten**.

5. Ärzte

614 Wie das Verhältnis von Anwalt zu Mandanten ist erst recht dasjenige zwischen Arzt und Patienten durch ein besonderes gegenseitiges Vertrauen gekennzeichnet.[1180] Die Informationen, die der Patient notwendigerweise für eine Behandlung dem Arzt anvertraut, sind in aller Regel höchstpersönlicher Natur. Die Verschwiegenheit des Arztes

---

1176 BVerfG NJW 2005, 1917 (1919).
1177 BVerfG NJW 1989, 2611 (2612).
1178 BVerfG NJW 1989, 2611 (2612).
1179 BVerfG NJW 2005, 1917 (1919).
1180 BGH NJW 1959, 811 (813).

dient hier also erneut dem Schutz des Klienten. Sie bildet das Kernstück der ärztlichen Berufsethik.[1181] Zwar gibt es auch im Bereich des Arztrechts berufsrechtliche Regelungen, die Mitteilung von Daten aus dem Verhältnis wird ebenfalls nach § 203 StGB mit Strafe bedroht; allerdings gibt es gesetzliche Regelungen, die ausdrücklich die Aufzeichnung und Übermittlung der Daten verlangen.

a) Berufsrecht[1182]

615 Die Berufsordnung der Ärzte dient der Festlegung von Einzelheiten für die Ausübung des ärztlichen Berufs; die Missachtung kann berufsgerichtlich sanktioniert werden.[1183] Die Berufsordnungen sind unmittelbar rechtsverbindliche autonome Satzungen der Landesärztekammern. Sie werden auf Grundlage der Kammergesetze der Länder erlassen, wobei sich die Landesberufsordnungen regelmäßig an den Vorschlägen bzw. Musterberufsordnungen der Bundesärztekammer und der Ärztetage orientieren.[1184] Die Praxis der Delegation der Regelung der Berufsordnung durch den Gesetzgeber an die autonomen Ärztekammern ist nur in gewissen Grenzen möglich, denn der Gesetzgeber muss weiterhin Einfluss auf die inhaltliche Rechtsetzung haben.[1185]

616 Die Pflicht zur Verschwiegenheit wird durch § 9 BerufsO geregelt; danach hat der Arzt über alles, was ihm in seiner Eigenschaft als Arzt anvertraut wurde, zu schweigen. Zeitlich gilt die Schweigepflicht unbegrenzt, sie endet insbesondere nicht mit der Aufgabe der Praxis[1186] oder dem Tode des Patienten, zumal bestimmte Diagnosen auch Rückschlüsse auf ähnliche Erkrankungen bei Verwandten ermöglichen könnten.[1187] Der Arzt kann jedoch durch die Einwilligung des Patienten von seiner Schweigepflicht entbunden werden oder zum Zwecke des erforderlichen Schutzes eines höherwertigen Rechtsgutes zur Preisgabe befugt sein.[1188] Mitarbeiter und andere in der Arztpraxis tätige Personen sind über ihre Schweigepflicht zu belehren. Des Weiteren kann der Arzt gesetz-

---

1181 *Laufs*, in: Laufs/Uhlenbruck, § 70 Rn. 1.

1182 Bezug genommen wird hier jeweils auf die (Muster-)Berufsordnung der Bundesärztekammer, Stand 2006, abrufbar unter: http://www.bundesaerztekammer.de/downloads/MBOStand20061124.pdf.

1183 *Laufs*, in: Laufs/Uhlenbruck, § 5 Rn. 4.

1184 *Laufs*, in: Laufs/Uhlenbruck, § 5 Rn. 5.

1185 BVerfG NJW 1972, 1504 (1507).

1186 *Ulsenheimer*, in: Laufs/Uhlenbruck, § 69 Rn. 14.

1187 *Spickhoff*, NJW 2005, 1983; *Ulsenheimer*, in: Laufs/Uhlenbruck, § 70 Rn. 10.

1188 *Deutsch/Spickhoff*, Medizinrecht, Rn. 478 ff.; *Ulsenheimer*, in: Laufs/Uhlenbruck, § 71 Rn. 1 ff. Eine Entbindung von der Schweigepflicht liegt zum Beispiel beim Bestehen von gesetzlichen Meldepflichten nach den §§ 11 II, 12, 13 GeschlechtskrankheitenG; §§ 7 ff., 11, 12, 49 Infektionsschutzgesetz etc. oder in § 12 GeldwäscheG vor.

lich zur Herausgabe von Daten verpflichtet werden;[1189] § 9 BerufsO schränkt solche Herausgabeverpflichtungen nicht ein. Hierin unterscheidet sich das Berufsrecht der Ärzte grundlegend von dem der Anwälte.

617 Die vorsätzliche (mindestens also bedingter Vorsatz)[1190] und unbefugte Verletzung der Schweigepflicht kann mit Berufsverbot nach § 70 Abs. 1 StGB durch die Berufsgerichte oder Strafgerichte sanktioniert werden.

618 Sowohl § 203 StGB als auch § 9 BerufsO regeln jedoch **nur** den typischen Fall der bewussten - sprich **vorsätzlichen - Weitergabe der anvertrauten Informationen**, auch durch Eröffnung des Zugriffs durch Unterlassen.[1191] Eine explizite Normierung zur Sicherung der Daten bzw. Informationskomponenten besteht hingegen nicht.

b) SGB

619 Die Sozialgesetzbücher enthalten grundsätzliche Regelungen für diejenigen, die Sozialleistungen in Anspruch nehmen. Hierzu gehören nach § 21 ff. SGB I u. a. diejenigen, die als gesetzlich Krankenversicherte ärztliche Hilfe in Anspruch nehmen. Die im Zuge der Behandlung erhobenen, verarbeiteten oder genutzten Daten, also personenbezogene Einzelangaben über persönliche oder sachliche Verhältnisse, sind nach § 67 SGB X Sozialdaten und unterliegen nach § 35 SGB I dem Sozialgeheimnis. Dazu gehören sowohl die behandelnden Ärzte sowie deren Diagnosen.[1192] Die Sozialdaten sollen einem besonderen, dem Steuergeheimnis vergleichbaren Schutz unterliegen.[1193]

620 Der Arzt ist jedoch keine Stelle i.S.d. § 35 SGB I, was sich z.B. aus § 76 SGB X ergibt, nach dem Daten von Ärzten den Sozialstellen nur zu übermitteln sind, sofern § 203 Abs. 1 StGB dies zulässt. Die Daten i.S.d. Sozialgesetzbücher werden folglich vom Arzt erhoben, nicht aber vom Patienten. Die diesbezüglichen Pflichten treffen damit die Sozialträger. Die Spezialregelungen bezüglich der Pflichten von Daten erhebenden Stellen in §§ 67 ff. SGB X treffen die Ärzte somit nicht.

621 Allerdings sehen die Sozialgesetzbücher gerade **Übermittlungstatbestände** vor: Nach § 295 SGB V sind z.B. für die Abrechnung die Daten bezüglich der Behandlung inklu-

---

1189 Zum Beispiel bei der Verpflichtung, die bei Versicherungsleistungen notwendigen Daten an die Krankenkassen herauszugeben, dazu: *Krauskopf*, in: Laufs/Uhlenbruck, § 36 Rn. 18.

1190 Schönke/Schröder-*Lenckner*, § 203 StGB Rn. 20.

1191 Schönke/Schröder-*Lenckner*, § 203 StGB Rn. 20; unklar bzw. nur auf den objektiven Tatbestand abstellend *Hermeler*, Rechtliche Rahmenbedingungen der Telemedizin, S. 46.

1192 v. Wulffen-*Bieresborn*, § 67 SGB X, Rn. 7 f.

1193 BT-Drucks. 8/4022, S. 80 (96).

sive Diagnose der Krankenkasse zu übermitteln.[1194] Diese Daten sind nicht etwa anonymisiert, sondern werden nach § 295 i.V.m. § 291 Abs. 2 SGB V unter Angabe der Patientendaten der Krankenkasse mitgeteilt. Eine absolute Verschwiegenheit wie beim Anwalt ist demnach gerade nicht gewährleistet, sie wird zugunsten der Sozialträger gelockert.

c) BDSG

622 Das BDSG findet auf die durch Ärzte erhobenen und verarbeiteten Daten Anwendung.[1195] Insofern gelten die zum Umfang der Pflichten von Anwälten gemachten Ausführungen, insbesondere zu § 9 BDSG.[1196] Die **Pflichten des Anhangs zu § 9 BDSG** werden allerdings durch eine **Empfehlung der Bundesärztekammer weiter konkretisiert**.[1197] So ist z.B. die Fernwartung ausgeschlossen. Zielrichtung des Anhangs ist jedoch hauptsächlich der Schutz vor dem direkten Zugriff von Unbefugten vor Ort oder durch unsachgemäßen Transport von Datenträgern. Im Rahmen der Benutzerkontrolle wird empfohlen, keine ständige Verbindung ins Internet zu halten und den Zugang von außen nur dann zu gestatten, wenn die Daten geschützt sind – was entsprechende Sicherungsmaßnahmen impliziert. § 39 BDSG enthält darüber hinausgehende Restriktionen hinsichtlich der Zweckbindung von Daten, die durch Stellen erhoben werden, die einem Berufsgeheimnis unterliegen. Hierzu gehören auch medizinische Daten.[1198]

623 Die Offenbarung von medizinischen Daten ist demnach sowohl **strafrechtlich als auch durch** das **BDSG** selbst **sanktioniert**. Problematisch ist erneut die Kontrolle. Die Aufsicht führen grundsätzlich die Aufsichtsbehörden der Länder. Der Arzt kann sich jedoch auf § 38 Abs. 3 Satz 2 BDSG berufen und die Herausgabe der Patientendaten verweigern. Die Kontrolle ist insofern beschränkt, erfolgt aber dennoch durch die Aufsichtsbehörden. Im Verhältnis zwischen Arzt und Patienten greifen nicht die Bedenken, die für den Anwalt gelten. Während beim Anwalt keine Datenzugriffsbefugnisse bestehen, werden im Rahmen der Sozialgesetzbücher weitreichend Daten unter strenger Zweckbindung übermittelt. Wenn staatliche Stellen die Abrechnung übernehmen und anhand

---

1194 Zu Einzelheiten *Krauskopf*, in: Laufs/Uhlenbruck, § 36 Rn. 18 ff.

1195 *Schlund*, in: Laufs/Uhlenbruck, § 76 Rn. 16; *Hermeler*, Rechtliche Rahmenbedingungen der Telemedizin, S. 55; Quaas/Zuck-*Zuck*, § 2 Rn. 45.

1196 S.o. Rn. 409 ff.; ebenso *Hermeler*, Rechtliche Rahmenbedingungen der Telemedizin, S. 82.

1197 Empfehlungen der Bundesärztekammer zur ärztlichen Schweigepflicht, Datenschutz und Datenverarbeitung in der Arztpraxis, abrufbar unter: http://www.bundesaerztekammer.de/page.asp?his=0.7.47.3228&all=true (zuletzt abgerufen am 06.06.2007).

1198 *Gola*, NJW 1993, 3109 (3115 f.).

der übertragenen Daten auch Kontrollen z.B. zur Abrechnung durchführen dürfen, so ist nicht ersichtlich, warum die staatlichen Aufsichtsbehörden von der Kontrolle ausgeschlossen sein sollten, solange der Schutz der höchstpersönlichen Daten durch das Verweigerungsrecht des Arztes gewährleistet ist.

624 Den Arzt treffen somit die in § 9 BDSG und dem zugehörigen Anhang konkretisierten speziellen Pflichten zur Ergreifung von Sicherungsmaßnahmen. Auf den Verhältnismäßigkeitsgrundsatz nach § 9 Satz 2 BDSG kann er sich nicht bzw. nur sehr eingeschränkt berufen.[1199]

d) Vertragliche Nebenpflichten

625 Patient und Arzt schließen regelmäßig einen Behandlungsvertrag. Das Verhältnis geht zwar über ein reines Vertragsverhältnis hinaus, dennoch ist der Behandlungsvertrag grundsätzlich als Dienstvertrag einzustufen.[1200] Insofern können sich auch hier Nebenpflichten zur Ergreifung von Sicherungsmaßnahmen entsprechend § 241 Abs. 2 BGB ergeben.[1201] Die Pflichten sind aufgrund des besonderen Vertrauensverhältnisses ähnlich denen beim Anwalt ausgestaltet.[1202]

e) Deliktische Haftung

626 Die deliktische Haftung ist zwar im Verhältnis zwischen Arzt und Patient besonders ausgeprägt;[1203] doch spielt sie im Rahmen der IT-Sicherheit keine andere Rolle als etwa bei anderen Berufsgruppen, die mit sensiblen Daten umgehen, so dass insofern auf die Ausführungen zu den Anwaltspflichten verwiesen werden kann.[1204] Allerdings werden aufgrund der stets vorliegenden Verletzung eines der absolut geschützten Rechtsgüter infolge der Heilbehandlung eher die IT-Sicherheitspflichten Eingang finden können in die Gesamtbeurteilung, ob der Arzt seine Verkehrspflichten verletzt hat.

f) Ergebnis

627 Auch der Arzt ist verpflichtet, den Pflichten eines kommerziellen Nutzers nachzukommen. Das besondere Vertrauensverhältnis und die Sensibilität der Daten begründen eine weiter gehende vertragliche Pflicht. Im Rahmen der deliktischen Haftung besteht ebenfalls eine erhöhte Sicherungspflicht.

1199 *Heibey,* in: Roßnagel, Handbuch Datenschutzrecht, Kap. 4.5. Rn. 26.
1200 BGHZ 63, 306 (309); 76, 249 (261); 97, 273; BGH NJW 1981, 613.
1201 Quaas/Zuck-*Zuck*, § 2 Rn. 48; vgl. *Schlund*, in: Laufs/Uhlenbruck, § 77 Rn. 2.
1202 S.o. Rn. 607 f.
1203 Zum deliktischen Arzthaftungsrecht Bamberger/Roth-*Spindler*, § 823 BGB Rn. 585 ff. mwN.
1204 S.o. Rn. 599 ff.

6. Zwischenergebnis: besondere Verantwortlichkeit von Experten und beratenden Berufen

628 Obwohl IT-Sicherheit nicht speziell für beratende Berufe und Experten geregelt ist, können die vorhandenen Regelungskomplexe dennoch ohne weiteres auf diese angewandt werden. Grundsätzlich sind die normierten Sicherungspflichten ausgeprägter, orientieren sich aber zumindest als Mindeststandard an dem für andere kommerzielle IT-Nutzer.

629 Unterschiede ergeben sich jedenfalls bei der vertraglichen und deliktischen Haftung. Aufgrund des besonderen Vertrauensverhältnisses lassen sich einerseits erhöhte vertragliche Nebenpflichten in Form von speziellen Sicherungspflichten und andererseits verschärfte Verkehrssicherungspflichten herleiten.

VI. Pflichten kommerzieller Nutzer – Übersicht

630 Die Pflichten der kommerziellen Nutzer werden wie gezeigt durch verschiedene Normen umschrieben bzw. geregelt. Wie dargestellt existieren teilweise sektorspezifische Regelungen, die bestimmte, bereichsspezifische Anforderungen an kommerzielle Nutzer festlegen. Hinzu können sich Ansprüche aus Deliktsrecht ergeben, sofern die festgelegten Pflichten als Schutzgesetz im Rahmen von § 823 II BGB einzuordnen sind. Schließlich können im Rahmen der Haftung nach § 823 I BGB allgemeine Schutzpflichten bestehen, die mit den Selbstschutzpflichten privater Nutzer spiegelbildlich korrelieren. Dadurch ergibt sich zwangsläufig eine gewisse Zersplitterung der Pflichten abhängig davon, welche tatbestandlichen Voraussetzungen ein kommerzieller Nutzer erfüllt. Um kommerziellen Nutzern eine möglichst kompakte und handhabbare Übersicht über die Pflichten zu geben, müssen demnach die insgesamt übereinstimmenden Pflichten, die Unterschiede sowie das Verhältnis der einschlägigen Normen zueinander bestimmt werden.

631 Dabei ist zu beachten, dass nur die wenigsten gesetzlichen Regelungen überhaupt ausdrücklich IT-spezifischen Inhalt besitzen, also die Konkretisierung auf einzelne Pflichten jeweils das Ergebnis einer Rechtsfortbildung seitens der Rechtsprechung oder durch die Anwendung von Auslegungsregeln ist. Zur Folge hat dies aber auch, dass Pflichten selten ganz konkret benannt werden können bzw. Alternativen nur in Ausnahmefällen tatsächlich ausgeschlossen sind. Vielmehr handelt es sich um „weiche“ Normen, deren Zielsetzung in unterschiedlicher Weise erreicht werden kann und erreicht werden darf, wobei die Anforderungen an das IT-Riskmanagement von den individuellen Faktoren

des jeweiligen Unternehmens wie Art, Umfang, Komplexität und Risikogehalt[1205] des Geschäftsbetriebs abhängen.

1. Betrachtete Normen

632 Im Folgenden soll deshalb übersichtshalber versucht werden, die bisher dargestellten Ergebnisse kompakt zusammenzufassen. In die Übersicht einbezogen werden § 91 Abs. 2 AktG sowie § 43 GmbHG für Unternehmen einer bestimmten Organisationsform, § 25a KWG für Kredit- und Finanzleistungsinstitute, § 33 Abs. 1 WpHG, dessen Adressaten Kreditinstitute und Wertpapierhandelsunternehmen sind, die einschlägigen Normen des Sarbanes-Oxley-Act für in den USA börsennotierte Unternehmen sowie das Datenschutzrecht, insbesondere BDSG und TMG sowie § 109 TKG für Telekommunikationsdiensteanbieter. Etwas außerhalb dieses Systems stehen schließlich die nur mittelbar wirkenden Pflichten, die Basel II impliziert.

2. Gemeinsame Pflichten

633 Am deutlichsten zeigen sich die Gemeinsamkeiten in der Regelungstechnik bei §§ 91 Abs. 2 AktG bzw. 43 GmbHG, 25a KWG sowie 33 Abs. 1 WpHG. Ihnen allen zugrunde liegt eine bestimmte Form des IT-Riskmanagements. Dies beinhaltet jedenfalls eine mindestens rudimentäre **einmalige Risikoanalyse** sowie eine Organisation, die dauerhaft die **Gefahrenerkennung** ermöglicht und **Verantwortlichkeiten** dergestalt festlegt, dass auf Gefahrensituationen angemessen reagiert werden kann. Diese Pflichten lassen sich jedoch auch für das Datenschutzrecht sowie § 109 TKG statuieren.

634 **Kriterien** für die Intensität der Risikoanalyse aber auch die Vorhaltung bzw. den Einsatz von entsprechenden Kapazitäten zur Risikominimierung und -behebung sind insbesondere die Art, der Umfang und die Bedeutung des Einsatzes von EDV für das Unternehmen, eingesetzte Hardware, die Organisation der Datenverarbeitung, Art und Sensitivität der Daten speziell auch im Hinblick auf den Geschäftsbetrieb, sowie die Gefahr der Verletzung von Interessen Dritter.

635 Als **konkrete Maßnahmen** wurden identifiziert:

- Festlegung von Zuständigkeiten,
- Vier-Augen-Prinzip,
- Einmalige Benennung und Bewertung möglicher Risiken (Risikoanalyse),

[1205] So konkretisiert in § 25a Abs. 2 Satz 1 KWG-RefE (2006) zur Umsetzung der MiFID.

- Ergreifung von Maßnahmen zur Risikoabwehr bzw. –minimierung, wobei sich die Konkretisierung insbesondere auch durch die allgemeinen Pflichten ergeben kann,
- Einrichtung eines Systems zur Erkennung von Veränderungen des Systems, also Gefahrerkennung,
- (regelmäßige) Prüfung von verwendeter Software,
- **Dokumentation** des Ergebnisses der Risikoanalyse als Ist-Zustand,
- Dokumentation der getroffenen Maßnahmen z.B. durch entsprechende Checklisten **und** ihrer Durchführung,
- Regelmäßige Datensicherungen und bei Bedarf Vorhaltung von Ersatzkapazitäten bzw. technischer Alternativen zur Bewältigung des Geschäftsbetriebs bzw. Teilen davon, z.B. der Buchhaltung, auch bei Ausfall der Primärsysteme,
- **Kontrolle** aller Maßnahmen durch das Management (insb. nach SOX).

3. Unterschiede

636 Unterschiede zwischen den Pflichten ergeben sich insbesondere im Hinblick auf die Zielrichtung. Während die Pflichten nach AktG und GmbHG Störungen des Geschäftsbetriebs verhindern bzw. beheben können sollen, zielen KWG und WpHG auch und besonders auf die störungsfreie Durchführung der Aufträge ab. Auf der einen Seite steht somit der Schutz des Unternehmens, auf der anderen der Schutz Dritter bzw. weiterer Verfahren wie denen des Finanzverkehrs.

637 Das Datenschutzrecht sowie die Pflichten von Telekommunikationsanbietern haben zudem einen stark technischen Charakter. Ziel ist hier der Schutz der Daten, verlangt werden deshalb **angemessene technische Vorkehrungen**. Daraus lassen sich zwar auch Pflichten in Richtung eines IT-Sicherheitsmanagements ableiten, aber im Vordergrund steht die Erreichung eines technischen Schutzes. Zudem kann nach § 4f BDSG die Bestellung eines Datenschutzbeauftragten erforderlich sein.

638 Eine Sonderstellung hat des Weiteren der **Sarbanes-Oxley-Act**. Er soll insbesondere die korrekte Rechnungslegung sichern (im Einzelnen siehe III.3.a)(3)(b)), fordert aber über die Festlegung von entsprechenden Zuständigkeiten hinaus auch sogenannte Whistleblowing-Verfahren, Audit-Commitees sowie eine interne Revision als Kontrollinstanz der Kontrollverfahren. Insgesamt erweitert der Sarbanes-Oxley-Act durch neue Verfahren den Pflichtenbereich der Unternehmen, ohne jedoch bisherige Verfahren und Methoden in Frage zu stellen.

639 Wesentliche **Widersprüche** hinsichtlich der zu ergreifenden Maßnahmen oder der Kriterien haben sich nicht ergeben, so dass sich Konfliktsituationen nur daraus ergeben können, wie unterschiedliche Intensitäten der normierten Pflichten zu behandeln sind.

4. Anwendbarkeit bzw. Verhältnis der Normen zueinander

640 Anknüpfungspunkt einer Pflicht kann nur die Erfüllung des Tatbestandes der die Pflicht statuierenden Norm sein. Die hier untersuchten Normen haben dabei insbesondere einen unterschiedlichen persönlichen Anwendungsbereich. Grundsätzlich gilt, dass der Betroffene die Pflichten **aller** Normen erfüllen muss, die für ihn gelten. Wer also der Organisationsform nach unter den Anwendungsbereich des AktG bzw. des GmbHG fällt, den können durchaus auch jene Pflichten treffen, die z.B. durch das WpHG zusätzlich zu erfüllen sind. Insofern ist grundsätzlich von einer parallelen Anwendung der Normen auszugehen. Unterscheiden sich die Normen in der Intensität der anzuwendenden Maßnahmen, so ist schwerlich einzusehen, warum nicht die schärferen Maßnahmen ergriffen werden sollen.

641 Das Verhältnis der datenschutzrechtlichen Normen ist ähnlich unkompliziert. Das TMG enthält bereichsspezifische Regelungen, die die Betreiber von Telemediendiensten betreffen.[1206] § 109 TKG wiederum konkretisiert die Verpflichtungen aus dem BDSG,[1207] steht also im Spezialitätsverhältnis zu § 9 BDSG, wobei dessen Anforderungen nicht verdrängt werden.[1208] Somit gilt auch hier, dass jeweils ein Basisschutz gewährleistet werden muss, der durch die weiteren Normen im Rahmen ihres Anwendungsbereichs ergänzt wird. Abgrenzungsschwierigkeiten aufgrund der Konvergenz von Diensten könnten mit Einführung des Telemediengesetzes aufgelöst werden.

5. Ergebnis

642 Kommerziellen Nutzern ist nach diesen Ausführungen zu raten, in jedem Fall die Erfüllung derjenigen Pflichten anzustreben und auch zu dokumentieren, die im Grunde allen hier dargestellten Normen gemein sind. Nicht nur erreichen sie damit bereits einen relativ hohen Grad des technischen Schutzes, zusätzlich wird sichergestellt, dass sie von eventuellen rechtlichen Folgen, die sich für sie ergeben können, profitieren. Wenn also z.B. Haftungserleichterungen oder Erleichterungen für die Beweisführung möglich sind,

---

1206 Spindler/Schmitz/Geis-*Schmitz*, Einf. TDDSG Rn. 1.
1207 Säcker-*Klesczewski*, § 109 TKG Rn. 8.
1208 Scheurle/Mayen-*Zerres*, § 87 TKG aF Rn. 4.

kann die Erfüllung der generellen Handlungspflichten bereits solche Rechtsfolgen in der Regel herbeiführen. Je nachdem, ob spezielle Funktionen erfüllt werden bzw. die Einordnung anhand der genannten Kriterien erhöhte Pflichten bedingt, muss aber auch über die gemeinsamen grundsätzlichen Maßnahmen hinausgegangen werden.

643 Am Anfang jedes Verfahrens steht also die Analyse des eigenen Unternehmens. Dabei sind insbesondere die folgenden Fragen zu beantworten:

- Welcher Art sind eingesetzte IT-Systeme und welchen Umfang hat ihr Einsatz?
- Wie wichtig ist der Einsatz der IT-Systeme für das Gesamtunternehmen, aber auch für einzelne Geschäftsbereiche bzw. Verfahrensabläufe? Als Kontrollfrage könnte der Ausfall eines oder mehrerer Systeme angenommen werden und die Auswirkungen betrachtet werden.
- Was für Daten werden verwendet? Welche Folge hätte ihr Verlust bzw. ihre Veränderung? Welche Geschäftsabläufe wären davon betroffen? Sind Dritte betroffen und wenn ja, in welchem Umfang?
- Wie verhalten sich die Antworten auf diese Fragen zur Gesamtgröße bzw. zur generellen wirtschaftlichen Leistungsfähigkeit des Unternehmens? Da insbesondere Zumutbarkeitsüberlegungen immer nur für den Einzelfall entschieden werden können, spielen auch solch ganz konkrete Gegebenheiten eine wesentliche Rolle. Allerdings können Exkulpationen nur greifen, wenn sich hierfür Anhaltspunkte in der anzuwendenden Norm ergeben; dies betrifft vor allem die allgemeinen haftungsrechtlichen Pflichten. Die Pflichten des AktG, des KWG, WpHG sowie des SOX sind diesen Überlegungen nur bedingt zugänglich.

644 Im Anschluss daran können die beschriebenen Maßnahmen, angefangen mit einer konkreten Risikoanalyse, ergriffen werden, wobei die Beantwortung der vorgeschlagenen Fragen als Indiz für die Intensität und damit auch den zumutbaren wirtschaftlichen und technischen Aufwand gewertet werden darf.

VII. Endergebnis

645 Die IT-Sicherungspflichten ebenso wie die Selbstschutzpflichten hängen erheblich davon ab, welche Tätigkeiten der IT-Nutzer durchführt, ob diese rein privater oder kommerzieller Natur sind. Ein Sonderwissen des IT-Nutzers, dass dieser im Rahmen seiner gewerblichen Tätigkeit gewonnen hat, muss diesem bei einer privaten Tätigkeit zugerechnet werden, sofern der IT-Nutzer auch außerhalb seiner gewerblichen Tätigkeit die Möglichkeit hat, auf die entsprechenden Ressourcen zuzugreifen, was bei Arbeitnehmern differenziert zu beurteilen ist. Generell sind kommerzielle IT-Nutzer zu wesentlich höheren Sicherungen verpflichtet als private IT-Nutzer.

646 Für **private Nutzer** bestehen jetzigen Zeitpunkt nur eingeschränkte Sicherungspflichten zum: Mangels ausreichender Bekanntheit von Problem und Lösung sind diese lediglich zum Einsatz von Virenscannern sowie zu entsprechenden Aktualisierungen verpflichtet. Im Bereich der Schadensminderungs- und Selbstschutzpflichten können die Grundsätze des Dialer-Urteils des BGH angewandt werden, indem private IT-Nutzer nicht routinemäßig ihre Systeme auf Dialer ohne besondere Verdachtsmomente überprüfen müssen und ihnen nicht die Überwachung des Aufbaus von Verbindungen ins Internet obliegt.[1209] Übertragen auf IT-Sicherungen entfällt jedenfalls derzeit zumindest bei privaten Softwarenutzern, und solange Bedrohungspotentiale nicht generell bekannt und einfach zu meistern sind, die Pflicht zu Selbstschutzmaßnahmen.

647 Bei **kommerziellen Nutzern** sind zunächst die gesellschaftsrechtlichen Anforderungen an IT-Nutzer im Rahmen des Risikomanagements zu berücksichtigen. Im Zuge der weiteren Ausdifferenzierung der von verschiedenen Seiten vorgegebenen Standards (ISO 27001, BSI-Grundschutzhandbuch, MaRisk etc.) müssen die kommerziellen IT-Nutzer höhere Aufwendungen im Bereich der Datenerfassung und –auswertung tätigen, um für ein robustes und effizientes internes Risikoerkennungssystem zu sorgen. Ferner müssen die kommerziellen Nutzer, abhängig auch von der Größe ihrer IT-Infrastruktur, Maßnahmen zur Sicherung ihrer IT-Systeme ergreifen. Dazu gehören die primäre Abwehr, die sekundäre Überprüfung durch Suchprogramme sowie die notwendige Aktualisierung der Programme. Welche Rolle indes diese IT-Standards im Rahmen dieser Pflichten spielen können, ist bislang weitgehend ungeklärt.

648 Dies gilt auch für die mittelbaren IT-Sicherungspflichten, denen Unternehmen infolge der durch die neuen Fremdkapitalvergabevorschriften nach Basel II unterliegen; auch hier werden zwar die genannten IT-Standards berücksichtigt, doch ohne dass bislang deren rechtlicher Stellenwert völlig geklärt wäre.

649 Besonderen Pflichten unterliegen schließlich einige Wirtschaftssektoren und Berufe, denen entweder eine besonders hohe volkswirtschaftliche Bedeutung zukommt (Banken, Finanzsektor) oder bei denen eine besonders intensive Vertrauensbeziehung zu den Kunden bestehen, wie etwa Anwälte, Steuerberater und Ärzte. Bei Letzteren lassen sich insbesondere aufgrund des besonderen Vertrauensverhältnisses erhöhte vertragliche

---

1209 BGH NJW 2004, 1590 (1592) = JZ 2004, 1124 (1127) m. Anm. *Spindler*.

Nebenpflichten in Form von speziellen Sicherungspflichten und andererseits verschärfte Verkehrssicherungspflichten herleiten.

650 Allerdings muss der Nutzer, insbesondere der kommerzielle, bei Programmen mit bekannten Sicherheitslücken dieses Programm sperren und darf es nicht mehr einsetzen. Benutzt er es dennoch sehenden Auges und entstehen hierdurch aufgrund von Hackerangriffen Schäden, kann sich, wie soeben erörtert, ein völliger Ausschluss des Schadensersatzanspruchs ergeben.

E. Verantwortlichkeit von IT-Intermediären

I. Überblick

651 Quasi zwischen IT-Hersteller und IT-Nutzer stehen die IT-Intermediäre, die gerade über elektronische Kommunikationsnetze Dienstleistungen erbringen. Die Anwendungsgebiete reichen von der Bereithaltung von elektronischen Plattformen für fremde Inhalte (Host-Provider), über die Zugänglichmachung elektronischer Netze (Access-Provider) bis hin zu verschiedensten Mehrwertdiensten, die über elektronische Netze angeboten werden, etwa sogenannten Web-Services, die es Unternehmen erlauben, mit Hilfe von Dritten spezifische Funktionen, wie den Einkauf und das electronic invoicing, auszulagern und über elektronische Kommunikationsnetze (wieder mit Hilfe von IT-Intermediären) abzuwickeln. Letzteres überlappt sich stark mit kommerziellen IT-Nutzern, die ihrerseits IT-Dienstleistungen erbringen, so dass diesbezüglich auf das entsprechende Kapitel verwiesen wird.

652 IT-Intermediäre können ebenso wie andere IT-Nutzer zahlreichen Gefahren ausgesetzt sein, die sich auf ihre IT-Nutzer durchschlagen können. Zahlreiche für kommerzielle IT-Nutzer beschriebene Szenarien (o. Rn. 584 ff.) sind mutatis mutandis auf IT-Intermediäre ohne Weiteres anwendbar, da sie häufig die IT-Infrastrukturen gerade für Unternehmen zur Verfügung stellen, die selbst diese Infrastrukturen nicht vorhalten wollen (Outsourcing). Als Beispiel seien etwa die Zurverfügungstellung von Web-Plattformen im elektronischen Handel für andere IT-Unternehmen oder Banken erwähnt, die mit Hilfe der IT-Dienstleistungen der Intermediäre ihre eigentlichen Dienstleistungen (Banking, Handel) etc. anbieten und abwickeln können.

653 Demgemäß greifen für IT-Intermediäre zahlreiche Pflichten in ähnlicher Weise wie für kommerzielle IT-Nutzer ein, allerdings modifiziert durch ihre jeweilige Funktion und durch eingreifende besondere **Haftungsprivilegierungen** zu ihren Gunsten, die ihr

Verantwortlichkeitsrisiko sowohl straf- als auch zivilrechtlich teilweise signifikant reduzieren. Dies gilt insbesondere für alle Anbieter von Leistungen, die gleichzeitig als Telekommunikationsdienstleistungen qualifiziert werden können, da hier die Haftungsbegrenzung nach § 44a TKG (eingefügt durch die jüngste **Reform des TKG**[1210] als Nachfolger der TKV aF) eingreift, wonach für Vermögensschäden die Haftung insgesamt auf 12.500 Euro beschränkt ist – im Gegensatz zum sonstigen Zivilrecht –, selbst bei grober Fahrlässigkeit. Begründet wird die Haftungsbegrenzung mit den kaum abschätzbaren wirtschaftlichen Risiken, die sich bei einem Verzicht auf eine Haftungshöchstgrenze ergeben könnten.[1211] Unerheblich für die Haftungsbegrenzung ist die Entstehungsgeschichte und der Rechtsgrund des Schadensersatzanspruchs.[1212] Allerdings gilt sie ausdrücklich nur für (primäre) Vermögensschäden, zu denen nach der Begründung des Verordnungsentwurfs[1213] Folgeschäden aus Sach- oder Personenschäden nicht zählen.[1214] Ferner kann § 44a TKG nicht für Schäden Dritter eingreifen, die keine vertragliche Beziehung zu dem Telekommunikationsunternehmen haben. Der Anwendungsbereich der §§ 43a ff. (Teil 3) beschränkt sich auf „Kunden“. Kunden sind nach der Legaldefition des § 1 I TKV aF, die nach der Ratio aber auch für das neue TKG genutzt werden kann, Personen, die Telekommunikationsdienstleistungen vertraglich in Anspruch nehmen oder begehren. Die Anwendbarkeit der §§ 43a ff. TKG auf Kunden ergibt sich zum einen aus der Teilbereichsüberschrift „Kundenschutz“ des Teil 3 TKG und zum anderen aus der Formulierung Endnutzer in § 44a TKG, womit aber lediglich Kunden gemeint sind.[1215] Diese Annahme entspricht auch der Tatsache, dass § 44a TKG im Wesentlichen dem § 7 Abs. 2 TKV aF entspricht. Die Telekommunikations-Kundenschutzverordnung, die nach § 1 Abs. 1 TKV aF auch nur auf Kunden anwendbar war, wurde jüngst durch das TK-Änderungsgesetz in Teil 3 des TKG integriert. Bei den meisten Schäden für Unternehmen oder andere IT-Nutzer durch Dienstleistungen von IT-Intermediären werden die Betroffenen jedoch vertragliche Beziehungen zu diesen unterhalten, etwa bei beim Hosting von Daten auf einem Web-Server oder der Zurverfügungstellung von Portalen, so dass oftmals die §§ 44a ff. TKG eingreifen können.

1210 S. Bundesgesetzblatt Teil 1 Nr. 5 vom 23.2.2007, S. 106 ff.

1211 BR-Drucks. 551/97, S. 28.

1212 BT-Drucks. 15/5213, S. 21; Beck`scher TKG-Kommentar-*Dahlke*, § 44a TKG-E Rn. 9; Scheurle/Mayer-*Schadow*, § 41 TKG Rn. 51.

1213 BR-Drucks. 551/97, S. 28 f.

1214 Zur Abgrenzung des reinen Vermögensschadens von anderen Folgeschäden vgl. nur Palandt-*Heinrichs*, vor § 249 BGB Rn. 8 ff. mwN.

1215 Beck`scher TKG-Kommentar-*Schütz*, § 3 Nr. 8 TKG Rn. 25.

654 Gegenüber der bislang geltenden TKV enthält § 44a TKG jedoch auch etliche Verbesserungen für den Geschädigten: Anders als in § 7 TKV aF entfällt in § 44a TKG die individuelle Haftungsbegrenzung zugunsten einer nur insgesamt wirkenden Haftungsbegrenzung, allerdings wie bisher auch für alle – selbst grob fahrlässig herbeigeführten – Vermögensschäden. Begründet wird dies von der Bundesregierung damit, dass „das Entfallen der individuellen Haftungsbeschränkung zu einer Besserstellung der Geschädigten in den Fällen (führe), in denen nur wenige von einer Schädigung betroffen sind. Damit wird in vielen Fällen vermieden, dass Ersatzansprüche selbst dann begrenzt werden, wenn ein Anbieter den von ihm verursachten Schaden tatsächlich ohne Not tragen kann, der jedoch für den Geschädigten - z.B. bei Datenverlusten - eine die wirtschaftliche Existenz bedrohende Dimension haben kann.“[1216]

655 Die Pflichtenstellung der IT-Intermediäre leitet über zu der Frage, welche Gemeinsamkeiten und Unterschiede zwischen der deliktischen Haftung und einer Haftung für Dienstleistungen (noch) bestehen. Ohne hier auf Details eingehen zu können,[1217] sind die grundsätzlichen Unterschiede noch einmal ins Gedächtnis zu rufen:

- die deliktische Haftung greift gegenüber jedermann, die vertragliche nur gegenüber dem Vertragspartner und den in den Schutzbereich einbezogenen Dritten (deren Kreis von der Rechtsprechung allerdings teilweise erheblich ausgedehnt wird),
- die deliktische Haftung ist weitgehend von der Verletzung bestimmter Rechtsgütern abhängig, indem insbesondere Vermögensschäden nicht erfasst werden, im Gegensatz zur vertraglichen Haftung,
- die deliktische Haftung erfasst nur das Integritätsinteresse, nicht das Äquivalenzinteresse
- Unterschiede bestehen ferner nach wie vor bei der Verjährung, trotz der Harmonisierung in der Schuldrechtsreform durch § 199 BGB, da die vertragliche Haftung hinsichtlich des Verjährungsbeginns nach wie vor von einem objektiven System ausgeht.

656 Tendenziell ist daher das nach wie vor größte Risiko beim IT-Einsatz, der Vermögensschaden und insbesondere der Betriebsausfallschaden, nicht von der deliktischen Haftung erfasst, sondern nur von der vertraglichen Haftung. Aber auch hier zeichnen sich Konvergenzen ab, indem zum einen vertragliche Haftungseingrenzungen für Vermögensschäden, teilweise sogar gesetzliche Haftungsbeschränkungen wie im TKG, zugelassen werden, zum anderen die Reichweite des Rechtsgüterschutzes in § 823 I BGB ausgedehnt wird auf Funktionalitäten des Eigentums.

1216 Begr RegE BT-Drucks. 16/2581 zu § 44a TKG, S. 24.

1217 S. dazu *Wendehorst,* AcP 206 (2006), 205 ff.

657 Für die Anwendung der Verantwortlichkeitsprivilegierungen müssen die verschiedenen Risiken für IT-Intermediäre unterschieden werden:

- Zum einen kann der IT-Intermediär selbst Opfer eines IT-Angriffs werden, etwa durch eine Denial-of-Access-Attacke oder das Hacken in das System mit der Folge der Datenausspähung oder Sabotage etc. Anders ausgedrückt ist die Sicherheit des IT-Systems des Intermediärs selbst betroffen, von ihm selbst geht die Gefahr für Dritte aus. In diesem Fall finden die allgemeinen Verkehrspflichten, je nach Funktion modifiziert, Anwendung.

- Zum anderen können Intermediäre in die Verantwortung genommen werden können, wenn sie als Zwischenstelle für Daten agieren, die anschließend beim Nutzer einen Schaden hervorrufen. Der Intermediär stellt also auch nicht mittelbar diese Daten selbst bereit, sondern leitet diese nur in irgendeiner Form weiter, wobei sich die Frage stellt, ob ihn eine Prüfungspflicht hinsichtlich der Gefährlichkeit der Daten trifft. Typisches Beispiel ist die Weiterleitung von virenbefallenen E-Mails an andere Nutzer (Rn. 295 ff.).

658 Unterschieden wird in diesem Zusammenhang gern zwischen Content-, Host- und Access-Provider – auch wenn diese Unterscheidung eher heuristischen Wert hat, da das Gesetz nicht auf diese Begriffe abstellt. Als Content-Provider wird bezeichnet, wer eigene Informationen zur Nutzung im Netz bereithält.[1218] Host-Provider ist, wer fremde Inhalte zum Abruf bereithält.[1219] Der Host-Provider stellt also seinen Kunden nur Speicherplatz bzw. eine Plattform zur Verfügung, den diese mit eigenen Inhalten füllen können. Access-Provider ist derjenige, der technisch den Zugang zum Netz bzw. die Einwahl ins Internet ermöglicht.[1220]

II. Sicherungspflichten der IT-Intermediäre für ihre eigenen Systeme

659 Grundsätzlich ist der IT-Intermediär ein kommerzieller Nutzer von Informationstechnik. Anknüpfungspunkt für Sicherungspflichten ist auch hier die Beherrschung seiner eigenen Systeme als Gefahrenquelle, allerdings auch kombiniert mit Schutzpflichten, da er in aller Regel direkten Zugriff auf alle Daten hat, aber auch der einzige ist, der die Daten Dritter (seiner Vertragspartner etc.) schützen kann:

660 Anders als bei den Verantwortlichkeitsprivilegierungen nach §§ 7 ff. TMG, deren Rechtsgrund die Unmöglichkeit einer Kontrolle durch die schiere Datenmenge und ent-

1218 *Sessinghaus*, WRP 2005, 697.
1219 *Stadler*, Haftung für Informationen im Internet, Rn. 10; *Sessinghaus*, WRP 2005, 697.
1220 *Stadler*, Haftung für Informationen im Internet, Rn. 11.

gegenstehende Rechte bildet,[1221] kann dieser Gedanke für die Sicherungen des eigenen Systems nicht verfangen, wie § 7 Abs. 1 TMG schon für eigene Informationen klarstellt. Die Haftungsmodifizierungen der §§ 8 - 10 TMG finden hier nur eingeschränkt Anwendung, da sie nur die Haftung für *Inhalte* betreffen, nicht aber die Haftung für die *Funktionstüchtigkeit* und die *Sicherheit* der vom Service Provider angebotenen Dienste.[1222] Hier muss differenziert werden:

661 Wird die Datei eines Nutzers durch einen Virus infiziert, der sich in einer Datei (bzw. Information) befand, die ein Dritter auf den Rechnern des Providers abgespeichert hat, findet § 10 TMG im Prinzip Anwendung – sofern es sich bei dem Dritten wiederum um einen Nutzer handelt, der berechtigterweise auf den Rechnern des Providers Dateien speichern durfte. Handelt es sich dagegen um einen „Hacker", der sich unberechtigterweise Zugang zu den Rechnern des Providers verschafft hat, kann § 10 TMG nicht eingreifen, da § 10 TMG nicht generell jede Verkehrssicherungsmaßnahme des Providers ausschalten will. Im Falle von Access Providern greift dagegen § 8 TMG ein, wenn der Virus sich in einer weitergeleiteten Datei befand, nicht dagegen, wenn der „Hacker" sich Zugang zu dem System des Providers verschafft hat. Werden die Daten und Informationen daher erst beim Intermediär schadhaft, so kann ihn grundsätzlich eine Haftung aus der Verletzung von Sicherungspflichten treffen.[1223] Es greifen die allgemeinen Haftungsnormen ein, sei es Vertrags- oder Deliktsrecht.[1224] Ungeachtet der Haftungsprivilegierungen werden jedoch aufgrund der oftmals vorhandenen vertraglichen Beziehungen über die deliktisch geschützten Rechtsgüter hinaus auch Vermögensschäden erfasst, da eine Verletzung von Sicherungspflichten gleichzeitig eine Vertragsverletzung impliziert (§ 280 Abs. 1 BGB). Sicherungspflichten der Provider werden in aller Regel zu den freizeichnungsfesten Kardinalpflichten gehören, so dass die §§ 8-10 TMG hier auch keine Leitbildfunktion im Sinne von § 307 Abs. 1 BGB entfalten.

1. Vertragliche Verantwortlichkeit

662 Für Schadensersatzansprüche des Vertragspartners gegen seinen IT-Intermediär sind zunächst die jeweils abgeschlossenen vertraglichen Bestimmungen maßgeblich, sei es

---

1221 Erwägungsgrund Nr. 42 ECRL; Spindler/Schmitz/Geis-*Spindler*, vor § 8 TDG Rn. 11.

1222 Anders offenbar *Schneider*/*Günther*, CR 1997, 389 (391), die Haftungseinschränkungen nach TDG/MDStV – ohne nähere Begründung – auch bei virenverseuchten Online-Diensten annehmen.

1223 Spindler/Schmitz/Geis-*Spindler*, vor § 8 TDG Rn. 25; *Koch*, NJW 2004, 801 (805 f.); *Pelz*, in: Bräutigam/Leupold, Kap. B I Rn. 72; *Dustmann*, Die privilegierten Provider, 136 f.; *Podehl*, MMR 2001, 17 (21); *Schwarz/Poll*, JurPC 73/2003, Rn. 72.

1224 Spindler/Schmitz/Geis-*Spindler*, § 8 TDG Rn. 10; i.E. ebenso *Christiansen*, MMR 2004, 185 (186).

der Vertrag über den Internetzugang, über die Nutzung der vom Provider angebotenen Dienste oder das Webhosting. Allgemeine Aussagen über die Verantwortlichkeit lassen sich hier aus Raumgründen kaum treffen, da die Verträge völlig unterschiedliche Leistungsinhalte haben und damit auch unterschiedlichen gesetzlichen Leitbilder folgen können, etwa das Webhosting dem Mietvertrag[1225] oder das Access-Providing dem Dienstvertrag[1226]. Darüber hinaus können Leistungsbeschreibungen in den AGB der IT-Intermediäre ebenso eine Rolle spielen wie die Anwendbarkeit des TKG.[1227]

663 Weitestgehend gemein ist jedoch allen Vertragstypen, dass sie Schutzpflichten für den Vertragspartner als Nebenpflichten vorsehen. Diese können auch nur in sehr eingeschränktem Maße durch Allgemeine Geschäftsbedingungen ausgeschlossen werden, da sie oftmals zwar selbst keine Hauptleistungspflicht darstellen, aber für die Erbringung der Hauptleistung des Vertrages doch so wesentlich sind, dass sie als sog. Kardinalpflichten bezeichnet werden können. Anders formuliert nützt dem Kunden die Erbringung einer Speicherleistung nichts, wenn der entsprechende Server in keinster Weise gegenüber unbefugten Zugriffen Dritter geschützt ist. Derartige Kardinalpflichten sind indes gemäß § 307 Abs. 2 Nr. 2 BGB freizeichnungsfest.[1228] Dieser Pflichtenkanon ist häufig weitgehend ähnlich den deliktischen Sicherungspflichten, wenngleich er auch nicht an bestimmte Rechtsgutsverletzungen allein anknüpft. Hinzu können im Einzelfall Pflichten zur Information über Gefahren oder Abwehr der Gefahren kommen. Des Weiteren kann als Nebenpflicht auch die Sicherung der Daten des Kunden bestehen.[1229] Dies befreit natürlich die Nutzer umgekehrt nicht von der Pflicht der eigenen regelmäßigen Datensicherung.[1230] Im Einzelfall kann vom Website-Host auch die Vorhaltung redundanter Hardware verlangt werden,[1231] z.B. eines gespiegelten Servers, etwa wenn

---

1225 *Schuppert*, in: Spindler, Vertragsrecht der Internet-Provider IV, Rn. 47; *Cichon*. Internetverträge, Rn. 182 f., 184 ff.

1226 BGH CR 2005, 816 (817) (obiter dictum); ausführlich *Spindler*, in: Spindler, Vertragsrecht der Internet-Provider IV, Rn. 93.

1227 Näher dazu *Spindler*, in: Spindler, Vertragsrecht der Internet-Provider IV, Rn. 21 ff.

1228 St.Rspr. BGH NJW 1993, 335; BGH NJW-RR 1993, 560 (561); BGH NJW 2002, 673 (674); zuletzt BGH NJW-RR 2005, 1496 (1505 ff.), wonach der Verwender von AGB sich nicht darauf beschränken dürfe, die Verletzung von Kardinalpflichten von der Haftungsfreizeichnung auszunehmen. Er müsse zwar die Kardinalspflichten nicht abschließend in der Klausel aufzählen, jedoch den Begriff zumindest abstrakt erläutern, um die Unwirksamkeit seiner Freizeichnungsklausel wegen Verstoßes gegen das Transparenzgebot (§ 307 I 2 BGB) zu vermeiden.

1229 Vgl. *Komarnicki*, in: Hoeren/Sieber, Teil 12 Rn. 73; *Czychowski*, in: Bröcker/Czychowski/Schäfer, § 13 Rn. 107.

1230 Zur Pflicht, Datensicherungen durchzuführen, s. OLG Karlsruhe CR 1996, 346 f.; OLG Karlsruhe NJW 1996, 200 (201); BGH NJW 1996, 2924 (2926) – Optikprogramm, wonach Datensicherung eine „Selbstverständlichkeit“ sei.

1231 *Schuppert*, in: Spindler, Vertragsrecht der Internet-Provider, Teil V Rn. 66.

bereits nach der vertraglichen Vereinbarung die hohe Sensibilität der Daten deutlich wird. Dies kann z.B. die Information über zuverlässige Abwehrprogramme sowie ihre Einrichtung umfassen.

2. Vertragsähnliche Ansprüche

664 Bislang nicht erörtert ist die Frage, ob der Nutzer vertragsähnliche Ansprüche gegen Betreiber von Rechnern hat, die nicht in das Vertragsverhältnis zwischen Nutzer und Provider eingeschaltet sind. Vor allem Ansprüche aus Vertrag mit Schutzwirkung zugunsten Dritter können hier zugunsten des Nutzers eingreifen, etwa wenn der Host Provider mit einem Content Provider Verträge über die Bereitstellung von Inhalten getroffen hat und durch mangelnde Sicherheitsvorkehrungen des Content Providers (Hacker, Virenbefall etc.) Schäden beim Nutzer eintreten. Aber auch Verträge zwischen Access- und Host Provider – soweit nicht bereits miteinander identisch – über die Bereitstellung von Speicherkapazitäten, der Weiterleitung von Daten etc. können grundsätzlich als Anknüpfungspunkt für Schutzpflichten gegenüber Dritten herangezogen werden. Von praktischer Bedeutung ist die Frage von Ansprüchen aus Verträgen mit Schutzwirkung zugunsten Dritter vor allem wegen der bekannten Unterschiede zum Deliktsrecht, insbesondere der nicht möglichen Entlastung für Erfüllungsgehilfen (§ 278 BGB) und der Erfassung von reinen Vermögensschäden.

665 In der Regel dürften die Voraussetzungen für derartige Ansprüche nicht gegeben sein. Denn Leitbild des Vertrages mit Schutzwirkung zugunsten Dritter ist (bislang), dass der Schuldner bei Vertragsabschluss damit rechnen kann, dass Dritte auf Seiten des Gläubigers in den Bereich des Vertrages einbezogen werden, wie etwa im Mietrecht.[1232] Erforderlich ist daher eine gewisse Überschaubarkeit derjenigen, die in den Genuss der Schutzpflichten des Vertrages kommen, nicht zuletzt damit der Schuldner seine Risiken kalkulieren kann. Zwar sind Aufweichungstendenzen in der Rechtsprechung feststellbar, etwa bei Überweisungsaufträgen im Mehr-Banken-Verkehr,[1233] doch handelt es sich hier in der Regel um bereichsspezifische Ausnahmen, die Risiken für den Kunden überwinden helfen sollen, die allein aufgrund der arbeitsteiligen Erledigung der Aufträge entstehen.

1232 S. nur Palandt-*Grüneberg*, § 328 BGB Rn. 16 ff. mwN.; MünchKommBGB-*Gottwald*, § 328 BGB Rn. 117, 154.

1233 OLG Frankfurt WM 1984, 726; für Lastschriften BGH WM 1985, 1391.

666 **Auf das Internet sind solche Überlegungen nicht übertragbar:** Denn zum einen ist bei Vertragsabschluss zwischen Providern untereinander in der Regel überhaupt nicht vorhersehbar, wie viele Nutzer auf Seiten eines Providers in den Vertrag einbezogen werden, woher diese stammen und welche Schutzmaßnahmen insbesondere bei diesem Personenkreis erforderlich wären. Das Risiko für den Provider, selbst für Vermögensschäden zu haften, wäre kaum mehr kalkulierbar. Zum anderen stellt sich die Tätigkeit der Provider im Internet für den Nutzer nicht als einheitlicher Vorgang dar, dessen besondere Risiken aus der Arbeitsteilung nicht auf den Nutzer überwälzt werden dürften. Stattdessen handelt es sich um jeweils spezifische Dienstleistungen im Internet, die miteinander verwoben sind, die aber keine Ähnlichkeit etwa mit einer Überweisungskette im Inter-Banken-Verkehr aufweisen.

667 Darüber hinaus mangelt es im Bereich der Übermittlung von Daten im Internet sogar häufig an jeglichen Vertragsbeziehungen, etwa für das Routing zwischen verschiedenen Rechnern. Hier versagen von vornherein alle Konstruktionen über vertragsähnliche Ansprüche.

3. Deliktische Verantwortlichkeit

668 Wendet man sich den deliktischen Pflichten (bzw. den Sicherungspflichten allgemein) der IT-Intermediäre zu, lassen sich drei Bereiche des Schutzes des Nutzers und anderer Internet-Teilnehmer unterscheiden:

- der Schutz des Eigentums, insbesondere an Daten,
- der Schutz der Privat- und Intimsphäre,
- der Schutz des Rechts am eingerichteten und ausgeübten Gewerbebetrieb.

669 Grundlage der Beurteilung ist auch hier eine Abwägung zwischen dem bestehenden Risiko sowie der wirtschaftlichen Zumutbarkeit der Ergreifung von Sicherungsmaßnahmen. Im Rahmen der wirtschaftlichen Zumutbarkeit ist Raum für eine konkrete Einzelfallbetrachtung, die auch die Umstände der Leistungserbringung einzubeziehen hat, einschließlich der Frage, welchen Preis ein Nutzer für einen Dienst aufbringt.[1234]

670 Dennoch können Intermediäre keinesfalls von den Privilegierungen für private Nutzer im Rahmen der allgemeinen Haftung profitieren: Denn aufgrund der **Multiplikations-**

[1234] BGH NJW 1990, 906 (907) - Pferdeboxen; BGH NJW 1990, 908 (909) - Weinkorken; Bamberger/Roth-*Spindler*, § 823 BGB Rn. 486; MünchKommBGB-*Wagner*, § 823 BGB Rn. 576; *Foerste*, in: v. Westphalen, ProdHaftHdb, § 24 Rn. 10, 48.

wirkung und -funktion der Intermediäre, und dies betrifft sowohl Host- als auch Access-Provider, besteht ein stark erhöhtes Risiko, etwa durch die schnelle Verbreitung von Gefahren. Andererseits sind Intermediäre für die Bereitstellung der Kommunikationsinfrastruktur essentiell, so dass an ihnen und ihren Diensten ein starkes öffentliches Interesse besteht.[1235] Ingesamt verschiebt sich die Beurteilung der Pflichten von Intermediären fast vollständig hin zur Beurteilung der Zumutbarkeit der Ergreifung von Sicherungsmaßnahmen, da sie die Gefahrenquelle tatsächlich beherrschen können, aber auch unabdingbar für die modernen Kommunikationstechnologien und neuen Dienste sind. Des Weiteren verfügen zumindest die Access-Provider in aller Regel über Expertenkenntnisse bzw. entsprechendes Personal, das auch die Beobachtung und Überwachung neuer Gefahrenpotentiale und -lösungen bewältigen kann.

671 Häufig sind Intermediäre allerdings auch nur Nutzer des Dienstangebots anderer Intermediäre. So verwendet der Host-Provider häufig die Dienste eines anderen Host-Providers, meist teilen sich mehrere eine Computeranlage, die teilweise vermietet wird. Hier treffen den Intermediär nur insoweit Pflichten, als er tatsächlich Zugriff hat und die Gefahrenquelle damit beherrscht.

a) Vernichtung von Daten des Nutzers

672 Das Eigentum eines Nutzers kann außerhalb des Bereichs der Übertragung von Inhalten, zu denen – wie oben dargelegt (Rn. 108 ff.) – grundsätzlich auch Software zählt, insbesondere dann verletzt sein, wenn sein Datenbestand durch einen „Angriff aus dem Netz“, etwa durch Viren, vernichtet oder jedenfalls teilweise beschädigt wird. Wie bereits dargelegt (Rn. 108 ff.), spricht hierfür, dass das Eigentum in der neueren Rechtsprechung des BGH auch im Hinblick auf seine Funktionsfähigkeit definiert wird,[1236] so dass auch Daten auf Festplatten oder Arbeitsspeichern etc. als möglicher Inhalt des Eigentums bzw. der Funktionsfähigkeit des Speichermediums angesehen werden können (ausführlich oben Rn. 109).[1237] Auch im Werkvertragsrecht betrachtet der BGH den

---

1235 Zu parallelen Überlegungen im Rahmen der Interessenabwägungen bei Sperrverfügungen gegenüber IT-Intermediären/Providern s. OVG Münster MMR 2003, 348 ff.; *Spindler/Volkmann*, K&R 2002, 398 ff.; Spindler/Schmitz/Geis -*Spindler*, § 8 TDG Rn. 41, § 9 Rn. 41 ff.

1236 Leitentscheidung: BGHZ 55, 153 - Fleet-Fall; wesentlich weitergehender *Boecken*, Deliktsrechtlicher Eigentumsschutz gegen reine Nutzungsbeschränkungen, S. 122 ff., 160 ff.

1237 Ebenso im Ergebnis OLG Karlsruhe NJW 1996, 200 (201); *Taeger*, Außervertragliche Haftung für fehlerhafte Computerprogramme, S. 261 unter Berufung auf BGHZ 76, 216 (220) für Sachgesamtheiten, „die gerade durch ihre Vollständigkeit und Ordnung einen Wert repräsentieren, der nicht nur der Summe der Werte der darin zusammengefassten Einzelsachen entspricht, sondern diese oft übersteigt (bspw. Briefmarkensammlungen, Bibliotheken, Fachmuseen etc.). Wird eine solche Sacheinheit durch eine unerlaubte physische Handlung zerstört (...), dann handelt es sich gleichfalls um einen Angriff auf das Eigen-

Verlust des Datenbestandes aufgrund einer fehlerhaften Sicherung als mögliche Verletzung eines „selbständigen, vermögenswerten Gutes“.[1238] Der Virenbefall über die Plattform des IT-Intermediärs oder andere Arten von Angriffen, die zur Vernichtung von Daten des Nutzers auf seinem Rechner führen, z.B. während eines offenen Kommunikationsvorgang mit dem IT-Intermediär, sind daher grundsätzlich geeignet, einen Anspruch aus § 823 Abs. 1 BGB zu begründen.

673 Sind indes Daten des Nutzers zerstört worden, die **auf dem Server des Providers abgelegt worden** sind, scheidet eine Eigentumsverletzung zu Lasten des Nutzers aus, da die Verkörperung der Daten eben nicht auf Eigentum des Nutzers – seiner Festplatte –, sondern auf dem Eigentum des Providers erfolgt. In Betracht kommen daher nur vertragliche Schadensersatzansprüche gegenüber dem Provider; hier kann indes wieder die Haftungsprivilegierung des § 44a TKG, sofern der Provider als Telekommunikationsanbieter agiert hat, zur Geltung kommen, soweit die Schadensursache in der technischen-organisatorischen Seite der Telekommunikation lag.[1239]

(1) Haftung von Host Providern

674 Entscheidend für die Haftung des IT-Intermediärs, insbesondere Host Providers ist daher, ob und gegebenenfalls wie weit er Verkehrspflichten zum Schutz des Eigentums des Nutzers unterliegt. Abgesehen von den vertraglichen Pflichten des Host Providers gegenüber dem Nutzer[1240] ist er verpflichtet, diejenigen Daten, die in seiner Einflusssphäre liegen, auf Virenbefall zu kontrollieren. In diesem Sinne trifft den Provider jedenfalls die Pflicht, grundlegende Anforderungen an die Sicherheit seiner Rechner und der dort gespeicherten Daten seiner Kunden gegenüber Ausspähversuchen oder Missbräuchen seitens Dritter einhalten.[1241] Da der Host Provider eine Gefahrenquelle betreibt, können die Überlegungen zu den Verkehrspflichten hinsichtlich der erforderlichen Abwehr von Viren, wie sie für die Produkthaftung entwickelt wurden (Rn. 150 ff.), und Angriffen aus dem Netz, aber auch hinsichtlich anderer technischer

---

tum, bei dem der deliktische Eigentumsschutz des § 823 Abs. 1 BGB eingreifen muss (...)“; *Wuermeling*, CR 1994, 585 (590); *Hoeren*, PHI 1989, 138 (141); *Meier/Wehlau*, NJW 1998, 1585 (1587 f.); offen gelassen *Koch*, BB 1996, 2049 (2057); offen *Schneider*/*Günther*, CR 1997, 389 (392 f.); abl. LG Konstanz, CR 1997, 84; ebenso *Ertl*, CR 1998, 179 (182).

1238 BGH NJW 1996, 2924 (2926) – Optikprogramm.

1239 Vgl. zur Abgrenzung der Anwendungsbereiche von TKG und TDG bei Access-Providern Spindler/Schmitz/Geis-*Spindler*, § 2 TDG Rn. 26.

1240 Dazu aus schweizerischer Sicht *Briner*, in: Hilty, Information Highway, S. 489 (511 f.).

1241 *Schmitz*/*v.Netzer*, in: Schuster, Vertragshandbuch Telemedia, Kap. 12 Rz. 21 f.; zurückhaltender wohl *Komarnicki*, in: Hoeren/Sieber, 12 Rz. 72: in der Regel nur gegen zusätzliche Vergütung.

Sicherungspflichten, hier entsprechend herangezogen werden. Geht allerdings die Gefahr von einer Information/Datei aus, die ein Dritter auf den Rechnern des Host-Providers gespeichert hat, greift grundsätzlich die Haftungsprivilegierung nach § 10 TMG ein; demgemäß muss grundsätzlich zwischen von außen kommenden Angriffen (Hacking) und vom Provider zugelassenen Informationsspeicherung unterschieden werden.

675 Unabhängig von der Frage des vertraglichen Haftungsausschlusses kann der Host Provider sich seiner Haftung allerdings weitgehend dadurch entziehen, dass er dem Nutzer **wirksame Anti-Viren-Programme** zur Verfügung stellt und ihn auffordert, diese regelmäßig zu benutzen; denn in diesem Fall ermöglicht der IT-Intermediär dem Nutzer Schutzmaßnahmen, die zu den Schutzmechanismen des Host Providers äquivalent sein können.

676 Für **sonstige Angriffe aus dem Netz**, die nicht nutzerseitig mit Hilfe von speziellen Software-Programmen aufgefangen werden können, gilt dies indes nicht. Soweit hier eine Absicherung aus technischen Gründen auf Seiten des IT-Intermediärs nicht vollständig möglich ist, ist der IT-Intermediär zumindest gehalten, den Nutzer zu warnen und ausführlich über Möglichkeiten des Selbstschutzes, wie etwa der Installation von Firewalls, zu instruieren. Die **Warn- und Instruktionshinweise** müssen so deutlich erfolgen, dass dem Nutzer die Tragweite der darin beschriebenen Sicherheitsrisiken klar vor Augen geführt wird.[1242] Unterlässt der Nutzer trotzdem entsprechende Sicherheitsmaßnahmen, so hat der Host seine Verkehrspflichten erfüllt.

(2) Haftung von Access-Providern

677 Aber auch der Access-Provider kann nicht von jeglicher Sicherungspflicht frei sein, insbesondere wenn er sowohl das Herunter- als auch das freie Heraufladen von Daten auf seine Server ermöglicht. Nicht empfehlenswert ist es entgegen vereinzelten Stellungnahmen im Schrifttum, im Vertrag mit dem Endnutzer festzulegen, dass die Dienste mit einem Risiko im Hinblick auf die Schädigung durch Dritte (z.B. Hacking oder Virenverseuchung) behaftet seien und der Nutzer die Dienste auf eigene Gefahr in Anspruch nehme.[1243] Eine entsprechende Klausel wäre als vollständiger Haftungsausschluss auch für Gefahren aus dem eigenen Verantwortungsbereich zu qualifizieren, der

1242 Zu den Anforderungen an Warnpflichten und Instruktionspflichten s. Bamberger/Roth-*Spindler*, § 823 Rn. 484 ff.;S. auch oben Rn. 128 f.

1243 So aber *Roth*, in: Loewenheim/Koch, Praxis des Online-Rechts, S. 57 (143).

insbesondere in AGB nach den §§ 307, 309 Nr. 7b BGB unwirksam ist. Im Rahmen des Zumutbaren obliegen auch dem Access-Provider grundlegende Verkehrspflichten, die sich auf den Schutz seines Systems vor Angriffen Unbefugter beziehen.[1244] Zu berücksichtigen ist in diesem Zusammenhang, dass der Provider Gefahren, die aus seinem System stammen oder sich darüber verbreiten aufgrund seiner personellen und technischen Ausstattung regelmäßig leichter und effektiver bekämpfen kann als der private Nutzer.[1245]

678 Vollständige Sicherheit kann und muss der Access-Provider nicht gewährleisten. Er ist jedoch verpflichtet, sein Medium zu beobachten, Meldungen oder Beschwerden seiner Nutzer nachzugehen, die Nutzer über erkannte Sicherheitsrisiken zu warnen und ggf. Sicherheitsmaßnahmen zu ergreifen.[1246] Der Access Provider hat dafür zu sorgen, dass heraufgeladene Dateien oder Software nicht mit Viren befallen sind. Ebenso wenig darf der Access Provider durch sorglosen Umgang mit Sicherungsmaßnahmen, seien sie technischer oder organisatorischer Natur, das Risiko für Eingriffe in die Sphäre des Nutzers erhöhen, beispielsweise durch Hacker. Der Nutzer darf insbesondere bei entgeltlichem Internet-Zugang ein Minimum an Kontrollen erwarten, die seiner eigenen technischen Sicherheit dienen. Wie für den Service Provider gilt auch hier, dass das Anbieten wirksamer Anti-Virus-Programme in der Regel genügt, um den Pflichten des Access Providers zu genügen.

(3) Haftung von Betreibern von Router-Rechnern

679 Davon zu unterscheiden ist die Haftung der Betreiber von im Internet-Verkehr zwischengeschalteten Rechnern. In Betracht können hier höchstens technische Sicherungspflichten kommen, wie sie z.B. auch für einen Spediteur bestünden, der fremde Güter transportiert.[1247] Auszuscheiden ist beispielsweise eine Haftung für die **Weiterleitung von Viren**, da die Router-Rechner die eingegangenen Datenmengen so weiterleiten, wie sie ankommen, und die Daten in der Regel in verschiedene Pakete unterteilt verschiedene Rechner passieren können.

1244 *Spindler*, in: Spindler, Vertragsrecht der Internet-Provider, Teil IV, Rn. 357; zust. *Mankowski*, in: Ernst, Hacker, Cracker & Computerviren, Rn. 495.

1245 *Spindler*, in: Spindler, Vertragsrecht der Internet-Provider, Teil IV, Rn. 357; zust. *Mankowski*, in: Ernst, Hacker, Cracker & Computerviren, Rn. 495.

1246 *Spindler*, in: Spindler, Vertragsrecht der Internet-Provider, Teil IV, Rn. 357.

1247 Zu diesem Vergleich s. *Koch*, CR 1997, 193 (199 Fußn. 30).

680 Dagegen müssen auch die Betreiber der zwischengeschalteten Rechner dafür Sorge tragen, dass ihr Transportgut **nicht in ihrer Einflusssphäre mit Viren *befallen*** werden kann und die transportierten Daten „verseucht“ werden. Diese Sicherheitsmaßnahmen werden vernünftigerweise vom Verkehr erwartet. Allerdings ist zu berücksichtigen, dass es sich hier stets um nur mittelbare Rechtsgutsverletzungen handelt, da an den verschickten Datenpaketen selbst kein Eigentum besteht. Selbst wenn man Daten – wie hier –[1248] als eigentumsfähiges Recht betrachtet, setzt dies doch in irgendeiner Weise eine Verkörperung, z.B. auf einer Festplatte voraus, deren Substanz oder Funktionsfähigkeit verletzt werden kann. Mit der Zwischenspeicherung auf dem Router-Rechner wird aber gerade nicht fremdes Eigentum durch Verkörperung begründet, sondern werden nur zugeleitete Daten abgelegt. Daher können nur mittelbare Rechtsgutsverletzungen beim Empfänger, die durch die Vernichtung oder Beeinträchtigung des Datenbestandes beim Empfänger infolge der „befallenen“ Nachrichten entstanden sind, in Frage kommen.

681 In gleicher Weise müssen die Betreiber für die notwendigen Sicherungsmaßnahmen sorgen, die verhindern, dass ihre **Rechner zu Angriffen auf andere Internet-Teilnehmer** missbraucht werden können.[1249] Die Situation ist hier nicht anders als in den oben diskutierten Fällen zu bewerten, wenn Dritten der Missbrauch einer Gefahrenquelle leichtfertig eröffnet wird.[1250] In beiden Fällen liegt eine fehlende Sicherung einer Gefahrenquelle vor, für deren Missbrauch der Betreiber der Gefahrenquelle einstehen muss.

b) Verletzungen des allgemeinen Persönlichkeitsrechts außerhalb von Äußerungsdelikten

682 Besondere Fragen werfen Verletzungen des allgemeinen Persönlichkeitsrechts auf, die nicht mit Äußerungen Dritter zusammenhängen, die also nicht auf Inhalte bezogen sind, die Dritte auf Rechnern der IT-Intermediäre gespeichert oder mit deren Hilfe weitergeleitet haben. Mit diesem Bereich ist der Schutz der Kommunikationskanäle von Privaten und Unternehmen angesprochen, der über IT-Intermediäre eröffnet wird. Die essentielle Bedeutung dieses Bereichs erschließt sich unmittelbar, wenn man sich die heutige Be-

---

1248 S. Nachw. Rn. 110 ff.

1249 Ebenso *Koch*, BB 1996, 2049 (2057).

1250 Vgl. BGH NJW 1991, 459 für die Haftung des Kfz-Halters eines ungesichert abgestellten Kfzs, das von Dritten zu deliktischen Handlungen verwendet wurde; BGH NJW 2004, 1449 (1450) zur Sicherung einer Wasserrutsche bei missbräuchlicher Benutzung durch Kinder und Jugendliche; OLG Koblenz NVwZ 2002, 745 - Fahrbahnbeschmutzung durch Sand.

deutung des electronic commerce und von Web-Portalen von Unternehmen, inzwischen aber auch von Privaten vor Augen hält. Die über IT-Intermediäre eröffneten Kommunikationsmöglichkeiten sind heute selbstverständlicher Bestandteil der „Schnittstelle“ des Unternehmens oder des Individuums mit der Außenwelt.

(1) Schutz der Intim- und Privatsphäre

683 Das Persönlichkeitsrecht umfasst auch den Schutz der Privat- und Intimsphäre, in zivilrechtlicher Hinsicht insbesondere das vom BVerfG so bezeichnete Recht auf informationelle Selbstbestimmung als Grundlage des Datenschutzes.[1251] Da die Darstellung des Datenschutzrechts des TMG, des BDSG und der Länderdatenschutzgesetze sowie der EG-Richtlinien zum Datenschutz den gebotenen Umfang sprengen würde, beschränkt sich die nachfolgende Untersuchung auf die haftungsrechtlichen Besonderheiten im Zusammenhang mit den allgemeinen deliktsrechtlichen Ansprüchen.

684 Das Betreiben von Internet-Rechnern stellt im Hinblick auf den Schutz der Intim- und Privatsphäre grundsätzlich eine Gefahrenquelle dar, etwa durch das Ausspähen von persönlichen Daten. Daher sind die IT-Intermediäre gehalten, entsprechende Schutzvorkehrungen zu treffen – und zwar sowohl vertraglich als auch deliktisch. Die Sicherungspflichten gegenüber Ausspähversuchen der Daten der Kunden sind ohne Weiteres als Nebenpflicht einzustufen.[1252]

685 Zur Konkretisierung der Schutzpflichten können die datenschutzrechtlichen Bestimmungen herangezogen werden. So schützt die EG-Richtlinie zum Datenschutzrecht[1253] auch die Übertragung von Dateien mit persönlichen Daten, Art. 2 b) („Übermittlung“), mithin den Datentransport über das Internet, z.B. E-Mails. Sie verlangt nach Art. 17 vom Verantwortlichen technische und organisatorische Maßnahmen zum Schutz der Daten mit persönlichem Charakter, insbesondere gegen Veränderung oder unerlaubten Zugriff. Einen Hinweis auf die Abgrenzung der Verantwortlichkeiten bietet auch Art. 2 d) der Richtlinie, wonach nur derjenige, der über die Zwecke und Mittel der Verarbeitung der Daten entscheidet, als Verantwortlicher zu betrachten ist und nicht derjenige, der die Dienstleistung anbietet.[1254] Das TMG enthält ebenfalls spezifische datenschutz-

---

1251 BVerfGE 65, 2 (42 ff.); BVerfGE 80, 367 (373); BVerfG MMR 2007, 93; BVerfG DVBl 2007, 497 ff.

1252 *Spindler*, in: Spindler: Vertragsrecht der Internet-Provider, Teil IV, Rn. 147.

1253 Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr ABl. EG Nr. L 281 vom 23. November 1995, S. 31.

1254 Nach Art. 2 I der Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002

rechtliche Bestimmungen, die fruchtbar gemacht werden können. So muss der Diensteanbieter gem. § 13 Abs. 4 TMG durch technische und organisatorische Vorkehrungen sicherstellen, dass der Nutzer Teledienste geschützt gegen die Kenntnisnahme Dritter in Anspruch nehmen kann.[1255]

686 Die von der EG-Richtlinie zum Datenschutz und vom TMG verlangten Sicherheitsvorkehrungen sind nach allgemeinem Deliktsrecht als grundlegende Sicherheitsstandards im Sinne von Verkehrspflichten von den Betreibern von Rechnern im Netz zu beachten. Das TMG schließt weitergehende zivilrechtliche Ansprüche nicht aus; vielmehr können die datenschutzrechtliche Vorgaben des TMG gegebenenfalls sogar als Schutzgesetze nach § 823 II BGB vom Betroffenen zur Stützung von Schadensersatzansprüchen herangezogen werden.[1256]

687 Demnach haben alle in die Übermittlungskette eingeschalteten Betreiber je nach ihrer Einflusssphäre dafür Sorge zu tragen, dass die Privatsphäre von abgesandten Nachrichten gewahrt bleibt. Insbesondere von Providern, die einen E-Mail-Dienst in ihr Angebot integriert haben, muss verlangt werden, dass die Nachrichten vor dem unbefugten Abhören und gegen den unbefugten Zugriff Dritter gesichert wird.

688 Allerdings ist auch hier wiederum zu berücksichtigen, welchen **Grad an Sicherheit der Verkehr erwartet**: Warnt der Provider den Absender einer E-Mail ausdrücklich vor möglichen Abhörmaßnahmen Dritter und bietet er beispielsweise Verschlüsselungen an, so kann sich der geschädigte Nutzer, der trotzdem eine ungesicherte E-Mail absendet, nicht auf ein Vertrauen in die Einhaltung von Sicherheitsstandards berufen. Häufig werden hier zudem bereits vertragliche Haftungsausschlüsse eingreifen. Macht der Nutzer von bereitgestellter Verschlüsselungssoftware keinen Gebrauch, muss er sich dies zumindest als Mitverschulden gem. § 254 BGB auf seinen Anspruch anrechnen lassen. Der geforderte Sicherheitsstandard kann wiederum bei kostenlosen Angeboten, insbesondere bei E-Mail-Accounts, abgesenkt werden, da hier zum einen der Grundgedanke des Schenkungsrechts durchschlägt, zum anderen auch eine analoge Anwendung der

---

über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation) gelten die Begriffsbestimmungen des Art. 2 der Richtlinie 95/46/EG auch für diese Richtlinie.

1255 Ausführlich Spindler/Schmitz/Geis-*Schmitz*, § 4 TDDSG Rn. 23 ff.

1256 Vgl. für das BDSG als Schutzgesetz: zuletzt OLG Frankfurt aM ZIP 2005, 654; OLG Hamm NJW 1996, 131; OLG Hamm ZIP 1983, 552.

Maßstäbe des Schenkungsrechts nahe liegt, da der Nutzer oftmals – wenn auch unentgeltliche – vertragliche Beziehung zu dem IT-Intermediär unterhalten wird.

689 Trotz entsprechender Warnungen muss jedenfalls ein Mindeststandard an Sicherungsmaßnahmen seitens der Provider ergriffen werden, der verhindert, dass E-Mail-Nachrichten von jedermann gelesen werden können. Hierzu dürfte die Vergabe von Passwörtern zählen und die stichprobenartige Überwachung der Mail-Server auf unerlaubte Zugriffsversuche Dritter.

690 Ferner kann eine Haftung der Betreiber von Router-Rechnern wegen unterlassener technischer Sicherungsmaßnahmen im Bereich des Zugriffs unautorisierter Dritter auf die Datenpakete in Betracht kommen, z.B. „Abhören" von Kreditkarteninformationen oder Zahlungsvorgängen. Aber auch hier ist zu bedenken, dass die Betreiber von Router-Rechnern in der Regel keinerlei Kenntnis von den Datenpaketen haben werden, für deren Transport ihr Rechner verwendet wird, so dass entsprechende Sicherungsmaßnahmen nicht zumutbar erscheinen. Zudem dürfte es in der Regel an jedem entgeltlichen Geschäftskontakt mit den Absendern der sensiblen Informationen fehlen, so dass im Sinne der Zuordnung der Verantwortung für Risiken dort, wo sie am besten beherrscht und versichert werden können, eine Verantwortlichkeit der Betreiber von Router-Rechnern auch unter diesem Gesichtspunkt ausscheidet. Sofern die **Kreditwirtschaft oder Unternehmen** das Internet durch vollautomatisierte Sofwarekomponenten zur Abwicklung ihrer Geschäftsvorfälle verwenden (**Web-Services**), müssen sie selbst sicherstellen, dass der Missbrauch der Daten verhindert wird, etwa durch die Wahl geeigneter Verschlüsselungsstandards.[1257]

(2) Unerbetene elektronische Post und Störerhaftung

691 Eine andere, eng mit Persönlichkeitsrechten verknüpfte Frage betrifft die deliktsrechtliche Verantwortlichkeit der IT-Intermediäre für die Zusendung unerbetener elektronischer Post. Diese Frage kann hier indes nur angedeutet werden, da sie eine eigene Untersuchung rechtfertigen würde (Spam-Versand und rechtspolitisch sinnvolle Gegenmaßnahmen). Im Weitesten Sinne kann auch die Vorkehr vor unerwünschten Mail-Sendungen zu Sicherungspflichten eines IT-Intermediärs gehören, etwa durch die Ein-

1257 Näher *Spindler*, DuD 2005, 139 ff.

richtung von Spam-Filtern, die aber durch den IT-Nutzer beherrschbar bleiben müssen.[1258]

c) Störung der Außenbeziehung des im Internet präsenten Unternehmens

692 Neben den zahlreichen Fällen, in denen ein Anspruch wegen Verletzung der Unternehmenskennzeichen neben namens-, wettbewerbs-, marken- oder sonstigen zeichenrechtlichen Ansprüchen gegeben sein kann und der daher in deren Zusammenhang zu behandeln ist, kann das Recht am eingerichteten und ausgeübten Gewerbebetrieb durch die Sperrung eines Internet-Zugangs verletzt sein. Eine solche Zugangsbehinderung kann beispielsweise durch die Verstopfung der E-Mail-Adresse oder durch den Zusammenbruch der Web-Seite des Unternehmens infolge technischer Probleme des Providers sowie von Denial-of-Service-Attacken erfolgen. Die daraus dem Unternehmen entstehenden Schäden können beträchtlich sein, z.B. wenn wichtige Nachrichten nicht empfangen werden konnten oder gar verloren gingen.

693 Neben etwaigen vertraglichen Schadensersatzansprüchen gegen den IT-Intermediär, kann fraglich sein, ob das Unternehmen auch **deliktische Schadensersatzansprüche** geltend machen kann. Solche Ansprüche können dann von Interesse sein, wenn die Ursache für den Schaden außerhalb der Vertragsbeziehung entstanden ist – andernfalls greift die Haftungsprivilegierung nach § 44a TKG ein – oder Verjährungsfristen anders geregelt sind. Im allgemeinen Deliktsrecht kommen hier nur Ansprüche aus Recht am eingerichteten und ausgeübten Gewerbebetrieb in Betracht, da sowohl der Informationszugang als auch der Informationsabgang kein anderes von § 823 Abs. 1 BGB geschütztes Rechtsgut verletzt. In entsprechender Anwendung der Energiezufuhr-Fälle[1259] könnte hier in der Tat an einen deliktsrechtlichen Schutz des Nutzers gedacht werden, indem der freie Zugang zum Unternehmen gewahrt wird. Bedenkt man, dass die Telekommunikationswege des Unternehmens heute mindestens genauso wichtig sind wie die Energieversorgung, so muss auch die Freihaltung dieser Schnittstellen des Unternehmens zur Außenwelt grundsätzlich dem Recht am eingerichteten und ausgeübten Gewerbebetrieb unterfallen. Daher gehört zum geschützten Bereich des Unternehmens

1258 Ausführlich und näher dazu *Spindler/Ernst*, CR 2004, 437 ff.; *Hoeren*, NJW 2004, 3513 ff.

1259 BGHZ 29, 65 ff.; BGHZ 41, 123 (125 f.), der allerdings im konkreten Fall eine Eigentumsverletzung annimmt; anders BGH NJW 1992, 41 f.; MünchKommBGB-*Wagner*, § 823 BGB Rn. 212; *Foerste*, in: v. Westphalen, ProdHaftHdb, § 21 Rn. 122 f.

auch der freie Zugang, hier per E-Mail und Web-Seite.[1260] Zwar hat der BGH es bisher abgelehnt, die Unterbrechung der Energiezufuhr als einen Eingriff in das Recht am eingerichteten und ausgeübten Gewerbebetrieb anzusehen.[1261] Auch für unterbrochene Telefon- und Telefaxkabel hat die Rechtsprechung einen deliktsrechtlichen Schutz ebenso wenig gewährt[1262] wie für unterbrochene Zugangswege.[1263] Eine Verletzung des deliktisch geschützten Rechtsguts des eingerichteten und ausgeübten Gewerbebetriebs soll nur dann vorliegen, wenn der Betrieb in seinen Grundlagen bedroht sei oder gerade der Funktionszusammenhang der Betriebsmittel auf längere Zeit aufgehoben sei.[1264]

694 Gerade wenn man aber akzeptiert, dass das Eigentum in seinem Wert ganz wesentlich von den ausübbaren Funktionen abhängt, kann nicht daran vorbeigegangen werden, dass die Beziehungen einer Sache, insbesondere eines **Unternehmens, zu seiner Außenwelt** erheblich dessen Wert beeinflussen.[1265] Auch wenn die Eigentumsverletzung von einer spürbaren Beeinträchtigung des Marktwertes abhängig gemacht wird,[1266] muss doch berücksichtigt werden, dass vor allem der fehlende Zugang zum Unternehmen dessen Marktwert für einen potenziellen Käufer mindert, sofern die Behinderung über einen nicht unerheblichen Zeitraum andauert.

695 Darüber hinaus können Ansprüche aus §§ 823 Abs. 1, 826 BGB vorliegen, wenn der E-Mail-Posteingang eines Unternehmens durch massenhaft versandte E-Mail – dem sog. Mail-Bombing –[1267] verstopft wird, z.B. im Rahmen von Boykott- oder anderen Kampagnen[1268] gegen ein Unternehmen.[1269] Derartige Ansprüche richten sich dann aller-

---

1260 Ebenso für das schweizerische Recht *Alder*, in: Hilty, Information Highway, S. 331 (344 ff.), allerdings unter dem Gesichtspunkt des Persönlichkeitsrechts.

1261 S. Fn. 1259.

1262 BGH VersR 1977, 616 (617); s. auch OLG Düsseldorf VersR 1997, 589: kein betriebsbezogener Eingriff in den eingerichteten und ausgeübten Gewerbebetrieb bei unterlassener Eintragung einer Telefonnummer in die „Gelben Seiten".

1263 Vgl. BGHZ 86, 152: Im entschiedenen Fall ging es um einen infolge verschuldeten Dammbruchs trockengelaufenen Kanal, der zu einem Umschlagbetrieb führte. Der BGH lehnte einen Anspruch ab, weil der Dammbruch nicht zu einem Eingriff in die Sachsubstanz der Lagerei- und Umschlaganlagen geführt habe (155).

1264 BGH NJW 1983, 812 (813) - Hebebühne; zust. *Foerste*, in: v. Westphalen, ProdHaftHdb, § 21 Rn. 122.

1265 S. bereits *Buchner*, Die Bedeutung des Rechts am eingerichteten und ausgeübten Gewerbebetrieb für den deliktsrechtlichen Unternehmensschutz, S. 109, 163 f.; *Taupitz*, Haftung für Energieleiterstörungen durch Dritte, S. 120.

1266 So MünchKommBGB-*Mertens*, 3. Aufl. 1997, § 823 BGB Rn. 113 f., 491; *Zeuner*, FS Flume, Bd. I, S. 775 (778 f.); krit. dagegen MünchKommBGB-*Wagner*, § 823 BGB Rn. 116.

1267 Vgl. *Strömer*, Online Recht, S. 108 f.; *Ernst*, JuS 1997, 776 (778); dazu auch *Roggenkamp*, jurisPR-ITR 8/2006 Anm. 4.

1268 Zur Problematik von „Online-Demonstrationen" AG Frankfurt/M, MMR 2005, 863 ff. (Strafrechtliche Verantwortlichkeit für die Aktion „Lufthansa goes offline"); *Kraft/Meister*, MMR 2003, 366 ff.; *Klutzny*, RDV 2006, 50 ff.

dings nicht gegen den IT-Intermediär, da dieser nur den vertraglich geschuldeten Posteingang sicherzustellen hat[1270] und keine darüber hinausgehenden deliktsrechtlich relevanten Sicherheitserwartungen beim Nutzer geweckt hat und zudem § 44a TKG eingreifen würde. Besonderheiten gegenüber den bekannten Ansprüchen bei Kampagnen gegen ein Unternehmen[1271] ergeben sich dadurch nicht.

696 Ebenso kann der „**Einbruch" von Hackern** in eine (auf einem Rechner des IT-Intermediärs gehostete) Web-Seite eines Unternehmens und deren Unbrauchbarmachung dazu führen, dass gegen die Hacker ein Anspruch aus §§ 823 Abs. 1, 823 Abs. 2, 826 BGB besteht – abgesehen von möglichen urheberrechtlichen Ansprüchen. Hat der Provider keine genügenden Sicherungsvorkehrungen gegen das Eindringen von Hackern in das System getroffen, ist auch er gem. § 823 Abs. 1 BGB haftpflichtig für etwaige eingetretene Schäden. Allerdings wird es hier in der Regel kaum möglich sein, einen konkreten Schaden nachzuweisen, da dieser darauf beruhen müsste, dass die Web-Seite nicht zugänglich gewesen ist.

697 Aber auch hinsichtlich des ***Versands* von E-Mail-Nachrichten** können grundsätzlich Ansprüche des Unternehmens gegen einen eingeschalteten Provider oder andere Betreiber von Rechnern geltend gemacht werden, wenn in deren Einflusssphäre die E-Mail infolge mangelnder Sicherungsvorkehrungen geöffnet bzw. abgehört wurde und das Unternehmen im Rahmen seines Rechts am eingerichteten und ausgeübten Gewerbebetrieb dadurch einen Schaden erlitten hat. Hier ergeben sich keine Unterschiede zu den oben behandelten Sicherungspflichten der Provider im Hinblick auf die Wahrung des allgemeinen Persönlichkeitsrechts.[1272] Für die wohl häufigsten Fälle von Schädigungen, dem Ausspähen von Kreditkartenangaben oder anderen finanziell sensiblen Daten, bietet das Deliktsrecht aber keinen Schutz, da diese Daten nicht dem Recht am eingerichteten und ausgeübten Gewerbebetrieb unterfallen, sondern reine Vermögensschäden darstellen.[1273]

1269 Ebenso für das schweizerische Recht *Alder*, in: Hilty, Information Highway, S. 331 (344 ff.); *R.H.Weber*, in: Hilty, Information Highway, S. 531 (554); viel zu kurz gegriffen daher *Strömer*, Online Recht, S. 109, der mangels vertraglicher Beziehungen und wegen reinen Vermögensschadens kategorisch Ansprüche aus § 823 Abs. 1 BGB verneint.

1270 Vgl. aus schweizerischer Sicht *Hilty*, in: Hilty, Information Highway, S. 437 (481) sowie *Briner*, in: Hilty, Information Highway, S. 489 (508 ff.).

1271 S. nur BGHZ 24, 200 ff. - Boykottaufruf; BGHZ 90, 113 ff.; MünchKommBGB-*Wagner*, § 823 BGB Rn. 201 ff. mwN.

1272 S. oben Rn. 682 ff.

1273 Zum fehlenden deliktsrechtlichen Schutz des Vermögens MünchKommBGB-*Wagner*, § 823 BGB Rn.

4. Einzelne Sicherungspflichten

a) Virenscanner

698 Wie die kommerziellen Nutzer trifft den Intermediär in jedem Fall die Pflicht zur Sicherung des eigenen Systems mit Hilfe von Virenscannern. Etwaige Privilegierungen privater Nutzer kann er aufgrund des hohen Gefährdungspotentials nicht geltend machen.[1274]

b) Firewall

699 Sofern der Provider selbst Netzwerktechnik einsetzt, muss er diese auch besonders sichern. Hierzu gehört auch die Einrichtung und Wartung einer Firewall.[1275] Dafür sprechen auch § 104 TKG, der die Gewährleistung der ausreichenden Datensicherheit vom Telekommunikationsanbieter verlangt, sowie aus datenschutzrechtlicher Sicht § 13 Abs. 4 TMG.[1276]

c) System- und Programmupdates

700 Die Programme, die der Intermediär nutzt, befinden sich in der Regel auf einem Computersystem, das für jeden zugängliche Dienste bereitstellt. Während der private Nutzer meist pseudonym agiert, ist der Provider bekannt und kann daher jederzeit Opfer auch gezielter Angriffe werden. Lücken im verwendeten System oder den Programmen stellen hierbei eine große Gefahr dar. Sofern der Intermediär wirtschaftlich tätig ist, ist ihm somit eine regelmäßige Beobachtung der Entwicklungen bei der von ihm eingesetzten Software zuzumuten. Diese kann z.B. über die Teilnahme an den jeweiligen sogenannten Mailing-Listen erfolgen. Sollten Sicherheitslücken bekannt werden, so muss er unverzüglich versuchen, diese Lücken zu schließen. Ist dies nicht sofort möglich, kann auch von ihm verlangt werden, die gefährdeten Funktionen nicht weiter anzubieten. Fraglich ist, ob ihm die vollständige Einstellung des Betriebs aufgebürdet werden kann. In dieser Situation kann sich aus Art. 12 GG eine Beeinflussung des Haftungsmaßstabs zugunsten des Providers ergeben. Allerdings ist dabei auf die Art der Gefahr abzustellen. Ist das Risiko gering und die erwarteten Schäden ebenso, so müsste der Betrieb so lange aufrechterhalten werden können, bis eine Lösung zur Verfügung steht. Bei einer höheren Gefährdung[1277] müsste der Betrieb jedoch eingestellt werden. Insgesamt ob-

176 ff.

1274 Vgl. zusätzlich *Spindler*, in Spindler: Vertragsrecht der Internet-Provider, Teil IV, Rn. 356 f.; insofern keine Nutzung auf eigene Gefahr; aA noch zu § 5 TDG aF *Sieber*, in: Hoeren/Sieber, Teil 19 Rn. 248.

1275 Zutr. *Czychowski*, in: Bröcker/Czychowski/Schäfer, § 13 Rn. 106.

1276 Darauf weist zu Recht *Schmitz*/*v.Netzer*, in: Schuster, Vertragshandbuch Telemedia, Kap. 12 Rz. 21 hin.

1277 Häufig kategorisieren die Hersteller die Sicherheitslücken. Kritische Sicherheitslücken führen jedenfalls zu einer nicht abwälzbaren Pflicht.

liegt dem Intermediär somit eine Beobachtungs- und Abhilfepflicht in Hinsicht auf System- und Programmupdates.

701 Den **nicht-kommerziellen Intermediär** kann die Beobachtungspflicht nur in abgeschwächter Form treffen. Er sollte sich dennoch regelmäßig informieren und schnellstmöglich Gegenmaßnahmen ergreifen.

d) Nutzung von Nutzerkonten mit eingeschränkten Rechten

702 Die Nutzung von speziellen Nutzerkonten ist dem Intermediär in jeder Hinsicht zuzumuten, sofern ihm dies möglich ist.

e) Intrusion Detection-Systeme

703 Beim Einsatz von Netzwerken kann hier auch eher der Einsatz von Intrusion Detection-Systemen verlangt werden.

f) Malware-Entfernungsprogramme

704 Auch eine ständige Nachsorge ist dem Provider zuzumuten. Sollten Hinweise auf eine Gefährdung bestehen, so ist jedenfalls nach Schadprogrammen zu suchen, und diese sind zu entfernen. Hierzu besteht eine regelmäßige Verpflichtung, z.B. einmal in der Woche.

g) Ergebnis

705 Grundsätzlich tritt die Pflicht zum Einsatz von Sicherungsmaßnahmen beim Intermediär eher ein und ist auch schärfer anzusetzen. So kann eine ständige Beobachtung auch neuer Gefahrenpotentiale viel eher verlangt werden, notwendige Aktualisierungen sind so oft vorzunehmen, wie dies nötig ist.

5. Zusammenfassung

706 Deliktische und vertragliche Ansprüche gegen den IT-Intermediär wegen Verletzung seiner Sicherungspflichten können sich vor allem auf die Zerstörung von Daten oder die Beschädigung von Hardware infolge von Virenbefall oder anderen Arten von Angriffen aus dem Netz ergeben. Nur vertragliche Ansprüche sind dagegen für Daten des Nutzers auf einem Server des Providers einschlägig.

707 Der IT-Intermediär hat den Nutzer vor Angriffen aus dem Netz durch entsprechende Sicherungsmaßnahmen für seine Rechner zu bewahren. Bei Virenbefall genügt es allerdings, dass der Provider den Nutzer entsprechende Anti-Viren-Programme anbietet und bereithält. Ist dem Provider eine technische Sicherung gegen Angriffe nach dem Stand

der Technik nicht möglich, so hat er den Nutzer intensiv auf entsprechende Gefahren hinzuweisen und Schutzmaßnahmen zu empfehlen. Dies gilt auch für den reinen Access Provider, dem Systemsicherungspflichten obliegen. Auch Betreiber von Router-Rechnern müssen dafür sorgen, dass Daten im Bereich ihres Einflusses nicht von außen beschädigt werden können; allerdings wird es hier oftmals an einer Rechtsgutsverletzung mangels Eigentums an den Daten fehlen. Allerdings werden entsprechende Ansprüche durch § 44a TKG begrenzt, sofern es sich um Vermögensschäden und entsprechende Telekommunikationsdienste handelt.

708 Ansprüche aus Vertrag mit Schutzwirkung zugunsten Dritter zwischen verschiedenen Providern scheitern an der erforderlichen Überschaubarkeit der beteiligten Nutzer. Für Provider wäre das Risiko eines Vermögensschadens von Nutzern, die ihrerseits in Beziehung mit einem Provider stehen, nicht mehr zu kalkulieren.

709 Provider haben Nutzer aber auch vor Angriffen auf die Privat- und Intimsphäre zu schützen, insbesondere vor dem Ausspähen von E-Mails. Auch wenn Nutzer weitgehend darauf verwiesen werden können, ihre E-Mail zu verschlüsseln, muss der Provider zumindest Passwörter für den Zugang zu E-Mail-Konten vergeben und für gelegentliche Stichproben auf unbefugten Zugang sorgen.

710 Entgegen der Rechtsprechung ist ein deliktsrechtlicher Schutz der Außenbeziehungen des Unternehmens anzuerkennen, der auch den Zugang mittels E-Mail und Website umfasst. Darüber hinaus bestehen selbstverständlich Ansprüche aus §§ 823 Abs. 1, 826 BGB gegen Versender sog. E-Mail-Bomben, die den Zugang des Unternehmens verstopfen, oder gegen Hacker, die Informationen des Unternehmens ausspähen.

III. Intermediär als reiner Mittler von Informationen

711 Geht der Angriff dagegen nicht direkt vom Intermediär aus, leistet der IT-Intermediär aber einen wesentlichen Beitrag zur Verletzung Dritter, indem er die schädigende Information weitergeleitet, gespeichert oder bereitgestellt hat, stellt sich parallel zu den Sicherungspflichten für eigene Systeme die Frage, ob der Intermediär gehalten ist, den Datenverkehr auf seinen Systemen im Hinblick auf Rechtsverletzungen Dritter zu kontrollieren. So könnte etwa ein Host-Provider verpflichtet sein, das Angebot seiner Kunden auf Viren zu untersuchen, um die Schädigung Dritter zu verhindern.

712 Auf diesen Problemkreis haben sowohl der deutsche als auch der europäische Gesetz- bzw. Richtliniengeber reagiert, indem die Verantwortlichkeitsprivilegierungen der §§ 7

- 10 TMG bzw. die entsprechenden Regelungen der E-Commerce-Richtlinie Art. 12 – 15 ECRL[1278] eingeführt wurden.[1279] Greifen diese Privilegierungen, so ist die Haftung bzw. Verantwortlichkeit ausgeschlossen, allerdings mit der für die Praxis gewichtigen Ausnahme der Störerhaftung bzw. des Unterlassungsanspruchs nach § 1004 BGB.[1280]

713 Grundsätzlich treffen den IT-Intermediär nach § 7 Abs. 2 TMG keine allgemeinen (!) Pflichten, übermittelte oder gespeicherte Informationen, die nicht eigene Informationen nach § 7 Abs. 1 TMG sind, zu überwachen. Grundsätzlich fallen damit auch Viren sowie spezielle Datenpakete unter den Informationsbegriff des § 7 TMG,[1281] so dass Viren, Trojaner, aber auch manipulierte Pakete eines Denial-of-Service-Angriffs erfasst sind. Die Voraussetzungen dieser Privilegierungen hängen von der jeweiligen Funktion des Intermediärs ab:

1. Content-Provider

714 Content-Provider sind nach § 7 Abs. 1 TMG diejenigen, die eigene Informationen speichern und bereitstellen.[1282] Für sie gilt keine Privilegierung. Auf die strittige Frage, wann es sich um eigene, wann um fremde Informationen handelt,[1283] kommt es nicht an, da es sich bei der hier behandelten Information jedenfalls nicht um eine handelt, die sich der Intermediär zu eigen macht und von der er regelmäßig auch keine Kenntnis hat.[1284]

2. Host-Provider

715 Anders ist dies beim Host-Provider. Er vermittelt gerade fremde Informationen. Die Haftung ist nach § 10 TMG ausgeschlossen, wenn er keine Kenntnis von der Information oder den einen Schadensersatzanspruch begründenden Tatsachen hat und die Information entfernt oder den Zugang sperrt, sobald er Kenntnis erlangt.

716 Auf den Fall eines **Angriffs mittels Informationstechnik** übertragen bedeutet dies, dass der Inhaber eines Rechnersystems bzw. der IT-Intermediär, von dem ein Angriff ausgeht, den Angriff sofort unterbinden muss, sowie er davon Kenntnis erlangt. Es han-

---

1278 Richtlinie 2000/31/EG des Europäischen Parlaments und des Rates vom 8. Juni 2000 über bestimmte rechtliche Aspekte der Dienste der Informationsgesellschaft, insbesondere des elektronischen Geschäftsverkehrs im Binnenmarkt („Richtlinie über den elektronischen Geschäftsverkehr“) .

1279 Dazu Spindler/Schmitz/Geis-*Spindler*, vor § 8 TDG Rn. 10.

1280 BGH NJW 2004, 3102; *Spindler*, JZ 2005, 37; *Leible/Sosnitza*, NJW 2004, 3225 (3226).

1281 *Koch*, NJW 2004, 801 (806); *Spindler*, NJW 2002, 921 (922); *Hoffmann*, MMR 2002, 284 (288).

1282 *Schwarz/Poll*, JurPC 73/2003, Rn. 61.

1283 S. nur Spindler/Schmitz/Geis-*Spindler*, § 8 TDG Rn. 4 ff. mwN.

1284 Zu Schutzpflichten bei eigenen Angeboten s. z.B. OLG Nürnberg NJW-RR 2003, 628 (629).

delt sich hierbei um Informationen, die der Diensteanbieter im Auftrag des Nutzers speichert, was auch unbewusst geschehen kann. Möglich ist dies z.B. dadurch, dass der Nutzer mit Viren verseuchte Dateien ablegt oder selbst Programme installiert, von denen Angriffe auf Dritte ausgehen. Eine Beendigung der Schädigung durch den Provider wäre durch Abschaltung der Anlage oder durch die Entfernung des den Angriff verursachenden Programms, z.B. des Virus. Für die Kenntnis der Umstände zur Begründung eines Schadensersatzanspruchs (nicht für die strafrechtliche Verantwortlichkeit) kann es nach § 10 S. 1 Nr. 2 TMG genügen, wenn auffällige Netzwerkaktivitäten erkannt und gemeldet werden, z.B. durch ein Intrusion Detection-System, sofern ein solches installiert ist.[1285]

3. Access-Provider

717 Der Access-Provider speichert zunächst keine Informationen. Seine Funktion ist nach § 8 TMG vielmehr die Durchleitung von Informationen durch Kommunikationsnetze oder die Vermittlung des Zugangs zu fremden Informationen. Die Verantwortlichkeit ist danach ausgeschlossen, wenn der Provider die Übermittlung der Information nicht veranlasst, und weder Adressat noch Information ausgewählt, sowie die Information nicht verändert hat. Die bloße Bereitstellung von Einwahlknoten kennzeichnet gerade den sog. Access-Provider und ist deshalb als Zugangsvermittlung i.S.v. § 8 TMG anzusehen.[1286] Das TMG hat in diesem Zusammenhang den alten Streit beigelegt, ob Access-Provider überhaupt unter die Haftungsprivilegierungen fallen.[1287]

718 Die Übertragung von **Schadprogrammen** (**Malware**) oder manipulierten Paketen durch ein Kommunikationsnetz fällt demnach auch in den Anwendungsbereich des § 8 TMG. Nach § 8 Abs. 2 TMG ist auch die kurzfristige Speicherung der übermittelten Information gestattet, sofern sie nur zur Übermittlung und nicht länger als für die Übermittlung üblicherweise erforderlich erfolgt. Im Gegensatz zu § 9 TMG ist nur die sehr kurzfristige, technisch notwendige Speicherung, nicht das sog. Caching von der Haftung freigestellt.[1288] Es handelt sich bei den gespeicherten Informationen zudem um solche, auf die der Nutzer keinen Zugriff hat.[1289]

1285 Dazu Rn. 65.

1286 LG München I CR 2000, 117; OVG Münster MMR 2003, 348 (350); *Kühne*, NJW 1999, 188; Spindler/Schmitz/Geis-*Spindler*, § 9 TDG Rn. 14.

1287 *Spindler*, CR 2007, 242.

1288 *Hoffmann*, MMR 2002, 284 (287); Spindler/Schmitz/Geis-*Spindler*, § 9 TDG Rn. 8.

1289 Begr. RegE BT-Drucks. 14/6098, S. 24.

719 Entsprechend § 9 TMG ist auch die zeitlich begrenzte, automatische Zwischenspeicherung von der Haftung freigestellt. Hierunter fällt insbesondere das **Caching** zur effizienteren Gestaltung der Übertragung.

IV. Öffentlich-rechtliche Anforderungen

1. Anwendbarkeit des TKG auf IT-Intermediäre

720 Das TKG regelt anders als das TMG nicht Fragen des Inhalts von Tele- oder Mediendiensten, sondern den technischen Vorgang der Telekommunikation und damit des Aussendens, der Übermittlung und des Empfangens von Signalen mittels Telekommunikationsanlagen (vgl. § 3 Nr. 22 TKG). Es handelt sich hierbei im Wesentlichen um öffentliches Marktregulierungsrecht.[1290] Zweck des Gesetzes ist nach § 1 TKG, durch eine technologieneutrale Regulierung den Wettbewerb im Bereich der Telekommunikation und leistungsfähige Telekommunikationsinfrastrukturen zu fördern und flächendeckend angemessene und ausreichende Dienstleistungen zu gewährleisten. Auch nach der Neufassung des TKG bleibt die Abgrenzung der Telekommunikationsdienste (§ 3 Nr. 24 TKG) zu den Telemediendiensten eines der umstrittensten Probleme. Internet-Provider unterfallen nach hM den Regelungen des TKG, soweit sie Telekommunikationsdienste erbringen, wobei eine **funktionale Abgrenzung** zugrunde zu legen ist.[1291] Entscheidend ist demnach die Art der erbrachten Dienste: Bestehen diese lediglich in der Bereitstellung von Übertragungskapazitäten (Network-Provider) oder handelt es sich ausschließlich um die Bereitstellung des Internetzugangs (Internet-by-Call-Anbieter), dann werden nur Telekommunikationsdienste erbracht. Content-Provider, welche allein Inhalte auf mit dem Internet verbundenen Servern zur Verfügung stellen, erbringen dagegen allein Telemediendienste. Handelt es sich um einen kombinierten Dienst, welcher Telekommunikationsdienste und Telemediendienste miteinander verbindet (z.B. t-online), ist nicht der Schwerpunkt des Dienstes maßgeblich, sondern das jeweils einschlägige Gesetz auf die einzelnen Bestandteile anzuwenden, d.h. der Dienst ist in seine Bestandteile aufzuteilen,[1292] was auch § 1 Abs. 3 TMG zeigt, der davon spricht, dass das TMG das Telekommunikationsrecht unberührt lässt.

2. Anforderungen des TKG an die IT-Sicherheit

1290 Säcker-*Säcker*, Einl. I Rn. 2 f.

1291 Beck'scher TKG-Kommentar-Gersdorf, Einleitung, Teil C, Rn 18, 20; Säcker-*Säcker*, § 3 TKG Rn. 38; Spindler/Schmitz/Geis-*Spindler*, § 2 TDG Rn. 22.

1292 Beck'scher TKG-Kommentar-Gersdorf, Einleitung, Teil C, Rn. 22 f.; Säcker-*Säcker*, § 3 TKG Rn. 40; Spindler/Schmitz/Geis-*Spindler*, § 2 TDG Rn. 22; *Spindler*, CR 2007, 239 (242).

721 Das TKG enthält in den §§ 108 ff. besondere Regelungen im Interesse der öffentlichen Sicherheit, zu denen gemäß § 109 TKG auch technische Schutzmaßnahmen gehören – wobei § 109 TKG nicht durch die im November 2006 verabschiedete Reform berührt wird. § 109 TKG findet, wie auch schon die Vorgängervorschrift des § 87 TKG,[1293] europarechtlich seine Vorgabe in Art. 4 der Datenschutzrichtlinie.[1294] Dabei entspricht § 109 Abs. 2 TKG sinngemäß Art. 4 Abs. 1 DSRL. Durch § 109 Abs. 1 TKG geht er aber über die Vorgabe der Datenschutzrichtlinie noch hinaus, indem er auch jeden Diensteanbieter (anstatt lediglich den Betreiber von Telekommunikation) zum Treffen von technischen Schutzmaßnahmen verpflichtet.[1295] Nicht erwähnt wird dagegen die Unterrichtungspflicht des Art. 4 Abs. 2 der Datenschutzrichtlinie in § 109 TKG. Nach Art. 4 Abs. 2 der Datenschutzrichtlinie muss der Betreiber eines öffentlich zugänglichen elektronischen Kommunikationsdienstes, wenn ein besonderes Risiko der Verletzung der Netzsicherheit besteht, die Teilnehmer über dieses Risiko und – wenn das Risiko außerhalb des Anwendungsbereichs der vom Diensteanbieter zu treffenden Maßnahmen liegt – über mögliche Abhilfen, einschließlich der voraussichtlich entstehenden Kosten, unterrichten. Da diese Umsetzung fehlt, wird vorgeschlagen, in richtlinienkonformer Auslegung, die Unterrichtungspflicht als sonstige Maßnahme im Sinne des § 109 TKG zu qualifizieren.[1296]

722 Im Unterschied zur Vorgängerregelung des § 87 TKG 1996 richtet sich die Vorschrift nicht nur an die Betreiber von Telekommunikationsanlagen, sondern an jeden Diensteanbieter. **Diensteanbieter** ist nach § 3 Nr. 6 TKG jeder, der Telekommunikationsdienste (§ 3 Nr. 24 TKG) ganz oder teilweise geschäftsmäßig erbringt oder an der Erbringung solcher Dienste mitwirkt; Internet-Provider können danach den Anforderungen des § 109 TKG unterliegen, wenn sie nach den obigen Grundsätzen Telekommunikationsdienste erbringen.

723 Nach **§ 109 Abs. 1 TKG** haben Diensteanbieter angemessene (vgl. § 109 Abs. 2 S. 4 TKG) technische Vorkehrungen oder sonstige Maßnahmen zum Schutze des Fernmeldegeheimnisses, personenbezogener Daten und der Telekommunikations- und Datenverarbeitungssysteme gegen unerlaubte Zugriffe zu treffen. Geschützt werden soll da-

---

1293 S. dazu Trute/Spoerr/Bosch-*Trute*, § 87 Rn. 6.

1294 Richtlinie 2002/48/EG über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation) vom 12. Juli 2002.

1295 S. dazu auch Säcker-*Klesczewski*, § 109 TKG Rn. 4.

1296 So Säcker-*Klesczewski*, § 109 TKG Rn. 5.

durch vor allem die Vertraulichkeit der Telekommunikation (gegen den Eingriff von Dritten)[1297] und der störungsfreie Betrieb. Darüber hinausgehend sind die Betreiber von Telekommunikationsanlagen, die als solche den unmittelbaren technischen Zugriff auf die Systeme haben,[1298] die dem Erbringen von Telekommunikationsdiensten für die Öffentlichkeit dienen, nach § 109 Abs. 2 TKG verpflichtet, angemessene technische Vorkehrungen und sonstige Maßnahmen zum Schutz gegen Störungen, die zu erheblichen Beeinträchtigungen von Telekommunikationsnetzen führen und gegen äußere Angriffe (z.B. durch Hacker) und Einwirkungen von Katastrophen zu treffen. Darunter fällt insbesondere die Pflicht zur **Datensicherung**, wodurch Daten vor Verlust, Zerstörung infolge von Beschädigung der Daten verarbeitenden Systeme, vor unbefugter Veränderung und vor Missbrauch geschützt werden sollen.[1299] Unter Missbrauch sind Angriffe von Außenstehenden (Hackern) und die unbefugte Datenverwendung durch Mitarbeiter gemeint.[1300] Welche Schutzmaßnahmen angemessen sind, muss anhand des Einzelfalles entschieden werden.[1301] Hierzu haben sie einen Sicherheitsbeauftragten zu benennen und ein Sicherheitskonzept zu erstellen (§ 109 Abs. 3 TKG). Technische Anforderungen im Sinne von § 109 TKG sind Maßnahmen mit Bezug auf die Funktionsweise der Telekommunikationsanlagen.[1302] Hierunter sind für den Bereich der Störungsabwehr (§ 109 Abs. 1 Nr. 2, Abs. 2 TKG) beispielsweise die Vorhaltung redundanter Systeme oder von Überbrückungsaggregaten zu verstehen.[1303] Bietet ein Diensteanbieter beispielsweise Voice over IP an, so werden Sprachpakete über das Internet versendet. Um zu verhindern, dass dadurch ein offenes Netz entsteht, ist der Diensteanbieter gem. § 109 Abs. 1 TKG gehalten, durch entsprechende Verschlüsselung der Datenpakete für sichere Verbindungen zu sorgen und unerbetene Lauschangriffe auf die Internet-Telefonie wirksam zu verhindern.[1304] Die sonstigen Maßnahmen betreffen vor allem Kontroll- und Organisationsmaßnahmen (z.B. Zugangskontrollen, Zugriffsbeschränkungen bzgl. Daten, Mit-

1297 *Koenig/Loetz/Neumann*, Telekommunikationsrecht, S. 209.
1298 *Koenig/Loetz/Neumann*, Telekommunikationsrecht, S. 209.
1299 *Elbel*, Die datenschutzrechtlichen Vorschriften für Diensteanbieter im neuen Telekommunikationsgesetz auf dem Prüfstand des europäischen und deutschen Rechts, S. 104.
1300 *Geppert/Ruhle/Schuster*, Handbuch Recht und Praxis der Telekommunikation, Rn. 785; *Elbel*, Die datenschutzrechtlichen Vorschriften für Diensteanbieter im neuen Telekommunikationsgesetz auf dem Prüfstand des europäischen und deutschen Rechts, S. 104; Beck`scher TKG-Kommentar-*Bock*, § 109 TKG Rn. 29.
1301 *Koenig/Loetz/Neumann*, Telekommunikationsrecht, S. 209.
1302 Scheurle/Mayen-*Zerres*, § 87 TKG Rn. 16; Säcker-*Klesczewski*, § 109 TKG Rn. 10.
1303 Säcker-*Klesczewski*, § 109 TKG Rn. 18.
1304 *Katko*, CR 2005, 189 (192).

arbeiterschulung) sowie vertragliche Absicherungen.[1305] Ergreift ein Provider also Maßnahmen zur Abwehr eines Angriffes durch Computerviren, so wird er sich auf § 109 TKG berufen können.[1306] Ähnliches gilt für ein Unternehmen, dass ihren Arbeitgebern die private Internetnutzung gestattet. In diesem Fall ist das Unternehmen Diensteanbieter iSd § 109 Abs. 1 TKG und muss danach angemessene Vorkehrungen und Maßnahmen zu Schutz des Fernmeldegeheimnisses, personenbezogener Daten sowie der Telekommunikations- und Datenverarbeitungssysteme treffen, was auch den Schutz gegen Spam und Viren umfasst.[1307]

724 Zur Durchsetzung der die Diensteanbieter und Betreiber von Telekommunikationsanlagen nach dem TKG treffenden Verpflichtungen kann die Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen als zuständige Regulierungsbehörde (§ 116 TKG) nach §§ 115, 126 TKG Anordnungen, Verwaltungsakte und andere Maßnahmen treffen.[1308]

725 Das Problem an der Regelung des § 109 TKG ist, dass er dem Betreiber und Diensteanbietern zwar gewisse Sicherheitspflichten aufgibt, ein Mindestniveau für die Sicherheit aber durch die zum Teil wenig konkreten Anforderungen kaum ersichtlich ist.[1309] Noch im alten § 87 TKG war eine Verordnungsermächtigung enthalten, nach der die Bundesregierung die Möglichkeit gehabt hätte, die Maßnahmen zur Gewährleistung der technischen Sicherheit verbindlich festzulegen. Diese Verordnungsermächtigung wurde aber im neuen § 109 TKG gestrichen, da davon nach aktueller Einschätzung kein Gebrauch gemacht werden solle,[1310] weil aufgrund aktueller Studien belegt sei, dass eine hohe Sicherheit und Leistungsfähigkeit in der deutschen Telekommunikationsinfrastruktur bestünde.[1311] Empfehlungen zur Verbesserung des Sicherheitsniveaus wurden zwar bereits vom Bundesamt für Sicherheit in der Informationstechnik abgegeben,[1312] so dass ein Schritt in Richtung Mindeststandard vollzogen wurde. Allerdings handelt es sich dabei um einen Maßnahmenkatalog aus dem Jahr 1998, der aufgrund der schnellen Entwick-

---

1305 Säcker-*Klesczewski*, § 109 TKG Rn. 10.
1306 So *Cornelius/Tschoepe*, K&R 2005, 269 (271).
1307 *Dendorfer/Niedderer*, AuR 2006, 214 (217).
1308 Zum Verhältnis der Anordnungsbefugnisse nach § 115 und § 126 TKG Säcker-*Klesczewski*, § 115 TKG Rn. 5; Säcker-*Ruffert*, § 126 TKG Rn. 4.
1309 IdS auch *Geppert/Ruhle/Schuster*, Handbuch Recht und Praxis der Telekommunikation, Rn. 777.
1310 So ausdrücklich die Gesetzesbegründung zu § 107 TKG-E BT-Drucks. 15/2316, S. 91.
1311 S. dazu Beck`scher TKG-Kommentar-*Bock*, § 109 TKG Rn. 3.
1312 BSI, Sicherer Einsatz von digitalen Telekommunikationsanlagen, abrufbar unter: http://www.bsi.bund.de/literat/tkanlage/6001.pdf (zuletzt abgerufen am 06.06.2007).

lung im Telekommunikationsbereich heute als veraltet angesehen werden kann. Auch existieren neben § 109 TKG zahlreiche weitere Vorschriften im Post und Telekommunikationssicherstellungsgesetz (PTSG), sowie den daraus erlassenen Verordnungen (Richtlinie für den betrieblichen Katastrophenschutz (RichtlBKO) und Post- und Telekommunikations-Zivilschutzverordnung (PTZSV)), in der Telekommunikations-Sicherstellungsverordnung (TKSIV) sowie dem § 9 BDSG samt Anlage zu Satz 1, die sich teilweise mit dem Anwendungsbereich von § 109 TKG überschneiden. Dabei sind das PTSG und seine Rechtsverordnungen gegenüber § 109 TKG spezieller und § 109 TKG ist gegenüber § 9 BDSG die Spezialvorschrift.[1313] Daher wird § 109 TKG zum Teil sogar als überflüssig angesehen.[1314] Daraus resultiert die weitere Problematik, dass die technische Sicherheit in zahlreichen Normen verstreut zum Teil ohne konkrete Anforderungen geregelt wird, was wiederum zu Rechtsunsicherheiten führt.[1315]

V. Ergebnis

726 Im Bereich der IT-Sicherheit trifft die IT-Intermediäre grundsätzlich eine volle zivilrechtliche Verantwortlichkeit für die Sicherheit ihrer eigenen Systeme, wobei im Einzelfall Haftungsbeschränkungen aufgrund von § 7 TKV aF bzw. § 44a TKG und durch Regelungen in AGB in Betracht kommen. Soweit der Provider als bloßer Mittler für Dritte agiert, kommen ihm dagegen – abhängig von der jeweils ausgeübten Funktion – die Haftungsprivilegierungen der §§ 7 - 10 TMG zugute. Die Rechtslage ist jedoch geprägt durch ein kompliziertes Ineinandergreifen verschiedener Regelungsmaterien, welche die rechtliche Einordnung des Providers im Einzelfall erschweren und zu nicht unerheblicher Rechtsunsicherheit in diesem Bereich beitragen. Dies zeigt sich insbesondere am Beispiel der Anwendbarkeit des TKG auf Internet-Provider, welche wegen der Haftungsregelung des § 7 TKV aF bzw. § 44a TKG praktisch bedeutsam werden kann.

F. Endergebnis dieses Gutachtens: Verantwortungsverteilung und Anreizdefizite im nationalen Recht

1313 Beck`scher TKG-Kommentar-*Bock*, § 109 TKG Rn. 12 ff.

1314 So z.B. der BITKOM, Stellungnahme zu BT-Drucks. 15/2316, vom 3.02.2004, abrufbar unter: http://www.bitkom.org/files/documents/StN_BITKOM_TKG_Wirtschaftsausschuss_03.02.04.pdf; Beck`scher TKG-Kommentar-*Bock*, § 109 TKG Rn. 2.

1315 *Geppert/Ruhle/Schuster*, Handbuch Recht und Praxis der Telekommunikation, Rn. 777; kritisch wegen der unpräzisen Anforderungen in der TKSiV auch Beck`scher TKG-Kommentar-*Bock*, § 109 TKG Rn. 14.

727 Die Verantwortungsverteilung im nationalen Recht für die IT-Sicherheit kann anhand der IT-Wertschöpfungskette (IT-Hersteller – IT-Intermediär – IT-Nutzer bzw. Ersteller weiterer IT-Dienstleistungen) analysiert und differenziert werden.[1316] Einheitliche Regelungen oder ein übergreifender Ansatz zur Gewährleistung einer grundlegenden IT-Sicherheit – unabhängig von vertraglichen Regelungen – fehlen indes; die Strukturen stellen sich als inhomogen dar. Lediglich die Regelungen im Datenschutzrecht bezüglich einer datenschutzsichernden Organisation, die Elemente eines IT-Riskmanagements umfassen, erstrecken sich als spezifische IT-bezogene Normen breitflächig auf zahlreiche Nutzer und IT-Anbieter. Im geltenden Recht muss daher im Wesentlichen auf die allgemeinen Regelungen im bürgerlichen sowie im öffentlichen Recht rekurriert werden. Dabei kann grob zwischen produkt-, dienstleistungs- und organisationsbezogenen Regelungen unterschieden werden:

728 Für **IT-Hersteller** sind vor allem die produktbezogenen Sicherungspflichten des Produkthaftungs- und des Produktsicherheitsrecht einschlägig. Allerdings offenbaren sich hier erhebliche Defizite:

- Im öffentlich-rechtlichen Produktsicherheitsrecht finden sich bislang kaum relevante technische Regeln für IT-Produkte, wenn, dann nur als „Abfallprodukt“ anderer Normungen. Ausnahmen wie das Medizinproduktegesetz bestätigen hier die Regel. Zudem sind die meisten Produktsicherheitsnormen, erst recht das allgemeine GPSG, auf Körperschäden sowie auf Verbraucherschutz beschränkt; die für IT-Produkte typischen Schäden, wie Vermögens- oder Eigentumsschäden, werden gerade nicht erfasst.

- Im Produkthaftungsrecht ist im Rahmen der verschuldensunabhängigen Haftung zunächst die Eigenschaft der Software als Produkt nach wie vor nicht vollkommen geklärt. Für die allgemeine deliktische Haftung zeigen sich ähnlich dem Produktsicherheitsrecht die gleichen Probleme, indem Vermögensschäden nur ausnahmsweise erfasst werden. Zudem bedarf es einer extensiven Interpretation des Eigentumsbegriffs, die bislang nicht höchstrichterlich abgesichert ist, um Schäden an Daten und Datenbeständen zu erfassen. Gleiches gilt für das Recht am eingerichteten und ausgeübten Gewerbebetrieb.

- Der Geschädigte trägt zudem die Beweislast für die Fehlerhaftigkeit der Software sowie für die Kausalität zwischen fehlerhaftem Produkt und Rechtsgutsverletzung sowie Schaden. Trotz der Umkehr der Beweislast für die Frage der Pflichtwidrigkeit sieht sich der Geschädigte daher gerade bei IT-Produkten einer schier unüberwindlichen Beweislast gegenüber, da zum einen IT-Produkte häufig gemeinsam mit anderen IT-Produkten und –dienstleistungen eingesetzt werden, zum anderen Bedienungs- oder Installationsfehler nie auszuschließen sind.

1316 Oben Rn. 91 ff.

- Das Deliktsrecht kann keine Schäden erfassen, die grundsätzlich vom Äquivalenzinteresse gedeckt sind. Ob Patches bzw. die nachträgliche Schließung von Sicherheitslücken noch vom Deliktsrecht als Pflichten erfasst werden (etwa als Rückrufpflichten) ist mehr als fraglich.

729 Hingegen können Produktsicherheits- und Produkthaftungsrecht als Modelle auch für andere Regelungen im Hinblick auf die rechtliche Bedeutung von technischen Standards und Regeln herangezogen werden. So wie DIN-Normen oder andere technische Standards Vermutungswirkungen (Produktsicherheitsrecht) oder Beweiserleichterungen auslösen (Produkthaftungsrecht) können auch die für IT-Produkte entwickelten Common Criteria im Zusammenhang mit Protection profiles als allgemein anerkannte Regeln der Technik im Bereich der Software für bestimmte Produkte angesehen werden.

730 Von den produktbezogenen Regeln und Standards sind die **tätigkeitsbezogenen Pflichten** der IT-Intermediäre und IT-Nutzer zu unterscheiden:

731 Hier besteht für **IT-Intermediäre** eine Gemengelage aus Haftungsprivilegierungen durch das TMG bzw. die E-Commerce-Richtlinie einerseits, Pflichten zur Sicherung der eigenen IT-Systeme andererseits. Letztere werden schließlich im Bereich der Telekommunikationsdienste, die die meisten der IT-Intermediäre erfasst, wenn sie selbst elektronische Kommunikationsnetze betreiben, erheblich durch die Haftungsprivilegierung des § 44a TKG abgeschwächt. Ob und inwieweit diese Haftungsbegrenzungen gegenüber dem IT-Intermediär auch auf Schäden anzuwenden sind, die der Nutzer eines Netzes infolge von Einwirkungen Dritter erleidet (Hacking etc.), ist bislang noch ungeklärt, wohl aber anzunehmen. Allerdings greifen diese Haftungsprivilegierungen nicht gegenüber Dritten, die über die Netze des IT-Intermediärs geschädigt werden, da keine vertragliche Beziehungen zwischen geschädigtem Dritten und dem IT-Intermediär bestehen, die § 44a TKG aber voraussetzt; indes sieht sich hier der geschädigte Dritte sämtlichen Einschränkungen und Beweisproblemen gegenüber, die auch gegenüber IT-Herstellern eingreifen, insbesondere Kausalität, Anspruchsgrundlage (deliktisch bzw. kein Schutz von Vermögensschäden etc.). Aus öffentlich-rechtlicher Sicht trifft die IT-Intermediäre zwar eine grundsätzlich vorgesehene Pflicht zur Sicherung ihrer Netze; aber auch diese ist offenbar nicht spezifisch auf IT-Sicherheitsfragen ausgerichtet und bislang wenig konkretisiert worden, wenngleich im Grundsatz hier Ermächtigungsgrundlagen zur Verfügung stünden. § 109 TKG ist aber schwerpunktmäßig auf die Sicherung des Netzes gegen Kommunikationsstörungen ausgerichtet, nicht aber hinsichtlich des Schutzes auch Dritter gegenüber Angriffen über das Netz. Die anderen Sicherungspflichten entsprechen denjenigen des Datenschutzrechts. Auch ist bislang unge-

klärt, in welchem Verhältnis solche Anforderungen zu denjenigen der IT-Sicherheit von Intermediären stehen. Selbst im Vergleich zu den IT-Herstellern bestehen daher für IT-Intermediäre insgesamt nur geringe Anreize, die IT-Sicherheit zu verbessern.

732 Anders sieht die Situation dagegen für **IT-Nutzer** aus, insbesondere bei kommerziellen IT-Nutzern, die ihrerseits wiederum Dienstleistungen erbringen oder Produkte mit Hilfe der eingesetzten IT erzeugen: Diese unterliegen zahlreichen Selbstschutzpflichten, die ihrerseits auch wiederum Verkehrssicherungspflichten gegenüber Dritten entsprechen – wobei diese Dritthaftung in ähnlicher Weise wie bei den IT-Herstellern auf die Verletzung bestimmter Rechtsgüter beschränkt ist. Hier ist zu unterscheiden zwischen tätigkeits- und organisationsbezogenen Pflichten: So können etwa bei der Erbringung von IT-Dienstleistungen, wozu auch das Online-Banking gehört, bestimmte Mindestsicherheitsstandards vom Kunden (vertraglich) erwartet werden, deren Verletzung sowohl Konsequenzen im prozessualen Bereich als auch im materiell-rechtlichen Bereich für die Bank hat, etwa fehlende Verschlüsselungen etc. All dies sind **auf die jeweilige Tätigkeit bzw. IT-Dienstleistung bezogene Anforderungen**. Defizite bestehen hier im Wesentlichen nicht bei den rechtlichen Grundlagen an sich, da die allgemeinen rechtlichen Vorgaben, wie die im Verkehr übliche Sorgfalt nach § 276 BGB in der Lage sind, flexible Antworten auf neue Gefahren zu geben; vielmehr besteht hier in erster Linie das Problem im Fehlen weitgehend konsentierter Standards, die als Mindestsicherheit auf jeden Fall zu beachten sind, und deren Verletzung per se eine Haftung auslöst. Häufig zeigt sich, dass Kunden nicht über die nötigen Informationen verfügen, um gegebenenfalls ihre Ansprüche durchsetzen zu können (Enforcement-Problem). Auch ist häufig unklar, innerhalb welcher Zeit und wann z.B. Banken auf geänderte Sicherheitsanforderungen und Gefährdungslagen reagieren müssen, z.B. durch Übergang von TAN-Verfahren auf neue sicherere Verfahren. Hier können anderweitig gesetzte Standards Abhilfe schaffen.

733 Davon zu trennen sind die **organisationsbezogenen Pflichten**, die sich auf das IT-Riskmanagement eines Unternehmens beziehen. Das deutsche Recht verweist im Wesentlichen in zwei Materien auf Riskmanagement im weiteren Sinne, zum einen in § 91 Abs. 2 AktG, der auch auf andere Gesellschaften anwendbar ist, zum anderen in § 9a BDSG. Doch sind auch hier Defizite zu konstatieren: Die gesellschaftsrechtlichen Regelungen weisen einen hohen Abstraktionsgrad auf, bedürfen der Konkretisierung. Zudem wirken sie nur im Innenverhältnis, bei fehlender Durchsetzung gehen die Vorgaben da-

her ins Leere. Hinsichtlich §§ 9, 9a BDSG ist der Schutz nur für personenbezogene Daten von natürlichen Personen gegeben, der zwar weit reicht, keineswegs aber alle Fragen eines IT-Riskmanagements erfasst, etwa des Einkaufs von IT-Produkten, der Sicherheit von unternehmensinternen Netzen gegenüber davon ausgehenden Angriffen gegenüber Dritten. Ebenso wenig werden Daten von juristischen Personen oder nichtpersonenbezogene Daten vom Schutz erfasst – wenngleich die meisten Maßnahmen nach §§ 9, 9a BDSG wohl gleichzeitig auch diese Daten schützen werden. Eines der wesentlichen Probleme neben dem eingeschränkten Anwendungsbereich des §§ 9, 9a BDSG ist aber der Vollzug – es ist keineswegs gesichert, dass die teilweise umfangreichen Anforderungen des Datenschutz-Riskmanagements auch tatsächlich durchgeführt werden, zumal die §§ 9, 9a BDSG zivilrechtlich nicht durchsetzbar sind. Herangezogen werden können in diesem Rahmen bereits vorhandene Standards, die auf das IT-Riskmanagement bezogen sind, wie die ISO 27001 oder das BSI-IT-Grundschutzhandbuch. Diese Standards können wie allgemein anerkannte Regeln wirken und Vermutungswirkungen auslösen, sei es bei ihrer Einhaltung oder Verletzung. Inwieweit hier indes Zertifizierungen eine entlastende Wirkung auslösen, ist bislang noch weitgehend ungeklärt.

734 Für **private IT-Nutzer** hingegen ergeben sich nur rudimentäre (Selbst-) Schutzpflichten, die sich auf allgemein bekannte und leicht zugängliche Schutzmaßnahmen beschränken. Je weiter verbreitet indes derartige Eigenschutzmaßnahmen sind, desto eher sind sie auch den privaten IT-Nutzern zuzumuten. Darüber hinausgehende Pflichten lassen sich aber dem geltenden Recht nicht entnehmen, weder dem bürgerlichen noch dem öffentlichen Recht. Insbesondere wenn Gefahren von privaten Nutzern ausgehen, z.B. durch Weiterverbreitung von Viren durch ungesicherte Rechner, kommt in den meisten Fällen keine Haftung in Betracht. Hier stellen sich zum einen dieselben Probleme wie im Rahmen der IT-Produkthaftung (keine Erfassung von Vermögensschäden, Beweisprobleme), zum anderen kann lediglich für völlig offensichtliche Gefährdungslagen von einem Verschulden der privaten IT-Nutzer ausgegangen werden.

735 Überlappt werden alle Probleme schließlich durch **Darlegungs- und Beweisprobleme** für Geschädigte – was wiederum zu einer Abschwächung von rechtlichen Anreizen für Verantwortliche führt. Diese Beweisprobleme betreffen sowohl den Nachweis, dass eingesetzte IT-Produkte fehlerhaft sind, als auch den Nachweis, dass genau dieser Fehler zu dem eingetretenen Schaden geführt hat. Ferner sind IT-Nutzer häufig mit der Fra-

ge konfrontiert, welche Standards gelten, insbesondere welche Beweiserleichterungen, wenn es um den Nachweis der Identität und der Authentizität geht, etwa im Bereich des Online-Banking. Der bislang angenommene Anscheinsbeweis beruht auf der Annahme, dass die eingesetzten Verfahren sicher sind – was wiederum im Prozess der Nutzer derzeit zu erschüttern hat, was ihm meist nicht gelingt, schon aufgrund seiner Unterlegenheit bei den einsetzbaren Ressourcen (Kosten für Sachverständigengutachten, Informationsdefizite).

Tabellarische Übersicht

Verantwortlicher	**Zivilrecht**	**Öffentliches Recht**	**Standards**
IT-Hersteller	Vertragsrecht: - Haftungsausschlüsse - Schwierige Einordnung der Software als Sache (Verbrauchsgüterkauf?) - Keine Haftung von Händler für Mangelfolgeschäden - Kein zwingender Regress bei internationalem Softwareüberlassung (Händlerkette) Produkthaftungsrecht: - Anwendung ProdHaftG auf	Produktsicherheitsrecht: - im Wesentlichen nur anwendbar auf Körperschäden - nur Verbraucher eingeschlossen	Common Criteria und Protection Profiles – insgesamt noch stark im Fluss

	Software umstritten - Eigentumsbegriff unklar (Daten?) - keine Vermögensschäden - schwierige Beweislage (Kausalität)		
IT-Intermediär	Deliktsrecht: wie bei IT-Hersteller Vertragsrecht: Haftungsbegrenzung durch TKG selbst bei grober Fahrlässigkeit	Telekommunikationsrecht: ähnlich Datenschutzrecht; Sicherungspflichten nur hinsichtlich der ungestörten Kommunikation	Nur wenige Standards (ISO-Norm zur Netzwerksicherheit); zukünftige Normen BSI?
Kommerzielle IT-Nutzer allgemein (IT-Riskmanagement)	Gesellschaftsrecht: prinzipiell Ansatz über Pflicht zum Riskmanagement, aber ausfüllungsbedürftig Vertragsrecht: - Haftungsausschlüsse - umstr. Anscheinsbeweis, Sicherheitsanforderungen Deliktsrecht: Pflicht zur Sicherung der eigenen Systeme, auch gegenüber Dritten	Aufsichtsrecht: - § 9a BDSG: Pflichten zur Organisation zum Datenschutz (allerdings Enforcement-Probleme)	ISO 27.001 ff.; IT-Grundschutzhandbuch BSI

Kommerzielle IT-Nutzer branchenspezifisch: Finanzdienstleistungssektor	Zusammenspiel Sicherheitsanforderungen und Anscheinsbeweis bzw. Pflichtenbestimmung gegenüber Kunden	Aufsichtsrecht: allgemeine Pflicht zum IT-Riskmanagement (§ 25a KWG), Konkretisierung bislang unklar	MaRisk (BaFin) – aber relativ abstrakt

G. Literaturverzeichnis

Abel, Ralf Bernd (Hrsg.)	Datenschutz in Anwaltschaft, Notariat und Justiz, 2. Auflage, München 2003 zitiert: *Bearbeiter*, in: Abel, Datenschutz in Anwaltschaft, Notariat und Justiz
Adams, Michael	Ökonomische Analyse der Gefährdungs- und Verschuldenshaftung, Heidelberg 1985
Adams, Heinz/ Löhr, Volker	„Bedeutung von Qualitätssicherungssystemen in der entstehenden Haftungsgesellschaft“ in: QZ 36 (1991), 24-26
Altmeppen, Holger	„Die Auswirkungen des KonTraG auf die GmbH“ in: ZGR 1999, 291-313
Altmeppen, Holger	„Haftung der Geschäftsleiter einer Kapitalgesellschaft für Verletzung von Verkehrssicherungspflichten“ in: ZIP 1995, 881-882, 884-891
Angermüller, Niels O./ Eichhorn, Michael/ Ramke, Thomas	„MaRisk - Noch mehr Regulierung in Sicht?“ in: Kreditwesen 2004, 833-834
Angermüller, Niels O./ Eichhorn, Michael/ Ramke, Thomas	„MaRisk - der Nebel lichtet sich“ in: Kreditwesen 2005, 396-398
Anonymus	Der neue Hacker’s Guide, 2. Auflage, München 2001
Arbeitskreis "Externe und Interne Überwachung	„Auswirkung des Sarbanes-Oxley Act auf

der Unternehmung" der Schmalenbach-Gesellschaft für Betriebswirtschaft e. V.	die Interne und Externe Unternehmensüberwachung“ in: BB 2004, 2399-2407
Arendts, Martin	„Betrügerische Verhaltensweisen bei der Anlageberatung und der Vermögensverwaltung“ in: ÖBA 1996, 775-781
Assmann, Heinz-Dieter/ Schneider, Uwe H.	Wertpapierhandelsgesetz, Kommentar, 4. Auflage, Köln 2006 zitiert: Assmann/Schneider-*Bearbeiter*
Assmann, Heinz-Dieter/ Kirchner, Christian/ Schanze, Erich	Ökonomische Analyse des Rechts, Tübingen 1993 zitiert: *Bearbeiter*, in: Assmann/Kirchner/Schanze
Auernhammer, Herbert	Bundesdatenschutzgesetz, 3. Auflage, Köln, Berlin, Bonn, München 1993 zitiert: Auernhammer-*Bearbeiter*
Aufhauser, Rudolf/ Hindinger-Back, Helmut	Bundesdatenschutzgesetz, Kochel am See 1996 zitiert: Aufhauser/Hindinger-Back-*Bearbeiter*
Backu, Frieder	„Pflicht zur Verschlüsselung?“ in: ITRB 2003, 251-253
Balzer, Peter	„Rechtsfragen des Effektengeschäfts der Direktbanken“ in: WM 2001, 1533-1542
Balzer, Peter	„Haftung von Direktbanken bei Nichterreichbarkeit“ in: ZBB 2000, 258-268

Bamberger, Heinz Georg/ Roth, Herbert	Kommentar zum Bürgerlichen Gesetzbuch, Bd. 1-3, München 2003 zitiert: Bamberger/Roth-*Bearbeiter*
Bartl, Harald	Produkthaftung nach neuem EG-Recht: Kommentar zum deutschen Produkthaftungsgesetz, Landsberg (Lech) 1989
Bartsch, Michael	„Software und das Jahr 2000“ in: CR 1998, 193-196
Bartsch, Michael	„Computerviren und Produkthaftung“ in: CR 2000, 721-725
Bartsch, Michael	Rechtsmängelhaftung bei Überlassung von Software, CR 2005, 1-10
Bartsch, Michael	Software und das Jahr 2000 – Haftung und Versicherungsschutz für ein technisches Großproblem, Baden-Baden 1998
Bauer, Axel	„Produkthaftung für Software nach geltendem und künftigem deutschen Recht“, Teile 1 und 2 in: PHi 1989, 38-48, 98-108
Baum, Florian	„Gestaltung von Software-Maintenance-Verträgen in der internationalen Praxis“ in: CR 2002, 705 ff.
Baumbach, Adolf/ Hueck, Alfred	GmbH-Gesetz, 18. Auflage, München 2006 zitiert: Baumbach/Hueck-*Bearbeiter*
Baumbach, Adolf/ Hopt, Klaus J.	Handelsgesetzbuch, Kommentar, München 2006

	zitiert: Baumbach/Hopt-*Bearbeiter*
Bäumler, Helmut	„Ein Gütesiegel für den Datenschutz“ in: DuD 2004, 80-84
Baumol, Wiliam J.	Ecomonic Theory and Operations Analysis, 5. Auflage, London 1977
Bayer, Thomas	Auswirkungen eines zertifizierten Qualitätsmanagements nach DIN EN ISO 9000ff. auf die Haftungssituation im Unternehmen, Berlin 1988
Becker, Bernhard/ Janker, Bernd/ Müller, Stefan	„Die Optimierung des Risikomanagements als Chance für den Mittelstand“ in: DStR 2004, 1578-1584
Beckmann, Kirsten/ Müller, Ulf	„Online übermittelte Informationen - Produkte iSd Produkthaftungsgesetzes?“ in: MMR 1999, 14-18
Behnke, Alexander/ Schäffter, Markus	„IT-Entscheider in der Haftung“ in: DSB 2002, Nr. 7/8, 10-11
Behrens, Peter	Die ökonomischen Grundlagen des Rechts, Tübingen 1986
Benöhr, Hans-Peter	„Die Entscheidung des BGH für das Verschuldensprinzip“ in: Tijdschrift voor Rechtsgeschiedenis 46, 1978, 1-32
Berndt, Thomas/ Hoppler, Ivo	„Whistleblowing - ein integraler Bestandteil effektiver Corporate Governance“ in: BB 2005, 2623-2629
Bigdoli, Hossein	Handbook of Information Security, Volume

	1: Key Concepts, Infrastructure, Standards, and Protocols, 2006
Bigdoli, Hossein	Handbook of Information Security, Volume 2: Information Warfare; Social, Legal, and International Issues; and Security Foundations, 2006
Bigdoli, Hossein	Handbook of Information Security – Volume 3: Threats, Vulnerabilities, Prevention, Detection, and Management, 2006
Bigdoli, Hossein	Encyclopedia of Informationsystems Volume 1, Academic Press, Boston 2002
Bigdoli, Hossein	Encyclopedia of Informationsystems Volume 2, Academic Press, Boston 2002
Bigdoli, Hossein	Encyclopedia of Informationsystems Volume 4, Academic Press, Boston 2002
Birkmann, Andreas	„Produktbeobachtungspflicht bei Kraftfahrzeugen - Entwicklung und Weiterentwicklung der Produktbeobachtungspflicht durch die Rechtsprechung des Bundesgerichtshofs“ in: DAR 1990, 124-130
Bizer, Johann	„Bausteine eines Datenschutzaudits“ in: DuD 2006, 5-12
Blaurock, Uwe	„Haftung der Banken beim Einsatz neuer Techniken im Zahlungsverkehr“ in: CR 1989, 561-567

Böcker, Klaus/ Spielberg, Holger	„Basel II und ökonomisches Kapital: Risikoaggregation und Kopulas“ in: Die Bank 2005, 56-59
Bockslaff, Klaus	„Die eventuelle Verpflichtung zur Errichtung eines sicherungstechnischen Risikomanagements durch das KonTraG“ in: NVersZ 1999, 104-110
Bodewig, Theo	Vertragliche Pflichten „post contractum finitum“, JURA 2005, 505-512.
Boecken, Winfried	Deliktsrechtlicher Eigentumsschutz gegen reine Nutzungsbeeinträchtigungen, Berlin 1995
Bohne, Marco	„Zugriffsrechte effizient verwalten“ in: VW 2004, 1583-1584
Bölscher, Jens/ Kaiser, Christian/ v. Schulenurg, Johann-Matthias	„Hacker gibt es wirklich! Wachsende Gefährdung der Versicherungswirtschaft durch Hacker-Angriffe“ in: VW 2002, 565
Bömer, Roland	„Risikozuweisung für unvermeidbare Softwarefehler“ in: CR 1989, 361-367
Boos, Karl-Heinz/ Fischer, Reinfried/ Schulte-Mattler, Hermann	Kreditwesengesetz, Kommentar zu KWG und Ausführungsvorschriften, 2. Auflage, München 2004 zitiert: Boos/Fischer/Schulte-Mattler-*Bearbeiter*
Borges, Georg	Rechtsfragen des Phishing – Ein Überblick in: NJW 2005, 3313-3317

Borsum, Wolfgang/ Hoffmeiser, Uwe	„Rechtsgeschäftliches Handeln unberechtigter Personen mittels Bildschirmtext“ in: NJW 1985, 1205-1207
Borsum, Wolfgang/ Hoffmeister, Uwe	„Rechtsgeschäftliches Handeln unberechtigter Personen mittels Bildschirmtext“ in: NJW 1985, 1205-1207
Brandi-Dohrn, Matthias	Gewährleistung bei Hard- und Softwaremängeln: BGB, Leasing und UN-Kaufrecht, 2. Auflage, München 1994
Bräutigam, Peter/ Leupold, Andreas (Hrsg.)	Online-Handel, München 2003 zitiert: *Bearbeiter*, in: Bräutigam/Leupold
Breulmann, Günter	Normung und Rechtsangleichung in der Europäischen Rechtsangleichung, Berlin 1993
Bröcker, Klaus Tim/ Czychowski, Christian/ Schäfer, Detmar	Praxishandbuch Geistiges Eigentum im Internet, München 2003 zitiert: *Bearbeiter*, in: Bröcker/Czychowski/Schäfer
Brown, John Prather	„Toward an Economic Theory of Liability“, in: The Journal of Legal Studies, Bd. 2, 1973, 323-349
Brüggemeier, Gert	Deliktsrecht, Baden-Baden 1986
Brüggemeier, Gert	„Produzentenhaftung nach § 823 Abs. 1 BGB – Bestandsaufnahme und Perspektiven weiterer judizieller Rechtsentwicklung“ in: WM 1982, 1249-1309

Brüggemeier, Gert	„Organisationshaftung“ in: AcP 191 (1991), 33-68
Bruns, Alexander	Informationsansprüche gegen Medien – Ein Beitrag zur Verbesserung des Persönlichkeitsschutzes im Medienprivatrecht, Diss. Iur. Universität Freiburg, Tübingen, 1997
Buchner, Herbert	Die Bedeutung des Rechts am eingerichteten und ausgeübten Gewerbebetrieb für den deliktsrechtlichen Unternehmensschutz, München 1971
Büchting, Hans-Ulrich (Hrsg.)	Beck’sches Rechtanwalts-Handbuch, München 2004 zitiert: *Bearbeiter*, in: RAnwHdb
Büllingen, Franz/ Hillebrad, Annette	„Biometrie als Teil der Sicherungsinfrastruktur?“ in: DuD 2000, 339-343
Bülow, Dieter	„Regulatorische Anforderungen an die IT: Lösungswege einer ITSM/Provisioning-Plattform“ in: DSB 10/2005, 13-14
Bundesamt für Sicherheit in der Informationstechnik (BSI)	IT-Grundschutzhandbuch, Köln 2003
Bundesamt für Sicherheit in der Informationstechnik (BSI)	Einführung von Intrusion-Detection-Systemen, http://www.bsi.bund.de/literat/studien/ids02/dokumente/Rechtv10.pdf
Bundesamt für Sicherheit in der Informationstechnik (BSI)	BSI-Lagebericht 2005, http://www.bsi.de/literat/lagebericht/lagebericht2005.pdf
Bundesamt für Sicherheit in der Informations-	Zertifizierung nach ISO 27001 auf der Ba-

technik (BSI)	sis von IT-Grundschutz, Prüfungsschema für ISO 27001 Audits, http://www.bsi.bund.de/gshb/zert/ISO27001/Pruefschema06.pdf
Bundesrechtsanwaltskammer, Ausschuss Datenschutzrecht	Stellungnahme der Bundesrechtsanwaltskammer zu der Frage der Bestellung eines Beauftragten für Datenschutz in Rechtsanwaltskanzleien, BRAK-Stellungnahme-Nr. 31/2004, http://www.brak.de/seiten/pdf/Stellungnahmen/2004/StnBDSinKanzleien.pdf
Burg, Michael/ Gimnich, Martin	„Illegale Dialer im Internet“ in: DRiZ 2003, 381-385
Burgartz, Dieter/ Blum, Thomas	QM-Optimizing in der Softwareentwicklung, 2. Auflage, Braunschweig 1998
Bürkle, Jürgen	„Auswirkungen der Unternehmensaufsicht nach dem KWG auf organisatorische Pflichten von Versicherungsunternehmen“ in: WM 2005, 1496-1505
Büssow, Thomas/ Taetzner, Tobias	„Sarbanes-Oxley Act Section 404: Internes Kontrollsystem zur Sicherstellung einer effektiven Finanzberichterstattung im Steuerbereich von Unternehmen - Pflicht oder Kür?“ in: BB 2005, 2437-2444
C & L Deutsche Revision (Hrsg.)	6. KWG-Novelle und neuer Grundsatz I, Frankfurt am Main, 1998
Cahn, Andreas	„Produkthaftung für verkörperte geistige

	Leistungen“ in: NJW 1996, 2899-2905
Calabresi, Guido	The Cost of Accidents, Yale, 2000
Callies, Christian/ Ruffert, Matthias	Kommentar zu EU-Vertrag und EG-Vertrag, 2. Auflage, Neuwied Kriftel Berlin 2006 zitiert: *Bearbeiter* in: Callies/Ruffert
Canaris, Claus-Wilhelm	Die Vertrauenshaftung im deutschen Privatrecht, München 1971 zitiert: *Canaris*, Die Vertrauenshaftung im deutschen Privatrecht
Canaris, Claus-Wilhelm	Bankvertragsrecht 3. Auflage, Berlin New York 1988 zitiert: *Canaris*, Bankvertragsrecht
Capellaro, Christoph/ Füser, Karsten	„Basel II: IT-Risiken als Ratingkriterium“ in: Die Bank 2005, 68-71
Christiansen, Per	„Wahrheitswidrige Tatsachenbehauptung in einem Internetportal“ in: MMR 2004, 185-186
Cichon, Caroline	Internet-Verträge, 2. Auflage, Köln 2005
Coase, Ronald H.	„The Problem of Social Cost“ in: The Journal of Law and Economics, Bd. 3, 1960, 1-44
Coase, Ronald H.	“Law and Economics at Chicago” in: The Journal of Law and Economics, Bd. 1, 2, 1993, 239-254
Coleman, James S.	Foundations of Social Theory, 3. Auflage, Cambridge, Mass. 2000

Conrad, Isabell	„Wege zum Quellcode“ in: ITRB 2005, 12-16
Cooter, Robert	“Economic Theories of Legal Liability” in: Journal of Economic Perspectives, Summer 1991, Volume 5 Issue 3, 11-30
Cooter, Robert/Ulen, Thomas	Law and Economics, Boston, Mass. 2004
Cosack, Tilman	Umwelthaftung im faktischen GmbH-Konzern, Frankfurt am Main, Berlin, Bern, New-York 1999
Cornelius, Kai/ Tschoepe, Sven	„Strafrechtliche Grenzen der zentralen E-Mail-Filterung und –Blockade“ in: K&R 2005, 269-271
Dauses, Manfred A. (Hrsg.)	Handbuch des EU-Wirtschaftsrechts, 16. Ergänzungslieferung, München 2006 zitiert: *Bearbeiter*, in: Dauses, Handbuch des EU-Wirtschaftsrechts
Dendorfer, Renate/ Niedderer, Sven-Erik	„Spam und andere Belästigungen aus dem Web. Einsatz von Filtertechnologie“ in: AuR 2006, 214-219
Derleder, Peter/ Knops, Kai-Oliver/ Bamberger, Heinz Georg	Handbuch zum deutschen Bankrecht, Wien New York 2004 zitiert: *Bearbeiter* in: Derleder/Knops/Bamberger, Handbuch zum deutschen und europäischen Bankrecht
Deutsch, Erwin/ Spickhoff, Andreas	Medizinrecht, 5. Auflage, Berlin, Heidelberg, New York 2003
Dietrich, Kay	„Typisierung von Softwareverträgen nach der Schuldrechtsreform“

	in: CR 2002, 473
Dietrich, Martin	Produktbeobachtungspflicht und Schadenverhütungspflicht der Produzenten, Frankfurt/M 1994
Dörner, Heinrich	„Rechtsgeschäfte im Internet“ in: AcP 202 (2002), 363-396
Dornseif, Maximillian/ Schumann, Kay H./ Klein, Christian	„Tatsächliche und rechtliche Risiken drahtloser Computernetzwerke“ in: DuD 2002, 226-230
Dreier, Thomas/ Schulze, Gernot	Urhebergesetz, Kommentar, 2. Aufl., München 2006 zitiert: Dreier/Schulze/*Bearbeiter*
Drygala, Tim/ Drygala, Anja	„Wer braucht ein Frühwarnsystem?“ in: ZIP 2000, 297-305
Dustmann, Andreas	Die privilegierten Provider, Baden-Baden 2001
Eckert, Claudia	IT-Sicherheit: Konzepte – Verfahren – Protokolle, 4. Auflage, München 2006
Eder, Klaus	„Die Autorität des Rechts“ in: Zeitschrift für Rechtssoziologie 8, 1987, 193-230
Ehmann, Eugen/ Helfrich, Marcus	EG-Datenschutzrichtlinie, Kurzkommentar, Köln 1999
Ehmann, Horst	„Informationsschutz und Informationsverkehr im Zivilrecht“ in: AcP 1888 (1988), 230 – 380
Eidenmüller, Horst	Effizienz als Rechtsprinzip, Tübingen 2005
Elbel, Thomas	Die datenschutzrechtlichen Vorschriften für

	Diensteanbieter im neuen Telekommunikationsgesetz auf dem Prüfstand des europäischen und deutschen Rechts, Berlin 2005
Endres, Alfred	Ökonomische Grundlagen des Haftungsrechts, Heidelberg 1991
Endres, Johannes	„Heute ein Admin“ in: c’t – Archiv 23/2005, 112-114
Endres	„Haftungsregeln für gentechnische Unfälle, das Problem der Haftungsobergrenze“ in: Jahrbuch für Sozialwissenschaft, Bd. 24, 1, 51-76
Engel, Friedrich-Wilhelm	„Produzentenhaftung für Software“ in: CR 1986, 702-708
Ensthaler, Jürgen/ Füßler, Andreas/ Nuissl, Dagmar	Juristische Aspekte des Qualitätsmanagements, Berlin 1997
Erben, Meinhard/ Zahrnt, Christoph	„Die Rechtsprechung zur Datensicherung“ in: CR 2000, 88-91
Erfurth, René	„Haftung für Missbrauch von Legitimationsdaten durch Dritte beim Online-Banking“ in: WM 2006, 2198-2207
Erman, Walter	Bürgerliches Gesetzbuch, Kommentar, Bd. 1 und 2, 11. Aufl., Köln 2004 zitiert: Erman/*Bearbeiter*, BGB, Bd.
Ernestus, Walter	„Protection Profile – Formale Beschreibung von Sicherheitsanforderungen“

	in: DuD 2003, 68
Ernst, Stefan	„Die Verfügbarkeit des Source Code“ in: MMR 2001, 208-213
Ernst, Stefan	„Wireless LAN und das Strafrecht“ in: CR 2003, 898-901
Ernst, Stefan	„Internet und Recht“ in: JuS 1997, 776-782
Ernst, Stefan	Trojanische Pferde und die Telefonrechnung in: CR 2006, 590-594
Ernst, Stefan	Vertragsgestaltung im Internet, München 2003 zitiert: *Ernst*, Vertragsgestaltung im Internet
Ernst, Stefan (Hrsg.)	Hacker, Cracker und Computerviren: Recht und Praxis der Informationssicherheit, Köln 2004 *Bearbeiter*, in: Ernst, Hacker, Cracker & Computerviren
Ertl, Gunter	„Zivilrechtliche Haftung im Internet“ in: CR 1998, 179-185
Faber, Wolfgang	„Elemente verschiedener Verbraucherbegriffe in EG-Richtlinien, zwischenstaatlichen Übereinkommen und nationalem Zivil- und Kollisionsrecht“ in: ZeuP 1998, 854-892
Falke, Josef	Rechtliche Aspekte der Normung in den EG-Mitgliedsstaaten und der EFTA,

	Luxemburg 2000
Faustmann, Jörg	„Der deliktische Datenschutz“, in: VuR 2006, 260-263.
Fervers, Martin	„Die Haftung der Banken bei automatisierten Zahlungsvorgängen“ In: WM 1988, 1037-1044
Feuerich, Wilhelm E./ Weyland, Dag	Bundesrechtsanwaltsordnung, 6. Auflage, München 2003 zitiert: Feuerich/Weyland-*Bearbeiter*
Finke, Katja	Die Auswirkungen der europäischen technischen Normen und des Sicherheitsrechts auf das nationale Haftungsrecht, München 2001
Fischer, Hartmut	„Die rechtliche Bedeutung technischer Normen im Telekommunikationsbereich“ in: RDV 1995, 221-230
Fleischer, Holger	„Vorstandsverantwortlichkeit und Fehlverhalten von Unternehmensangehörigen – Von der Einzelüberwachung zur Errichtung einer Compliance-Organisation“ in: AG 2003, 291-300
Fleischer, Holger	„Zur Leitungsaufgabe des Vorstands im Aktienrecht“ in: ZIP 2003, 1-11
Fleischer, Holger (Hrsg.)	Handbuch des Vorstandsrechts, München 2006 zitiert: *Bearbeiter*, in: Fleischer, Handbuch des Vorstandsrechts
Flume, Werner	Allgemeiner Teil des Bürgerlichen Rechts

	Erster Band, Zweiter Teil – Die juristische Person, Berlin Heidelberg New York Hongkong u.a. 1983 zitiert: *Flume* AT II
Foerste, Ulrich	„Deliktische Haftung für Schlechterfüllung“ in: NJW 1992, 27-28
Foerste, Ulrich	„Zur Rückrufpflicht nach § 823 BGB und § 9 ProdSG – Wunsch und Wirklichkeit“ in: DB 1999, 2199-2201
Foerste, Ulrich	„Nochmals – Persönliche Haftung der Unternehmensleitung – die zweite Spur der Produkthaftung?“ in: VersR 2002, 1-6
Freiwald, Susan	“Comparative Institutional Analysis in Cyberspace: The Case of Intermediary Liability for Defamation” in: Harvard Journal of Law and Technology, Vol. 14, 2001, 569-654
Fritz-Aßmus, Dieter/ Tuchtfeld, Egon	„Basel II als internationaler Standard zur Regulierung von Banken“ in: ORDO 54 (2003), 269-288
Fritzsche, Jörg/ Malzer, Hans M	„Ausgewählte zivilrechtliche Probleme elektronisch signierter Willenserklärungen“ in: DNotZ 1995, 3-26
Frühauf, Karol/ Ludewig, Jochen/ Sandmayr, Helmut	Software-Projektmanagement und –Qualitätssicherung, 4. Auflage, Zürich 2004

Fuhrberg, Kai/ Häger, Dirk/ Wolf, Stefan	Internet-Sicherheit, 3. Auflage, München 2001
Gaumert, Uwe/ Zattler, Michaela	„Basel II: Handelsbuch-Risiken und Double Default-Effekt“ in: Die Bank 2005, 55-59
Geiß, Joachim/ Doll, Wolfgang	Geräte- und Produktsicherheitsgesetz, Kommentar und Vorschriftensammlung, Stuttgart 2005
Geppert, Martin/ Piepenbrock, Hermann-Josef/ Schütz, Raimund/ Schuster, Fabian (Hrsg.)	Beck’scher TKG-Kommentar, 3. Auflage, München 2006 zitiert: Beck’scher TKG-Kommentar-*Bearbeiter*
Geppert, Martin/ Ruhle, Ernst-Olav/ Schuster, Fabian	Handbuch Recht und Praxis der Telekommunikation, 2. Aufl., Baden-Baden 2002
Gesmann-Nuissel, Dagmar/ Wenzel, Christian	„Produzenten- und Produkthaftung infolge abfallrechtlicher Produktverantwortung“ in: NJW 2004, 117-122
Gliss, Hans	„IT-Sicherheit aus Sicht des Datenschutzbeauftragten“ in: DSB 1996, Nr 5, 1-11
Gola, Peter	„Zwei Jahre neues Bundesdatenschutzgesetz - Zur Entwicklung des Datenschutzrechts seit 1991“ in: NJW 1993, 3109-3118
Gola, Peter/ Schomerus, Rudolf	Bundesdatenschutzgesetz, Kommentar, 8. Auflage, München 2005
Gorny, Peter	„Kategorien von Softwarefehlern“

	in: CR 1986, 673-677
Göttert, Helmut	„Sicherheit für Datennetze“ in: VW 2001, 1972
Gounalakis, Georgius (Hrsg.)	Rechtshandbuch Electronic Business, München 2003 zitiert: *Bearbeiter*, in: Gounalakis
Grabau, Maik/ Schlee, Klaus	„Die neuen MaRisk – Herausforderungen aus Sicht der Sparkassen-Finanzgruppe“ in: Kreditwesen 2005, 392-394
Grant, Colin	“Whistle Blowers: Saints of Secular Culture” in: Journal of Business Ethics 2002, Vol. 39, Nr. 4, 391 – 399
Greger, Reinhard	„Mitverschulden und Schadensminderungspflicht – Treu und Glauben im Haftungsrecht?“ in: NJW 1985, 1130-1134
Gross, Werner	„Deliktische Außenhaftung des GmbH-Geschäftsführers“ in: ZGR 1998, 551-569
Grundmann, Stefan	„Europäisches Vertragsrechtsübereinkommen, EWG-Vertrag und § 12 AGBG“ in: IPRax 1992, 1-5
Gruson, Michael/ Kubicek, Matthias	„Der Sarbanes-Oxley Act, Corporate Governance und das deutsche Aktienrecht“, http://www.jura.uni-frank-

	furt.de/ifawz1/baums/Bilder_und_Daten/Arbeitspapiere/paper113.pdf
Gruson, Michael/ Kubicek, Matthias	„Der Sarbanes-Oxley-Act, Corporate Governance und das deutsche Aktienrecht, Teile I und II“ in: AG 2003, 337-352, 393-406
Günther, Andreas	Produkthaftung für Informationsgüter, Köln 2001
Hadding, Walther/ Hopt, Klaus J/ Schimansky, Herbert (Hrsg.)	Entgeltklauseln in der Kreditwirtschaft und E-Commerce von Kreditinstituten – Bankrechtstag 2001, Berlin, New York 2002 zitiert: *Bearbeiter*, in: Hadding/Hopt/Schimansky
Hager, Günter	„Zum Schutzbereich der Produzentenhaftung“ in: AcP 184 (1984), 413-438
Hager, Johannes	„Die Kostentragung bei Rückruf fehlerhafter Produkte“ in: VersR 1984, 799-807
Hammer, Volker/ Bizer, Johann	„Beweiswert elektronisch signierter Dokumente“ in: DuD 1993, 689-699
Hanau, Peter/ Hoeren, Thomas	Private Internetnutzung durch Arbeitnehmer, München 2003 zitiert: Hanau/Hoeren, Private Internetnutzung durch Arbeitnehmer
Härting, Niko	„IT-Sicherheit in der Anwaltskanzlei“ in: NJW 2005, 1248-1250

Härting, Niko	„Unverschlüsselte E-Mails im anwaltlichen Geschäftsverkehr – Ein Verstoß gegen die Verschwiegenheitspflicht?“ in: MDR 2001, 61-63
Härting, Niko/ Schirmbacher, Martin	„Dialer: Das Urteil fällt und viele Fragen offen“ in: CR 2004, 334-338
Hartung, Wolfgang/ Holl, Thomas	Anwaltliche Berufsordnung, 2. Auflage, München 2001
Hasselblatt, Gordian N.	Die Grenzziehung zwischen verantwortlicher Fremd- und eigenverantwortlicher Selbstgefährdung im Deliktsrecht, Frankfurt/Oder 1996
Hauschka, Christoph E.	„Corporate Compliance – Unternehmensorganisatorische Ansätze zur Erfüllung der Pflichten von Vorständen und Geschäftsführern“ in: AG 2004, 461-475
Häusgen, Frank	„Mit durchgängigen IT-Infrastrukturen die Möglichkeiten des Kapitalanlagemanagements erweitern“ in: VW 2004, 1552-1554
Heckeroth, Klaus	„Die Anforderungen der Jahr-2000-Anpassung an Geschäftsleiter und Abschlussprüfer“ in: DB 1999, 702-707
Heiss, Helmut	„Inhaltskontrolle von Rechtswahlklauseln in AGB nach europäischem Internationalem Privatrecht?“ in: RabelsZ 2001, 634-653

Hellner, Thorwald	„Rechtsfragen des Zahlungsverkehrs unter besonderer Berücksichtigung des Bildschirmtextverfahrens“ in: Hadding, Walther/Mertens, Hans-Joachim/Immenga, Ulrich/Pleyer, Klemens/Schneider, Uwe W (Hrsg.), Festschrift für Winfried Werner zum 65. Geburtstag am 17. Oktober 1984, Berlin, New York 1984, S. 251-280
Hellner, Thorwald/ Steuer, Stephan	Bankrecht und Bankpraxis – Loseblatt – Stand Oktober 2006, Köln zitiert: *Bearbeiter* in: Hellner/Steuer
Henssler, Martin	„Das anwaltliche Berufsgeheimnis“ in: NJW 1994, 1817-1824
Henssler, Martin/ Prütting, Hanns	Bundesrechtsanwaltsordnung, 2. Auflage, München 2004 zitiert: *Bearbeiter*, in: Henssler/Prütting
Hermeler, Angelika Elisabeth	Rechtliche Rahmenbedingungen der Telemedizin, München 2000
Herrmann, Harald	„Die Rückrufhaftung des Produzenten“ in: BB 1985, 1801-1812
Heun, Sven-Erik	„Die elektronische Willenserklärung“ in: CR 1994, 595-600
Heussen, Benno	„Unvermeidbare Softwarefehler“ in: CR 2004, 1-10
Heussen, Benno/ Damm, Maximilian	„Millennium Bug: Manager- und Beraterhaftung bei unterlassener Systemprüfung und Notfallplanung“

	in: BB 1999, 481-489
Heussen, Benno/ Schmidt, Markus	„Inhalt und rechtliche Bedeutung der Normenreihe DIN/ISO 9000 bis 9004 für die Unternehmenspraxis“ in: CR 1995, 321-332
Hilber, Marc/ Hartung, Jürgen	„Auswirkungen des Sarbanes-Oxley Act auf deutsche WP-Gesellschaften: Konflikte mit der Verschwiegenheitspflicht der Wirtschaftsprüfer und dem Datenschutzrecht“ in: BB 2003, 1054-1060
Hilty, Reto M. (Hrsg.)	Information Highway, Bern 1996 zitiert: *Bearbeiter*, in: Hilty, Information Highway
Hinsch, Christian	„Eigentumsverletzungen an neu hergestellten und an vorbestehenden Sachen durch mangelhafte Einzelteile“ in: VersR 1992, 1053-1058
Höckelmann, Eckhard	Die Produkthaftung für Verlagserzeugnisse, Baden-Baden 1994
Hölzlwimmer, Gerhard	Produkthaftungsrechtliche Risiken des Technologietransfers durch Lizenzverträge, München 1995
Hoeren, Thomas	„Die Pflicht zur Überlassung des Quellcodes“ in: CR 2004, 721-724
Hoeren, Thomas	„Produkthaftung für Software - Zugleich eine kritische Erwiderung auf Bauer, PHI 1989, 38ff und 98ff“

	in: PHi 1989, 138-144
Hoeren, Thomas	„Virenscanning und Spamfilter - Rechtliche Möglichkeiten im Kampf gegen Viren, Spams & Co“ in: NJW 2004, 3513-3517
Hoeren, Thomas	„Risikoprüfung in der Versicherungswirtschaft“ in: VersR 2005, 1014-1023
Hoeren, Thomas/ Ernstschneider, Thomas	„Das neue Geräte- und Produktsicherheitsgesetz und seine Anwendung auf die IT-Branche“ in: MMR 2004, 507-513
Hoeren, Thomas/ Schüngel, Martin (Hrsg.)	Rechtsfragen der digitalen Signatur, Berlin 1999 zitiert: *Bearbeiter*, in: Hoeren/Schüngel
Hoeren, Thomas/ Sieber, Ulrich (Hrsg.)	Handbuch Multimedia-Recht, 13. Ergänzungslieferung, München 2006 zitiert: *Bearbeiter*, in: Hoeren/Sieber
Hörl, Bernhard	„Nachbesserung und Gewährleistung für fehlende Jahr-2000-Fähigkeit von Software“ – Anmerkung zu LG Leipzig, Urteil v. 23.07.1999 – 03 O 2479/99 in: CR 1990, 605-609
Hoffmann, Helmut	„Zivilrechtliche Haftung im Internet“ in: MMR 2002, 284-289
Hofmann, Christof/ Lesko, Michael/ Vorgrimler, Stefan	„Risikomanagement: Eigene EAD-Schätzung für Basel II“ in: Die Bank 2005, 48-52

Hohmann, Harald	„Haftung der Softwarehersteller für das'Jahr-2000' Problem" in: NJW 1999, 521-526
Hollmann, Hermann H	„Die EG-Produkthafungslinie, Teile (I) und (II)" in: DB 1985, 2389-2396 und 2439-2443
Holznagel, Bernd	Recht der IT-Sicherheit, München 2003
Hommelhoff, Peter	„Risikomanagement im GmbH-Recht" in: Berger, Klaus P./Ebke, Werner F./Elsing, Siegfried H. (Hrsg.), Festschrift für Otto Sandrock zum 70. Geburtstag, Heidelberg 2000, 373-383
Honsell, Heinrich	„Produkthaftungsgesetz und allgemeine Deliktshaftung" in: JuS 1995, 211-215
Hopt, Klaus J.	„Grundsatz- und Praxisprobleme nach dem Wertpapiergesetz" in: ZHR 159, 135-163 (1965)
Hüffer, Uwe	Aktiengesetz, 7. Auflage, München 2006
Huth, Rainer	Die Bedeutung technischer Normen für die Haftung des Warenherstellers nach § 823 BG und dem Produkthaftungsgesetz, Frankfurt am Main, Berlin, Bern, New-York 1992
Hütten, Christoph/ Stromann, Hilke	„Umsetzung des Sarbanes-Oxley Act in der Unternehmenspraxis" in: BB 2003, 2223-2227
Imhof, Ralf/ Wahl, Adalbert	„Auf der Suche nach der verlorenen Zeit:

	Das Jahr-2000-Problem“ in: WpK-Mitt. 1998, 136-141
Intveen, Michael	„Weitere Einzelheiten zu Haftungsklauseln in Allgemeinen Geschäftsbedingungen im kaufmännischen/unternehmerischen Verkehr“ in: ITRB 2003, 13-15
Jaeger, Lothar	“Grenzen der Kündigung von Softwarepflegeverträgen über langlebige Industrie-Software“ in: CR 1999, 209-213
Janisch, Sonja/ Schartner, Peter	„Internetbanking“ in: DuD 2002, 162-169
Jaskulla, Ekkehard M	“Direct Banking im Cyberspace” in: ZBB 1996, 214-224
Jhering, Rudolf	Das Schuldmoment im römischen Privatrecht, Giessen 1867
Johnson, Roberta Ann	Whistleblowing – When it works and why, London 2003
Jungk, Antje	„Haftpflichtfragen“ in: AnwBl 2001, 170-173
Junker, Abbo	„Die Entwicklung des Computerrechts im Jahre 1999“ in: NJW 2000, 1304-1312
Junker, Abbo	„Die Entwicklung des Computerrechts in den Jahren 2003/2004“ in: NJW 2005, 2829-2834
Jürgens, Andreas	Technische Standards im Haftungsrecht,

	Göttingen 1995
Kahlert, Henning	„Unlautere Werbung mit Selbstverpflichtungen“ in: DuD 2003, 412-416
Karger, Michael	„Kooperation bei komplexer Softwareentwicklung“ in: ITRB 2004, 208-210
Karper, Irene	Sorgfaltspflichten beim Online-Banking – Der Bankkunde als Netzwerkprofil? in: DuD 2006, 215-219
Kassebohm, Kristian/ Malorny, Christian	„Auditing und Zertifizierung im Brennpunkt wirtschaftlicher und rechtlicher Interessen“ in: ZfB 1994, 693-716
Kassebohm, Kristian/ Malorny, Christian	„Die strafrechtliche Verantwortung des Managements“ in: BB 1994, 1361-1371
Katko, Peter	„Voice over IP“ in: CR 2005, 189-193
Kaufmann, Bernd	„Neuordnung des Rechts der technischen Anlagensicherheit im Hinblick auf den Europäischen Binnenmarkt“ in: DB 1994, 1033-1038
Keenan, J.P.	“Blowing the Whistle on Less Serious Forms of Fraud: A Study of Executives and Managers” in: Employee Responsibilities and Rights Journal Vol. 12, Nr. 4, 199-217
Keller, Gernot/ Schlüter, Kai Grit	„Peer Review: Perspektiven nach dem Sar-

	banes-Oxley Act of 2002“ in: BB 2003, 2166-2174
Kilian, Wolfgang	„Vertragsgestaltung und Mängelhaftung bei Computersoftware“ in: CR 1986, 187-196
Kilian, Wolfgang/ Heussen, Benno	Computerrechts-Handbuch : Computer-technologie in der Rechts- und Wirtschaftspraxis, Loseblatt-Ausg., München 1990 – zitiert; *Bearbeiter*, in: Kilian/Heussen
Kind, Michael/ Werner, Dennis	„Rechte und Pflichten im Umgang mit PIN und TAN“ in: CR 2006, 353-360
Kirchgässner, Gebhard	Homo oeconomicus, 2. Auflage, Tübingen 2000
Klapdor, Martin	„IT-Risiken im virtuellen Netzwerk realitätsnah prüfen“ in: VW 2005, 507
Klindt, Thomas	„Der new approach im Produktrecht des europäischen Binnenmarkts - Vermutungswirkung technischer Normung“ in: EuZW 2002, 133-136
Klindt, Thomas	„Das neue Geräte- und Produktsicherheitsgesetz“ in: NJW 2004, 465-471
Klindt, Thomas	Geräte- und Produktsicherheitsgesetz (GPSG), München 2007 zitiert: *Klindt*, GPSG

Klinger, Max	Die Produktbeobachtungspflicht bezüglich Fremdzubehörteilen, Tübingen 1998
Klutzny, Alexander	Online-Demonstrationen und virtuelle Sitzblockaden – Grundrechtsausübung oder Straftat? in: RDV 2006, 50-59
Knolmayer, Gerhard/ Wermelinger, Thomas	Der Sarbanes-Oxley Act und seine Auswirkungen auf die Gestaltung von Informationssystemen, http://www.ie.iwi.unibe.ch/publikationen/berichte/resource/WP-179.pdf
Koch, Frank A.	Computer-Vertragsrecht, 6. Auflage, Freiburg 2002
Koch, Frank A.	„Rechtsfragen der Nutzung elektronischer Kommunikationsdienste“ in: BB 1996, 2049-2058
Koch, Frank A.	„Zivilrechtliche Anbieterhaftung für Inhalte in Kommunikationsnetzen“ in: CR 1997, 193-203
Koch, Robert	„Haftung für die Weiterverbreitung von Viren durch E-Mails“ in: NJW 2004, 801- 807
Koch, Robert	„»Mängelbeseitigungsansprüche« nach den Grundsätzen der Produzenten-/ Produkthaftung“ in: AcP 203 (2003), 603-632
Koch, Robert	Versicherbarkeit von IT-Risiken, Berlin 2005
Koenig, Christian/ Loetz, Sascha/ Neumann,	Telekommunikationsrecht, Heidelberg

Andreas	2004
Köhler, Helmut	„Die haftungsrechtliche Bedeutung technischer Regeln“ in: BB 1985, Beilage 4, 10-15
Köhler, Helmut	„Die Problematik automatisierter Rechtsvorgänge, insbesondere von Willenserklärungen“ in: AcP 182 (1982), 126-270
Köndgen, Johannes (Hrsg.)	Neue Entwicklungen im Bankhaftungsrecht, Köln 1989
Kötz, Hein	Deliktsrecht, 10. Auflage, München 2006
Kötz, Hein/ Schäfer, Hans-Bernd	Judex oeconomicus, Tübingen 2003
Kraft, Dennis/ Meister, Johannes	„Rechtsprobleme virtueller Sit-ins“ in: MMR 2003, 366-374
Kröger, Detlef/ Gimmy, Marc A. (Hrsg.)	Handbuch zum Internet-Recht, 2. Auflage Berlin Heidelberg, New York 2002 zitiert: *Bearbeiter*, in: Kröger/Gimmy
Kropff, Bruno/ Semler, Johannes (Hrsg.)	Münchener Kommentar zum Aktiengesetz, 2. Auflage, München 2000 ff. zitiert: MünchKommAktG-*Bearbeiter*
Krüger, Thomas/ Bütter, Michael	„Elektronische Willenserklärungen im Bankgeschäftsverkehr - Risiken des Online-Banking“ in: WM 2001, 221-231
Krüger, Thomas/ Büttner, Michael	„Justitia goes online – Elektronischer Rechtsverkehr im Zivilprozess“ in: MDR 2003, 181-189
Kübler, Friedrich	„Effizienz als Rechtsprinzip“ in: Baur, Jür-

	gen F./Hopt, Klaus J./Mailänder, Festschrift für Ernst Steindorff zum 70. Geburtstag am 13. März 1990, 687-704
Kuhn, Matthias	Rechtshandlungen mittels EDV und Telekommunikation, München 1991
Kühne, Hans-Heiner	„Strafbarkeit der Zugangsvermittlung von pornographischen Informationen im Internet“ in: NJW 1999, 188-190
Kühnhauser, Winfried E.	„Root Kits“ in: DuD 2003, 218-222
Kullmann, Hans-Josef	„Die Rechtsprechung des BGH zum Produkthaftungspflichtrecht in den Jahren 1989/90“ in: NJW 1991, 675-683
Kullmann, Hans-Josef	„Die Rechtsprechung des BGH zum Produkthaftungspflichtrecht in den Jahren 1994-1995“ in: NJW 1996, 18-26
Kullmann, Hans-Josef	„Die Rechtsprechung des BGH zum Produkthaftpflichtrecht in den Jahren 1995-1997“ in: NJW 1997, 1746-1753
Kullmann, Hans-Josef	„Die Rechtsprechung des Bundesgerichtshofs zum Produkthaftpflichtrecht in den Jahren 1997/98“ in: NJW 1999, 96-102
Kullmann, Hans-Josef	„Die Rechtsprechung des BGH zum Produkthaftpflichtrecht in den Jahren

	1992-1994“ in: NJW 1994, 1698-1707
Kullmann, Hans-Josef	„Die Rechtsprechung des BGH zum Produkthaftpflichtrecht in den Jahren 2000 und 2001“ in: NJW 2002, 30-36
Kullmann, Hans-Josef/ Pfister, Bernhard	Produzentenhaftung, 1/05 Ergänzungslieferung, Berlin 2005 zitiert: Kullmann/Pfister-*Bearbeiter*
Kümpel, Siegfried	Bank- und Kapitalmarktrecht, 3. Auflage, Köln 2004
Kümpel, Siegfried/ Veil, Rüdiger	Wertpapierhandelsgesetz, 2. Auflage, Berlin 2006
Kunst, Diana	„Rechtliche Risiken des Internet-Banking“ in: MMR Beilage 9/2001, 23-26
Kunz, Jürgen	„Die Produktbeobachtungs- und Befundsicherungspflicht als Verkehrssicherungspflichten des Warenherstellers“ in: BB 1994, 450-455
Kurose, James F./ Ross, Keith, W.	Computer Networking, Second Edition, Boston 2003
Lachmann, Jens Peter	„Ausgewählte Probleme aus dem Recht des Bildschirmtextes“ in: NJW 1984, 405-408
Lang, Markus	„PC, aber sicher! – Sicherheit beim Einsatz von Personalcomputern“ in: JurPC Web-Dok. 205/2001, Abs. 1-166
Lang, Volker	„Die Beweislastverteilung im Falle der

	Verletzung von Aufklärungs- und Beratungspflichten bei Wertpapierdienstleistungen“ in: WM 2000, 450-476
Lange, Hermann/ Schiemann, Gottfried	Schadensersatz, 3. Auflage., Tübingen 2003
Lange, Knut W./ Wall, Friederike (Hrsg.)	Risikomanagement nach dem KonTraG, München 2001 zitiert: *Bearbeiter*, in: Lange/Wall
Langenbucher, Katja	Die Risikozuordnung im bargeldlosen Zahlungsverkehr, München 2001
Lapp, Thomas	„Fax- und E-Mail-Kommunikation“ in: BRAK-Mitt 1997, 106-108
Larenz, Karl	Lehrbuch des Schuldrechts, Erster Band, Allgemeiner Teil, 14. Auflage, München 1987
Larenz, Karl	Lehrbuch des Schuldrechts, Zweiter Band, Besonderer Teil, 1. Halbband, 13. Auflage, München 1986
Larenz, Karl/ Canaris, Claus-Wilhelm	Lehrbuch des Schuldrechts, Zweiter Band, Besonderer Teil, 2. Halbband, 13. Auflage, München 1994
Laufs, Adolf/ Uhlenbruck, Wilhelm (Hrsg.)	Handbuch des Arztrechts, 3. Auflage., München 2002 zitiert: *Bearbeiter*, in: Laufs/Uhlenbruck,
Lehmann, Michael (Hrsg.)	Rechtsschutz und Verwertung von Computerprogrammen, 2. Auflage, Köln 1993 zitiert: *Bearbeiter*, in: Lehmann, Rechtsschutz und Verwertung von Compu-

	terprogrammen
Leible, Stefan/ Sosnitza, Olaf	„Schadensersatzpflicht wegen Virenbefall von Disketten“ in: K&R 2002, 51-52
Leible, Stefan/ Sosnitza, Olaf	„Neues zur Störerhaftung von Internet-Auktionshäusern“ in: NJW 2004, 3225
Leible, Stefan/ Sosnitza, Olaf	Versteigerung im Internet, Heidelberg 2004 zitiert: *Bearbeiter* in: Leible/Sosnitza, Versteigerung im Internet
Leible, Stefan/ Wildemann, Andree	Kommentar zu BGH, Urteil v. 04.03.2004 – III ZR 96/03 in: K&R 2004, 288-290
Leisinger, Klaus M.	Whistleblowing und Corporate Reputation Management, München, Mering 2003
Lenz, Hansrudi	„Sarbanes-Oxley-Act of 2002 - Abschied von der Selbstregulierung der Wirtschaftsprüfer in den USA“ in: BB 2002, 2270-2275
Lenz, Tobias	„Das neue Geräte- und Produktsicherheitsgesetz“ in: MDR 2004, 918-922
Libertus, Michael	„Zivilrechtliche Haftung und strafrechtliche Verantwortlichkeit bei unbeabsichtigter Verbreitung von Computerviren“ in: MMR 2005, 507-512
Lier, Monika	„Dies und das aus der elektronischen Ver-

	sicherungswelt“ in: VW 2004, 554-563
Lindacher, Walter F.	„Unlauterer Wettbewerb bei einem DIN-Norm-Verstoß“ in: BB 1981, 144-145
Littbarski, Sigurd	„Herstellerhaftung ohne Ende – Ein Segen für den Verbraucher?“ in: NJW 1995, 217-222
Littbarski, Sigurd	„Kapriolen um die Instruktionspflichten des Herstellers“ in: NJW 2004, 1161-1163
Littbarski, Sigurd	„Das neue Geräte- und Produktsicherheitsgesetz: Grundzüge und Auswirkungen auf die Haftungslandschaft“ in: VersR 2005, 448-458
Litzenburger, Wolfgang	„Das Ende des vollständigen Gewährleistungsausschlusses beim Kaufvertrag über gebrauchte Immobilien“ in: NJW 2002, 1244-1247
Lobinger, Thomas	„Zur vertraglichen Einstandspflicht des Anschlussinhabers für die Annahme von R-Gesprächen durch unbefugte Dritte“ in: JZ 2006, 1076-1080
Loewenheim, Ulrich/Koch, Frank A. (Hrsg.)	Praxis des Online-Rechts zitiert: *Bearbeiter* in Loewenheim/Koch (Hrsg.), Praxis des Online-Rechts
Looschelders, Dirk	Schuldrecht Allgemeiner Teil, 4. Aufl., München 2006

Looschelders, Dirk	Internationales Privatrecht, Art. 3-46 EGBGB, Kommentar, Berlin 2004
Lorenz, Egon	„Zur Haftung für durch einen Stromausfall verursachte Schäden, der durch einen Kurzschluß an einem einer BGB-Gesellschaft gelieferten fehlerhaften Baustromverteiler hervorgerufen worden ist“ in: VersR 1990, 1284- 1285
Löwe, Walter	„Rückrufpflicht des Warenherstellers“ in: DAR 1978, 288-296
Lüke, Gerhard/ Wax, Peter	Münchener Kommentar zur Zivilprozessordnung Band 1 §§ 1-354, 2. Auflage, München 2000 zitiert: MünchKommZPO-*Bearbeiter*
Lüke, Gerhard/ Wax, Peter	Münchener Kommentar zur Zivilprozessordnung Aktualisierungsband ZPO-Reform 2002, München 2002 zitiert: MünchKommZPO-*Bearbeiter*
Lutter, Markus/ Hommelhoff, Peter	GmbH-Gesetz, 16. Auflage, Köln 2004 zitiert: Lutter/Hommelhoff-*Bearbeiter*
Luttermann, Claus	„Unabhängige Bilanzexperten in Aufsichtsrat und Beirat“ in: BB 2003, 745-750
Malzer, Hans Michael	„Anspruch des Verwenders von Individualsoftware auf Herausgabe des Quellenprogramms (Quellcode) und der Herstellerdokumentation“ in: CR 1989, 991-992

Mankowski, Peter	„Kein Telefonentgeltanspruch für Verbindungen durch ein heimlich installiertes Anwahlprogramm – Dialer“ in: MMR 2004, 312-315
Mankowski, Peter	„Die Beweislastverteilung in 0190er-Prozessen“ in: CR 2004, 185-189
Mankowski, Peter	„Schuldrechtsreform: Werkvertragsrecht - Die Neuerungen durch § 651 BGB und der Abschied vom Werklieferungsvertrag“ in: MDR 2003, 854-860
Mankowski, Peter	„Für einen Anscheinsbeweis hinsichtlich der Identität des Erklärenden bei E-Mails“ in: CR 2003, 44-50
Mankowski, Peter	„Sofort-Option bei E-Bay“ in: MMR 2004, 181-183
Mankowski, Peter	„Überlegungen zur sach- und interessengerechten Rechtswahl für Verträge des internationalen Wirtschaftsverkehrs“ in: RIW 2003, 2-15
Marburger, Peter (Hrsg.)	Technische Regeln im Umwelt- und Technikrecht (UTR), Band 86, Berlin 2006 zitiert: *Bearbeiter*, in: Marburger, Technische Regeln im Umwelt- und Technikrecht

Marburger, Peter	„Herstellung nach zwingenden Rechtsvorschriften als Haftungsausschlussgrund im neuen Produkthaftungsrecht“ in: Leßmann, Herbert/Großfeld, Bernhard/Vollmer, Lothar (Hrsg.), Festschrift für Rudolf Lukes zum 65. Geburtstag, Köln, Berlin, Bonn, München 1989, 97-119
Marburger, Peter	Die Regeln der Technik im Recht, Köln, Bonn, Berlin, München 1979
Marburger, Peter	„Die haftungs- und versicherungsrechtliche Bedeutung technischer Regeln“ in: VersR 1983, 597-608
Marburger, Peter	„Produktsicherheit und Produkthaftung“ in: Ahrens, Hans-Jürgen/v. Bar, Christian/Fischer, Gerfried/Spickhoff, Andreas/Taupitz, Jochen (Hrsg.), Festschrift für Erwin Deutsch zum 70. Geburtstag, Köln, Berlin, Bonn, München 1999, 271-289
Marburger, Peter	„Grundsatzfragen des Haftungsrechts unter dem Einfluß der gesetzlichen Regelungen zur Produzenten- und zur Umwelthaftung“ in: AcP 192 (1992), 1-34
Marly, Jochen	Softwareüberlassungsverträge, 4. Auflage, München 2004
Mathis, Klaus	Effizienz statt Gerechtigkeit?, 2. Auflage, Berlin 2006

Maul, Silja/ Lanfermann, Georg	„Europäische Corporate Governance – Stand der Entwicklungen" in: BB 2004, 1861-1868
Mayer, Kurt	„Produkthaftung und Gefahrbeseitigungsanspruch,(Stichwort – ‚Rückrufpflicht')" in: DB 1985, 319-326
Medicus, Dieter	Bürgerliches Recht, 20. Auflage, Köln Berlin Bonn München 2004 zitiert: *Medicus*, Bürgerliches Recht
Meier, Klaus/ Wehlau, Andreas	„Die zivilrechtliche Haftung für Datenlöschung, Datenverlust und Datenzerstörung" in: NJW 1998, 1585-1591
Meier, Klaus/ Wehlau, Andreas	„Produzentenhaftung des Softwareherstellers" in: CR 1990, 95-100
Meister, Herbert	Datenschutz im Zivilrecht – Das Recht am eigenen Datum, 2. Aufl., Bergisch-Gladbach 1981
Melullis, Klaus-J.	„Zum Regelungsbedarf bei der elektronischen Willenserklärung" in: MDR 1994, 109-114
Mertens, Hans-Joachim/ Mertens, Georg	„Zur deliktischen Eigenhaftung des Geschäftsführers einer GmbH bei Verletzung ihm übertragener organisatorischer Pflichten" – Anmerkung zu BGH Urteil –. 05.12.1989 - VI ZR 335/88

	in: JZ 1990, 488-490
Meyer, Andreas	„Die Haftung für fehlerhafte Aussagen in wissenschaftlichen Werken“ in: ZUM 1997, 26-34
Meyer-Sparenberg, Wolfgang	„Rechtswahlvereinbarungen in Allgemeinen Geschäftsbedingungen“ in: RIW 1989, 347-351
Michalski, Lutz	„Produktbeobachtung und Rückrufpflicht des Produzenten“ in: BB 1998, 961-965
Miceli, Thomas J.	Economics of the Law, New York 1997
Mitglieder des Bundesgerichtshofs (Hrsg.)	Das Bürgerliche Gesetzbuch, Kommentar mit besonderer Berücksichtigung des Reichsgerichts und des Bundesgerichtshofes, 12. Auflage, Berlin 2000 zitiert: RGRK-*Bearbeiter*
Möller, Klaus/ Kelm, Stefan	„Distributed Denial-of-Service Angriffe (DDoS)” in: DuD 2000, 292-293
Möllers, Thomas M. J.	Rechtsgüterschutz im Umwelt- und Haftungsrecht: präventive Verkehrspflichten und Beweiserleichterungen in Risikolagen, Tübingen 1996
Möllers, Thomas M. J.	„Qualitätsmanagement, Umweltmanagement und Haftung“ in: DB 1996, 1455-1461
Möllers, Thomas M. J.	„Versicherungspflichten gegenüber Kindern“

	in: VersR 1996, 153-160
Moritz, Hans-Werner	„Quo vadis elektronischer Geschäftsverkehr?“ in: CR 2000, 61-72
Müller-Hengstenberg, Claus D.	„Der Vertrag als Mittel des Risikomanagements“ in: CR 2005, 385-392
Müller-Hengstenberg, Claus D./ Krcmar, Helmut	„Mitwirkungspflichten des Auftraggebers bei IT-Projekten“ in: CR 2002, 549 ff.
Müller-Hengstenberg, Claus D.	„Computersoftware ist keine Sache“ in: NJW 1994, 3128-3134
Müller-Reichart, Matthias/ Dura, Annett/ Fischer, Harry/ Nosty, Filip	„Finanzberater und Versicherungsmakler als Risk Advisors nach Basel II“ in: VW 2002, 625
Münch, Peter	„Harmonisieren – dann Auditieren und Zertifizieren“ in: RDV 2003, 223-231
Musielak, Hans-Joachim	„Beweislastverteilung nach Gefahrenbereichen“ in: AcP 176 (1976), 465-486
Musielak, Hans-Joachim	Zivilprozessordnung, Kommentar (ZPO), 5. Auflage, München 2007 zitiert: Musielak-*Bearbeiter*
Near, J.P./Miceli, M.P.	“Organizational Dissidence: The Case of Whistle-blowing” in: Journal of Business Ethics 1985, Nr. 4, 1-16

Neumann, Diana/Bock, Christian	Zahlungsverkehr im Internet, München 2004
Nickel, Friedhelm/Kaufmann, Lars	„Produktsicherheit und Produzentenhaftung“ in: VersR 1998, 948-954
Niebling, Jürgen	Die CE-Kennzeichnung, Stuttgart, Hannover 1995
Niebling, Jürgen	„Gewährleistung und Produkthaftung bei fehlender CE-Kennzeichnung“ in: DB 1996, 80-81
Otto, Franz	„Verkehrssicherungspflichten“ – Anmerkung zu OLG Karlsruhe, Urteil v. 2.10.1996 – 7 U 210/93 in: VersR 1997, 1155-1157
Palandt, Otto	Bürgerliches Gesetzbuch, 66. Auflage, München 2007 zitiert: Palandt-*Bearbeiter*
Paul, Stephan/Stein, Stefan/Kaltofen, Daniel	„Kapitalanforderungen für Retail-Portfolios nach Basel II“ in: Die Bank 2004, 342-349
Pauli, A.	„Die Produktbeobachtungspflichten in der verbraucherpolitischen Auseinandersetzung“ in: PHi 1985, 134 ff.
Pauly, Mark V./Kenneth, J. Arrow	„The Economics of Moral Hazard“ in: The American Economic Review, Nashville, Tenn. Bd. 58, 1968, 531-537
Pawlowski, Hans-Martin	Allgemeiner Teil des BGB, 6. Auflage,

	Heidelberg 2000 zitiert: *Pawlowski*, Allgemeiner Teil des BGB
Peikari, Cyrus/ Chuvakin, Anton	Kenne Deinen Feind, Köln 2004
Peine, Franz-Joseph	Gesetz über technische Arbeitsmittel, Kommentar, 3. Auflage, Köln 2002
Pellens, Bernhard	„Überregulierung der Kapitalmärkte?“ in: DBW 2003, 473-476
Peters, Falk/ Kersten, Heinrich	„Technisches Organisationsrecht i– Datenschutz - Bedarf und Möglichkeiten“ in: CR 2001, 576-581
Petrasch, Roland	Einführung in das Software-Qualitätsmanagement, Berlin 2001
Pfeifer, Uwe	„Solvency II – ein Thema für die IT?“ in: VW 2005, 1558-1564
Pfeiffer, Thomas	„Vom kaufmännischen Verkehr zum Unternehmensverkehr“ in: NJW 1999, 169-174
Pfingsten, Andreas/ Maifarth, Michael/ Rieso, Sven	„Grundkonzeption und Allgemeine Regelungen der MaRisk“ in: Bank 2005, Nr 6, 34-36, 38-39
Pfister, Bernhard	„Zur Produzentenhaftung wegen Verletzung der Produktbeobachtungspflicht gegenüber fremdem Zubehör“ in: EWiR 1987, 235-236
Pieper, Helmut	„Verbraucherschutz durch, Pflicht zum ‚Rückruf’ fehlerhafter Produkte?“

	in: BB 1991, 985-992
Podehl, Jörg	„Internetportale mit journalistisch-redaktionellen Inhalten“ in: MMR 2001, 17-23
Polke, Peter	Die darlehensvertragliche Umsetzung der Eigenkapitalgrundsätze nach Basel II, Berlin 2005
Popp, Andreas	„Von Datendieben und Betrügern – Zur Strafbarkeit des sogenannten phishing“ in: NJW 2004, 3517-3518
Potinecke, Harald W	„Das Geräte- und Produktsicherheitsgesetz“ in: DB 2004, 55-60
Preußner, Joachim	„Risikomanagement im Schnittpunkt von Bankaufsichtsrecht und Gesellschaftsrecht“ in: NZG 2004, 57-61
Preußner, Joachim	„Deutscher Corporate Governance Kodex und Risikomanagement“ in: NZG 2004, 303-307
Probst, Thomas	„Datenschutzbeauftragte fordern vertrauenswürdige Informationstechnik“ in: DSB 2003, Nr 5, 10-12
Probst, Thomas	„Automatisierte Software-Updates“ in: DuD 2003, 508
Prölss, Jürgen	Beweiserleichterungen im Schadensersatzprozess, Karlsruhe 1966

	zitiert: *Prölss*, Beweiserleichterungen im Schadensersatzprozeß
Prütting, Hanns	„Die Beweislast im Arbeitsrecht“ in: RdA 1999, 107-112
Quaas, Michael/ Zuck, Rüdiger	Medizinrecht, München 2006 zitiert: Quaas/Zuck-*Bearbeiter*
Quack-Grobecker, Alexander/ Funke, Guido	„Internetrisiken – eine Herausforderung für die Haftpflichtversicherung“ in: VW 1999, 157-160
Raab, Thomas	„Die Bedeutung der Verkehrspflichten und ihre systematische Stellung im Deliktsrecht“ in: JuS 2002, 1041-1048
Rebmann, Kurt/ Säcker Franz Jürgen/ Rixecker, Roland (Hrsg.)	Münchener Kommentar zum Bürgerlichen Gesetzbuch, 4. Auflage, München 2000 ff. zitiert: MünchKommBGB-*Bearbeiter*
Recknagel, Einar	Vertrag und Haftung beim Internet-Banking, München 2005 zitiert: *Recknagel*, Vertrag und Haftung beim Internet-Banking
Redeker, Helmut	„Softwareerstellung und § 651 – Die typischen Vertragsgestaltungen verlangen differenzierte Ergebnisse“ in: CR 2004, 88-91
Redeker, Helmut	„Wer ist Eigentümer von Goethes Werther?“ in: NJW 1992, 1739-1740

Redeker, Helmut	„Geschäftsabwicklung mit externen Rechnern im Bildschirmtextdienst“ in: NJW 1984, 2390-2394
Reese, Jürgen	„Produkthaftung und Produzentenhaftung für Hard- und Software“ in: DStR 1994, 1121-1127
Reiländer, Frank/ Weck, Gerhard	„Datenschutzaudit nach I–-Grundschutz - Konvergenz zweier Welten“ in: DuD 2003, 692-695
Reinicke, Dietrich/ Tiedtke, Klaus	Kaufrecht, 7. Auflage, München 2004
Reiser, Cristof/ Werner, Stefan	Rechtsprobleme des Zahlungsverkehrs im Zusammenhang mit EDIFACT in: WM 1995, 1901-1908
Rigamonti, Cyrill P	„Das Jahr-2000-Computer-Problem: Ein Rechtsproblem?“ in: SJZ 1998, 430-434
Roggenkamp, Jan Dirk	Massenhafter Versand von Werbe-E-Mails, Anmerkung zu Anm. zu OLG Düsseldorf, Urt. v. 24.5.2006 – I 15 U 45/06, jurisPR-ITR 8/2006 Anm. 4
Rolland, Walter	Produkthaftungsrecht, Kommentar, München 1990
Rönck, Rüdiger	Technische Normen als Gestaltungsmittel der europäischen Gemeinschaftsrechts, Berlin 1995
Rösler, Hannes	„Zur Zahlungspflicht für heimliche Dialereinwahlen“ in: NJW 2004, 2566-2569
Rösser, Heinz	„quid! Datenschutzzertifizierung“

	in: DuD 2003, 401-405
Roßnagel, Alexander	„Europäische Techniknormen im Lichte des Gemeinschaftsvertragsrechts“ in: DVBl 1996, 1181-1189
Roßnagel, Alexander	„Marktwirtschaftlicher Datenschutz – eine Regulierungsperspektive“ in: Bizer, Johann/Lutterbeck, Bernd/Rieß, Joachim (Hrsg.), Umbruch von Regulierungssystemen in der Informationsgesellschaft, Freundesgabe für Alfred Büllesbach, Stuttgart 2002, S. 131-150
Roßnagel, Alexander	Datenschutzaudit, Braunschweig 2000
Roßnagel, Alexander	„Auf dem Weg zu neuen Signaturregelungen“ in: MMR, 451-461
Roßnagel, Alexander (Hrsg.)	Recht der Multimedia-Dienste, Kommentar, 7. Ergänzungslieferung, München 2005 zitiert: *Bearbeiter*, in: Roßnagel, Recht der Multimedia-Dienste
Roßnagel, Alexander (Hrsg.)	Handbuch Datenschutzrecht, München 2003 zitiert: *Bearbeiter*, in: Roßnagel, Handbuch Datenschutzrecht
Roth, Birgit/ Schneider, Uwe K.	„IT-Sicherheit und Haftung“ in: ITRB 2005, 19-22
Rücker, Daniel	„Softwareerstellung und § 651 BGB – Diskussion ohne Ende oder Ende der Diskussion?“

	in: CR 2006, 361-368
Rühl, Christiane	Rechtswahlfreiheit und Rechtswahlklauseln in allgemeinen Geschäftsbedingungen, Baden-Baden 1999
Runte, Christian/ Potinecke, Harald	„Software und GPSG“ in: CR 2004, 725-729
Runte, Christian/ Potinecke, Harald	„Software und GPSG“ in: CR 2004, 725-729
Rüpke, Giselher	„Ein Beauftragter für den Datenschutz in der Anwaltskanzlei?“ in: AnwBl 2004, 552-555
Sack, Rolf	„Produzentenhaftung und Produktbeobachtungspflicht“ in: BB 1985, 813-819
Säcker, Franz Jürgen (Hrsg.)	Berliner Kommentar zum Telekommunikationsgesetz, Frankfurt am Main 2006 zitiert: Säcker-*Bearbeiter*
Sailer, Kathrin	Prävention im Haftungsrecht, Frankfurt am Main 2005
Salje, Peter	„Ökonomische Analyse des Rechts aus deutscher Sicht“ in: RECHTSTHEORIE 15 (1984), 277-312
Schäfer, Hans-Bernd/ Ott, Claus	Lehrbuch der ökonomischen Analyse des Zivilrechts, 4. Auflage, Berlin, Heidelberg, Bonn, New York 2005
Schenke, Wolf Rüdiger/ Ruthig, Josef	„Amtshaftungsansprüche von Bankkunden bei der Verletzung staatlicher Bankenaufsichtspflichten“

	in: NJW 1994, 2324-2329
Scherer, Josef/ Butt, Mark Eric	„Rechtsprobleme bei Vertragsschluss via Internet“ in: DB 2000, 1009-1016
Scheurle, Klaus D./ Mayen, Thomas (Hrsg.)	Telekommunikationsgesetz (TKG), 2. Auflage, München 2006 zitiert: Scheurle/Mayen-*Bearbeiter*
Schieble, Christoph	Produktsicherheitsgesetz und europäisches Gemeinschaftsrecht, Baden-Baden 2003
Schiessl, Maximilian	„Deutsche Corporate Governance post Enron“ in: AG 2002, 593-604
Schimansky, Herbert/ Bunte, Hermann-Josef/ Lwowski, Hans-Jürgen (Hrsg.)	Bankrechts-Handbuch, Band I-III, München 2001 zitiert: *Bearbeiter*, in: Bankrechts-Handbuch
Schläger, Uwe	„Gütesiegel nach Datenschutzauditverordnung Schleswig-Holstein“ in: DuD 2004, 459-461
Schlechtriem, Peter	„Angleichung der Produkthaftung in der EG – Zur Richtlinie des Rates der Europäischen Gemeinschaften vom 25-7-1985“ in: VersR 1986, 1033-1043
Schlutz, Joachim H.	„Deutschland - Rechtliche Auswirkungen der ISO-Zertifizierung, insbesondere auf Produkthaftungsklagen“ in: PHi 1996, 122-135

Schmatz, Hans/ Nöthlichs, Matthias	Sicherheitstechnik, Berlin 1969-
Schmid, Viola	Informations- und Datenschutzrecht I, http://www.bwl.tu-darmstadt.de/jus4/lehre/IuD-I_ws_05/ws_0506_vorl_ueb_iud_1_modul_6_060123.pdf
Schmidl, Michael	„Softwareerstellung und § 651 BGB – ein Versöhnungsversuch“ in: MMR 2004, 590-593
Schmidt-Salzer, Joachim	Produkthaftung, 2. Auflage, Heidelberg – 1990
Schmidt-Salzer, Joachim	Entscheidungssammlung Produkthaftung, 5. Ergänzungslieferung 1996
Schmidt-Salzer, Joachim/ Hollmann, Hermann H.	Kommentar EG-Richtlinie Produkthaftung, Bd. 1, 2. Auflage, Heidelberg 1988 zitiert: Schmidt-Salzer/Hollmann-*Bearbeiter*
Schnauder, Franz	„Delikts- und bereicherungsrechtliche Haftung bei gefälschter Giroüberweisung“ in: ZIP 1994, 1069-1078
Schneider, Jochen	„Projektsteuerung – Projektrisiken bei Software“ in: CR 2005, 27-34
Schneider, Jochen	„Softwareerstellung und Softwareanpassung – Wo bleibt der Dienstvertrag?“ in: CR 2003, 317-323
Schneider, Jochen	„Projektsteuerung – Projektrisiken bei

	Software“ in: CR 2000, 27-34
Schneider, Jochen	Handbuch des EDV-Rechts, 3. Auflage, Köln 2003
Schneider, Jochen/Günther, Andreas	„Haftung für Computerviren“ in: CR 1997, 389-396
Schneider, Jochen/ Westphalen, Friedrich Graf von	Software-Erstellungsverträge, Köln 2006 Zitiert: *Bearbeiter*, in: Schneider/von Westphalen, Software-Erstellungsverträge
Schöning, Stephan/Weber, Marcus	„Basel II Rahmenwerk: Die Risiken der Projektfinanzierung“ in: Die Bank 2005, 47-51
Schönke, Adolf/ Schröder, Horst (Hrsg.)	Strafgesetzbuch, Kommentar, 27. Auflage, München 2006 zitiert: Schönke/Schröder-*Bearbeiter*
Schöttle, Hendrik	Anwaltliche Rechtsberatung via Internet, Stuttgart 2004
Schricker, Gerhard (Hrsg.)	Urheberrecht, Kommentar, 3. Auflage, München 2006 zitiert: Schricker-*Bearbeiter*
Schubert, Thomas/ Grießmann, Gundula	„Solveny II = Basel II + X“ in: VW 2004, 1399
Schulte, Martin (Hrsg.)	Handbuch des Technikrechts, Berlin 2003 zitiert: *Bearbeiter*, in: Schulte, Handbuch des Technikrechts
Schulte-Mattler, Hermann/Manns, Thorsten	„Basel II: Falscher Alarm für die Kredit-kosten des Mittelstandes“

	in: Die Bank 2004, 376-380
Schulte-Mattler, Hermann/von Kenne, Ulrich	"Basel II Framework: Meilenstein der Bankenaufsicht " in: Die Bank 2004, 37-40
Schulze, Reiner/ Ebers, Martin	„Streitfragen im neuen Schuldrecht" in: JuS 2004, 462-468
Schulze-Melling, Jyn	„IT-Sicherheit in der anwaltlichen Beratung" in: CR 2005, 73-80
Schumann, Jochen	Grundzüge der mikroökonomischen Theorie, Berlin 1999
Schuster, Fabian (Hrsg.)	Vertragshandbuch Telemedia, München 2001 zitiert: *Bearbeiter*, in: Schuster, Vertragshandbuch Telemedia
Schwab, Hans-Josef	„Zur Mithaftung des Befüllpersonals, das bei vorhandener elektronischer Füllstandsanzeige von einer manuellen Freiraummengenmessung abgesehen hatte, für den beim Überlaufen eines Öltanks verursachten Schaden" – Anmerkung zu OLG Köln, Urteil v. 24.06.1994 – 19 U 275/93 in: VersR 1995, 1250
Schwalbach, Joachim	„Effizienz des Aufsichtsrats" in: AG 2004, 186-190
Schwark, Eberhard	Kapitalmarktrechtskommentar, 3. Auflage, München 2004 zitiert: Schwark-*Bearbeiter*

Schwarz, Günter C./Holland, Björn	„Enron, WorldCom… und die Corporate-Governance-Disskussion“ in: ZIP 2002, 1661-1672
Schwarz, Mathias/Peschel-Mehner, Andreas	Recht im Internet, Augsburg 2002
Schwarz, Mathias/Poll, Karolin	„Haftung nach TDG und MDStV“ in: JurPC Web-Dok. 73/2003, Als. 1-154
Schweinoch, Martin/ Roas, Rudolf	„Paradigmenwechsel für Projekte: Vertragstypologie der Neuerstellung von Individualsoftware“ in: CR 2004, 326-331
Schwenzer, Ingeborg	„Rückruf- und Warnpflichten des Warenherstellers“ in: JZ 1987, 1059-1065
Schwintowski, Hans-Peter/Schäfer, Frank A.	Bankrecht, Köln, Berlin, Bonn, München 2004
Schwintowski, Hans-Peter	„Gesellschaftsrechtliche Anforderungen an Vorstandshaftung und Corporate Governance durch das neue System der kartellrechtlichen Legalausnahme“ in: NZG 2005, 200-203
Schwirten, Christian/Zattler, Michaela	„Die Konfliktpunkte“ in: Die Bank 2005, Heft 10, 52-55
Seibert, Ulrich	„Die Entstehung des § 91 Abs. 2 AktG im KonTraG – »Risikomanagement« oder »Frühwarnsystem«?“ in: Westermann, Harm Peter/Mock, Klaus (Hrsg.), Festschrift für Gerold Bezzenberger zum 70. Geburtstag, Ber-

	lin, New York 2000, 427-438
Sessinghaus, Karel	„BGH???-Internet-Versteigerung" - ein gemeinschaftsrechtswidriges Ablenkungsmanöver?“ in: WRP 2005, 697-703
Shavell, Steven	Foundations of Economic Analysis of Law, Harvard 2004
Sieber, Stefanie/ Nöding, Toralf	„Die Reform der elektronischen Unterschrift“ in: ZUM 2001, 199-210
Siebert, Lars Michael	Das Direktbankgeschäft, Baden-Baden 1998
Siegel, Volker	„Die Auswirkungen von Solvency II auf IT-Projekte“ in: ITRB 2006, 13-15
Siemer, John Philipp	Das Coase-Theorem: Inhalt, Aussagewert und Bedeutung für die ökonomische Analyse des Rechts, Münster 1999
Simitis, Spiros (Hrsg.)	Kommentar zum Bundesdatenschutzgesetz, 6. Auflage, Baden-Baden 2006 zitiert: Simitis-*Bearbeiter*
Simitis, Spiros/ Dammann, Ulrich/ Mallmann, Otto/ Reh, Hans-Joachim (Altauflage)	Kommentar zum Bundesdatenschutzgesetz, 3. Auflage, Baden-Baden 2003 zitiert: Simitis/Dammann/Mallmann/Reh (Altauflage)-*Bearbeiter*
Smith, Graham P./Hamill, Robert M.	“ Neuregelung der Produkthaftpflicht im Vereinigten Königreich - Der Consumer Protection Act 1987“ in: PHi 1988, 82-88

Sodtalbers, Axel	Softwarehaftung im Internet, Frankfurt am Main 2006
Soergel, Hans Theodor	Bürgerliches Gesetzbuch, 13. Auflage, Stuttgart, Berlin, Köln, Mainz 1999 ff. zitiert: Soergel-*Bearbeiter*
Sommerville, Ian	Software Engineering, 7. Auflage, Harlow 2004
Sonntag, Matthias	IT-Sicherheit kritischer Infrastrukturen, München 2005
Spickhoff, Andreas	„Postmortaler Persönlichkeitsschutz und ärztliche Schweigepflicht“ in: NJW 2005, 1982-1984
Spindler, Gerald	„Das neue Telemediengesetz – Konvergenz in sachten Schritten“ in: CR 2007, 239-245
Spindler, Gerald	Unternehmensorganisationspflichten, Köln, Berlin, Bonn, München 2001
Spindler, Gerald	„Das Jahr 2000-Problem in der Produkthaftung - Pflichten der Hersteller und der Softwarenutzer“ in: NJW 1999, 3737-3745
Spindler, Gerald (Hrsg.)	Rechtsfragen bei Open Source, Köln 2004 zitiert: *Bearbeiter*, in: Spindler, Rechtsfragen bei Open Source
Spindler, Gerald	Vertragsrecht der Internet-Provider, 2. Auflage, Köln 2004 zitiert: *Bearbeiter*, in: Spindler, Vertragsrecht der Internet-Provider

Spindler, Gerald	Vertragsrecht der Telekommunkations-Anbieter, Köln 2000 zitiert: *Bearbeiter*, in: Spindler, Vertragsrecht der TK-Anbieter
Spindler, Gerald	„IT-Sicherheit und Produkthaftung - Sicherheitslücken, Pflichten der Hersteller und der Softwarenutzer“ in: NJW 2004, 3145-3150
Spindler, Gerald	„Der Jahr-2000-Fehler: Vertragsrechtliche Haftungsfragen des Softwareveräußerers“ in: DB 1999, 1991-1998
Spindler, Gerald	„Haftung und Verantwortlichkeit im IT-Recht“ in: CR 2005, 741-747
Spindler, Gerald	„Risiko der heimlichen Installation eines automatischen Einwahlprogramms (Dialer)“ – Anmerkung zu BGH Urteil v. 04.03.2004 - III ZR 96/03 in: JZ 2004, 1128-1132
Spindler, Gerald	„Haftungs- und vertragsrechtliche Probleme von Web-Services“ in: DuD 2005, 139-141
Spindler, Gerald	„Verantwortlichkeit eines Plattformbetreibers für fremde Inhalte“ in: JZ 2005, 37-40
Spindler, Gerald	„Das Gesetz zum elektronischen Geschäftsverkehr - Verantwortlichkeit der Diensteanbieter und Herkunfts-

	landprinzip“ in: NJW 2002, 921-927
Spindler, Gerald	Steuerungsfunktionen des Produkthaftungsrecht im IT-Recht und Reformbedarf, in: Hänlein, Andreas/ Roßnagel, Alexander (Hrsg.), Wirtschaftsverfassung in Deutschland und Europa. Festschrift für Bernhard Nagel, Kassel 2007, 21-30 zitiert: *Spindler*, in: FS Nagel
Spindler, Gerald	„Risiko der heimlichen Installation eines automatischen Einwahlprogramms (Dialer)“ in: JZ 2004, 1128-1132
Spindler, Gerald	„Verschuldensunabhängige Produkthaftung im Internet“ in: MMR 1998, 119-124
Spindler, Gerald/ Börner, Fritjof	E-Commerce-Recht in Europa und den USA, Berlin u.a. 2003 zitiert: *Bearbeiter*, in: Spindler/Börner
Spindler, Gerald/ Ernst, Stefan	„Vertragsgestaltung für den Einsatz von E-Mail-Filtern“ in: CR 2004, 437-445
Spindler, Gerald/ Kasten, A. Kasten	Organisationsverpflichtungen nach der MiFID und ihre Umsetzung in: AG 2006, 785-791
Spindler, Gerald/ Klöhn, Lars	„Neue Qualifikationsprobleme im E-Commerce – Verträge über die Verschaffung digitalisierter Informationen als Kaufvertrag, Werkvertrag,

	Verbrauchsgüterkauf?“ in: CR 2003, 81-86
Spindler, Gerald/ Klöhn, Lars	„Fehlerhafte Informationen und Software – Die Auswirkungen der Schuld- und Schadensrechtsreform“, Teile 1 und 2 in: VersR 2003, 273-282, 410-414
Spindler, Gerald/ Schmitz, Peter/ Geis, Ivo	Teledienstegesetz, Teledienstedatenschutzgesetz, Signaturgesetz : TDG, Kommentar, München 2004 zitiert: Spindler/Schmitz/Geis-*Bearbeiter*
Spindler, Gerald/ Volkmann, Christian	„Die öffentlich-rechtliche Störerhaftung der Access-Provider“ in: K&R 2002, 398-409
Spindler, Gerald/ Wiebe, Andreas (Hrsg.)	Internet-Auktionen und Elektronische Marktplätze, 2. Auflage, Köln 2005 zitiert: *Bearbeiter*, in: Spindler/Wiebe, Internet-Auktionen und Elektronische Marktplätze
Stadler, Thomas	Haftung für Informationen im Internet, 2. Auflage, Berlin 2005
Staudinger, Ansgar	„Der Rückgriff des Unternehmers in grenzüberschreitenden Sachverhalten“ in: ZGS 2002, 63-64
Staudinger, Julius von	J. von Staudingers Kommentar zum Bürgerlichen Gesetzbuch mit Einführungsgesetz und Nebengesetzen, 13. Bearbeitung, Berlin 1993 ff. zitiert: Staudinger-*Bearbeiter*

Steffen, Erich	„Haftung im Wandel“ in: ZVersWiss 82 (1993), 13-37
Steffen, Erich	„Die haftungsrechtliche Bedeutung der Qualitätssicherung in der Krankenversorgung“ in: Ahrens, Hans-Jürgen/v. Bar, Christian/Fischer, Gerfried/Spickhoff, Andreas/Taupitz, Jochen (Hrsg.), Festschrift für Erwin Deutsch zum 70. Geburtstag, Köln, Berlin, Bonn, München 1999, 799-814
Stein, Friedrich/ Jonas, Martin	Kommentar zur Zivilprozessordnung, 22. Auflage, Tübingen 2002 - zitiert: Stein/Jonas-*Bearbeiter*
Shavell, Steven	„Strict Liability versus Negligence“ in: The Journal of Legal Studies, Vol. 9, No. 1 1980, 1-25
Stichtenoth, Jonas	„Softwareüberlassungsverträge nach dem Schuldrechtsmodernisierungsgesetz“ in: K&R 2003, 105-110.
Stober, Rolf	„Customer Relationship Management, Risikomanagement und Wirtschaftsverwaltungsmanagement“ in: DÖV 2005, 333-338
Stockhausen, Lothar	„Die Einführung des HBCI-Standards aus bankrechtlicher Sicht“ in: WM 2001, 605-619
Stodolkowitz, Heinz Dieter	„Beweislast und Beweiserleichterung bei

	der Schadensursächlichkeit von Aufklärungspflichtverletzungen“ in: VersR 1994, 11-15
Stoll, Hans	„Anmerkung zu BGH Urteil v. 18.1.1983 – VI ZR 310/79“ in: JZ 1983, 499-504
Stollberger, Thomas	Marktreport: IT-Störfälle in Unternehmen nehmen zu – Risikomanagement beeinflusst auch Kreditwürdigkeit, http://www.verivox.de/news/ArticleDetails.asp?PM=1&aid=2542
Stone, Robert	CenterTrack: An IP Overlay Network for Tracking DoS Floods, http://www.arbornetworks.com/downloads/research51/stone00centertrack_new.pdf
Streinz, Rudolf	Europarecht, 7. Auflage, Heidelberg 2005
Streinz, Rudolf (Hrsg.)	EUV/EGV: Vertrag über die europäische Union und Vertrag zur Gründung der Europäischen Gemeinschaft, München 2003 zitiert: EUV/EGV-*Bearbeiter*
Streitz, Siegfried	„Sicherheit und Datenkommunikation“ in: NJW-CoR 2000, 208-214
Strömer, Tobias H.	Online-Recht, Heidelberg 1997
Taeger, Jürgen	Außervertragliche Haftung für fehlerhafte Computerprogramme, Tübingen 1995
Taeger, Jürgen	„Produkt- und Produzentenhaftung bei Schäden durch fehlerhafte Compu-

	terprogramme“ in: CR 1996, 257-271
Tanenbaum, Andrew S.	Computer Networks, Fourth Edition, Upper Saddle River 2003
Tappert, Rainer	EDV-System-Prüfung - bankbetriebliche Revisionsinformatik, Köln 1994
Taschner, Hans Claudius/ Frietsch Edwin	Produkthaftungsgesetz und EG-Produkthaftungslinie, Kommentar, 2. Auflage, München 1990
Taupitz, Jochen	Haftung für Energieleiterstörungen durch Dritte, Berlin 1981
Taupitz, Jochen	Ökonomische Analyse und Haftungsrecht – Eine Zwischenbilanz, AcP 196 (1996), 114-167
Terlau, Matthias	„Das Jahr-2000-Problem und das Risiko-management im Unternehmen“ in: CR 1999, 284-292
Thaller, Georg Erwin	ISO 9001: Software-Entwicklung in der Praxis, 3. Auflage, Hannover 2001
Thomas, Heinz/ Putzo, Hans	ZPO Kommentar, 27. Auflage, München 2005 zitiert: Thomas/Putzo-*Bearbeiter*
Tiedemann, Stefan	„Kollidierende AGB-Rechtswahlklauseln im österreichischen und deutschen IPR“ in: IPRax 1991, 424-427
Tiedtke, Klaus	„Die Haftung des Produzenten für die Verletzung von Warnpflichten“ in: Lange, Hermann/Nörr, Knut Wolf-

	gang/Westermann, Harm Peter (Hrsg.), Festschrift für Joachim Gernhuber, Tübingen 1993, 471-487
Tiedtke, Klaus	„Produkthaftung des Herstellers und des Zulieferers für Schäden an dem Endprodukt seit dem 1. Januar 1990“ in: NJW 1990, 2961-2963
Tietzel, Manfred	„Die Rationalitätsannahme in den Wirtschaftswissenschaften oder Der homo oeconomicus und seine Verwandten“ in: Jahrbuch für Sozialwissenschaft, Bd. 32, 1981, Heft 2, 115-139
Tilborg, Henk C. A. van	Enyclopedia of Cryptography and Security, berlin u.a. 2005.
Tinnefeld, Marie-Therese/ Ehmann, Eugen/ Gerling, Rainer W.	Einführung in das Datenschutzrecht, 4. Auflage Oldenburg 2005
Tita, Rolf-Thomas	„Umfang und Grenzen der Softwareversicherung nach Kl. 028 zu den ABE Teil (I) und Teil (II)“ in: VW 2001, 1696, 1781-1785
Trapp, Andreas	„Zivilrechtliche Sicherheitsanforderungen an eCommerce“ in: WM 2001, 1192-1202
Trute, Hans-Heinrich/ Spoerr, Wolfgang/ Bosch, Wolfgang	Telekommunikationsgesetz mit FTEG, Kommentar, Berlin New York 2001 zitiert: Trute/Spoerr/Bosch-*Bearbeiter*

Ulmer, Peter	„Produktbeobachtungs-, Prüfungs- und Warnpflichten eines Warenherstellers in Bezug auf Fremdprodukte?“ in: ZHR 152, 564-599
Ultsch, Michael	„Zugangsprobleme bei elektronischen Willenserklärungen - Dargestellt am Beispiel der Electronic Mail“ in: NJW 1997, 3007-3009
Unbekannt	„Italien: Höhere Haftung für Boote“ in: VW 1995, 580
v. Bar, Christian	Produktverantwortung und Risikoakzeptanz, München 1998 zitiert: *Bearbeiter*, in: Produktverantwortung und Risikoakzeptanz
v. Bar, Christian	Vorbeugender Rechtsschutz vor Verkehrspflichtverletzungen“ in: 25 Jahre Karlsruher Forum, Jubiläumsausgabe 1983, S. 80-85
v. Bar, Christian	Verkehrspflichten, Köln, Berlin, Bonn, München 1980
v. Gamm, Otto-Friedrich	„Datenschutz und Wettbewerbsrecht“ in: GRUR 1996, 574-579
v. Lewinski, Kai	„Anwaltliche Schweigepflicht und E-Mail“ in: BRAK-Mitt 2004, 12-17
v. Westphalen, Friedrich	„ Die allgemeine Verkehrssicherungspflicht und die Beleuchtungspflicht auf öffentlichen Straßen“ in: DB 1987, Beilage Nr. 11, 1-15

v. Westphalen, Friedrich	„Warn- oder Rückrufaktion bei nicht sicheren Produkten: §§ 8, 9 ProdSG als Schutzgesetz i.S. von § 823 Abs.–2 BGB - Rechtliche und versicherungsrechtliche Konsequenzen“ in: DB 1999, 1369-1374
v. Westphalen, Friedrich	„Jahr-2000-Fehler und deliktische Haftung“ in: DStR 1998, 1722-1724
v. Westphalen, Friedrich	„Die Millennium-Garantie und ihre Rechtsfolgen“ in: PHi 1998, 222-227
v. Westphalen, Friedrich (Hrsg.)	Vertragsrecht und AGB-Klauselwerke, Loseblatt, Stand Oktober 2006 zitiert: *Bearbeiter*, in: v. Westphalen, Vertragsrecht und AGB-Klauselwerke
v. Westphalen, Friedrich	Produkthaftungshandbuch, Band I, München 1997 zitiert: *Bearbeiter*, in: v. Westphalen, ProdHaftHdb
v. Westphalen, Friedrich/ Langheid, Theo/ Streitz, Siegfried	Der Jahr-2000-Fehler: Haftung und Versicherung, Köln 2001 zitiert: *Bearbeiter*, in: v.Westphalen/Langheid/ Streitz, Der Jahr-2000-Fehler
v. Wulffen, Matthias	SGB X, Kommentar, 5. Auflage, München 2005 zitiert: v. Wulffen-*Bearbeiter*
Voßbein, Reinhard	„Datenschutzauditierung“

	in: DuD 2003, 92-97
Wagner, Christoph/ Lerch, Janusz-Alexander	„Mandatsgeheimnis im Internet?“ in: NJW-CoR 1996, 380-385
Wagner, Gerd Rainer/ Janzen, Henrik	„Umwelt-Auditing als Teil des betrieblichen Umwelt- und Risikomanagements“ in: BFuP 1994, 573-604
Wagner, Gerhard	„Das neue Produktsicherheitsgesetz – Öffentlich-rechtliche Produktverantwortung und zivilrechtliche Folgen (Teil II)“ in: BB 1997, 2541-2546
Wagner, Gerhard	Öffentlich-rechtliche Genehmigung und zivilrechtliche Rechtswidrigkeit, Köln 1989
Waldenberger, Arthur	„Grenzen des Verbraucherschutzes beim Abschluss von Verträgen im Internet“ in: BB 1996, 2365-2371
Wandt, Manfred	Internationale Produkthaftung, Heidelberg 1995
Weber, Rolf	Informatik und das Jahr 2000. Risiken und Vorsorgemöglichkeiten aus rechtlicher Sicht, Zürich 1998
Wendehorst, Christiane	„Das Vertragsrecht der Dienstleistungen im deutschen und künftigen europäischen Recht“ in: AcP 206 (2006), 205-299
Wente, Jürgen K.	Das Recht der journalistischen Recherche,

	UFITA Band 71, Jur. Diss. Universität Göttingen, Baden-Baden 1987
Werner, Stefan	„Elektronischer Zahlungsverkehr“ in: MMR 1998, 338-342
Westermann, Harm Peter (Hrsg.)	Erman, Bürgerliches Gesetzbuch, Handkommentar, Bd. 1 und 2, 11. Auflage, Münster, Köln 2004 zitiert: Erman-*Bearbeiter*
Weyers, Hans-Leo	Unfallschäden, 1971
Wiebe, Andreas	„Wettbewerbs- und zivilrechtliche Rahmenbedingungen der Vergabe und Verwendung von Gütezeichen“ in: WRP 1993, 74-90
Wiebe, Andreas	„Identität eines Teilnehmer an einer Internetauktion“ in: MMR 2002, 257-258
Wiesgickl, Margareta	„Rechtliche Aspekte des Online-Banking“ in: WM 2000, 1039-1050
Wilhelm, Rudolf	„Qualitätsmanagement-Systeme nach den Normen DIN ISO 9.000 ff in Software-Unternehmen“ in: DuD 1995, 330-337
Wilrich, Thomas	Geräte- und Produktsicherheitsgesetz, Kommentar, Berlin 2004
Wimmer, Konrad	„MaRisk: Überblick und Konsequenzen für die Geschäftsleitung“ in: BKR 2006, 146-153
Winter, Ralf	„Darlegungs- und Beweislast bei Onlineauktion“

	in: MMR 2002, 836-837
Witte, Jürgen/ Hrubesch, Boris	„Die persönliche Haftung von Mitgliedern des Aufsichtsrats einer AG - unter besonderer Berücksichtigung der Haftung bei Kreditvergaben“ in: BB 2004, 725-732
Wohlgemuth, Hans H./ Gerloff, Jürgen	Datenschutzrecht: eine Einführung mit praktischen Fällen, Neuwied, 2005
Wohlgemuth, Michael	„Das Jahr 2000-Problem – Vertragliche und vertragsähnliche Haftung“ in: MMR 1999, 59-67
Wuermeling, Ulrich	„Einsatz von Programmsperren“ in: CR 1994, 585-595
Zahrnt, Christoph	„Abschlußzwang und Laufzeit beim Softwarepflegevertrag“ in: CR 2000, 205-207
Zerbe, Richard O.	Economic efficiency in law and economics, Cheltenham, UK 2001
Zeuner, Albrecht	„Störungen des Verhältnisses zwischen Sache und Umwelt als Eigentumsverletzung – Gedanken über Inhalt und Grenzen von Eigentum und Eigentumsschutz“ in: Jakobs, Horst Heinrich/Knobbe-Keuk, Brigitte/Picker, Eduard/Wilhelm, Jan (Hrsg.), Festschrift für Werner Flume zum 70. Geburtstag, Köln 1978, 775-787
Zeuner, Albrecht	„Zum Verhältnis zwischen Fremd- und Eigenverantwortlichkeit im Haf-

	tungsrecht“ in: Beuthien, Volker/Fuchs, Maximilian/Roth, Herbert/Schiemann, Gottfried/Wacke, Andreas (Hrsg), Festschrift für Dieter Medicus zum 70. Geburtstag, Köln, Berlin, Bonn, München 1999, 693-706
Zimmermann, Steffen	„Die MaRisk als regulatorischer Imperativ“ in: BKR 2005, 208-217
Zöller, Richard	Zivilprozessordnung, Kommentar (ZPO), 25. Auflage, Köln 2005 zitiert: Zöller-*Bearbeiter*
Zscherpe, Kerstin A./Lutz, Holger	„Geräte- und Produktsicherheitsgesetz: Anwendbarkeit auf Hard- und Software“ in: K&R 2005, 499-502

H. Abkürzungsverzeichnis

aA	andere Ansicht
ABl.	Amtsblatt
ABlEG	Amtsblatt der Europäischen Gemeinschaften
Abs.	Absatz
abw.	abweichend
AcP	Archiv für die civilistische Praxis
aF	alte Fassung
AfP	Archiv für Presserecht
AG	Aktiengesellschaft
AG	Amtsgericht
AGB	Allgemeine Geschäftsbedingungen
AktG	Aktiengesetz
Alt.	Alternative
Anh.	Anhang
Art.	Artikel
ASB	Anti-Blockier-System
Aufl.	Auflage
AtA	Ausschuss für technische Arbeitsmittel
AtAV	Ausschuss für technische Arbeitsmittel und Verbraucherprodukte
B2B	Business to Business
B2C	Business to Consumer
BaFin	Bundesanstalt für Finanzdienstleistung

BAG	Bundesarbeitsgericht
BB	Der Betriebs-Berater
Bd.	Band
BDSG	Bundesdatenschutzgesetz
BegrRegE	Begründung zum Regierungsentwurf
BFH	Bundesfinanzhof
BGB	Bürgerliches Gesetzbuch
BGBl.	Bundesgesetzblätter
BGH	Bundesgerichtshof
BGHZ	Entscheidungssammlung des Bundesgerichtshofs in Zivilsachen
BImSchG	Bundesimmissionsschutzgesetz
BMWI	Bundesministerium für Wirtschaft und Arbeit
BORA	Berufsordnung für Rechtsanwälte
BOStB	Berufsordnung der Steuerberater
BRAO	Bundesrechtsanwaltsordnung
BR-Drucks.	Bundesratsdrucksache
BSI	Bundesamt für Sicherheit in der Informationstechnik
BSIG	Gesetz über die Errichtung des Bundesamtes für Sicherheit in der Informationstechnik
bspw.	beispielsweise
BT-Drucks.	Bundestagsdrucksache
Btx	Bildschirmtext
BVerfG	Bundesverfassungsgericht
BVerwG	Bundesverwaltungsgericht

bzw.	beziehungsweise
CE	Communautés Européenes
CEN	Europäische Komitee für Normung
CENELEC	Europäisches Komitee für Elektrotechnische Normung
CEO	Chief Executive Officer
CFO	Chief Financial Officer
ChemG	Chemikaliengesetz
CR	Computer und Recht
DB	Der Betrieb
d.h.	das heißt
DDoS	Distributed-Denial-of-Service
DIN	Deutsche Institut für Normung e.V.
DKE	Deutsche Elektrotechnische Kommission im DIN und VDE
DNS	Domain Name Server
DoS	Denial-of-Service
DRDoS	Distributed-Reflected-Denial-of-Service
DRL	Datenschutz-Richtlinie
DSB	Datenschutzberater
DuD	Datenschutz und Datensicherung
EC	Eurocheque
EDV	Elektronische Datenverarbeitung
EG	Europäische Gemeinschaft
Einf	Einführung
E-Mail	Electronic Mail

ESP	elektronisches Stabilitätsprogramm
etc.	et cetera
ETSI	Europäisches Institut für Telekommunikationsstandards
EU	Europäische Union
EuGH	Europäischer Gerichtshof
EWG	Europäische Wirtschaftsgemeinschaft
f.	folgende
ff.	fort folgende
Fn.	Fußnote
FS	Festschrift
FSA	Financial Services Authority
GPSG	Geräte- und Produktsicherheitsgesetz
GPSGV	Verordnungen zum Geräte- und Produktsicherheitsgesetz
GRUR	Gewerblicher Rechtsschutz und Urheberrecht
GRUR-Int	Gewerblicher Rechtsschutz und Urheberrecht, Internationaler Teil
GRUR-RR	Gewerblicher Rechtsschutz und Urheberrecht Rechtsprechungsreport
GS	geprüfte Sicherheit
GSG	Gerätesicherheitsgesetz
HBCI	Homebanking Computer Interface
Hdb	Handbuch
HGB	Handelsgesetzbuch
hL	herrschende Lehre
hM	herrschende Meinung

Hrsg.	Herausgeber
HTML	Hypertext Markup Language
HTTP	Hypertext Transport Protocol
i.w.S.	im weiteren Sinne
idR	in der Regel
idS	in diesem Sinne
IDS	Intrusion-Detection-Systeme
IP	Internet Protocol
IPS	Intrusion-Prevention-Systeme
ISO	Internationale Organisation für Normung
ISP	Internet Service Provider
IT	Information Technology
ITRB	IT-Rechtsberater
iVm	in Verbindung mit
JMStV	Jugenmedienschutz-Staatsvertrag
JZ	Juristenzeitung
K&R	Kommunikation und Recht
Kap.	Kapitel
KG	Kapitalgesellschaft
krit.	kritisch
KWG	Gesetz über das Kreditwesen
LDSG	Landesdatenschutzgesetz
LG	Landgericht
Lit.	Literatur
MaH	Mindestanforderungen an das Betreiben von Handelsgeschäften

MaIR	Mindestanforderungen an die Interne Revision
MaK	Mindestanforderungen an das Kreditgeschäft
MaRisk	Mindestanforderungen an das Risikomanagement
MiFID	Markets in Financial Instruments Directive
MMR	Multimedia und Recht
MPG	Medizinproduktegesetz
mTAN	Mobile Transaktionsnummer
MünchKommAktG	Münchner Kommentar zum AktG
MünchKommBGB	Münchner Kommentar zum BGB
mwN.	mit weiteren Nachweisen
NJW	Neue juristische Wochenschrift
NJW-RR	Neue juristische Wochenschrift - Rechtsprechungsreport
Nr.	Nummer
NZG	Neue Zeitschrift für das Gesellschaftsrecht
OLG	Oberstes Landgericht
ÖNORM	Österreichisches Normungsinstitut
OVG	Oberstes Verwaltungsgericht
PDA	Personal Digital Assistant
PDCA	Plan-Do-Check-Act
PIN	Persönliche Identifikationsnummer
ProdHaftG	Produkthaftungsgesetz
ProdSG	Produktsicherheitsgesetz
PTSG	Post und Telekommunikationssicherstellungsgesetz

PTZSV	Post- und Telekommunikations-Zivilschutzverordnung
RAID-Systeme	
RDV	Recht der Datenverarbeitung
RichtlBKO	Richtlinie für den betrieblichen Katastrophenschutz
Rn.	Randnummer
Rspr.	Rechtsprechung
s.	siehe
S.	Seite/ Satz
SEC	Securities and Exchange Commission
SEPA	Single Euro Payments Area
SH	Schleswig Holstein
SigG	Signaturgesetz
SigV	Signaturverordnung
sog.	sogenannte
SolvV	Solvabilitätsverordnung
SOX	Sarbanes-Oxley-Act
SSL	Secure Sockets Layer
StGB	Strafgesetzbuch
StPO	Strafprozessordnung
TAN	Transaktionsnummer
TDG	Teledienstegesetz
TKG	Telekommunikationsgesetz
TKSIV	Telekommunikations-Sicherstellungsverordnung

TMG	Telemediengesetz
TÜV	Technischer Überwachungs-Verein
u.U.	unter Umständen
ULD	Unabhängige Landeszentrum für Datenschutz
UrhG	Urhebergesetz
URL	Uniform Resource Locator
UWG	Gesetz gegen den unlauteren Wettbewerb
VersR	Versicherungsrecht
VG	Verwaltungsgericht
vgl.	vergleiche
WEP	Wired Equivalent Privacy
WHG	Gesetz zur Ordnung des Wasserhaushalts
WM	Wertpapiermitteilungen
WpHG	Wertpapierhandelgesetz
WRP	Wirtschaft in Recht und Praxis
z.B.	um Beispiel
ZGR	Zeitschrift für Unternehmens- und Gesellschaftsrecht
ZIP	Zeitschrift für Wirtschaftsrecht
ZKA	Der Zentrale Kreditausschuss
ZLG	Zentralstelle der Länder für Gesundheitsschutz bei Arzneimitteln und Medizinprodukten
ZLS	Zentralstelle der Länder für Sicherheitstechnik
ZPO	Zivilprozessordnung

z.T.	zum Teil
ZUM	Zeitschrift für Urheber- und Medienrecht,