Jörg Becker, Thomas Hoeren

IT-Sicherheit – rechtliche Vorgaben und Implikationen für die Systemgestaltung

Die deutsche Rechtsordnung enthält, wie auch europäische sowie ausländische Rechtsordnungen, eine Fülle von Normen, aus denen sich Pflichten zur Sicherung von Informationssystemen ergeben. Die gravierenden Rechtsfolgen von Sicherheitslücken in Informationssystemen machen deutlich, dass das Aufstellen effektiver Sicherheitsvorkehrungen nicht nur eine rechtliche Frage ist, sondern zudem ein existenzielles betriebswirtschaftliches Erfordernis darstellt. Folglich müssen bereits bei der Gestaltung der im Unternehmen eingesetzten Informationssysteme rechtliche Vorschriften beachtet werden.

Inhaltsübersicht

1 Notwendigkeit von Sicherheitsmaßnahmen auf Anbieter- und Nutzerseite

Der Begriff IT-Sicherheit beschreibt einen Zustand, in dem Gefahren oder Schäden im Bereich der Informations- und Kommunikationstechnik verhindert werden. Derartige Gefahren können sowohl externer als auch interner Natur sein – wie etwa bei unsachgemäßer Handhabung durch eigene Mitarbeiter. Um einen sicheren Zustand zu erreichen, müssen die Risiken klar benannt, rechtlich bewertet und technische Schutzmaßnahmen umgesetzt werden. Dabei sind Fragen der Produkthaftung beim Softwarekauf ebenso dem Bereich der IT-Sicherheit zuzuordnen [Spindler 2004, S. 3145 ff.] wie etwa Hackerangriffe, Virenattacken oder gezielter Datenmissbrauch. Gemeinsam ist all diesen Konstellationen, dass bestimmte Sicherungspflichten bei der Erstellung oder im Umgang mit einem IT-System konstituiert werden, deren Verletzung im Schadensfalle zu Ersatzansprüchen führen kann. Der vorliegende Beitrag konzentriert sich auf die Darstellung dieser haftungsrechtlichen Problematik, wenngleich der Bereich IT-Sicherheit ebenfalls gesellschafts-, finanz- sowie wirtschaftsverwaltungsrechtliche Bezüge aufweist.

Dass der Anbieter eines IT-Systems bestimmte Vorkehrungen zur Sicherung der in diesem System kursierenden Daten zu treffen hat, wird auch dem Nichtjuristen schlüssig erscheinen. Schon undurchsichtiger gestaltet sich jedoch die Antwort auf die Frage, ob und welche Sicherheitsvorkehrungen und Sorgfaltspflichten dem Nutzer eines IT-Systems obliegen. Diese müssen sich keineswegs decken. So etwa beim Onlinebanking: Die Bank als Anbieter des Systems hat durch technisch-organisatorische Maßnahmen ganz andere Möglichkeiten, IT-Sicherheit zu bewerkstelligen – etwa durch Zugangsbeschränkung zu Daten – als etwa der Bankkunde. Dieser kann sich durch Information, durch aufmerksamen Umgang mit seinen Zugangsdaten oder durch Sicherungs-

programme auf seinem eigenen Computer vor Angriffen Dritter schützen.

Erst das Zusammenspiel der Sicherheitsmaßnahmen sowohl auf Anbieter- als auch auf Nuterzseite bewirkt einen hinreichenden IT-Sicherheitsstandard, sodass beide Sphären nicht isoliert betrachtet werden sollten. Zudem können auf beiden Seiten gleichzeitig Sicherheitslücken bestehen: Folglich wird dieses Wechselspiel bei der Frage des Mitverschuldens nach § 254 BGB abermals relevant. In den nachstehenden Abschnitten ist daher sowohl für den Anbieter als auch für den Nutzer eines IT-Systems aufzuschlüsseln, welche Sicherheitspflichten das geltende Recht vorschreibt und welche technischen Maßnahmen deren Erfüllung verlangt. Gleichwohl wird der Schwerpunkt der Darstellung auf die Anforderungen an den Anbieter eines IT-Systems gelegt.

2 Anforderungen an den Anbieter

2.1 Spezialgesetzliche Vorschriften

Datenschutz

Insbesondere im Bereich des Datenschutzes existieren in Deutschland innerhalb bestimmter bereichsspezifischer Gesetze kodifizierte Vorschriften, die dem Verwender von IT-Systemen Sicherheitsmaßnahmen auferlegen. So beispielsweise in § 18 Abs. 4 Nr. 3 Mediendienstestaatsvertrag (MDStV) bzw. in § 4 Abs. 4 Nr. 3 Teledienstedatenschutzgesetz (TDDSG), wonach Anbieter von Medien- bzw. Telediensten durch technische und organisatorische Maßnahmen sicherzustellen haben, dass der Nutzer gegen Kenntnisnahme Dritter bei der Inanspruchnahme des jeweiligen Dienstes geschützt ist. Wie dies technisch umzusetzen ist, wird von diesen Normen nicht vorgeschrieben.

Auch § 109 Abs. 1 Nr. 1 und 2 Telekommunikationsgesetz (TKG) verpflichtet die Anbieter von Telekommunikationsdiensten dazu, technische Vorkehrungen zum Schutz des Fernmeldegeheimnisses und personenbezogener Daten gegen unerlaubte Zugriffe zu treffen. § 109 Abs. 3 TKG geht noch darüber hinaus und verlangt die Erstellung eines Sicherheitskonzeptes; über die technische Beschaffenheit dieser Maßnahmen schweigt jedoch auch diese Norm.

Wie weit die Pflicht zum Einsatz von IT-Sicherheitsmaßnahmen zum Schutz personenbezogener Daten geht, manifestiert sich in § 9 Abs. 1 Bundesdatenschutzgesetz (BDSG), der als Auffangnorm eine Pflicht zur Installation technischer Maßnahmen bei öffentlichen und nicht öffentlichen Stellen normiert. Die Anlage 1 zu § 9 BDSG enthält eine Aufzählung von Maßnahmen, die zum Schutz personenbezogener Daten zu ergreifen sind: Danach hat der Anbieter unter anderem Unbefugten den Zutritt zur Datenverarbeitungsanlage zu verwehren (Zutrittskontrolle), die Nutzung des Systems durch Unbefugte zu verhindern (Zugangskontrolle), sicherzustellen, dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können (Zugriffskontrolle). Gleiches hat der Anbieter auch bei der elektronischen Weitergabe zu gewährleisten (Weitergabekontrolle) sowie sicherzustellen, dass nachträglich festgestellt werden kann, von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind (Eingabekontrolle). Wenngleich auch diese Norm sich nicht über die konkrete technische Umsetzung auslässt, so sorgt sie im Bereich des Datenschutzes dennoch für ein Mindestmaß an Rechtssicherheit, indem sie einzelne Kontrollmöglichkeiten aufführt.

Kreditwesen

Von Kreditinstituten verlangt § 25a Abs. 1 Nr. 4 Kreditwesengesetz (KWG) gleichfalls die Installation besonderer technischer Sicherheitsvorkehrungen beim Einsatz elektronischer Datenverarbeitung.

Weitere Vorgaben für das Kreditwesen finden sich in der Baseler Eigenkapitalüberein-

kunft (kurz Basel II), wonach deutsche Kreditinstitute spätestens Ende 2006 bei der Vergabe von Krediten eine Risikoeinschätzung des beantragenden Unternehmens vornehmen müssen, wozu gleichfalls der Grad der Sicherheit von eingesetzten IT-Systemen seitens des Kreditbeantragenden gehört. Die Transformation in deutsches Recht wird über eine von der Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin) erlassene Solvabilitätsverordnung aufgrund von § 10 Abs. 1 S. 2 KWG erfolgen (vgl. hierzu den am 15.02.2006 vom Bundeskabinett beschlossenen »Gesetzesentwurf zur Umsetzung der neu gefassten Bankenrichtlinie und der neu gefassten Kapitaladäquanzrichtlinie«). Anhang 7 des Abkommens (Operationelle Risiken – Detaillierte Klassifikation von Verlustereignissen) enthält die Ereigniskategorie »Systemsicherheit«, in der beispielhaft Schäden durch Hackeraktivitäten und Diebstahl von Informationen aufgezählt werden. Basel II richtet sich somit zum einen an den Kreditgeber und verlangt von ihm die Unterlegung operationeller IT-Risiken mit Eigenkapital; zum anderen richtet sich Basel II aber auch an den Kreditnehmer und verlangt von ihm eine detaillierte Offenlegung seiner IT-Risiken gegenüber dem Kreditgeber. Unternehmen mit IT-Sicherheitslücken werden folglich in der von den Kreditinstituten durchzuführenden Risikobewertung niedriger eingestuft und mit höheren Zinsen belastet. Auch wenn diese Vorgaben – juristisch betrachtet – nicht als unmittelbare Sicherungspflicht ausgestaltet sind, so stellen sie Obliegenheiten dar, deren Nichtbeachtung finanzielle Nachteile zur Folge haben kann; wirtschaftlich betrachtet können sie sich für ein Unternehmen wie eine Sicherungspflicht auswirken.

Den Begriff »operationelles Risiko« definiert Basel II als »Gefahr von Verlusten, die infolge der Unangemessenheit oder des Versagens von internen Verfahren, Menschen und Systemen oder von externen Ereignissen eintreten«. Eine weiter gehende Normierung, wie ein solches internes System technisch ausgestaltet sein sollte, enthält Basel II jedoch nicht.

2.2 Analog anwendbare Vorschriften

Eine Pflicht zur Installation von Sicherheitsmaßnahmen bei der IT-Verwendung kann sich auch aus Normen ergeben, die nicht unmittelbar wörtlich einen IT-Bezug aufweisen, die jedoch eine analoge Anwendung erlauben.

In Betracht kommt insofern Art. 1 Nr. 9 des Gesetzes zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG), der Eingang in § 91 Abs. 2 AktG gefunden hat. Demnach hat der Vorstand geeignete Maßnahmen zu treffen, wozu insbesondere die Implementierung von Überwachungssystemen zählt, damit bestimmte, den Fortbestand der Gesellschaft gefährdende Entwicklungen früh erkannt werden. Nach einer starken Meinung im juristischen Schrifttum gehört dazu innerhalb eines Analogieschlusses auch das Ergreifen entsprechender IT-Sicherheitsmaßnahmen [Barton 2004, S. 305 f.]. Aber auch für Unternehmen in der Rechtsform einer GmbH wird eine entsprechende Pflicht aus einer analogen Anwendung von § 43 Abs. 1 GmbHG befürwortet [Schultze-Melling 2005, S. 73 ff.]. Hierfür lässt sich die Begründung zum Regierungsentwurf, Bundestagsdrucksache 13/9712, anführen, in der es heißt, es sei davon auszugehen, dass für Gesellschaften mit beschränkter Haftung je nach ihrer Größe, Komplexität und ihrer Struktur nichts anderes gilt.

Gleichfalls analog lässt sich eine Verpflichtung zur Installation von IT-Sicherheitsmaßnahmen innerhalb des Wertpapierhandels herleiten. So bestimmt Art. 1 Nr. 1e des Gesetzes zur Verbesserung des Anlegerschutzes (AnSVG) Sicherheitsmaßnahmen in Bezug auf Insiderwissen. Die Vorschrift wurde in § 15b Wertpapierhandelsgesetz (WpHG) umgesetzt und verlangt von den Emittenten das Führen von Verzeichnissen betreffend derjenigen Personen, die Zugang zu Insiderwissen besitzen. Da die Erfassung der Daten dieser Personen regelmäßig

über ein IT-System erfolgt, kommt auch hier eine Pflicht zur Installation von IT-Sicherheitssystemen in Betracht.

2.3 Allgemeine Sicherungspflichten

Auch außerhalb spezialgesetzlicher bzw. analog anwendbarer Regelungen können IT-Sicherungspflichten bestehen.

Vertragliche Sicherungspflichten

Im Rahmen vertraglicher Beziehungen kann eine solche Pflicht ausdrücklich zur Hauptleistungspflicht, wie etwa bei sogenannten Managed Security Services, gemacht werden. Auch in anderen Branchen, wie beispielsweise bei Escrow-Dienstleistungen, ist dies üblich. Hierbei hinterlegt ein Softwareanbieter, der den Quelltext nicht dem Anwender überlassen will, diesen bei einem unabhängigen Dritten. Daneben können sich Sicherungspflichten auch aus sogenannten Vertraulichkeitsklauseln ergeben [Schultze-Melling 2005, S. 73 ff.]; solche werden vereinbart, wenn ein Unternehmen einem anderen Unternehmen für eine gemeinsame Geschäftsbeziehung oder für einen Dienstleistungsauftrag sensible Informationen vorab zur Verfügung stellt.

Oftmals sind IT-Sicherungspflichten Bestandteil von allgemeinen Geschäftsbedingungen. So konstituieren etwa die besonderen Vertragsbedingungen der öffentlichen Hand (BVB) sowie die neuen EVB-IT (Ergänzende Vertragsbedingungen für die Beschaffung von Informationstechnik), die bei der Vergabe öffentlicher Aufträge regelmäßig Bestandteil des Vertrages werden, bestimmte Nebenpflichten. Beispielsweise verpflichtet § 13 BVB Planung den Auftragnehmer, besondere Sicherheitsmaßnahmen zum Schutz personenbezogener Daten und zur Geheimhaltung zu treffen. Entsprechende Geheimhaltungspflichten enthalten auch die neuen EVB-IT. Lücken in der IT-Sicherheit können eine Verletzung dieser Pflicht darstellen.

Es fragt sich zudem, ob die Gewährleistung von IT-Sicherheit auch eine ungeschriebene vertragliche Nebenpflicht im Sinne des § 241 Abs. 2 BGB sein kann. Das hängt davon ab, ob dies mit Rücksicht auf die Rechtsgüter und Interessen des anderen Teils nach der Verkehrsauffassung erforderlich erscheint. Bei einem IT-System, das gerade dazu angelegt ist, sensible Daten der Vertragspartei abzufragen, zu speichern oder zu übermitteln, wird man dies bejahen können. Hierzu zählen etwa das Onlinebanking, aber auch alle entgeltlichen Onlineangebote, die ein Zahlungssystem mittels Kreditkarte enthalten.

Sonstige, haftungspräventive Sicherungspflichten

Auch außerhalb vertraglicher Beziehungen können allgemeine IT-Sicherungspflichten bestehen. Zu denken ist etwa an eine deliktsrechtliche Haftung; hierfür wäre eine sogenannte Verkehrssicherungspflicht erforderlich [Bamberger & Roth-Spindler 2006, S. 255 f.]. Unproblematisch zu bejahen ist dies, soweit das IT-System selbst ein Produkt darstellt, wie etwa bei einem kommerziell vertriebenen Softwareprogramm. Dies folgt bereits aus den Grundsätzen der sog. Produkthaftung.

Generell wird eine Verkehrssicherungspflicht aus der Eröffnung einer Gefahrenquelle hergeleitet (vgl. Bundesgerichtshof (BGH), Neue Juristische Wochenschrift (NJW) 1985, S. 1076 f.). Somit ist fraglich, ob ein IT-System stets eine Gefahrenquelle in diesem Sinne darstellt. Erste Ansätze hierzu finden sich etwa im erstinstanzlichen Urteil zum sogenannten CompuServe-Fall (vgl. Amtsgericht (AG) München, Multimedia und Recht (MMR) 1998, S. 429 ff.; [Kaufmann 1998, S. 166]): Hierbei ging es um die Verantwortlichkeit eines Zugangsproviders für den Inhalt seiner Server. Diese Entscheidung wurde indes in zweiter Instanz aufgehoben [Barton 2000, S. 195]. Neuerdings ist jedoch wiederum eine strengere Tendenz in der Rechtsprechung erkennbar. So stufte erst vor kurzem das Landgericht (LG) Hamburg ein Internetforum als »besonders gefährliche Gefahrenquelle« ein. Hierbei handelt es sich um das

sogenannte »Heise-Urteil« des Hamburger LG vom 02.12.2005 (Az. 324 O 721/05); hierin wurde der Heise-Verlag verpflichtet, künftig eine Vorabkontrolle der Einträge auf seinen Foren durchzuführen. Die insbesondere in der IT-Fachpresse viel beachtete Entscheidung wurde jedoch vom Oberlandesgericht (OLG) Hamburg aufgehoben und eine generelle Pflicht zur Vorabkontrolle abgelehnt (Az. 7 U 50/06). Gleichwohl statuierte das OLG für bereits eingestellte Beiträge in Onlineforen eine »spezielle Überwachungspflicht«, wenn der Betreiber geradezu rechtswidrige Beiträge provoziert oder es bereits zu einer einmaligen Rechtsverletzung gekommen ist [Kaufmann 2006].

Richtigerweise ist ein IT-System nicht per se als Gefahrenquelle einzustufen. Vielmehr ist auf das konkrete IT-System im Einzelfall abzustellen. Als Kriterien müssen die berechtigten Sicherheitserwartungen der betroffenen Verkehrskreise (vgl. BGH, NJW 1985, S. 1076 f.), die wirtschaftliche Zumutbarkeit für den Anbieter (vgl. Wagner im Münchener Kommentar zum BGB, 4. Aufl. München 2003 § 823 Rn. 249), die Möglichkeiten des Selbstschutzes des Nutzers, die Bedeutung der betroffenen Rechtsgüter sowie Voraussehbarkeit und Umfang der drohenden Gefahren [Bamberger & Roth-Spindler 2006, S. 255 f.] herangezogen werden.

Was bedeutet dies im Klartext für im Internet tätige Unternehmen? Angesichts der gestiegenen Bedeutung von IT-Systemen für sämtliche Bereiche eines Unternehmens und der sowohl qualitativ als auch quantitativ gestiegenen Bedrohungen wird man gleichwohl eine Vielzahl von IT-Systemen, mit denen Unternehmen Informationen mit Dritten austauschen bzw. Daten Dritter speichern, als Gefahrenquelle im Sinne des Deliktsrechts einstufen müssen. Hieraus erwächst folglich eine allgemeine, gesetzliche IT-Sicherungspflicht. So verzeichnete beispielsweise T-Online jüngst eine Milliarde Spammails pro Tag, während die Zahl der ordnungsgemäßen Mails hingegen nur bei 30 Millionen liege, so Vorstandsmitglied Andreas Kindt am 25.04.2006 in Berlin auf dem 2. Gipfel zur Sicherheit in der Informationstechnik.

2.4 Inhalt der Sicherungspflichten

Den genannten spezialgesetzlichen Normen ist gemeinsam, dass sie den Inhalt der Sicherungspflicht mit einem unbestimmten Rechtsbegriff beschreiben – wie etwa »technische und organisatorische Vorkehrungen« (§ 18 Abs. 4 MDStV; § 4 Abs. 4 TDDSG; § 9 Abs. 1 BDSG), »angemessene technische Vorkehrungen oder sonstige Maßnahmen zum Schutze« (§ 109 Abs. 1 TKG) sowie »angemessene Sicherheitsvorkehrungen« (§ 25a Abs. 1 Nr. 4 KWG). Die konkrete Ausgestaltung des technisch-organisatorischen Inhalts dieser Pflichten überlässt das Gesetz folglich Rechtsprechung und Praxis. Lediglich § 9 BDSG enthält, wie dargelegt, in seiner Anlage 1 eine gewisse Ausformung der Verpflichtung. Es mag dahingestellt bleiben, ob eine genauere Normierung der technischen Umsetzung durch den Gesetzgeber aufgrund der sich ständig verändernden Missbrauchs- und Schutzmöglichkeiten im IT-Bereich sinnvoll wäre. So hat etwa die Postbank 2005 bundesweit eine sogenannte mobile TAN eingeführt, die per SMS verschickt wird, um neuartigen Phishing- und Pharming-Angriffen vorzubeugen. Gleichzeitig entwickeln sich fortlaufend neue Angriffsvarianten, wie etwa das sogenannte Man-in-the-Middle-Verfahren, um auch derartige Schutzmaßnahmen zu umgehen.

Ob die vom Anbieter getroffenen Maßnahmen die Anforderungen der genannten Normen erfüllen, muss folglich im konkreten Einzelfall anhand des Verkehrskreises, der Sensibilität der Daten, dem Grad der Gefährdung sowie am Stand der Technik bestimmt werden.

Gleichwohl kann zur Auslegung der in den genannten Normen verwendeten unbestimmten Rechtsbegriffe auf verschiedene standardisierte Verfahren zurückgegriffen werden.

Der sogenannte IT-Grundschutz des Bundesamtes für Sicherheit in der Informations-

technik (BSI) ist ein Standard zu Methoden, Prozessen und Verfahren. Angefangen von der Initiierung des IT-Sicherheitsprozesses über die Einbindung der Mitarbeiter bis zur Auswahl der technischen Maßnahmen gibt ein Handbuch (*www.bsi.de/literat/bsi_standard/index.htm*) detaillierte wie praxisnahe Empfehlungen für ein IT-Sicherheitsmanagement ab. Dieser Standard ist in Deutschland weit verbreitet und genießt hohes Ansehen – was nicht zuletzt daran liegt, dass das BSI Zertifikate über die Einhaltung des Standards vergibt. Ein möglicher Nachteil: Es handelt sich um einen rein nationalen Standard.

Ein international anerkanntes Verfahren ist der Code of Practice for Information Security (ISO 17799). Er enthält einen Maßnahmenkatalog für die Sicherheitspolitik, die Organisationsstrukturen sowie Einstufung der Sicherheitsrisiken. Daneben ist weiterhin der britische Standard BS 7799 zu beachten. Anders als ISO 17799 bietet dieser Standard die Möglichkeit der Zertifizierung.

Mit den Information Technology Security Evaluation Criteria (ITSEC) existiert daneben auch ein europäischer Standard (*www.bsi.de/zertifiz/itkrit/itsec-dt.pdf*). Er soll das Vertrauen in die Sicherheit von IT-Produkten und IT-Systemen herstellen, indem er detailliert ausgestaltete Schutzprofile für bestimmte Produktklassen vorsieht. Dieser Standard genießt ebenfalls internationales Ansehen, ist jedoch nicht ohne einen gewissen Aufwand zu implementieren.

Zur Konkretisierung des Inhalts der Vorgaben von Basel II und der Sicherungspflicht aus § 25a Abs. 1 S. 3 Nr. 4 KWG könnte zudem auf den »Entwurf der Mindestanforderungen an das Risikomanagement« (MaRisk), den die BaFin am 2. Februar 2005 vorgelegt hat, zurückgegriffen werden. Dieses Rundschreiben stellt Mindestanforderungen auf, die von allen Kreditinstituten bei der Ausgestaltung des Risikomanagements zu beachten sind. Zwar bezieht es sich laut seiner Vorbemerkung direkt nur auf die Pflichten aus § 25a Abs. 1 S. 3 Nr. 1 und 2 KWG. Dieses Risikomanagement ist jedoch nur ein beispielhaft aufgezählter Bestandteil einer »ordnungsgemäßen Geschäftsorganisation« im Sinne des § 25a Abs. 1 S. 1 KWG. Insofern wird man den in MaRisk enthaltenen Ausführungen zur ordnungsgemäßen Geschäftsführung hinsichtlich angemessener Sicherheitsvorkehrungen für den Einsatz elektronischer Datenverarbeitungssysteme auch eine Ausstrahlungswirkung auf die Pflicht nach § 25a Abs. 1 S. 3 Nr. 4 KWG, die ihrerseits exemplarisch aufgezählter Bestandteil der »ordnungsgemäßen Geschäftsorganisation« ist, zugestehen müssen. Nichts anderes gilt für die Vorgaben aus Basel II, da mit MaRisk »wesentliche qualitative Elemente der 2. Säule des Baseler Akkords (...) in deutsches Recht umgesetzt werden« sollen – so die BaFin in ihrem Anschreiben vom 02.02.2005 zum Entwurf über die »Mindestanforderungen an das Risikomanagement«.

Hinsichtlich der technisch-organisatorischen Ausstattung schreibt MaRisk vor, dass sich diese an betriebsinternen Erfordernissen, den Geschäftsaktivitäten, der Strategie sowie der Risikosituation zu orientieren habe. Das IT-System sei vor seinem erstmaligen Einsatz und nach wesentlichen Veränderungen zu testen und von den fachlich sowie grundsätzlich auch von den technisch zuständigen Mitarbeitern abzunehmen. Produktions- und Testumgebung seien hierbei grundsätzlich voneinander zu trennen (vgl. Konsultation 07/05, Zweiter Entwurf der Mindestanforderungen an das Risikomanagement vom 22.09.2005, AT 7.2 Rn. 3). Bei der Ausgestaltung des IT-Systems und der zugehörigen IT-Prozesse sei grundsätzlich auf gängige Standards abzustellen (vgl. Konsultation 07/05, Zweiter Entwurf der Mindestanforderungen an das Risikomanagement vom 22.09.2005, AT 7.2 Rn. 2 f.). Hiermit wird wiederum auf Standards wie BS 7799, ISO 17779 sowie den IT-Grundschutz des BSI verwiesen.

Diese Standards eignen sich gleichfalls als Anhaltspunkte zur Bestimmung der technisch-

organisatorischen Anforderungen der allgemeinen vertraglichen wie auch deliktischen Sicherungspflichten. Jedoch sind auch hier wiederum im Einzelfall der Verkehrskreis, die Sensibilität der Daten, der Grad der Gefährdung sowie der Stand der Technik maßgebend.

3 Anforderungen an den Nutzer

3.1 Spezialgesetzliche Sicherungspflichten

Die bislang genannten speziellen Vorschriften richten sich an die Anbieter von IT-Systemen. Im Hinblick auf Sicherungspflichten, die der Nutzer dieser Systeme zu erfüllen hat, sah der Gesetzgeber offensichtlich keinen Regelungsbedarf. Dies mag nicht zu verwundern: Hat doch in der Regel allein der Anbieter eines IT-Systems die Möglichkeit, durch technische Ausgestaltung des Systems Gefahren, sowohl interner als auch externer Natur, abzuwehren. Es handelt sich folglich nicht um eine planwidrige Regelungslücke des Gesetzgebers, sodass auch eine analoge Anwendung der spezialgesetzlichen Sicherungspflichten ausscheidet.

Dass Sicherungspflichten für Nutzer von IT-Systemen bislang nicht kodifiziert worden sind, mag zudem daran liegen, dass im Einzelfall die Feststellung, welche der Parteien Anbieter und welche Nutzer eines IT-Systems ist, Schwierigkeiten bereiten kann. Zu denken ist etwa an den Fall, dass ein Unternehmen, das in E-Mail-Kontakt mit einem anderen Unternehmen steht, aufgrund einer Sicherheitslücke im IT-System Schadprogramme an das andere Unternehmen überträgt. Ist hier auf das E-Mail-System abzustellen, sodass beide Unternehmen unter Umständen als Nutzer anzusehen sind? Oder ist vielmehr darauf abzustellen, dass letztlich die beiden IT-Systeme der Unternehmen miteinander kommunizieren, sodass beide Unternehmen als Anbieter einzustufen sind? Oder ist nur das die E-Mail versendende Unternehmen Anbieter?

Hier wird zu berücksichtigen sein, dass ein Computer oder Netzwerk, das von einem Virus befallen ist, eine Gefahrenquelle darstellt [Koch 2004, S. 803]. Somit trifft das die infizierte E-Mail versendende Unternehmen wiederum eine deliktische Verkehrssicherungspflicht. Hiermit sei aufgezeigt, dass die bereits geschilderten allgemeinen IT-Sicherungspflichten keineswegs allein für klassische Anbieter von IT-Systemen, wie etwa einen Zugangsprovider, gelten.

3.2 Allgemeine Sicherungspflichten

Gleichwohl bestehen bei den allgemeinen Sicherungspflichten für Nutzer von IT-Systemen Besonderheiten.

Vertragliche Sicherungspflichten

IT-Sicherungspflichten für Nutzer können Vertragsbestandteil sein – in der Praxis meist als allgemeine Geschäftsbedingungen (AGB) ausgestaltet. So werden beispielsweise im Bereich des Online-Bankverkehrs spezifizierte AGB verwendet, die entsprechende Pflichten konstituieren. Ein Muster für eine derartige Vertragsgestaltung findet sich in Wertpapier-Mitteilungen (WM) 2001, S. 650. Hiernach sollen PIN und TAN nicht elektronisch gespeichert werden; auch soll die TAN-Liste sicher verwahrt werden. Zudem wird meist eine Mitteilungspflicht des Kunden gegenüber der Bank normiert, sobald der Kunde Verdacht bezüglich eines Missbrauchs schöpft. Eine weitere Besonderheit besteht darin, dass im Onlinebanking-Verfahren – im Gegensatz zum EC-Karten-Verfahren [Borges 2005, S. 3314] – in der Regel einfache Fahrlässigkeit als Haftungsmaßstab vereinbart wird.

Fraglich ist, ob darüber hinaus für den Nutzer bestimmte Sicherungspflichten als ungeschriebene Nebenpflichten existieren. Hierbei sei auf ein Urteil des AG Gelnhausen vom 6.10.2005 hingewiesen (AG Gelnhausen, MMR 2006, S. 124 ff.). Im dortigen Fall verlangte ein Zugangsprovider, der dem beklagten Reseller Webserver vermietet hatte, neben dem Mietzins noch die Zahlung für zusätzlichen Da-

tenverkehr, der dadurch entstanden war, dass der Server des Beklagten von einer sogenannten Distributed-Denial-of-Service-(DDoS-)Attacke betroffen war. Das Gericht entschied, der Angriff falle grundsätzlich in den Risikobereich des beklagten Resellers. Für den erhöhten Datentransfer und die Leistungen zur Analyse und dem Stoppen der Attacken müsse daher nicht der Zugangsprovider aufkommen. Mit anderen Worten: Der Reseller hätte selbst bestimmte Sicherungsvorkehrungen zur Abwehr der DDoS-Attacken von Dritten treffen müssen.

Sicherungspflichten aus Gründen von Haftungsprävention

Zurückhaltung ist hingegen bei der Annahme von deliktischen Sicherungspflichten für den Nutzer eines IT-Systems geboten. Schließlich ist es nicht er, der durch das Bereitstellen des IT-Systems eine Gefahrenquelle eröffnet. Etwas anderes könnte allenfalls für den Fall gelten, dass der Nutzer Kenntnis davon erlangt hat, dass sich Schadprogramme auf seinem Computer befinden, und er nichts unternimmt, um diese Sicherheitslücken zu schließen. Die Feinheiten in diesem Bereich sind jedoch bislang nicht geklärt, sodass die weitere Rechtsprechung abzuwarten bleibt.

3.3 Inhalt der Sicherungspflichten

Sofern die IT-Sicherungspflicht nicht vertraglich ausgestaltet und hierbei detailliert beschrieben ist, bereitet die Frage der technisch-organisatorischen Ausgestaltung ähnliche Schwierigkeiten wie bei den Sicherungspflichten der Anbieter. Grundsätzlich können hierfür die gleichen Auslegungskriterien zur Konkretisierung verwendet werden, wobei jedoch dem Kriterium der wirtschaftlichen Zumutbarkeit für den Nutzer besondere Beachtung geschenkt werden sollte.

Auch ist entscheidend, ob der Nutzer ein Unternehmen oder ein privater Verbraucher ist. Von einem Unternehmer als Nutzer können in der Regel höhere Sicherheitsanstrengungen erwartet werden als von einem privaten Nutzer.

Es ist fraglich, inwiefern ein privater Nutzer, der keine konkreten Anhaltspunkte für einen Befall seines Computers hat, Sicherheitsmaßnahmen ergreifen muss. Für den Sachverhalt unbemerkt aktivierter Dialer im Internet hat beispielsweise der BGH im Jahre 2004 eine Pflicht zur Installation entsprechender Anti-Dialer-Software abgelehnt, da diese IT-Schutzmaßnahme vom durchschnittlichen Bürger nicht verlangt werden könne (BGH, MMR 2004, S. 311). Im Klartext: Den Nutzer treffe keine Pflicht, seinen Anschluss durch Einsatz von Sicherungsmechanismen so weit, wie nach dem Stand der Technik möglich, gegen das Unterschieben von Dialern zu schützen ([Mankowski 2004a, S. 312]; AG Freiburg, MMR 2002, S. 634 ff.; LG Kiel, MMR 2003, S. 422 ff.).

Diese grundlegende Entscheidung des BGH betrifft jedoch nur einen Teilaspekt. So ist etwa noch ungeklärt, ob beispielsweise ein privater Nutzer für sogenannte Trojaner haftet, die sich unbemerkt auf seinen Computer »eingenistet« haben, von dort aus andere Computer befallen und dort Schäden verursachen. Angesichts der Komplexität des Gefahrenpotenzials und der sich beständig ändernden Angriffsmodi, mit denen sich der private Anwender auseinanderzusetzen hat, wird man dies wohl verneinen müssen.

Auch erscheint es schon zweifelhaft, ob ein privater Anwender – ohne dass erschwerende Besonderheiten, wie etwa Kenntnis von einer konkreten Bedrohung, hinzukommen – verpflichtet ist, überhaupt nur irgendein Schutzprogramm auf seinem Computer zu installieren.

Das heißt jedoch keineswegs, dass sich diese nutzerfreundliche Beurteilung, wie sie aus BGH, MMR 2004, S. 308 ff. hervorgeht und mit der der BGH der anbieterfreundlichen Auslegung vieler Amtsgerichte (AG Trier, Urteil vom 14.12.2001 – 32 C 404/01; AG Bremen, Urteil vom 08.05.2002 – 2 C 0386/91; AG Torgau, MMR 2003, S. 760) entgegentrat, mit der Zeit nicht ändern könnte. Je tiefer das Internet in den All-

tag des Durchschnittsbürgers eindringt, desto mehr wird man mittelfristig auch vom durchschnittlichen Internetbenutzer eine Befassung mit IT-Sicherheitsrisiken und den technischen Maßnahmen zu deren Abwehr erwarten können. Mit diesem dynamischen Prozess werden sich daher auch die Gerichte in den kommenden Jahren auseinanderzusetzen haben.

3.4 Beweislastumkehr

Eng verbunden mit den gegenseitigen Pflichten auf Anbieter- und auf Nutzerseite ist die Frage, wer im Schadensfalle die Beweislast für unzureichende oder fehlende IT-Sicherheitsmaßnahmen zu tragen hat. Insbesondere Streitigkeiten im Zusammenhang mit Dialern wurden von der Rechtsprechung teilweise über eine sachgerechte Beweislastverteilung gelöst [Mankowski 2004b, S. 185 ff.].

Grundsätzlich unterliegen auch Ansprüche aus der Verletzung von IT-Sicherungspflichten den allgemeinen zivilprozessrechtlichen Regeln: Nach dem sogenannten Beibringungsgrundsatz hat der Anspruchssteller alle seinen Anspruch begründenden Tatsachen zu beweisen (vgl. einführend [Musielak 2005, Einleitung Rn. 37 ff.]).

Allerdings hat die Rechtsprechung das Rechtsinstitut des sogenannten Anscheinsbeweises entwickelt (auch als *Prima-facie-Beweis* bezeichnet; zur Herleitung dieses Grundsatzes vgl. BGH, NJW 1996, S. 1828; BGH, NJW-RR 1986, S. 384): Nach ihm kann in bestimmten Fallgruppen für den Ablauf eines typischen Geschehens auf die allgemeine Lebenserfahrung zurückgegriffen werden – was letztlich zu einer Beweislastumkehr führt. Derartige Fallgruppen werden auch im Bereich der IT-Sicherheit diskutiert.

Onlinebanking

Für das Onlinebanking wird erwogen, der erste Anschein spreche dafür, dass der Inhaber des Kontos bei der Eingabe der korrekten PIN und TAN die Überweisung entweder persönlich vorgenommen oder durch Verletzung seiner vertraglichen Sorgfaltspflichten verursacht oder zumindest zum Missbrauch beigetragen haben muss [Karper 2006, S. 218; Borges 2005, S. 3317]. Grundlage dieser Erwägung ist die Rechtsprechung des BGH zum EC-Kartenmissbrauch, nach der bei Verwendung von EC-Karte und richtiger PIN ein Anschein dahingehend bestehe, dass der Kontoinhaber die Transaktion selbst vorgenommen oder dem Täter die Kenntnis der PIN durch grobfahrlässige Verletzung der Geheimhaltungspflicht ermöglicht habe (BGH, MMR 2004, S. 3624). Zum Onlinebanking fehlen indes bislang gerichtliche Entscheidungen. Allerdings deutet das Urteil des LG Bonn (LG Bonn, MMR 2004, S. 181), in dem es gleichwohl um einen etwas anders gelagerten Sachverhalt ging, darauf hin, dass die Rechtsprechung den Anscheinsbeweis auch auf das Onlinebanking-Verfahren anwenden wird.

Fraglich ist zudem, ob dieser Anschein durch das vermehrte Auftreten von Phishing- und Pharming- oder Keylogging-Attacken erschüttert wird ([Borges 2005, S. 3317], ablehnend hingegen [Karper 2006, S. 218]). Jedenfalls hat der Nutzer die Möglichkeit nachzuweisen, dass er Sicherheitsprogramme sowie aktuelle Updates installiert hatte, und kann hierdurch den Beweis des ersten Anscheins zu Fall bringen.

Onlineauktionen

Bei Onlineauktionen hingegen verneint die bisherige Rechtsprechung die Anwendbarkeit des Anscheinsbeweises. Selbst bei der passwortgeschützten Teilnahme an einer Internetauktion besteht weder eine tatsächliche Vermutung für die Identität von Teilnehmer und Inhaber des Mitgliedsnamens noch eine Anscheinsvollmacht für ein Handeln unter fremdem Mitgliedsnamen (LG Bonn, MMR 2004, S. 180). Mit Blick auf den derzeitigen Sicherheitsstandard der im Internet verwendeten Passwörter und auf die Art ihrer Verwendung könne nicht der Schluss gezogen werden, dass der Verwender

eines Passworts nach der Lebenserfahrung auch derjenige sei, auf den dieses Passwort ursprünglich ausgestellt wurde.

Diese Beurteilung lässt sich über Auktionen hinaus auf jede Dienstleistungsplattform im Internet übertragen, auf der Willenserklärungen unter durch einfache Passwörter geschützte Benutzernamen abgegeben werden. Hierfür lässt sich anführen, dass das Ausspähen von Passwörtern, beispielsweise durch Trojaner, eine durchaus reale Gefahr darstellt. So bereits festgestellt im Urteil vom 19.04.2002 des LG Konstanz (2 O 141/01 A), wobei anzumerken ist, dass diese Gefahr seit dem Jahr 2002 noch gestiegen ist.

4 Fazit und Implikationen für die Systemgestaltung

Die Umsetzung rechtlicher Vorgaben im Rahmen der Neu- oder Umgestaltung von Informationssystemen impliziert die Bereitstellung von Methoden, die den Informationssystemgestalter explizit bei der Einbeziehung rechtlicher Aspekte in den Entwicklungsprozess unterstützen. Anbietern von Informationssystemen liegen rechtliche Vorschriften in Form von datenschutzrechtlichen, kreditwesenbezogenen und analog anwendbaren Vorschriften sowie allgemeinen Sicherungspflichten vor. Da diese Vorschriften rein inhaltlichen, jedoch nicht technischen Charakter haben, besteht für den Informationssystemgestalter bei der *technischen* Umsetzung eine gewisse Wahlfreiheit, nicht jedoch bei der *inhaltlichen* Ausgestaltung. Aus diesem Umstand folgt, dass eine unmittelbare Unterstützung des Informationssystemgestalters bei der Einbeziehung von rechtlichen Aspekten in Informationssysteme vornehmlich im Rahmen der konzeptionellen Spezifikation möglich ist. Existente konzeptionelle Methoden zur Informationssystemgestaltung bieten hierfür eine Grundlage. Im Rahmen der konkreten rechtsbezogenen Erweiterungen dieser Methoden besteht weiterhin Forschungsbedarf [Knackstedt et al. 2006].

Bezüglich der Wahlfreiheit des Einsatzes technischer Standards ist auf situative Aspekte (z.B. Sensibilität der Daten sowie Gefährdungsgrad) abzustellen, die determinieren, welchen Sicherheitsgrad die einzelnen Standards repräsentieren. Abhängig von diesen Aspekten ist es möglich, bereits in der konzeptionellen Phase der Informationssystemgestaltung Empfehlungen zum Einsatz eines entsprechend adäquaten Standards auszusprechen, der in einer späteren, technischeren Phase der Informationssystemgestaltung umgesetzt wird. Hierzu bieten sich beispielsweise Methoden der konfigurativen Referenzmodellierung an [Delfmann & Knackstedt 2007].

Firmennutzern wird ein analoges Vorgehen zu Anbietern vorgeschlagen. Speziell sind hier fachkonzeptionelle Methoden für die Konstruktion von Informationssystemen, die den Firmennutzer dazu befähigen, angebotene Informationssysteme zu nutzen, in Betracht zu ziehen.

5 Literatur

[Bamberger & Roth-Spindler 2006] *Bamberger, H. G.; Roth-Spindler, H.:* Beck'scher Onlinekommentar zum BGB. München, 31.03.2006.

[Barton 2000] *Barton, D.-M.:* K&R Kommentar. In: Kommunikation & Recht, 3. Jg., 2000, Heft 4, S. 195.

[Barton 2004] *Barton, D.-M.:* Risikomanagement und IT-Sicherheit. In: Kommunikation & Recht, 7. Jg., 2004, Heft 7, S. 305-312.

[Borges 2005] *Borges, G.:* Rechtsfragen des Phishing – Ein Überblick. In: Neue Juristische Wochenschrift, 58. Jg., 2005, Heft 46, S. 3313-3317.

[Delfmann & Knackstedt 2007] *Delfmann, P.; Knackstedt, R.:* Konfiguration von Informationsmodellen. Untersuchungen zu Bedarf und Werkzeugunterstützung. In: Oberweis, A.; Weinhardt, C.; Gimpel, H.; Koschmider, A.; Pankratius, V.; Schnizler, B. (Hrsg.): eOrganisation: Service-, Prozess-, Market-Engineering. Proceedings der 8. Internationalen Tagung Wirtschaftsinformatik. Band 2. Karlsruhe 2007, S. 127-144.

[Karper 2006] *Karper, I.:* Sorgfaltspflichten beim Online-Banking – Der Bankkunde als Netzwerkprofi? In: Datenschutz und Datensicherheit, 30. Jg., 2006, Heft 4, S. 215-219.

[Kaufmann 1998] *Kaufmann, N. C.:* Fehlerhafte Rechtsanwendung – Mangelndes Verständnis für Online-Medien führt zu unhaltbaren Rechtssprüchen. In: c't, 1998, Heft 18, S. 166.

[Kaufmann 2006] *Kaufmann, N. C.:* Generelle Vorabprüfung von Online-Foren abgelehnt – Heise-Urteil zur Haftung für fremde Beiträge bringt mehr Klarheit. DFN-Infobrief Recht, September 2006, *www.dfn.de/content/fileadmin/3Beratung/Recht/1infobriefearchiv/Infobrief-sept06.pdf*.

[Knackstedt et al. 2006] *Knackstedt, R.; Brelage, C.; Kaufmann, N. C.:* Entwicklung rechtssicherer Web-Anwendungen – Strukturierungsansatz, State-of-the-Art und ausgewählte Aspekte der fachkonzeptionellen Modellierung. In: Wirtschaftsinformatik, 48. Jg., 2006, Heft 1, S. 27-35.

[Koch 2004] *Koch, R.:* Haftung für die Weiterverbreitung von Viren durch E-Mails. In: Neue Juristische Wochenschrift, 57. Jg., 2004, Heft 12, S. 801-807.

[Mankowski 2004a] *Mankowski, P.:* Die Beweislastverteilung in »0190er-Prozessen«. In: Computer und Recht, 20. Jg., 2004, Heft 3, S. 185-189.

[Mankowski 2004b] *Mankowski, P.:* BGH: Kein Telefonentgeltanspruch für Verbindungen durch ein heimlich installiertes Anwahlprogramm – Dialer. In: Multimedia und Recht, 7. Jg., 2004, Heft 5, S. 308-315.

[Musielak 2005] *Musielak, H.-J.:* Kommentar zur Zivilprozessordnung. 4. Auflage. Vahlen, München, 2005.

[Schultze-Melling 2005] *Schultze-Melling, J.:* IT-Sicherheit in der anwaltlichen Beratung. In: Computer und Recht, 21. Jg., 2005, Heft 1, S. 73-80.

[Spindler 2004] *Spindler, G.:* IT-Sicherheit und Produkthaftung – Sicherheitslücken, Pflichten der Hersteller und der Softwarenutzer. In: Neue Juristische Wochenschrift, 57. Jg., 2004, Heft 44, S. 3145-3150.

Prof. Dr. Jörg Becker
Prof. Dr. Thomas Hoeren
Universität Münster
European Research Center for Information Systems
Leonardo-Campus 3
48149 Münster
{becker, hoeren}@ercis.uni-muenster.de
www.ercis.uni-muenster.de