Ausgabe
Nr. 3

Schriftenreihe
zu aktuellen Themen
der Schadenversicherung

I. Geis · Th. Hoeren · Chr. Nießen · J. Roth

Neue Medien – Neue Risiken:

Haftpflichtfragen rund um das Internet

e+s rück

Schriftenreihe
zu aktuellen Themen
der Schadenversicherung

Ausgabe Nr. 3

I. Geis · Th. Hoeren · Chr. Nießen · J. Roth

Neue Medien – Neue Risiken:

Haftpflichtfragen rund um das Internet

e+s rück

Inhalt

Kapitel Seite

1. Einführung in das Thema

von Jörg-Christian Deister

Neue Medien dringen täglich in immer neue Bereiche des Wirtschaftslebens ein. Allen voran ist hier das Internet zu nennen. Technik und Schnelligkeit dieses weltweiten Kommunikationsmittels werden ständig optimiert und bieten Anwendern und Verbrauchern vielerlei Verwendungsmöglichkeiten.

Die Versicherungswirtschaft hat sich des Mediums bemächtigt und befasst sich seit geraumer Zeit mit den Möglichkeiten des so genannten elektronischen Vertriebes von Versicherungsprodukten. Das Spektrum reicht dabei von der Schaffung von B2B-Plattformen, über die Präsentation auch beratungsintensiver Produkte im Netz bis hin zur Schadenmeldung via E-Mail. Schnelligkeit beim Abschluss von Verträgen, Genauigkeit bei der Produktinformation und damit einhergehend die Zuverlässigkeit bei der Beschreibung von Finanzdienstleistungen wird immer mehr zum Wettbewerbsfaktor.

Die gleichzeitige verstärkte Ausrüstung privater Haushalte mit immer leistungsfähigeren PCs scheint unaufhaltbar zu sein und gibt dem Konsumenten zumindest die Möglichkeit eines jederzeitigen Zugriffes auf sein persönliches Konto bzw. seine individuellen Verträge. Gleichwohl ist eine spürbare Zurückhaltung beim Vertragsabschluss online zu verzeichnen. Je größer die Unsicherheit über Authentizität und Zuverlässigkeit von Datenquellen ist, desto höher wird die Hürde für die Akzeptanz des Internets und seiner Vertriebsmöglichkeiten angesetzt werden müssen.

Und dies nicht ohne Grund, birgt doch die globale Vernetzung die Möglichkeit der Ausspähung, Veränderung und des Missbrauches von Daten. Darüber hinaus werden vorsätzlich Viren in das Netz eingespeist, die zu echten Schäden in Form von Datenverlusten oder Datenveränderungen führen. Die Wiederherstellung einer gelöschten Festplatte ist oft nur mit hohem Zeit- und finanziellen Aufwand zu leisten. Die Verursacher sind nicht bekannt. Für die Verursachung fahrlässiger Schäden im Internet benötigt der Verursacher hingegen Deckungsschutz.

Dabei findet der Umgang mit dem Internet nicht im rechtsfreien Raum statt. Das Recht des Internets entwickelt sich vielmehr zu einer eigenen Sparte und viele Fachzeitschriften widmen diesem Rechtsgebiet eigene Rubriken, darunter auch die NJW, die mit ihrer Beilage zu Heft 14 im Jahr 2001 die regelmäßige Berichterstattung zu Entwicklungen in diesem Bereich aufgenommen hat.

Der Umgang mit dem Netz erfordert vom Verbraucher immer wieder eine Risikoabwägung zwischen den vielen Vorteilen und den Unwägbarkeiten, die dieses neue Medium mit sich bringt. Die Versicherungswirtschaft ist insgesamt aufgefordert, diesen voranschreitenden Prozess zu begleiten und sich mit innovativen Produkten und neuen Ideen einzubringen. Im Schadenfall ist eine hohe Expertise gefordert, um einerseits dem Anspruchsteller eine adäquate Ersatzleistung zu erbringen, andererseits auch internationale Haftungsaspekte zu berücksichtigen.

E+S Rück möchte mit seiner Fachtagung 2001 an dieser breit geführten Diskussion teilnehmen und hat mit Erlaubnis der Autoren die einzelnen Beiträge in diesem Tagungsband zusammengefasst, um sie der interessierten Fachöffentlichkeit zur Verfügung zu stellen. Sollten Sie Bedarf an weiteren Exemplaren haben, wenden Sie sich bitte an die im Einband genannten Ansprechpartner oder an Ihre bekannten Gesprächspartner in unserem Haus.

2. Informationsbeschaffung durch das Internet: Gefahrenpotenziale und Sicherheitsaspekte

von Jörg Roth

Das Internet hat sich zum weltgrößten und mächtigsten globalen Informations- und Kommunikationsmedium entwickelt. Die Thematik „Sicherheit im Internet" zeigt gerade in letzter Zeit eine bemerkenswerte Entwicklung. Während sich noch vor kurzem nur wenige Spezialisten mit diesem Gebiet befassten, muss die Kenntnis und Umsetzung von Sicherheitsmaßnahmen bei Unternehmen heute zum Kerngeschäft gezählt werden. Neben den in der Presse häufig genannten Gefahren, die bei der Nutzung des Internet auftreten können (offene Übertragung der Daten, Angriffe durch Hacker), sind neue Risiken und Gefahren entstanden, die auch für jeden Internet-Nutzer, ob privat oder am Arbeitsplatz eine Beschäftigung mit dem Thema Sicherheit, hier Datensicherheit, unerlässlich machen.

2.1 Was ist überhaupt das World Wide Web? – Wem „gehört" es?

Ein Blick zurück auf die Ursachen dieser Entwicklung: Anfang der 90er-Jahre bestand bereits eine globale Vernetzung, – das Internet – doch war sie nicht so einfach benutzbar, wie wir das heute gewohnt sind. Der Gebrauch war viel umständlicher, es gab zwar Dienste auf dem Internet wie Telnet, FTP oder E-MAIL, jedoch keine einfachen, benutzerfreundlichen Oberflächen. Der breiten Masse war das Internet somit verschlossen.

Zu den Begriffen: Häufig werden Internet und das World Wide Web – WWW – in ein und denselben Topf geworfen, es bestehen aber gravierende Unterschiede:

Das Internet stellt ein physisches Netzwerk dar, es ist der greifbare Teil der globalen Vernetzung, bestehend aus Verbindungen zwischen einzelnen Maschinen, seien es Kabel oder Satelliten-Funkverbindungen.

Das WWW hingegen ist kein Netzwerk in diesem Sinne, es ist lediglich ein virtuelles Netzwerk, ein Dienst, der das Internet benutzt. Weitere Dienste sind etwa NEWSGROUPS oder E-MAIL.

Das WWW bietet die Möglichkeit der Verbreitung von in der Sprache HTML geschriebenen Dokumenten, die weit über die Anzeige bloßen Textes hinausgehen: Enthalten sind auch Bilder, Videos oder Musik. Um diese Seiten betrachten zu können, müssen sie nicht erst auf den eigenen Rechner geladen und dazu explizit abgespeichert werden, um erst dann die Dateien in einem entsprechenden Programm betrachten zu können: Das WWW bietet die Möglichkeit der Online-Betrachtung, diese ist auch die Voraussetzung für das Surfen, das fortlaufende Verfolgen von Links, die auf Dokumente, welche sich auf einem WWW-Server irgendwo auf dem Internet befinden verweisen. Vielleicht die wichtigste Voraussetzung für die ab etwa 1993 einsetzende explosionsartige Ausweitung des WWW war die Freigabe der HTML-Technologie durch das europäische Kernforschungszentrum CERN im April 1993: Jedermann konnte die Technologie benutzen, ohne irgendwelche Patentrechte erwerben oder Copyrightgebühren entrichten zu müssen.

Das WWW war so vollständig der Öffentlichkeit zugänglich gemacht worden, der Boom des Web war nicht mehr zu bremsen: Während 1993 weltweit 50 HTTP-Server existierten, waren es Ende 1994 schon 100.000. Und 1995 war WWW der führende Dienst innerhalb des Internets.

Das Internet gehört also niemanden, oder allen, wie auch immer man das sehen mag: Das „Internet" an sich gibt es nicht: Es ist ein Zusammenschluss aus vielen einzelnen Netzwerken zu einem Großen. Deswegen kann man auch nie genau sagen, ab wann ein Rechner im Internet steht: So gesehen gehören also Stücke des Internets zu verschiedenen Personen.

2.2 Gefahren bei der Nutzung der so genannten virtuellen Welt

Die alltägliche Nutzung dieses Mediums zeigt neben offenen Angriffen durch Viren auch versteckte Risiken, der PC eines Benutzers scheint über den Zugang in die Welt des Internets zur unerlaubten Nutzung der Informationen durch andere offen wie ein Scheunentor zu stehen:

Jede Bewegung in den Netzen hinterlässt für den Benutzer oft nicht wahrnehmbare Informationsreste, eine Art „Datenspur". Mit Hilfe automatisierter Erhebungsverfahren, die unbemerkt im Hintergrund einer Anwendung laufen, können mittlerweile exakte Protokollierungen der jeweiligen Aktivitäten des Nutzers erstellt werden.

Grund dafür ist, dass das Internet ursprünglich nur unter Verfügbarkeitsaspekten (wie bereits ausgeführt) entwickelt wurde und Sicherheitsaspekten somit keine Rechnung trägt.

2.3 Kritische aktuelle Erscheinungen

Welche Einstellungen erlauben Datenspionage bzw. unbemerkte Manipulationen?

2.3.1 Aktive Diebe: Active Contents

Zunächst sei die Hauptmöglichkeit angesprochen, beim Empfänger aktiv Veränderungen am Zustand seines Systems vornehmen zu können: Der Browser oder weitere, nachträglich installierte Zusatzprogramme, so genannte Plug-ins, ermöglichen das Ausführen so genannter aktiver Inhalte (Active Contents): Das sind Programme, die in die Informationsangebote der Server-Betreiber, der Web-Seite oder auch in E-Mails eingebunden sind und das System des Nutzers um multimediale Elemente ergänzen. Derartige Programme sind meist in den Programmiersprachen Java, JavaScript oder ActiveX erstellt. Der Benutzer hat dabei keinerlei Kontrolle darüber, was diese Programme auf seinem PC ausführen, sobald sie zugelassen wurden.

Aktive Komponenten können vollen Zugriff auf alle Ressourcen des Benutzerrechners haben und bei ihrer Ausführung genau die Rechte des gerade angemeldeten Benutzers besitzen, wie z. B. die Rechte von Netzwerkfreigaben. Sie erlauben die Fernsteuerung des Rechners oder auch die (unbemerkte) Installation von Systemprogrammen im Hintergrund, die in der Folgezeit automatisch beim Systemstart mit geladen werden: Diese analysieren in aller Ruhe unbemerkt den Rechner und sein Umfeld.

Immer wenn der Anwender „Online" ist, liefern sie die am interessantesten erscheinenden Daten an den Server des Systemprogramm-Besitzers.

Ein Beispiel ist das Programm Webhancer, das beim Einrichten eines neuen Benutzers beim mp3-Anbieter audiogalaxy installiert wird: Es forscht den PC nach „unerlaubten" Musiktiteln aus. Ebenso kann ein so genanntes trojanisches Pferd installiert werden, welches einen Schädling ins System trägt, auch wenn es keine Online-Funktion zu besitzen vorgibt.

Da aktive Komponenten sämtliche Verteidigungsstrategien unterlaufen können, müssen in diesem Zusammenhang die Browser, hier wegen ihrer Verbreitung insbesondere die Surf-Bretter von Netscape und Microsoft, in der Praxis einer besonderen Betrachtung unterzogen werden: sie verfügen über die verschiedensten Möglichkeiten, aktive Inhalte aus dem Web herunterzuladen und auszuführen. Die wesentlichen Systeme aktiver Inhalte seien im Folgenden kurz angeführt:

2.3.2 ActiveX

ActiveX ist eine Entwicklung der Firma Microsoft. Es sorgt dafür, dass Windows-Anwendungen mit dem Internet bzw. Intranet zusammenarbeiten. Internetseiten können mit dieser Technologie um eine Vielzahl von multimedialen Effekten und ausführbaren Applikationen erweitert werden.

Die Komponenten der ActiveX-Technologie (das sind etwa Controls: Programme, die auf einer Internetseite dargestellt oder als eigene Programme aufgerufen werden und Scriptings zum Verwalten und zur Kommunikation mit ActiveX-Controls) übernehmen die Rechte des angemeldeten Benutzers und unterliegen keinerlei Einschränkungen der Windows- und System-Funktionalität: Es existieren mithin keine Sicherheitsarchitekturen, sie stellen ein immenses Sicherheitsrisiko dar.

Microsoft setzt zum Schutz die (selbst entwickelte) Authenticode-Technologie ein; sie sieht im Wesentlichen vor, dass Programmierer bzw. Softwarefirmen ihre Identität offen legen, diese für den Anwender vertrauenswürdig sind und das ActiveX-Control nach seiner Veröffentlichung, der so genannten Zertifizierung nicht mehr verändert wird.

Grundlage für diese Zertifizierung ist, dass ein Unternehmen zunächst für sein ActiveX-Control einen so genannten „öffentlichen Schlüssel" (= „Zertifikat") bei einer Zertifizierungsstelle (einem privatem Unternehmen) beantragt.

Hat es diesen erhalten, wird das ActiveX-Control mit einer „digitalen Signatur" (= „privater Schlüssel") versehen und auf einem Webserver innerhalb der dort angebotenen Seiten bereitgestellt. Zugleich wird dieser Schlüssel auf einem oder mehreren Sicherheitsservern abgelegt, der kontrolliert, ob der Schlüssel manipuliert wurde.

Ruft der Anwender dieses ActiveX-Control beim Seitenanbieter auf, prüft sein Browser beim Sicherheitsserver, ob die mitgelieferte Signatur (noch) stimmt.

Die Zertifizierung schützt allerdings nicht „von Haus aus" vor Beschädigungen oder Manipulationen eines Systems:

Die Zertifizierung macht weder eine Aussage über die Funktionsweise des ActiveX-Controls, noch ist es dem Anwender möglich, darüber zu entscheiden, wann und warum er einer bestimmten Zertifizierung vertrauen soll. Bei entsprechender Aktivierung von Warnfunktionen erscheint lediglich eine Aufforderung, dem entsprechenden Unternehmen pauschal zu vertrauen oder das Ausführen der Funktion zu unterlassen, ohne zuvor überhaupt Informationen über deren Funktionsweise zu erhalten.

2.3.3 Javascript

JavaScript ist eine von der Firma Netscape entwickelte Scriptsprache, die innerhalb einer HTML-Seite direkt an den Browser übertragen wird: Es besteht so die Möglichkeit, Browser-Fenster zu öffnen oder zu schließen, Einstellungen anzupassen und Formularelemente zu manipulieren. Obwohl der Name eine enge Verwandtschaft zu Java andeuten könnte, haben die beiden Sprachen nur wenig Gemeinsamkeiten. Um die Gefährdungen, die bei der Ausführung von JavaScript-Programmen entstehen, beherrschen zu können, wurden von Netscape verschiedene Sicherheitsmodelle wie etwa die „Same Origin Policy" oder die „Signed Script Policy" entwickelt: JavaScript-Programme dürfen dann z.B. bestimmte Objekte innerhalb des Browsers nicht ausführen oder sie werden digital signiert, um so die Authentizität zu gewährleisten. Ein signiertes JavaScript-Programm kann erweiterte Zugriffsrechte auf Ressourcen des lokalen Rechners bekommen.

Doch auch hier sind verschiedene Probleme bekannt, durch die ein JavaScript-Programm Schäden verursachen kann, wie etwa ein „Denial-of-Service-Angriff": Die Möglichkeit, beliebig viele Fenster mit Meldungen zu öffnen oder die „History"-Liste der besuchten Seiten abzufragen und dadurch Benutzernamen, Passworteingaben oder andere Informationen abzufangen. Durch ein entsprechendes JavaScript-Programm kann die Statuszeile eines Browsers so verändert werden, dass nicht mehr die richtige URL eines Links angezeigt wird, sondern eine beliebige andere.

Zuletzt als System aktiver Inhalte sei der Windows Scripting Host erwähnt: Windows Scripting Host (WSH) ist eine Zusatzanwendung, die es dem Programmierer erlauben sollte, per Fernzugriff einen Rechner steuern und Anwendungen installieren und entfernen zu können. Das Programm wird automatisch mitinstalliert und kann – zusammen mit dem Internet Explorer – ungeahnte Risiken entwickeln: Es ermöglicht den Aufruf sämtlicher im System enthaltenen Befehle wie Löschen, Formatieren, Durchsuchen von Ordnern und Kopieren von Daten. Besonders bedenklich ist WSH in Zusammenhang mit Online-Registrierung, denn die Versprechung, dass keine Systemdateien übermittelt werden, sind nicht nachprüfbar und werden auch nicht von den großen Softwareherstellern beachtet, wie die Praxis zeigt. Windows XP etwa versucht, über Signaturen die einwandfreie Herkunft von Scripten zu kennzeichnen. Allerdings ist der Schutz standardmäßig auf „Kein Schutz" gestellt: Alle Scripte etwa vom Typ .vbs und .js werden ohne Nachfrage ausgeführt.

2.3.4 Cookies: Bittere Kekse oder die heimlichen Läuse im Pelz

Eine versteckte Möglichkeit der Datenerhebung bieten Cookies: Dies sind kleine Datenmengen, die vom Betreiber einer Internet-Präsentation auf dem Anwender-Rechner gespeichert werden. Dadurch wird im einfachsten Fall ein wiederholter Zugriff eines bestimmten Benutzers (genauer: des Browsers auf dem PC, den er verwendet) auf das Internet-Angebot erkennbar, doch die Anwendungsmöglichkeiten gehen weit über diese Feststellung hinaus: Mit Hilfe von Cookies kann der Nutzer beim Betreten einer Seite eindeutig markiert und seine Zugriffe auf Folgeseiten ihm zugeordnet werden: So ist es möglich, aus den eingerichteten Cookies ein Nutzungsprofil zu erstellen, das vielfältige Auskunft über den Benutzer gibt und ihn so als Zielperson, z. B. für Werbebotschaften, identifiziert. Die Bedeutung von Cookies wird regelmäßig verharmlost: So wird etwa argumentiert, dass eine Manipulation des Computers über die Speicherung und Abfrage der Cookies hinaus nicht möglich ist, da Cookies reine Textdateien sind und somit nicht selbst aktiv werden können wie etwa Scripte. Da Cookies aber auch benutzerbezogene Passwörter enthalten können, steht einer Nutzung dieser Informationen durch Unberechtigte beispielsweise durch Zugriff mit Hilfe von ActiveX-Controls nichts im Wege.

Ursprünglich sollten Cookies das elektronische Einkaufen erleichtern: Ein Benutzer wählt in einem Angebot Waren aus, die er kaufen möchte. Der Server speichert die Kennungen dieser Produkte auf dem Nutzer-PC und kann auf der Bestellseite diese Informationen wieder abrufen, um die Bestellung automatisch auszufüllen. Cookies sollten auch dazu eingesetzt werden, das Angebot des gewählten Web-Servers auf die persönlichen Belange und (vermuteten) Bedürfnisse des Benutzers einzustellen.

Cookies sind wegen des vergleichsweise geringen Gefährdungspotenzials weniger ein Problem der Computersicherheit als vielmehr aufgrund ihrer geringen Transparenz für den Benutzer ein Problem der Datensicherheit: Der Datenaustausch mittels Cookies erfolgt vollkommen im Hintergrund zwischen den beteiligten Computern, ohne dass der Benutzer über Inhalte, Zweck, Umfang, Speicherdauer oder Zugriffsmöglichkeiten auf die Cookie-Datei informiert wird. Diese Parameter sind innerhalb des Cookies selbst festgelegt und werden somit vom Betreiber des WWW-Servers bestimmt.

Online-Agenturen wie DoubleClick haben unlängst eine „Informationsallianz" bekannt gegeben, um die Informationen über Benutzer auszutauschen. Damit wird es möglich, dass Werbeagenturen die Benutzer, von denen sie persönliche Informationen besitzen, mit Cookies von den anderen Agenturen verbinden können, so dass sich ein umfassenderes Bild der Wege von Surfern im Web ergibt.

Problematisch ist das Setzen von Cookies, wenn sie zur späteren Identifizierung des Benutzers dienen sollen. Die deutschen gesetzlichen Multimediaregelungen verlangen, dass der Dienstanbieter den Benutzer unterrichtet, wenn ein solcher Cookie gesetzt werden soll. Dies wird bisher allerdings kaum beachtet. Dabei können sich die Dienstanbieter nicht darauf berufen, dass die Browser eine Warnung anzeigen; diese Warnhinweis-Funktion entbindet den Anbieter nicht von seinen gesetzlichen Pflichten.

2.3.5 Web-Bugs: Fleißige Bilder

Obgleich schon bald fast jede Website und natürlich jede Internet-Werbeagentur Cookies verwendet, um die Surfer und potenziellen Kunden zu identifizieren, haben diese die – für die Anbieter – „schlechte" Eigenschaft, dass ihr Setzen über die Browser-Einstellung verhindert werden oder man zumindest sehen kann, ob ein Cookie gesetzt werden soll. Mit einem bislang noch wenig bekannten Verfahren lässt sich aber auch diese Abwehr der Benutzer, die nicht so gern ihre Daten bereitwillig abliefern wollen, möglicherweise umgehen:

Web-Bugs oder auch „clear GIFs" sind winzige Bilder im GIF-Format mit einer Größe von normalerweise 1x1 Pixel, die auch in anderen Grafiken versteckt werden können. Nur wer sich den Quellcode einer Website ansieht, kann die Web Bugs als so genannte IMG-Tags erkennen.

Die Auswirkungen dieser praktisch unsichtbaren Cookie-Nachfolger auf den Datenschutz werden erstmals durch die Federal Trade Commission (kurz FTC) untersucht. Beauftragt wurde Richard Smith, der durch die Aufdeckung der heimlich von Microsoft gesetzten GUID's (einen Browser-Client für einen Webserver eindeutig identifizieren) bekannt wurde. Bedenken bestehen vor allem darin, dass die Besucher einer Website meist gar nicht erfahren, dass ihr Surfverhalten registriert wird: Ein Web Bug sendet neben der IP-Adresse des Nutzers, die Internetadresse der besuchten Webseite, den Zeitpunkt, an dem der Web Bug angeschaut wurde, den Browsertyp sowie die Informationen eines zuvor gesetzten Cookies an einen Server.

2.3.6 Würmer, Viren und Trojaner: Versteckte Angriffe aus Ihrem PC

Am Rande seien der Vollständigkeit halber die Funktionen erwähnt, deren Ziel vorrangig die Beschädigung oder Manipulation eines Systems beinhalten:

Dies sind zunächst Viren: Programmroutinen, die sich selbst reproduzieren und für den Benutzer nicht kontrollierbare Manipulationen bzw. Schäden am Betriebssystem oder anderen Programmen verursachen.

Ferner treten zur Zeit vermehrt Trojaner oder trojanische Pferde auf: Programme ohne Selbstreproduktion, die versteckte Schadensfunktion enthalten. Im Gegensatz zu den Viren verbergen sie sich nicht und offenbaren sich dem Benutzer als angeblich nützliche Helfer (z. B. Bildschirmschoner oder „gekrackte" (= entschlüsselte) Software). Da Trojaner direkt Manipulationen am System vornehmen, sind sie eher dem Bereich der Computersicherheit und weniger dem Bereich der Datensicherheit zuzuordnen.

Schließlich finden sich häufig Würmer, selbst reproduzierende Programme ähnlich Trojanern, die sich vor allem in Rechnernetzen ausbreiten, indem sie sich selbst an neue Empfänger verschicken. Die aus den Medien bekannten Infektionsbeispiele (z. B. „I love you", „NIMDA") sind durch E-Mail übertragen worden. Neu ist, dass auch schon in der eigentlichen E-Mail-Nachricht und nicht nur wie bisher im Attachment (angehängte Datei) der Mail ein solches Schaden stiftendes Element enthalten sein kann, z.B. wenn zusätzlich zum E-Mail-Empfang Multimedia-Elemente wie bunte E-Mail Hintergründe, etc. angezeigt werden. Möglich ist dies durch Scripte und deren automatisches Ausführen durch Funktionen wie das „Vorschaufenster" von Microsoft Outlook. Hier empfiehlt sich bereits das Deaktivieren dieser Funktionen.

2.3.7 Dialer

Eine weitere Gefahr unkontrollierbarer Aktivierungen sind Dialer: Viele Webseiten bieten zur Abrechnung Ihrer Leistungen nicht mehr nur die herkömmliche Art und Weise an (per Kreditkarte, Überweisung oder Abbuchung) sondern auch die Abrechnung per Telefonrechnung, indem eine Verbindung über eine 0190-Servicenummer aufgebaut wird. Zu diesem Zweck werden so genannte Dialer oder auch Highspeedzugänge zum Download angeboten. Der Kunde installiert dieses Programm und wählt sich ein. Der Preis für eine Minute kann von Anbieter zu Anbieter schwanken, (z.Zt. 1,86 EUR/Min).

In der Regel wird eine neuer DFÜ-Zugang über die Telefonverbindung erstellt oder die Einstellungen der Zugangssoftware verändert; in allen Fällen muss der Anwender sich das Programm selber herunterladen und installieren.

Häufig kommt es vor, dass sich Dialer als zusätzliches Chat- oder Movie-Programm ausgeben und die teuren Einwahlkosten verschwiegen werden. Auch sind Webseiten bekannt, wo sofort bei Eintritt auf das Angebot eine EXE-Datei (die Dialer-Software) als Downloadlink startet. Der Anwender braucht „nur" noch den Button „Speichern [unter]" zu betätigen. Zumindest befindet sich die Software so schon einmal auf dem System des Besuchers. Ferner sind die Beschreibungen der Funktionsweise in englisch und eine „Abbrechen"-Schaltfläche ist meist nicht vorhanden. Programme dieser Art werden in die Registrierungsdatenbank eines Rechners eingetragen und sind nur mit großem Aufwand deinstallierbar.

2.4 Fazit: Ob ein PC ausgeforscht werden kann, bestimmt seine Umgebung

Die sichere Kommunikation zwischen außen und innen ist meist durch eine Firewall bereits hinreichend gewährleistet: Diese Systeme schützen vor Angriffen von außen. Durch die aktiven Inhalte können jedoch Angriffe quasi von innen gestartet werden, so dass hier eine besondere Sensibilisierung der Administratoren und Anwender notwendig erscheint: Wer aus Angst vor Ausforschung oder Schäden aus dem Internet gleich zur Sperrung des Zugangs greift, tut den zweiten Schritt vor dem ersten: Denn absolute Sicherheit im Internet gibt es nicht, wie bereits zuletzt der NIMDA-Virus eindrucksvoll bewiesen hat.

Zunächst gilt es, Betriebssystem und Anwendungen im Rahmen ihrer Möglichkeiten sicher zu konfigurieren: Welche Einstellungen sind notwendig, welche Rechte hat ein Programm auf einem Arbeitsplatz-PC?

Zudem gilt es, selbstständig abzuwägen zwischen Bedienungskomfort und Risikobereitschaft; informierte Anwender sind kritische Anwender: Wer etwa in einem Internet-Seminar nicht nur vermittelt bekommt, wie bequem Informationen erreichbar sind, sondern auch erfährt, welche Funktionen Gefahren beinhalten und wie diese von ihm selbst eingeschränkt werden können, hält die Augen offen und agiert verantwortungsbewusst.

Internationale Kontrollierbarkeit

Zum Schluss noch kurz ein Wort zur nationalen bzw. internationalen Kontrollierbarkeit der veröffentlichten Inhalte im Internet:

Durch die Internationalität des Netzes sind kaum einheitliche Werte zu finden. Ein Angebot kann beliebig auf einen Server in einem anderen Land – mit anderen Grundwerten – verlagert werden. Zudem hat die Vergangenheit gezeigt, dass Regulierungsversuche – getreu dem bekannten Internet-Motto der absoluten Freiheit – als technische Störung interpretiert und umgangen werden.

Trotzdem ist das Web kein rechtsfreier Raum und bietet durchaus, wenn auch nur im begrenzten Rahmen, Sanktionsmöglichkeiten mit Spielraum für staatliche Eingriffe. Weder der Versuch, sich nationalem Recht durch multinationale Unternehmensbildung zu entziehen noch die Tatsache, dass Sperren leicht umgangen werden können – etwa Nachbars Gartenzaun – sind der Rechtsordnung fremde Probleme. Es ist aber immer zu bedenken, dass jede staatliche Steuerung ultima ratio sein muss.

Besonders das häufig beschworene Problem der Anonymität unseriöser Anbieter existiert nicht in dem Ausmaß: Wer etwa strafbare Inhalte vertreibt oder Informationen mit Hilfe von Cookies oder Web-Bugs ausspäht, wird damit auch Geld verdienen wollen und ist dementsprechend auf offene und nachvollziehbare Wege angewiesen. Schon heute bestehen internationale Abkommen, auf die zurückgegriffen werden könnte.

3. Das Recht der Informationstechnologie

von Prof. Dr. Thomas Hoeren

Literatur: Karsten Altenhain, Die strafrechtliche Verantwortlichkeit für die Verbreitung missbilligter Inhalte in Computernetzen, in: CR 1997, 485; Kirsten Beckmann/Ulf Müller, Online übermittelte Informationen: Produkte i. S. d. Produkthaftungsgesetzes, in: MMR 1999, 14; Torsten Bettinger/Stefan Freytag, Privatrechtliche Verantwortlichkeit für Links, in: CR 1998, 545; Nils Bortloff, Neue Urteile in Europa betreffend die Frage der Verantwortlichkeit von Online-Diensten, in: ZUM 1997, 167; ders., Die Verantwortlichkeit von Online-Diensten, in: GRUR Int. 1997,

387; Emanuel Burkhardt, Medienfreiheit quo vadis – Das Somm-Urteil aus presserechtlicher Sicht, in: CR 1999, 38; Ute Decker, Haftung für Urheberrechtsverletzungen im Internet (Anforderungen an die Kenntnis des Host Providers), in: MMR 1999, 7; Engels, Zivilrechtliche Haftung für Inhalte im Word Wide Web, in: AfP 2000, 524; Stefan Engels/Oliver Köster, Haftung für „werbende Links" in Online-Angeboten, in: MMR 1999, 522; Gunter Ertl, Zivilrechtliche Haftung im Internet, in: CR 1998, 179; Norbert Flechsig/Detlef Gabel, Strafrechtliche Verantwortlichkeit im Netz durch Einrichten und Vorhalten von Hyperlinks, in: CR 1998, 351; Stefan Freytag, Providerhaftung im Binnenmarkt, in: CR 2000, 600; Gercke, „Virtuelles" Bereithalten i.S.d. § 5 TDG – Die straf- und zivilrechtliche Verantwortlichkeit bei Einrichtung eines Hyperlinks, in: ZUM 2001, 34; Gounalakis/Rhode, Haftung des Host-Providers: ein neues Fehlurteil, in: NJW 2000, 2168; Haft/Eisele, Zur Einführung: Rechtsfragen des Datenverkehrs im Internet, in: JuS 2001, 112; Heghmanns, Strafrechtliche Verantwortlichkeit für illegale Inhalte im Internet, in: JA 2001, 71; Thomas Hoeren, Vorschlag für eine EU-Richtlinie über E-Commerce. Eine erste kritische Analyse, in: MMR 1999, 192; ders./Rufus Pichler, Zivilrechtliche Haftung im Online-Bereich, in: Loewenheim/Koch, Praxis des Online-Rechts, Weinheim (VCH) Verlag 1997; Bernd Holznagel, Zukunft der Haftungsregeln für Internet-Provider, in: K & R 1999, 103; ders., Verantwortlichkeiten im Internet und Free Speech am Beispiel der Haftung für illegale und jugendgefährdende Inhalte, in: ZUM 2000, 1007; Frank A. Koch, Zivilrechtliche Anbieterhaftung für Inhalte in Kommunikationsnetzen, in: CR 1997, 193; Michael Lehmann, Unvereinbarkeit des § 5 Teledienstgesetzes mit Völkerrecht und Europarecht, in: CR 1998, 232; Wolfram Lohse, Verantwortung im Internet, Münster 2000; Bernd Martenczuk, Die Haftung für Mediendienste zwischen Bundes- und Landesrecht, in: ZUM 1999, 104; Petra Marwitz, Haftung für Hyperlinks, in: K & R 1998, 369; Christian Pelz, Die strafrechtliche Verantwortlichkeit von Internet-Providern, in: ZUM 1998, 530; Rufus Pichler, Haftung des Host Providers für Persönlichkeitsrechtsverletzungen vor und nach dem TDG, in: MMR 1998, 79; Satzger, Strafrechtliche Verantwortlichkeit von Zugangsvermittlern, in: CR 2001, 109; Haimo Schack, Neue Techniken und Geistiges Eigentum, in: JZ 1998, 753; Martin Scharfer/Clemens Rasch/-Thorsten Braun, Zur Verantwortlichkeit von Online-Diensten und Zugangsvermittlern für fremde urheberrechtsverletzende Inhalte, in: ZUM 1998, 451; Eric Schlachter, Cyberspace, The Free Market and the Free Marketplace of Ideas: Recognizing Legal Differences in Computer Bulletin Board Functions, in: Hastings Communication and Entertainment Law Journal 16, 87; Jürgen Schneider, Urheberrechtsverletzungen im Internet bei Anwendung des § 5 TDG, in: GRUR 2000, 969; Ulrich Sieber, Verantwortlichkeit im Internet, München 2000; ders., Strafrechtliche Verantwortlichkeit für den Datenverkehr in internationalen Datennetzen, in: JZ 1996, 429 und 494; ders., Kontrollmöglichkeiten zur Verhinderung rechtswidriger Inhalte in Computernetzen, in: CR 1997, 581 und 653; Gerald Spindler, Deliktsrechtliche Haftung im Internet – nationale und internationale Rechtsprobleme, in: ZUM 1996, 533; ders., Haftungsrechtliche Grundprobleme der neuen Medien, in: NJW 1997; ders., Verschuldensabhängige Produkthaftung im Internet, in: MMR 1998, 23; ders., Verschuldensunabhängige Produkthaftung im Internet, in: MMR 1998, 119; ders., Störerhaftung im Internet, K & R in: 1998, 177; ders., Die Haftung von Online-Dienstanbietern im Konzern, in: CR 1998, 745; ders., Dogmatische Strukturen der Verantwortlichkeit der Diensteanbieter nach TDG und MDStV, in: MMR 1998, 639; ders. Verantwortlichkeit von Diensteanbietern nach dem Vorschlag einer E-Commerce-Richtlinie, in: MMR 1999, 99; ders. Haftungsklauseln in Provider-Verträgen, in: CR 1999, 626; ders., E-Commerce in Europa. Die E-Commerce-Richtlinie in ihrer endgültigen Fassung, in: MMR-Beilage 7/2000, 4; ders., Urheberrecht und Haftung der Provider – ein Drama ohne Ende?, in: CR 2001, 324; Irini Vassilaki, Strafrechtliche Verantwortlichkeit der Diensteanbieter nach dem TDG, in: MMR 1998, 630; Arthur Waldenberger, Zur zivilrechtlichen Verantwortlichkeit für Urheberrechtsverletzungen im Internet, in: ZUM 1997, 188; ders., Teledienste, Mediendienste und die „Verantwortlichkeit" ihrer Anbieter, in: MMR 1998, 129; Wimmer, Die Verantwortlichkeit des Online-Providers nach dem neuen Multimediarecht, in: ZUM 1999, 436.

3.1 Kollisionsrechtliche Vorfragen

Fraglich ist, welche kollisionsrechtlichen Vorgaben über die Anwendbarkeit deliktsrechtlicher Vorschriften entscheiden. Zu beachten ist hier Art. 40 EGBGB. Hiernach hat der Verletzte die Wahl zwischen dem Recht des Handlungs- und dem des Erfolgsortes. Dieses Wahlrecht muss er bis zum Beginn der ersten mündlichen Verhandlung ausüben. Handlungsort ist regelmäßig der Ort, an dem der Server des Providers steht. Erfolgsort ist überall dort, wo die Homepage abgerufen werden kann; einige Gerichte stellen auf den „bestimmungsgemäßen" Abruf ab. Ähnliches gilt für das Strafrecht. Entscheidend ist hier nach § 9 StGB, ob der zum Tatbestand gehörende Erfolg im Sinne von § 9 StGB in Deutschland eingetreten ist, unabhängig vom Wohnsitz des Angeklagten. In diesem Sinne hat der BGH einen Australier wegen Volksverhetzung verurteilt, der von Adelaide aus NS-Theorien über das Internet verbreitete.[1]

3.2 Das Teledienstegesetz

Für das Straf- und Zivilrecht hat der Gesetzgeber im Informations- und Kommunikationsdienstegesetz, genauer gesagt im Teledienstegesetz (TDG), Regeln festgesetzt, die wie ein Filter vor der Anwendung spezieller Haftungsregeln zu prüfen sind. Allerdings finden sich für Mediendienste, zu denen auch einige Bereiche der Online-Dienste gehören, besondere Regelungen im Mediendienste-Staatsvertrag. Strittig ist überdies die Anwendbarkeit dieser Bestimmungen auf das Urheberrecht, seitdem das OLG München in einer fragwürdigen Entscheidung eine Anwendung aufgrund des Wortlauts und der Entstehungsgeschichte von § 5 TDG ausgeschlossen hat.[2]

All diese Regelungen werden derzeit im Rahmen des so genannten Elektronischen Geschäftsverkehrsgesetz (EGG) überarbeitet. Dieses Gesetz, das bislang nur in Entwürfen vorliegt, soll die Vorgaben der EU-Richtlinie über bestimmte rechtliche Aspekte des elektronischen Handels (E-Commerce-Richtlinie) umsetzen.[3] Es wird im Folgenden an geeigneter Stelle mitberücksichtigt.

Das TDG ist das Ergebnis eines harten Ringens. Nach zähen Verhandlungen zwischen den beteiligten Ministerien, vor allem dem Bundesjustiz-, Bundesforschungs- und dem Bundesinnenministerium, sowie weiteren betroffenen Kreisen wurde, nach einem ersten Vorentwurf vom 6. Juni 1996, der erste amtliche Entwurf aus dem BMFT am 28. Juni 1996 der Öffentlichkeit vorgestellt. Es folgten eine Reihe verschiedener interner Texte, die teilweise über „dunkle Kanäle" an die Außenwelt drangen. Am 8. November 1996 konnte der Referentenentwurf verabschiedet werden, der am 11. Dezember 1996 durch das Bundeskabinett gebilligt wurde. Damit war das Zittern um das weitere Schicksal des Gesetzes noch nicht zu Ende. Erst nach schwierigen parlamentarischen Diskussionen passierte das Gesetzespaket, in inzwischen mehrfach veränderter Gestalt[4], im Juni 1997 Bundestag und Bundesrat und trat schließlich doch noch am 1. August 1997 in Kraft[5].

Das Gesetz unterscheidet drei verschiedene Provider (genannt: „Diensteanbieter"). Nach § 5 Abs. 1 TDG sind Diensteanbieter für eigene Inhalte, die sie zur Nutzung bereithalten, nach den allgemeinen Gesetzen verantwortlich. Für das Bereithalten fremder Inhalte sind sie hingegen nur verantwortlich, wenn sie von diesen Inhalten Kenntnis haben und es ihnen technisch möglich und zumutbar ist, deren Nutzung zu verhindern (§ 5 Abs. 2 TDG). Für fremde Inhalte, zu denen die Diensteanbieter nur den Zugang zur Nutzung vermitteln, sind sie nicht verantwortlich (§ 5 Abs. 3 S. 1 TDG). Diese Regelungen klingen erst langweilig und trocken. Doch hier spielt die straf- und zivilrechtliche Musik.

[1] *Urteil des BGH vom 12.Dezember 2000 - 1 StR 184/00.*
[2] *Urteil vom 8. März 2001 - 29 U 3282/00. Ähnlich auch Schaefer/Rasch/Braun, ZUM 1998, 451; Waldenberger, MMR 1998, 124, 127. Dagegen zu Recht kritisch Spindler, CR 2001, 324.*
[3] *Siehe dazu Bröhl, MMR 2001, 67.*
[4] *Beschlussempfehlung und Bericht des Ausschusses für Bildung, Wissenschaft, Forschung, Technologie und Technikfolgenabschätzung, BT-DrS 13/7934 vom 11. Juni 1997.*
[5] *BGBl. I, 1870.*

3.2.1 Der Content-Provider

Der Content-Provider ist ein Informationslieferant. Bietet er eine Homepage im Internet an, muss er für deren Inhalt einstehen. Das neue Gesetz verweist in § 5 Abs. 1 TDG deklaratorisch auf die „allgemeinen Gesetze". Die E-Commerce-Richtlinie ändert an dieser Rechtslage nichts. Es bleibt beim Grundsatz der Haftung des Content Providers nach den allgemeinen Gesetzen. Im Folgenden sollen einige Überlegungen zur allgemeinen Haftung von Content-Providern vorgestellt werden.

Vertragliche Haftung

Für die vertragliche Haftung kann auf die allgemeinen Grundsätze des Zivilrechts zurückgegriffen werden, die neben der Sachmängelhaftung aus §§ 434, 440, 463, 480 Abs. 2 BGB auch die Grundsätze der positiven Forderungsverletzung und der culpa in contrahendo zur Anwendung kommen lassen. Neben dieser allgemeinen Haftung hat der BGH jedoch eine besondere Verantwortlichkeit für Informationsdienste kreiert. In der Entscheidung „Börsendienst"[6] hat der BGH angenommen, dass auch das formularmäßige Werbeschreiben eines Börsendienstes das Angebot zum Anschluss eines gesonderten Beratungsvertrages beinhalte, sofern die Anbieter die Zuverlässigkeit und Richtigkeit ihrer Informationen hervorhöben. Diese Rechtsprechung hat der BGH in den Folgejahren noch ausgeweitet. Hiernach bedarf es für einen solchen Beratungsvertrag keiner besonderen Vereinbarung oder gar eines schriftlichen Vertrages. Vielmehr sei, nach Ansicht des Bundesgerichtshofes, ein solcher Auskunftsvertrag stillschweigend abgeschlossen, wenn eine Auskunft erkennbar von erheblicher Bedeutung und die Grundlage wichtiger Entscheidungen des Anwenders gewesen sei[7]. Der Anwender kann dann vollen Schadensersatz aus positiver Vertragsverletzung verlangen, wobei die generelle dreißigjährige Verjährungsfrist gilt.

Allerdings sind diese Fälle durch das Vorliegen einer bereits bestehenden vertraglichen Bindung gekennzeichnet gewesen. Im Falle etwa des Börsendienstes bestand ein Abonnement ähnlicher Dauervertrag zwischen Herausgeber und Kunden, der auch durch Beratungselemente geprägt war[8]. Von daher kann die Entscheidungspraxis des BGH zu den Beratungsverträgen nur für das Verhältnis eines Users zu einem entgeltlichen Online-Informationsdienst herangezogen werden. Allerdings kann eine solche vertragliche Haftung auch bei Verletzung vorvertraglicher Pflichten über culpa in contrahendo in Betracht kommen. Gibt etwa eine Sparkasse Anlageinformationen und kommt es aufgrund dessen zum Abschluss eines Online-Banking-Vertrages, liegt eine Haftung aus culpa in contrahendo nahe.

Hinsichtlich der vertraglichen Haftung kommt eine Beschränkung der Haftung – etwa in Allgemeinen Geschäftsbedingungen – von vornherein kaum in Betracht. Das AGBG und das BGB verbieten jeglichen Ausschluss sowie jegliche Beschränkung der Haftung für arglistiges Verhalten (§ 476 BGB), das Fehlen zugesicherter Eigenschaften (§ 11 Nr. 11 AGBG) sowie vorsätzliches und grob fahrlässiges Verhalten im Rahmen einer culpa in contrahendo oder einer positiven Vertragsverletzung (§ 11 Nr. 7 AGBG). Zusätzlich hat die Rechtsprechung aus § 9 Abs. 2 Nr. 2 AGBG abgeleitet, dass auch für mittlere und leichte Fahrlässigkeit des Lieferanten die Haftung nicht ausgeschlossen werden dürfe, sofern es um die Verletzung vertragswesentlicher Kardinalpflichten gehe[9]. Unwirksam sind daher folgende Vertragsbestimmungen[10]:

- „Jede Haftung für Mängel wird ausgeschlossen." [11]
- „Für fahrlässiges Verhalten des Verkäufers wird nicht gehaftet." [12]

[6] *BGH, NJW 1978, 997.*
[7] *BGH, NJW 1989, 1029; NJW 1986, 181.*
[8] *Siehe dazu auch Hopt, Festschrift für Fischer 1979, 237; Köndgen, JZ 1978, 389.*
[9] *Siehe dazu BGH, DB 1996, 1276.*
[10] *Vgl. hierzu auch Schneider, a. a. O., Rdnr. O 167, der zu Recht konstatiert, dass die „Haftungsklauseln der Provider eher noch 'Entwicklungsland' als die der Software-Anbieter" seien.*
[11] *Ähnlich die US-Disclaimers: „Limitation of Liability: You expressly understand and agree that Yahoo shall notbe liable for any direct, indirect, incidental, special, consequential or exemplary damages, including but not limited to, damages for loss or profits, goodwill, use, data or other intangible losses, resulting from the use or the inability to use the service...".*
[12] *OLG Köln, DAR 1982, 403.*

- „Wir haften nicht für Mangelfolgeschäden, Datenverlust und entgangenen Gewinn".[13]
- „Wir haften für Schäden (...) bis zur Höhe von ... DM."[14]
- „Wir schließen jegliche Haftung, soweit gesetzlich zulässig, aus."[15]
- „Wir schließen unsere Haftung für leicht fahrlässige Pflichtverletzungen aus."[16]

Zulässig bleibt nur eine Klausel wie folgt:

„Wir schließen unsere Haftung für leicht fahrlässige Pflichtverletzungen aus, sofern diese keine vertragswesentlichen Pflichten oder zugesicherte Eigenschaften betreffen oder Ansprüche nach dem Produkthaftungsgesetz berührt sind. Gleiches gilt für Pflichtverletzungen unserer Erfüllungsgehilfen."

Fraglich ist allerdings, ob es wirklich noch sinnvoll und mit dem AGB-rechtlichen Transparenzgebot vereinbart ist, eine solche Klausel in ein Vertragswerk aufzunehmen. Denn schließlich muss der Lieferant für alle wichtigen Pflichtverletzungen und Leistungsstörungen aufkommen und kann die Haftung insoweit auch nicht ausschließen. Letztendlich schuldet der Content Provider daher im Rahmen von entgeltlichen Infodiensten vollständige und richtige Informationen, ohne dass er seine Haftung ausschließen könnte.

Im Übrigen gilt es zu beachten, dass sich die Möglichkeiten zu einer Haftungsbeschränkung im Rahmen der Schuldrechtsmodernisierung erheblich verschlechtern werden. Zunächst ist zu berücksichtigen, dass das AGBG aufgehoben und in das BGB übernommen werden wird (§§ 307 - 309 BGB-RE). Nach § 309 Nr. 7 lit. b) BGB-RE sind Haftungsausschlüsse für grob fahrlässige Pflichtverletzungen unzulässig. Unwirksam sind auch Haftungsausschlüsse oder -beschränkungen bei grober Fahrlässigkeit, die Rechte nach §§ 280, 281, 283 oder § 311a Abs. 2 betreffen (§ 309 Nr. 8 lit. a). Individualvertraglich ist eine Beschränkung der Haftung bei Arglist oder Bestehens einer Garantie unwirksam (§ 444 BGB-RE).

Der Spielraum für Haftungsklauseln nach dem neuen BGB bleibt unklar. Denkbar wäre vielleicht folgende an obige Klausel angelehnte Formulierung: „Wir schließen unsere Haftung für Pflichtverletzungen aus, sofern es sich nicht um vorsätzliche oder grob fahrlässige Pflichtverletzungen handelt oder Ansprüche nach dem Produkthaftungsgesetz berührt sind. Gleiches gilt für Pflichtverletzungen unserer Erfüllungsgehilfen und gesetzlichen Vertreter."

Deliktische Haftung

Zu beachten ist hier die Haftung für die Rechtmäßigkeit des Inhalts (etwa in Bezug auf Urheberrechtsverletzungen) und für die Richtigkeit des Inhalts. Für die Rechtmäßigkeit des Inhalts gelten die spezialgesetzlichen Haftungsbestimmungen, etwa

- § 97 UrhG für Urheberechtsverletzungen
- §§ 14, 15 MarkenG für Domainfragen
- § 7 BDSG für Datenschutzverstöße oder
- § 1 UWG für rechtswidrige Marketingmaßnahmen im Internet.

Für falsche Inhalte bei Content-Providern kommt eine Haftung nach Maßgabe des Produkthaftungsgesetzes oder im Rahmen von § 823 Abs. 1 BGB in Betracht. Insbesondere könnte die Rechtsprechung zur Haftung des Verlegers bei Printmedien herangezogen werden. So hat der BGH eine Haftung des Herausgebers von Informationsdiensten bejaht, soweit dieser infolge

[13] LG Bayreuth, DB 1982, 1400; Erman/Hefermehl, § 11 Rdz. 6.

[14] Diese Klausel ist nach § 11 Nr. 11 für den Bereich der zugesicherten Eigenschaften gänzlich unwirksam. Sie wird für Ansprüche wegen c.i.c. oder pVV nur zugelassen, wenn alle vertragstypischen und vorhersehbaren Schäden abgedeckt sind (BGH, ZIP 1984, 971; BGH, BB 1980, 1011; BGH, NJW 1993, 335; Erman/Hefermehl, § 11 Nr. 7 AGBG, Rdnr. 15). Wann dies in concreto der Fall ist, lässt sich jedoch kaum feststellen; demnach ist die Klausel auf jeden Fall zu gefährlich.

[15] Ein solcher Rettungsanker ist nicht erlaubt; er gilt als unzulässige salvatorische Klausel. Siehe BGH, NJW 1987, 1815; NJW 1985, 623, 627; OLG Stuttgart, NJW 1981, 1105.

[16] BGHZ 49, 363.

grober Außerachtlassung der Sorgfaltspflicht falsche Anlageempfehlungen verbreitet und dem Kunden dadurch Schaden entsteht[17]. Allerdings ist dieser Fall dadurch gekennzeichnet, dass ein Abonnement ähnlicher Dauervertrag zwischen Herausgeber und Kunden bestand, der auch durch Beratungselemente geprägt war[18]. Von daher kann auch diese Entscheidung nur für das Verhältnis eines Users zu einem entgeltlichen Online-Informationsdienst herangezogen werden.

Abseits vertraglicher Bindungen kommt eine Haftung nur bei Verletzung absoluter Rechtsgüter in Betracht. Der BGH hat in der Kochsalz-Entscheidung betont, dass sowohl der Autor wie eingeschränkt der Verleger für fehlerhafte Angaben in medizinischen Verlagsprodukten einstehen muss. Bei medizinischen Informationen kommt es in der Tat schnell zur Verletzung von Körper und Gesundheit, beides geschützte Rechtsgüter im Sinne von § 823 Abs. 1 BGB. Daher ist bei der Bereitstellung von Gesundheitstipps und medizinischer Werbung ein hohes Haftungsrisiko zu erwarten. Ähnliches gilt für den Download von Software via Internet. Führt dieser zum Datenverlust, liegt eine Eigentumsverletzung im Hinblick auf die nicht mehr einwandfrei nutzbare Festplatte des Users vor. Dieser Haftung für Datenverlust kann sich der Provider aber durch Hinweis auf ein überwiegendes Mitverschulden des Users (§ 254 Abs. 1 BGB) entziehen, da dessen Schaden offensichtlich auf einer fehlenden Datensicherung beruht. Wichtig sind diesem Bereich deutliche Warnhinweise auf der Homepage: *„Wir übernehmen keine Gewähr für die Richtigkeit und Vollständigkeit der auf der Homepage befindlichen Informationen."*

3.2.2 Der Access-Provider

Access-Provider, die einen Internet-Zugang anbieten, sind für die insoweit erreichbaren Angebote nach § 5 Abs. 3 TDG nicht verantwortlich. Gleichwohl wurde teilweise durch komplizierte Konstruktionen (Verantwortlichkeit nach § 5 Abs. 4 TDG und den allgemeinen Strafgesetzen bei Kenntnis von rechtswidrigen Inhalten[19], Mittäterschaft mit dem eigentlichen Host-Provider[20]) versucht, die Access-Provider für die auf anderen als den eigenen Servern gespeicherten Inhalte verantwortlich zu machen. Diese, der eindeutigen Intention des Gesetzgebers widersprechenden, Ansichten konnten sich aber bislang nicht weiter durchsetzen. Die Aufsehen erregende Verurteilung des ehemaligen CompuServe-Geschäftsführers durch das AG München wurde in der Berufung zu Recht aufgehoben[21]. Die Freistellung von der Verantwortung gilt übrigens auch für die auf Proxy Servern gespeicherten Inhalte; denn das Gesetz nimmt eine automatische und zeitlich begrenzte Vorhaltung fremder Inhalte ausdrücklich von der Haftung aus (§ 5 Abs. 3 S. 2).

Hier greift künftig Art 12 der E-Commerce-Richtlinie ein. Hiernach ist der Diensteanbieter für die Durchleitung von Informationen von der Verantwortlichkeit freigestellt. Eine Durchleitung liegt aber nur vor, wenn es um die Weiterleitung von Nutzerinformationen oder um die Zugangsvermittlung zu einem Kommunikationsnetz geht. Die Übermittlung darf nicht vom Diensteanbieter selbst veranlasst worden sein; nur passive, automatische Verfahren sind privilegiert (Erwägungsgrund 42). Sonderbestimmungen regeln das Caching (Art. 13).

3.2.3 Der Host-Provider

Schwieriger ist die Rechtslage bei fremden Inhalten, die Provider zur Nutzung bereithalten (so genannt Host-Providing). Sie sind dafür nach dem Wortlaut von § 5 Abs. 2 TDG („nur ... wenn") grundsätzlich nicht verantwortlich. Eine Ausnahme gilt nur, wenn dem Anbieter die Inhalte bekannt sind und es ihm technisch möglich und zumutbar ist, ihre Verbreitung zu verhindern.

[17] *BGH, NJW 1978, 997.*
[18] *Siehe dazu auch Hopt, Festschrift für Fischer 1979, 237; Köndgen, JZ 1978, 389.*
[19] *Einstellungsverfügung des Generalbundesanwalts, MMR 1998, 93 (DFN-Verein) mit abl. Anm. Hoeren.*
[20] *AG München, NJW 1998, 2836 (CompuServe) = MMR 1998, 429 mit abl. Anm. Sieber.*
[21] *LG München, MMR 2000, 171.*

Ausweislich der amtlichen Begründung des Gesetzgebers zu § 5 Abs. 2 TDG soll eine Haftung des Diensteanbieters also nur gegeben sein, wenn er die fremden rechtswidrigen Inhalte bewusst zum Abruf bereit hält. Die Regelung ist zunächst, was die Abgrenzung von Access- und Service-Provider angeht, sehr extensiv formuliert. Der Provider würde damit auch die Verantwortung für alle Newsgroups übernehmen, die automatisch auf seinem Server gespeichert werden. Letztendlich kann zwischen eigenen und fremden Angeboten nur schwer unterschieden werden. Ist das Angebot eines Tochterunternehmens der Deutschen Bank AG ein eigener oder ein fremder Inhalt? Ist die Grenze zwischen beiden Kategorien gesellschaftsrechtlich zu bestimmen?

Ähnliche Bedenken bestehen hinsichtlich der Formulierung des subjektiven Tatbestands. Das TDG stellt auf die bloße Kenntnis von den Inhalten ab. Damit soll die Haftung der Service-Provider auf Vorsatzstraftaten und -delikte beschränkt werden. Es geht folglich um die unbedingte oder bedingte Kenntnis der objektiven Tatbestandsverwirklichung. Hiermit konterkariert der Gesetzgeber seine eigenen Bemühungen, die Provider zur innerbetrieblichen oder verbandsseitigen Selbstkontrolle zu verpflichten. Denn wenn die bloße Kenntnis vom Inhalt als subjektives Element ausreichen soll, wird niemand daran Interesse haben, Personal mit der Sichtung des Online-Angebots zu beauftragen. Er wird vielmehr auf jedwede Selbstkontrolle verzichten – getreu dem Motto: Nichts gesehen, nichts gehört. Auch das LG München hat dieses Problem gesehen. Seiner Auffassung nach würden bei der amtlichen Auslegung des Art. 5 Abs. 2 TDG sowohl Art. 14 GG, als auch die Regelungen in Art. 8,10 und 14 WIPO-Vertrag unterlaufen. Selbst „bewusstes Wegschauen" würde zu einem Haftungsausschluss führen. Dies könne nicht zugelassen werden[22]. Das Landgericht fordert, Prüfungspflichten hinsichtlich der die Rechtswidrigkeit begründenden Umstände aufzunehmen. Es hätte sich auch angeboten, wenigstens für die Fälle eine Prüfungspflicht zu bejahen, in denen ein Verstoß gegen Strafgesetze nahe liegt (etwa bei der Bezeichnung einer Newsgroup als „alt. binaries.children-pornography"). Eine solche Prüfungspflicht bei eklatanter Missbrauchsgefahr hätte auch der geltenden Rechtslage im Zivil- und Strafrecht entsprochen. Art. 15 Abs. 1 der E-Commerce-Richtlinie sieht jedoch ausdrücklich von einer Prüfungspflicht ab.

Im Übrigen reicht die bloße Kenntnis vom Inhalt für die Bejahung eines rechtsrelevanten Vorsatzdeliktes nicht aus. Zum einen stellen Straf- und Zivilrecht für den Vorsatz nicht nur auf die Kenntnis ab, sondern verlangen auch ein voluntatives Element. Man muss die Tatbestandsverwirklichung nicht nur kennen, sondern auch wollen. Auf letzteres Element scheint der Gesetzgeber verzichten zu wollen.

Für den Zivilrechtler ist auch das Fehlen jeglicher Überlegungen zum Bewusstsein der Rechtswidrigkeit auffällig. Die bloße Tatsache, dass ein Rechenzentrumsmitarbeiter eine Newsgroup gesichtet hat, heißt ja noch nicht, dass er deren Inhalt richtig, d. h. als Rechtsverstoß, bewerten kann. Zumindest für die zivilrechtliche Haftung schließt Vorsatz neben dem Wissen und Wollen der Tatbestandsverwirklichung auch das Bewusstsein davon ein, dass ein Angebot gegen geltendes Recht verstößt. Da diese Wertung gerade im noch fließenden Multimediarecht schwierig zu ziehen ist, hätte man sich hierzu Überlegungen gewünscht. Der Gesetzgeber will jedenfalls die Garantenstellung erst dann bejahen, wenn ein Diensteanbieter die fremden rechtswidrigen Inhalte bewusst zum Abruf bereithält[23]. Dabei wird aber nicht deutlich, wie Rechtswidrigkeit und Vorsatz zueinander in Beziehung stehen. Besser wird diese Frage in Art. 14 Abs. 1 der E-Commerce-Richtlinie geregelt, wonach bei Schadensersatzansprüchen erforderlich ist, dass der Anbieter sich der Tatsachen und Umstände bewusst ist, aus denen die rechtswidrige Information offensichtlich wird.

Deutlich dürfte auf jeden Fall sein, dass das TDG nicht nur geltendes Recht wiederholen, sondern das Haftungssystem des Zivil- und Strafrechts in Bezug auf Online-Dienste verändern soll. Wenn dies der Fall ist, muss allerdings auch die Frage nach der zeitlichen Dimension des Gesetzes gestellt werden. An keiner Stelle enthält das Ge-

[22] LG München I, Urteil vom 30.03.2000 (nicht rechtskräftig), MMR 2000, 434.

[23] So auch die Begründung zum Referentenentwurf vom 08.11.96.

setz Regelungen zu der Frage, ob die Haftungsbestimmungen auch auf Altfälle zur Anwendung kommen. Im Bereich des Strafrechts sind daher in der Regel nach § 2 Abs. 3 StGB die neuen Haftungsregeln des TDG als das mildere Gesetz anzuwenden.

Wichtig ist eine klare Abgrenzung eigener und fremder Inhalte auf der Homepage: „Sie verlassen jetzt unser Internetangebot. Für den Inhalt der folgenden Seiten ist der jeweilige Anbieter verantwortlich. Wir übernehmen insoweit keine Haftung."

3.2.4 Haftung für Links

Besonders schwer fällt die Einordnung von Hyperlinks[24], da diese sich keiner der drei verschiedenen Gruppen des § 5 TDG eindeutig zuordnen lassen. Auch die E-Commerce-Richtlinie sieht keine Regelung für die Verantwortung von Hyperlinks vor. Zunächst ist bei den Hyperlinks zu beachten, dass ein Hyperlink als solcher nie eine Haftung auslösen kann. Ein Link ist nur eine technische Referenz innerhalb eines HTML-Textes. Entscheidend ist daher die Aussage, die mit dem Link – unter besonderer Berücksichtigung seines inhaltlichen Kontextes – verbunden ist. So betonte das Amtsgericht Berlin-Tiergarten[25] als erstes Gericht in Deutschland, dass sich die Verantwortlichkeit des Link-Setzers nach dessen, mit dem Link getroffenen Gesamtaussage richte. In dem Fall des Amtsgerichts ging es um die Abgeordnete Angela Marquardt, die einen Link auf einen niederländischen Server gesetzt hatte, auf dem sich die strafrechtlich verbotene Zeitschrift „Radikal" befand. Der Generalbundesanwalt hatte die Bundestagsabgeordnete in der Beihilfe zur Bildung einer terroristischen Vereinigung angeklagt und sah in dem Link auf die Zeitschrift den entscheidenden Unterstützungsbeitrag. Dieser Ansicht hatte sich das Amtsgericht nicht angeschlossen. Strafrechtlich relevant sei nur eine konkrete Ausgabe der Zeitschrift „Radikal" gewesen. Es hätten sich aber keine Feststellungen darüber treffen lassen, ob und vor allem wann die Angeklagte von der Einspeisung der rechtswidrigen Ausgabe Kenntnis erlangt habe. Die bloße Weiterexistenz des Links könne eine Strafbarkeit jedenfalls dann nicht begründen, wenn nicht positiv festgestellt werden könne, dass die Angeklagte den Link bewusst und gewollt in Kenntnis des Inhalts und der Existenz der Ausgabe weiter aufrecht erhielt. Unter dem Gesichtspunkt der Ingerenz könne an das Unterlassen einer regelmäßigen Überprüfung des eigenen Links allenfalls der Fahrlässigkeitsvorwurf erhoben werden, der hier allerdings nicht relevant sei. Das (kurze) Urteil des Amtsgerichts verweist auf die entscheidende Frage, welchen Aussagegehalt der Link haben kann. Solidarisiert sich jemand mit dem rechtswidrigen Inhalt eines anderen durch das Setzen eines Links, ist er so zu behandeln, als sei er ein Content-Provider. Folglich kommt in diesem Fall § 5 Abs. 1 TDG zum Tragen; der Link-Setzer haftet für die gelinkten Inhalte so, als wären es seine eigenen. Anders ist der Fall zu beurteilen, wenn jemand sich den fremden Inhalt nicht zu eigen macht. Setzt jemand – etwa aus wissenschaftlichem Interesse heraus – einen Link auf fremde Inhalte ohne jedweden Solidarisierungseffekt, ist er wie ein Access Provider zu beurteilen, so dass § 5 Abs. 3 und 4 TDG zum Tragen kommt. Eine Haftung scheidet in einem solchen Fall regelmäßig aus. Im Strafrecht kommt hinzu, dass der Grundgedanke des „in dubio pro reo" zu beachten ist. Im Zweifel besteht daher – im Ergebnis genauso wie das Amtsgericht Berlin-Tiergarten – keine Verantwortlichkeit für das Setzen von Links auf strafrechtliche relevante Inhalte.

Anders ist die Grundkonzeption des Zivilrechts, das von dem Grundsatz „in dubio contra reum" ausgeht. Grundsatzurteil ist hier eine Entscheidung des Landgerichts Hamburg[26]. Hierbei ging es um die Einrichtung einer Link-Sammlung zu so genannten Steinhövel-Haßseiten. Der betroffene Anwalt nahm den Link-Setzer wegen Ehrverletzung in Anspruch. Das Landgericht Hamburg verurteilte den Anspruchgenommenen, weil er sich nicht hinreichend von den ehrverletzenden Äußerungen Dritter distanziert und sich dieselben durch seine Links zu eigen gemacht habe. Allerdings hat sich die Rechtsprechung auch hieraus differenziert. So soll zum Beispiel ein Link von

[24] *Vgl z. B. LG Hamburg, Urteil vom 12. Mai 1998, CR 1998, 565 = NJW-CoR 1998, 302; AG Berlin-Tiergarten, Urteil vom 30. Juni 1997, CR 1998, 111 mit Anm. Vassilaki.*

[25] CR 1998, 111.

[26] *Urteil v. 12. Mai 1998, CR 1998, 565.*

einem privaten Internetanbieter auf eine fremde Website keine Haftung auslösen.[27] Für Downloadlinks wird eine Haftung bejaht.[28] Die Haftung kann auch soweit gehen, dass wegen Förderung fremden Wettbewerbs für einen Link auf die nach deutschem Recht wettbewerbswidrigen Seiten der amerikanischen Muttergesellschaft gehaftet wird. [29]

Diese differenzierte Betrachtung entspricht inzwischen auch der herrschenden Meinung[30]. Nur noch wenige versuchen eine analoge Anwendung von § 5 Abs. 2 TDG, die darauf hinauslaufen würde, einen Link-Setzer ab und bei Kenntnis des Inhalts zur Sperrung zu verpflichten und widrigenfalls eine Haftung zu bejahen[31]. Andere wollen grundsätzlich Hyperlinks dem Anwendungsbereich von § 5 Abs. 3 TDG unterwerfen[32].

3.2.5 Haftung für sonstige Intermediäre

Die Rechtsprechung denkt auch über eine Haftung sonstiger Intermediäre nach. Nicht in Betracht kommen soll eine Haftung des Suchmaschinenbetreibers, etwa für markenrechtliche Unterlassungsansprüche.[33] Denn dieser stelle nur Einträge in ein Verzeichnis ein und unterliege daher keiner Prüfungspflicht, es sei denn, eine Rechtsverletzung ist offenkundig.

Ein Anbieter von Online-Auktionen muss sich nach Auffassung des LG Köln[34] die Angaben in den Angeboten Dritter als eigene Inhalte zurechnen lassen. Im vorliegenden Fall hatte sich ROLEX darüber beschwert, dass bei Ricardo Markenrecht verletzende Replika von Rolex-Uhren zum Verkauf angeboten wurden. Ricardo sah sich als Host-Provider, der erst nach Information durch Rolex tätig werden muss. Das Landgericht schloss sich jedoch der Klägerin an und betrachtete die Angebote als eigene Inhalte von Ricardo, da zumindest die Überschriften der Angebote von Ricardo als eigener Inhalt vorgestellt werden. Ein eigener Inhalt liege auch vor, wenn aus der Sicht des Nutzers eine Verquickung dergestalt stattfinde, dass Diensteanbieter und Fremdinhalt als Einheit erscheinen. Insofern wurde Ricardo als Content Provider wegen Markenrechtsverletzung zur Unterlassung verurteilt.

3.3 Der Mediendienste-Staatsvertrag

Unterschiede bei den Haftungstatbeständen finden sich im Mediendienste-Staatsvertrag. Zwar haben die Bundesländer versucht, das TDG weitestgehend zu kopieren. Jedoch konnten sie auf eine zusätzliche Sperrbefugnis zugunsten der Landesbehörden nicht verzichten (§ 5 Abs. 3 S. 2 i.V.m. § 18 Abs. 3 MDStV). Weitaus größere Schwierigkeiten macht die Bestimmung der Reichweite von § 5 Mediendienste-Staatsvertrag – gerade vor dem Hintergrund der von den Ländern so viel beschworenen verfassungsrechtlichen Bestimmungen zur Gesetzgebungszuständigkeit von Bund und Ländern. Die Abgrenzung von Bund- und Länderkompetenzen auf dem Gebiet der Online-Dienste ist ein schwieriges Thema, das während der Vorbereitungen für das IuKDG zu einer Reihe kontroverser Diskussionen geführt hat. Aufgrund eines im Juni 1996 verabschiedeten Kompromisspapiers beanspruchen die Länder die Regelungsbefugnis für Mediendienste für sich. Hierzu zählen nach § 2 Abs. 2 Nr. 4 MDStV auch die Abrufdienste, bei denen Text-, Ton- oder Bilddarbietungen auf Anforderung aus elektronischen Speichern zur Nutzung übermittelt werden, mit Ausnahme von solchen Diensten, bei denen der individuelle Leistungsaustausch oder die reine Übermittlung von Daten im Vordergrund steht. Diese Definition fügt sich nicht harmonisch in die Definition der Teledienste im TDG (siehe § 2 Abs. 1 TDG) ein. Auf diese Problematik soll hier jedoch nicht näher eingegangen werden. Wichtiger ist die Tatsache, dass nach der Definition des Mediendienste-Staatsvertrages eine Reihe von Online-Diensten als Mediendienste zu qualifizieren sind und unter den Staatsvertrag fallen. Dies gilt zum Beispiel für elektronische

[27] *OLG Schleswig, Urteil vom 19. Dezember 2000, K&R 2001, 220.*
[28] *LG Braunschweig, Urteil vom 6. September 2000, CR 2001, 47.*
[29] *Beschluss des Obersten Gerichtshofs Österreichs vom 19. Dezember 2000 – 4 Ob 225/00.*
[30] *s. etwa Engel/Flechsig/Maennel/Tettenborn, NJW 1997, 2981, 2985; Pichler, MMR 1998, 79, 87; Spindler, MMR 1998, 3193, 3198.*
[31] *s. in diesem Sinne etwa Waldenberger, MMR 1998, 124, 128 f.*
[32] *Eichler/ Helmers/Schneider, RIW Beilage 12/1997, 23, 25; Koch, NJW-CoR 1998, 45, 48; Koch, CR 1997, 193, 200 ff.*
[33] *LG München, Urteil vom 20. September 2000, MMR 2001, 56.*
[34] *Urteil vom 31. Oktober 2000, CR 2001, 417.*

Forschungsjournale, zahlreiche Newsgroups und inhaltlich orientierte Homepages.

Die Länder haben nun zwar im Staatsvertrag die Haftungsregelungen des Bundes übernommen. Sie besitzen jedoch keine Regelungskompetenz für Fragen des Straf- und Zivilrechts (siehe Art. 74 Nr. 1 GG). Die Haftungsbestimmungen im Mediendienste-Staatsvertrag können sich daher von vornherein nicht auf das Gebiet des Straf- und Zivilrechts beziehen[35]. Statt dessen sanktionieren sie nur Verstöße gegen den Staatsvertrag selbst. Theoretisch wäre zwar eine analoge Anwendung von § 5 TDG denkbar. Allerdings verbietet das TDG eine solche Analogie ausdrücklich in § 2 Abs. 4 Nr. 3. Hiernach soll das Gesetz nicht auf Mediendienste zur Anwendung kommen.

Folglich kommt im Bereich des Mediendienste-Staatsvertrages eine Anwendung der klassischen Regelungen des Zivil- und Strafrechts in Betracht. Da diese – wie bereits ausgeführt – eine Prüfungspflicht bei offenkundigen Verdachtsmomenten vorsehen, weichen die Haftungsbestimmungen von Mediendienste-Staatsvertrag und TDG entscheidend voneinander ab. Hier ist eine Klärung in der Praxis – insbesondere durch die Rechtsprechung – notwendig, um ein einheitliches Haftungssystem für alle Online-Dienste zu etablieren. Auch die Verabschiedung der E-Commerce-Richtlinie haben die Bundesländer nicht zum Einlenken bringen können; derzeit ist eine Novellierung des Staatsvertrages aufgrund der Richtlinie in Bearbeitung.

3.4 Versicherbarkeit

Das Haftungsrisiko führt zwangsläufig zu der Frage, inwieweit dieses Risiko versicherbar ist. Informationen darüber, ob und inwieweit einzelne Versicherungsunternehmen entsprechende Policen vereinbaren, waren nicht erhältlich. Es ist auch nicht bekannt, ob einzelne Unternehmen bereits Konzepte zur Absicherung solcher Risiken in Vorbereitung haben. Deshalb kann hier nur auf die Allgemeine Haftpflichtbedingungen (AHB)[36] zurückgegriffen werden, um die Anwendbarkeit der allgemeinen Betriebshaftpflichtversicherung auf diesen Versicherungsfall hin zu analysieren.[37] Grundsätzlich deckt die Haftpflichtversicherung deliktische Ansprüche, etwa aus § 823 Abs. 1 BGB, ab. Für vertragliche Schadensersatzansprüche, die ebenfalls mitversichert sind, wird jedoch eine Absicherung der Erfüllung von Verträgen ausgeschlossen (§ 4 Abs. 1 Zi 6 Abs. 3 AHB): Der Content-Provider trägt also regelmäßig das Risiko dafür, dass seine entgeltlich zum Abruf angebotenen Informationen richtig und rechtmäßig erlangt sind. Von der Versicherung ausgeschlossen sind ferner Haftpflichtansprüche, wenn sie aufgrund Vertrages oder besonderer Zusage über den Umfang gesetzlicher Haftungstatbestände hinausgehen (etwa bei zugesicherten Eigenschaften oder im Falle des oben erwähnten, zusätzlichen Beratungsvertrages). Für das Internet ist vor allem auch der Haftungsausschluss bei Schadenereignissen wichtig, die im Ausland eintreten (§ 4 Abs. 1 Zi 3 AHB). Eine Absicherung für Urheber- oder Persönlichkeitsrechtsverletzungen mit Auslandsbezug ist damit über die Allgemeine Betriebshaftpflichtversicherung nicht zu erreichen. Die Versicherung tritt schließlich auch nicht ein bei Schäden, die weder Personen- noch Sachschaden sind (§ 1 Abs. 3 AHB), also etwa bei Datenausfall oder Betriebsstillstand. Diese Vermögensschäden dürften aber diejenigen sein, die typischerweise im Online-Bereich auftreten. Die Unrichtigkeit einer Information führt nur selten zu unmittelbaren Personen- oder Sachschäden. Eine Erweiterung des Versicherungsschutzes für Provider ist deshalb notwendig.[38]. Diese Erweiterung sollte dann – ähnlich wie bei Softwarehaftpflichtversicherungen – die Haftung wegen besonderer Zusagen, im Falle der Nichterfüllung und der Auslandsberührung und für Vermögensschäden einschließen.

[35] *Streitig, wie hier: Pichler, MMR 1998, 79 (80 f.); Gounalakis, NJW 1997, 2993 (2995); a.A. Bettinger/Freytag CR 1998, 545 (547).*
[36] *Abgedruckt bei Dörner (Hg.), Allgemeine Versicherungsbedingungen, 2. Aufl. München 1996, unter Zi 11.*
[37] *Vgl. hierzu auch allgemein Schmidt-Salzer/Otto, Versicherungsrecht, in: Kilian/Heussen (Hg.), Computerrechtshandbuch, München Stand 1997, Kap. 112; Schulze Schwienhorst, CR 1995, 193.*
[38] *In diesem Zusammenhang sei auf die heute übliche Mitversicherung der Verletzung des BDSG hingewiesen; siehe dazu Schmidt-Salzer/Otto, a. a. O., Kap. 112 Rdnr. 37 f.*

4. Antwort des Versicherungsmarktes auf Online-Risiken – Schadenszenarien und Absicherungskonzepte

von Christoph J. Nießen

Einleitung

Wie sicher ist sicher?

Das Web-Portal „Yahoo", der Online-Buchhändler „Amazon.com", das Auktionshaus „eBay", die Shoppingsite „Buy.com", der Fernsehsender „CNN" und der Online-Wertpapierhändler „Etrade" – alle knickten Sie ein: Eine durch ein „Denial-of-Service-Programm" ausgelöste Lawine von Anfragen sorgte im Februar 2000 dafür, dass Ihre Computersysteme zusammenbrachen. Gefahr droht den IT-Systemen nicht nur durch Security risks (Bedrohung und Sabotage durch Menschen) sondern auch Safety risks (rein technische Risiken).

Ein Grund für die hohe Angreifbarkeit von IT-Systemen ist die schnelle Entwicklung auf dem IT-Markt. Es ist illusorisch zu glauben, dass es ein 100 %ig sicheres System gibt. Ein Grund für die Anfälligkeit von IT-Systemen liegt in der vorherrschenden Monokultur. In der Verschlüsselungstechnologie gibt es weltweit nur zwei Anbieter (Cisco und Checkpoint), die alle existierenden Firewalls zur Verfügung stellen. Ist die Technologie eines Anbieters bekannt und wird somit angreifbar, hat dies verheerende Auswirkungen auf das weltweite Internetgeschehen.

Der Markt für Betriebsysteme ist ebenfalls ein Oligopol. Fast jedes Unternehmen benutzt Microsoft- oder Macintosh-Betriebssysteme. Dies schafft ein enormes Angriffspotenzial. Denn ist erst eine Störung dieser Betriebssysteme bekannt, kann damit eine globale Katastrophe ausgelöst werden. Man stelle sich z.B. vor, ein Virus löscht weltweit sämtliche „*exe" und „*doc"-Dokumente.

Dass diese Vorstellung keineswegs unrealistisch ist, zeigt zum Beispiel der schon 1988 entstandene „Morris-Wurm", der 80 % des gesamten Internets lahm legte. Und der Programmierfehler, der für diese Katastrophe verantwortlich war, wurde bis heute nicht korrigiert. Ein ähnliches Szenario ist jederzeit wieder möglich.

Unsicherheitsfaktor Mensch

Warum lassen es Unternehmen zu, dass Ihre Systeme, trotz großer finanzieller und arbeitsintensiver Bemühungen um Sicherheitslösungen, dieses hohe Angriffspotenzial aufweisen? Das Problem liegt weniger in der Technologie, sondern vielmehr in marktpsychologischen und gesellschaftlichen Zusammenhängen.

Die Herstellerfirmen von „security and safety" Lösungen vermitteln den Kunden das Gefühl, dass Ihre Produkte absolut sicher vor Fremdeinwirkungen sind. Den Kunden fehlt jedoch häufig ein fundiertes Risikoverständnis. Sie verlassen sich auf Herstellerzusagen, ohne eine firmeninterne Risikoanalyse durchzuführen.

Riskobewusstsein stärken

Risikobewusstsein ist eine notwendige Voraussetzung für eine Minimierung der Gefahren. Erst wenn das gesamte Risikopotenzial erkannt wird, sind wirksame Sicherheitslösungen denkbar. Ein Restrisiko wird jedoch immer bleiben. Das KontraG ist hierbei ein erster Schritt, um Unternehmen die Notwendigkeit des Risk-Managements bewusst zu machen. Technologische Redundanzen sollten zur Sicherheit behalten werden und auch die Abhängigkeit von Monokulturen sollte so gering wie möglich sein.

Das Management ist gefragt – besonders im E-Business

Für ein effizientes Risk-Management-System benötigt man viel Zeit und die will man nicht investieren. Die Krise kommt von allein; für den Erfolg sind Fachkenntnisse und Engagement erforderlich. Immer mehr Unternehmen befinden sich auf dem Weg in die wirtschaftliche Schieflage. Die Gründe dafür sind nicht nur in den strukturellen Veränderungen und dem sich verschärfenden Wettbewerb zu suchen, sondern auch im Management, das auf Tendenzen und Entwicklungen nicht rechtzeitig reagiert.

Daher muss aufgezeigt werden, weshalb einem aufmerksamen Management bei ausreichenden Maßnahmen zur Risikovorsorge und frühzeitigem Gegensteuern fast immer genügend Zeit zur Krisenvermeidung bleibt. Erforderlich ist dafür vor allem die Kenntnis von den häufigsten Krisenarten und ihren typischen Entwicklungen.

Während Liquiditätskrisen selbst für den Laien leicht erkennbar sind und Erfolgskrisen aus den Jahresabschlüssen ermittelt werden können, bleiben die vorausgehenden strategischen Krisen oftmals viel zu lange unbeachtet.

Erste Lösungsvorschläge

Methoden zur Risikobewertung müssen gefunden werden, so dass Preise, Prämien und Eintrittswahrscheinlichkeiten berechnet werden können. Auch Risikovergleiche können Internetrisiken detaillierter definieren: Birgt die digitale Signatur wirklich mehr Risiken als die handschriftliche, die ebenfalls nicht fälschungssicher ist? Können Wettbewerber mit Hilfe des Internets mehr geschädigt werden als bisher durch unlauteren Wettbewerb?

Ermittlung der Total Cost of Risk

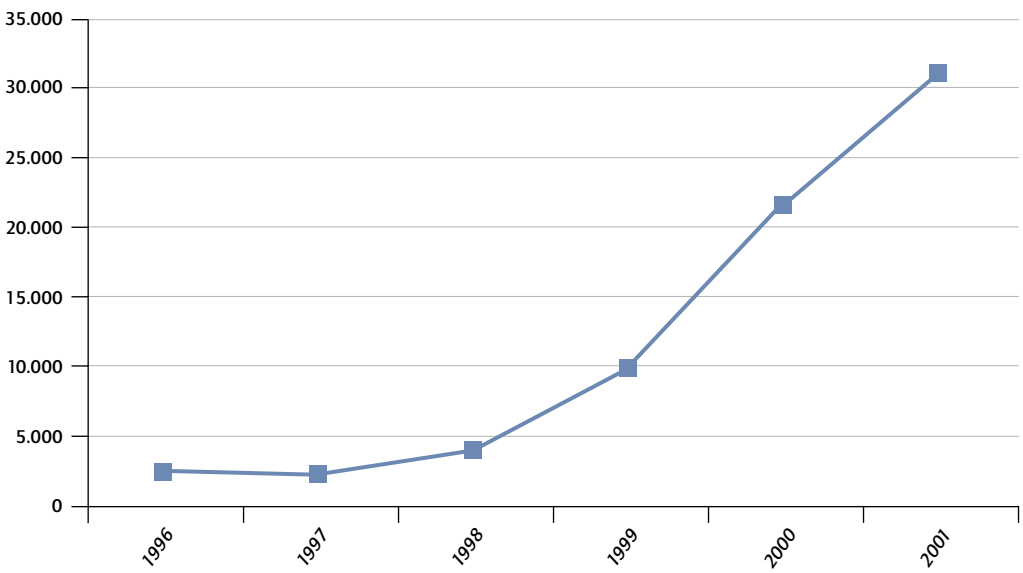
Für die effiziente und professionelle Erfassung, Bewertung und Analyse von Risikodaten benötigen Sie ein Risk Management Informations-System bzw. eine Software-Lösung.

Durch umfassende Datenbanken sowie flexible andere manuelle Anwendungen von zahlenmäßigen und grafischen Aufbereitungen nach Analyse von Risikodaten, erhalten Sie erstklassige Entscheidungsplattformen für die Ergreifung und Priorisierung von Risikokontromaßnahmen zur Reduzierung Ihrer „Total Cost of Risk".

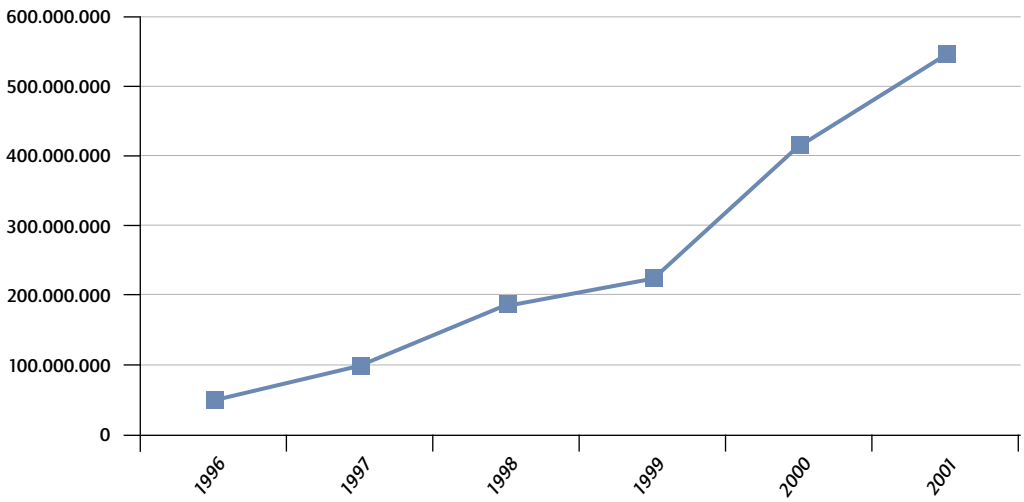
Dabei gilt es, darauf zu achten, dass die auf Ihre Anforderungen und Bedürfnisse individuell zugeschnittene Risikoanalyse stets ein ständiges Update erhält. Die Datenpflege erfolgt entweder direkt in webbasierten Datenbanken mittels benutzerfreundlicher Oberflächen oder über programmierte Links zu Datenquellen bei Versicherern, Schadenregulierern etc.

Mit einer solchen Datenbank entsteht ein flexibles Reporting-Tool, die „Total Cost of Risk" zu bestimmen und zu analysieren, Kostentreiber zu identifizieren sowie Benchmarks oder Prioritäten zur Umsetzung von Risikokontrollmaßnahmen festzusetzen und zu verfolgen. Die nachfolgenden Grafiken zeigen neben der Erhöhung der Internetuser auch den Anstieg der Eintrittswahrscheinlichkeiten bei Risikoereignissen.

Anzahl der eingetretenen Risikoereignisse



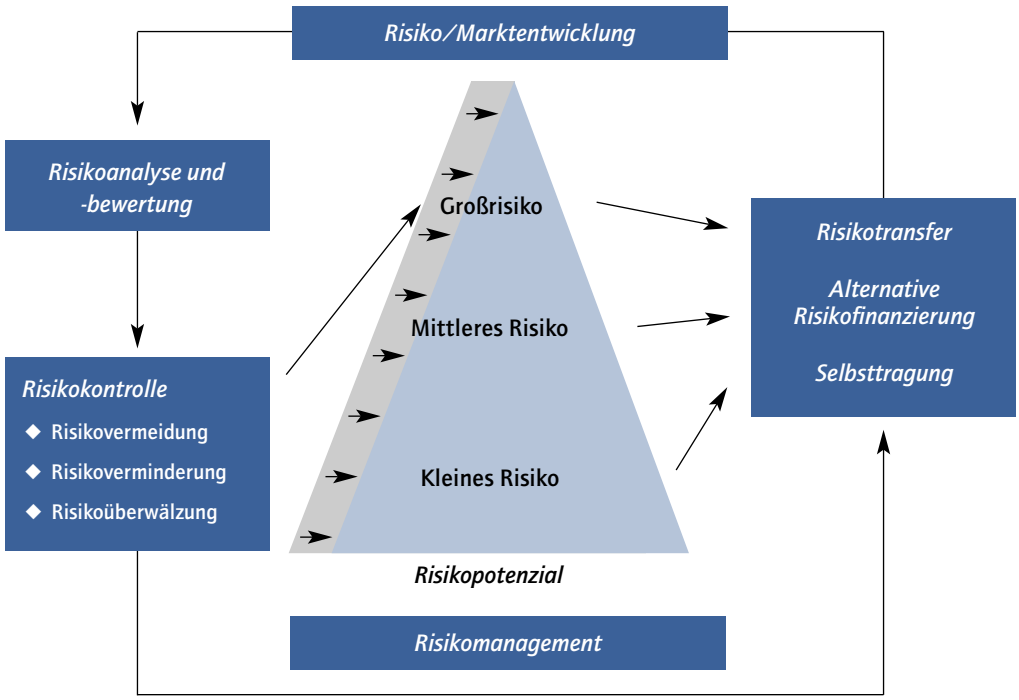
Anzahl der Internetuser



Errichtung eines Risikomanagement- und Überwachungssystems

Eine neuere Studie der KPMG zeigt, dass Unternehmen der T.I.M.E.S – Märkte zu 45 % das Hackerrisiko als größtes Risiko einschätzen. In einer Studie der Meta Group allerdings geht man davon aus, dass 70 % der Bedrohung aufgrund von Missbrauch von Benutzerrechten liegt. Die nachfolgende Darstellung soll die Einschätzungen der Risikopotenziale erleichtern.

Risiko/Marktentwicklung



5. Haftungsrisiken im E-Commerce

von Dr. Ivo Geis

Die Haftungsrisiken im E-Commerce entstehen durch die elektronische Kommunikation und die Präsentation von Inhalten auf der Website. Der deutsche Gesetzgeber hat für die elektronische Kommunikation mit dem Signaturgesetz eine Sicherheitstechnik definiert: die elektronische Signatur. Das rechtliche Risiko der Website-Inhalte wird durch die Verantwortlichkeitsregeln des Teledienstegesetzes bestimmt. Ein Maßstab für die unternehmerischen Pflichten zur Risikominimierung kann aus dem „Gesetz zur Kontrolle und Transparenz im Unternehmensbereich" abgeleitet werden.

5.1 Das Signaturgesetz: Ein Sicherheitsstandard für die elektronische Kommunikation

In der elektronischen Kommunikation können Nachrichten verfälscht und von Unberechtigten abgegeben werden. Die Rechtsrisiken sind die Integrität der Information und die Authentizität des Absenders. Für Absender und Empfänger ist das weltweite Netz als Informationsmedium nur akzeptabel, wenn diese Risiken auf ein Minimum reduziert sind. Die Partner der Kommunikation müssen sich darauf verlassen können, dass die Nachricht den Empfänger unverfälscht erreicht und der Absender für den Empfänger authentisch ist. Diese Sicherheit wird durch die Technik der elektronischen Signatur erreicht. Die elektronische Signatur ersetzt die Unterschrift, die den Unterschreibenden charakterisiert und damit auf seine Authentizität hinweist, durch eine Algorithmenkombination, den Hashwert. Zwei Algorithmen ergänzen sich in einer einmaligen Kombination zu einem Algorithmenpaar: Ein Algorithmus, der geheim bleibt und ein Algorithmus, der öffentlich ist und unter dem der Inhaber des Algorithmus identifiziert werden kann. Dieses Algorithmenpaar wird von einem vertrauenswürdigen Dritten, einem Zertifizierungsdienst, erzeugt und in Form einer Chipkarte dem Inhaber der elektronischen Signatur verliehen. Der öffentliche Algorithmus wird von dem Zertifizierungsdienst in ein öffentliches Schlüsselverzeichnis aufgenommen. Der Empfänger einer elektronisch signierten Nachricht kann den Absender in diesem öffentlichen Schlüsselverzeichnis über seinen öffentlichen Schlüssel identifizieren. Indem der Zertifizierungsdienst dieses öffentliche Verzeichnis zuverlässig verwaltet, kann sich der Empfänger auf die Identität des im öffentlichen Verzeichnis festgestellten Absenders verlassen: es besteht Authentizität der Nachricht. Erfüllen die technischen Komponenten der elektronischen Signatur Sicherheitsstandards, so wird der Inhalt des elektronischen Dokuments geschützt und dies bedeutet Integrität. Dieses „Public Key Infrastructure System" kann durch die Anforderungen an Zertifizierungsdienste und technische Komponenten unterschiedlich ausgestaltet werden. Höchste Anforderungen verlangt das Signaturgesetz für die qualifizierte elektronische Signatur. Das „Gesetz über Rahmenbedingungen für elektronische Signaturen und zur Änderung weiterer Vorschriften" ist am 22. Mai 2001 in Kraft getreten.[1] Dieses Gesetz löst das „Gesetz zur digitalen Signatur" vom 22.7.1997 ab und setzt die Richtlinie des Europäischen Parlaments und des Rates über gemeinschaftliche Rahmenbedingungen für elektronische Signaturen vom 18.11.1999 um.

5.1.1 Die qualifizierte elektronische Signatur

Ziel der Signaturrichtlinie ist es, eine EU-einheitliche Infrastruktur für elektronische Signaturen sicherzustellen, an die konkrete Rechtswirkungen geknüpft sind. Deshalb ist in dem Signaturgesetz eine elektronische Signatur mit Rechtswirkung vorgesehen, die den Anforderungen nach Artikel 5 Abs. 1 Richtlinie entspricht und als „qualifizierte elektronische Signatur" bezeichnet wird.[2] Die qualifizierte elektronische Signatur muss nach § 2 Nr. 2 und Nr. 3 SigG die folgenden Sicherheitsanforderungen erfüllen. Sie muss

[1] *Verkündet im Bundesgesetzblatt vom 21. Mai 2001 Teil I Nr. 22, abrufbar unter der Web Site des Bundeswirtschaftsministeriums www.iukdg.de/Aktuelles.*

[2] *Tettenborn, in: Geis (Hrsg.), Die digitale Signatur, Ziff. 2.2.2.*

- ausschließlich dem Signaturschlüssel-Inhaber zugeordnet sein und damit seine Identifizierung ermöglichen,
- mit Mitteln erstellt werden, die der Signaturschlüssel-Inhaber unter seiner alleinigen Kontrolle halten kann,
- mit den Daten, auf die sie sich bezieht, verknüpft sein, damit eine nachträgliche Veränderung der Daten erkannt werden kann,
- auf einem qualifizierten Zertifikat beruhen, das von einem angemeldeten oder freiwillig akkreditierten Zertifizierungsdiensteanbieter vergeben wird und
- mit einer sicheren Signaturerstellungseinheit erzeugt worden ist.

Nach diesem Qualitätssystem sind qualifizierte Zertifikate nach § 2 Nr. 7 SigG Zertifikate, die die Voraussetzungen des § 7 SigG erfüllen und von Zertifizierungsdienstanbietern ausgestellt werden, die alle Anforderungen des Signaturgesetzes und der künftigen Signaturverordnung erfüllen. „Sichere Signaturerstellungseinheiten" sind nach § 2 Nr. 10 SigG Software- oder Hardwareeinheiten zur Speicherung oder Anwendung des jeweiligen Signaturschlüssels, die für qualifizierte elektronische Signaturen bestimmt sind und die Gesetzesanforderungen erfüllen. Die Schlüsselrolle in dem Signatursystem haben danach die Produzenten und Lieferanten qualifizierter elektronischer Signaturen, die qualifizierten Zertifizierungsdienste.

5.1.2 Qualifizierte Zertifizierungsdienste

Entsprechend den Vorgaben der EG-Signaturrichtlinie sind durch das Signaturgesetz zwei Klassen von Zertifizierungsdiensteanbietern entstanden: angemeldet Zertifizierungsdienste und freiwillig akkreditierte Zertifizierungsdienste.

Die Aufnahme der Tätigkeit als Zertifizierungsdiensteanbieter ist der zuständigen Behörde nach § 66 des Telekommunikationsgesetzes anzuzeigen, § 4 Abs. 3 S.1 SigG. Mit der Anzeige ist schriftlich darzulegen, dass die erforderliche Zuverlässigkeit und Fachkunde vorhanden ist und die übrigen Voraussetzungen für den Betrieb eines Zertifizierungsdienstes nach diesem Gesetz und der Rechtsverordnung nach § 24 SigG vorliegen.[3]

Die freiwillige Akkreditierung nach Art. 3 Abs. 2 EG-Signaturrichtlinie ist ein Angebot an EU-Mitgliedstaaten, die bereits wie Deutschland und Italien die digitale Signatur gesetzlich geregelt haben, ihr bestehendes System als freiwilliges System EU-rechtskonform aufrechtzuerhalten. Von dieser Möglichkeit macht das Signaturgesetz Gebrauch. Auf Antrag können Zertifizierungsdiensteanbieter, die qualifizierte Zertifikate ausstellen, von der zuständigen Behörde akkreditiert werden, § 15 Abs. 1, S. 1 SigG. Die Akkreditierung ist zu erteilen, wenn Zertifizierungsdiensteanbieter vor Aufnahme ihrer Tätigkeit nachweisen, dass die Vorschriften nach diesem Gesetz und der Rechtsverordnung nach § 24 SigG erfüllt sind, § 15 Abs. 1 S. 2 SigG. Akkreditierte Zertifizierungsdiensteanbieter erhalten ein Gütezeichen, § 15 Abs. 1, S. 3 SigG. Mit diesem Gütezeichen wird der Nachweis zum Ausdruck gebracht, dass die technische und administrative Sicherheit für die auf ihren qualifizierten Zertifikaten beruhenden qualifizierten elektronischen Signaturen umfassend geprüft worden ist, § 15 Abs. 1 Nr. 4 SigG. Diese Zertifizierungsdienste dürfen sich als „akkreditierte Zertifizierungsdiensteanbieter" bezeichnen und sich im Rechts- und Geschäftsverkehr auf die nachgewiesene Sicherheit berufen, § 15 Abs. 1, Satz 5 SigG. Durch diese freiwillige Akkreditierung bleibt das Sicherheitsniveau für elektronische Signaturen vollständig erhalten, das durch das Signaturgesetz 1997 entstanden ist.

5.1.3 Vergabe der qualifizierten elektronischen Signatur

Um erstmals ein Signaturschlüssel-Zertifikat zu erhalten, muss sich der Antragsteller gemäß § 5 SigG bei einer Annahmestelle eines qualifizierten Zertifizierungsdienstes mit einem gültigen Personalausweis oder Reisepass ausweisen und

[3] *§ 4 Abs. 2 SigG.*

einen schriftlichen Antrag auf ein Zertifikat stellen. Der Antragsteller muss gegenüber dem Zertifizierungsdienst angeben, ob und inwieweit die Nutzung des Signaturschlüssels beschränkt werden soll. Ein Beispiel hierfür ist das Kreditlimit. Im Zertifikat wird das Kreditlimit und die Bank als Referenzstelle angegeben, die auf Anfrage Auskunft erteilt, ob ein bestimmter Betrag noch gedeckt ist. Dies dient der Schadensbegrenzung, falls Unbefugte in den Besitz der Karte gelangen sollten.

Vertretungsrechte, Vollmachten und berufsrechtliche Zulassungen können in einem zusätzlichen Attribut-Zertifikat bescheinigt werden. Damit können diese Rechte im elektronischen Verkehr nachgewiesen werden. Um Vertretungsrechte für einen Dritten in ein Zertifikat aufzunehmen, müssen diese zuverlässig nachgewiesen sein und muss der Dritte gegenüber dem Zertifizierungsdienst schriftlich oder durch elektronisch signierte Erklärung sein Einverständnis gegeben haben. Damit eine berufsrechtliche oder sonstige Zulassung in ein Zertifikat aufgenommen wird, genügt es, bei dem Zertifizierungsdienst die Zulassungsurkunde vorzulegen.

Die Zertifizierungsdienste sind verpflichtet, den Antragsteller über seine Schutz- und Sicherungspflichten zu informieren, vor allem über den sorgfältigen Umgang mit dem Signaturschlüssel, über den Schutz der Identifikationsdaten, über die Verwendung des Zeitstempels und über die Erneuerung elektronischer Signaturen, § 6 SigG. Der Zertifizierungsdienst nimmt die von ihm ausgestellten Zertifikate in ein öffentliches Zertifikatverzeichnis auf, das online abgefragt werden kann. [4]

Verletzt der Zertifizierungsdiensteanbieter die Vorschriften des Gesetzes oder der Rechtsverordnung, so haftet er gegenüber einem Dritten für den daraus entstehenden Schaden, wenn dieser in redlicher Weise auf die Angaben in dem qualifizierten Zertifikat vertraut hat, § 11 Abs. 1 SigG. Hat der Zertifizierungsdiensteanbieter die Verletzung nicht zu vertreten, so ist die Haftung ausgeschlossen, § 11 Abs. 2 SigG. Um den Schadensersatz sicherzustellen, hat der Zertifizierungsdiensteanbieter eine geeignete Mindestdeckungsvorsorge von 500.000 Deutsche Mark zu treffen, § 12 SigG.

5.2 Das Formgesetz

Mit der EG-Signatur-Richtlinie wird die qualifizierte elektronische Signatur der Unterschrift gleichgestellt, damit im EU-Binnenmarkt Rechtssicherheit für die elektronische Kommunikation entsteht. Diese europarechtliche Anforderung ist durch das „Gesetz zur Anpassung der Formvorschriften des Privatrechts und anderer Vorschriften an den modernen Rechtsgeschäftsverkehr" umgesetzt worden, das am 22. Juni 2001 von Bundestag und Bundesrat verabschiedet worden ist. [5]

5.2.1 Die gesetzliche elektronische Form § 126 Abs. 3 BGB

Die „elektronische Form" ersetzt die gesetzliche Schriftform, wenn sich nicht aus dem Gesetz etwas anderes ergibt. Die gesetzliche elektronische Form wird durch die qualifizierte elektronische Signatur erfüllt, § 126 Abs. 3 BGB. Der Aussteller der elektronischen Form muss dem Text seinen Namen hinzufügen und das elektronische Dokument mit einer qualifizierten elektronischen Signatur nach dem Signaturgesetz versehen, § 126a Abs. 1 BGB. Bei dem Abschluss eines Vertrages müssen die Parteien nach § 126a Abs. 2 BGB ein gleich lautendes Dokument elektronisch signieren. Dies ist nach der Begründung des Formgesetzes zulässig, da in diesem Falle die Beteiligten ausdrücklich oder durch schlüssiges Handeln die elektronische Form als Ersatz für die Schriftform gebilligt haben. [6] Das Formgesetz sieht nach Art. 1 Nr. 7-11 fünf Ausnahmen von dieser Regel vor. Nicht in elektronischer Form können erteilt werden: die Kündigung des Arbeitsvertrages gemäß § 623 BGB, das Zeugnis gemäß § 630 BGB, die Bürgschaftserklärung gemäß § 766 BGB, das Schuldversprechen gemäß § 780 BGB und das Schuldanerkenntnis gemäß § 781 Satz 1 BGB.

[4] *Bieser/Kersten, Elektronisch unterschreiben, S. 49 ff.*
[5] *BGBl. I Nr. 35 vom 18. Juli 2001, s. 1542 ff.*
[6] *Begründung S. 6.*

Für die elektronische Kommunikation zwischen Staat und Bürgern ist die qualifizierte elektronische Signatur eine Bedingung: Die qualifizierte elektronische Signatur wird nach dem „Entwurf des Verwaltungsverfahrensgesetzes" als Ersatz für die gesetzliche Schriftform von Verwaltungsakten verlangt, nach dem „Gesetz zur Senkung der Steuersätze" für den Vorsteuerabzug auf Grund elektronischer Rechnungen, nach der „Sozialversicherungsordnung" für die Archivierung elektronischer Dokumente der gesetzlichen Versicherung, nach der „Verordnung für die Vergabe öffentlicher Aufträge" für das Vergabeverfahren.

Höchste Beweisqualität für elektronische Erklärungen wird durch die qualifizierte elektronische Signatur akkreditierter Zertifizierungsdienste erreicht. Mit dem Gütezeichen der akkreditierten Zertifizierungsdiensteanbieter wird nach § 15 Abs. 1 S. 4 SigG „der Nachweis der umfassend geprüften technischen und administrativen Sicherheit für die auf ihren qualifizierten Zertifikaten beruhenden qualifizierten elektronischen Signaturen zum Ausdruck gebracht". Damit ist die Qualität qualifizierter elektronischer Signaturen akkreditierter Zertifizierungsdienste durch unabhängige Dritte umfassend geprüft, bestätigt und dokumentiert. Sie repräsentieren damit nachgewiesene Sicherheit. Hierauf kann sich ein Gericht in seiner freien Beweiswürdigung beziehen.

Das Formgesetz sieht zu Gunsten des Empfängers einer elektronischen Erklärung eine Vermutungsregel vor. Für den Empfänger spricht nach § 292a ZPO der Anschein der Echtheit einer in elektronischer Form vorliegenden Willenserklärung. Diese Vermutungsregel ist das Risiko des Inhabers einer elektronischen Signatur, wenn sie von Dritten ohne den Willen des Inhabers benutzt wird. Nur in einem Ausnahmefall kann sich der Inhaber der elektronischen Signatur von diesem Risiko befreien: Wenn er Tatsachen vorträgt, die es ernsthaft als möglich erscheinen lassen, dass die Erklärung nicht mit seinem Willen abgegeben worden ist. Mit dem Wort „ernsthaft" ist das Risiko für den Signatur-Inhaber gekennzeichnet. Er sollte sich darauf einstellen, dass er dem Empfänger haftet, wenn er durch fehlerhaftes Verhalten Unberechtigten ermöglicht, seine elektronische Signatur zu nutzen.[7]

5.2.2 Die vereinbarte elektronische Form § 127 Abs. 3 BGB

Ist die Schriftform nicht durch Gesetz vorgeschrieben, so kann die elektronische Form vereinbart werden. In diesem Falle genügt eine andere Signatur als die qualifizierte elektronische Signatur nach dem Signaturgesetz, § 127 Abs. 3 BGB. Dies sind elektronische Signaturen nach § 2 Nr. 1 SigG und fortgeschrittenen elektronische Signaturen nach § 2 Nr. 2 SigG.

Elektronische Signaturen sind Daten in elektronischer Form, die anderen elektronischen Daten beigefügt oder logisch mit ihnen verknüpft sind und die zur Authentifizierung dienen, § 2 Nr. 1 SigG. Diesen Anforderungen wird keinerlei Integritäts- und Authentifizierungsfunktion beigemessen. Der Anwendungsfall der elektronischen Signatur ist das fälschbare Dokument mit der vom Unberechtigten eingescannten Unterschrift.[8] Unter diesen Begriff der elektronischen Signatur fallen auch biometrische Verfahren, die einem Text beigefügt sind. Biometrische Verfahren können sich zu einer Technik der Zugangssicherheit zu elektronischen Signaturen jeder Qualität entwickeln. So könnte die elektronische Signatur statt durch eine PIN durch einen elektronischen Fingerabdruck aktiviert werden, um als elektronische Signatur genutzt werden zu können.

Die fortgeschrittene elektronische Signatur muss nach § 2 Nr. 2 SigG vier Funktionen erfüllen. Sie muss

- ausschließlich dem Signaturschlüssel-Inhaber zugeordnet sein und
- damit seine Identifizierung ermöglichen,
- mit Mitteln erstellt werden, die der Signaturschlüssel-Inhaber unter seiner alleinigen Kontrolle halten kann,

[7] *siehe hierzu die Begründung zu § 292a ZPO S. 52 des Referentenentwurfs.*

[8] *Roßnagel, NJW 2001, 1817, 1819.*

- mit den Daten, auf die sie sich bezieht, verknüpft sein, damit eine nachträgliche Veränderung der Daten erkannt werden kann.

Ein Anwendungsfall ist das Signaturverfahren „Pretty Good Privacy" (PGP), das von unternehmensinternen und unternehmensexternen Zertifizierungsdiensten vergeben wird. Anforderungen an die Sicherheit der organisatorischen Prozesse der Schlüsselverwaltung und der technischen Komponenten bestehen nicht.[9]

Im Ergebnis bedeutet dies, dass die vereinbarte elektronische Form durch elektronische Signaturen ersetzt werden kann, die nicht durch einen qualifizierten Zertifizierungsdienst vergeben und verwaltet werden. Dies ist für die rechtssichere elektronische Kommunikation im E-Commerce wichtig: Es ist nicht notwendig, qualifizierte elektronische Signaturen zu benutzen, sondern es reichen elektronische Signaturen.

Elektronische Signaturen, die nicht die Anforderungen an qualifizierte elektronische Signaturen erfüllen, erreichen nicht deren Beweisqualität. Damit ist die Entscheidung des Gerichts im Rahmen der freien Beweiswürdigung schwer einzuschätzen. Sie ist von der Ordnungsmäßigkeit der Archivierung, der technischen Qualität der elektronischen Signaturen und der Vertrauenswürdigkeit der Zertifizierungsdienste abhängig.

5.3 Rechtsrisiken der Website-Inhalte

5.3.1 Die Web Site als Teledienst

Werden Informationen in einer Web Site zum Abruf bereitgehalten, so ist dies eine eindeutige Situation: Es sind dies elektronische Informations- und Kommunikationsdienste, die für eine individuelle Nutzung mittels Telekommunikation bestimmt sind. Individuell ist die Nutzung, da die Informationen nur durch das Aufrufen der Web Site zugänglich ist. Telekommunikation ist nach der Definition des § 3 Nr. 16 TKG gegeben, da die Nachrichten durch elektromagnetische oder optische Signale, also durch Telekommunikationsanlagen gemäß § 3 Nr. 17 TKG übertragen und empfangen werden. Teledienst durch Telekommunikation ist nicht auf Informationen beschränkt, sondern umfasst gemäß § 2 Abs. 2 Nr. 5 TDG auch das Angebot von Waren und Dienstleistungen.[10] Im Ergebnis ist damit die Web Site als Teledienst zu qualifizieren. Mit dem Teledienst der Web Site wird über Waren und Dienstleistungen informiert und werden Waren und Dienstleistungen zum Downloading bereitgestellt.[11]

5.3.2 Die Verantwortlichkeit für eigene Inhalte

Für eigene Inhalte, die auf der Web Site angeboten werden, wird die Haftung gemäß § 5 Abs. 1 TDG nach allgemeinem Recht begründet. Dies ist damit ein Bereich, der durch das Gewährleistungsrecht und Produkthaftungsrecht geprägt wird. Damit besteht für eigene Inhalte eine uneingeschränkte Verantwortlichkeit. Bei eigenen Inhalten besteht kein Grund für eine Privilegierung. Wer als Diensteanbieter eigene Inhalte anbietet, kann dies in aller Regel kontrollieren, da er sie selbst ausgewählt hat.[12] Damit ist dieser Diensteanbieter auch in vollem Umfang für die Inhalte dieser Dienste verantwortlich: Er haftet also bei falscher Produktinformation nach den Grundsätzen des Produkthaftungsrechts und ist für fehlerhafte Produkte, die er auf der Web Site zur Verfügung stellt, nach dem Gewährleistungsrecht verantwortlich.

5.3.3 Die Verantwortlichkeit für fremde Inhalte

§ 5 Abs. 2 TDG enthält eine Begrenzung der Verantwortlichkeit: Diensteanbieter sind für fremde Inhalte, die sie zur Nutzung bereithalten, nur dann verantwortlich, wenn sie von diesen Inhalten Kenntnis haben und es ihnen technisch möglich und wirtschaftlich zumutbar ist, deren Nutzung zu verhindern. Diese Haftungsbegrenzung privilegiert die „Host-Provider". Für diese ist es aufgrund der gespeicherten Datenmengen unmöglich, alle fremden Inhalte zur Kennt-

[9] *Roßnagel, NJW 2001, 1817, 1819.*
[10] *Siehe zur Definition der Dienstleistung: Koch, CR 1997, 193, 196 f. und Spindler, NJW 1997, 3193, 3195.*
[11] *Spindler, NJW 1997, 3193, 3195.*
[12] *Sieber, Verantwortlichkeit im Internet, S. 140.*

nis zu nehmen und auf ihre Rechtmäßigkeit zu prüfen. Nur wenn sie Kenntnis von diesen Inhalten erlangen und es ihnen wirtschaftlich zumutbar und technisch möglich ist, sind sie verpflichtet, die Nutzung der Inhalte zu verhindern.[13] Diese Verantwortlichkeit ist in dem Urteil des Landgerichts München I in strenger Form interpretiert worden: Hält der Inhaber einer Web Site Chatrooms bereit und werden von den Nutzern in diesen Chatrooms rechtswidrige Inhalte abgeladen, so ist der Inhaber der Web Site für diese Inhalte verantwortlich, wenn er grob fahrlässig keine Kenntnis von den Inhalten hatte.[14] Das entscheidende Ergebnis dieser Rechtsprechung ist: Kenntnis der rechtswidrigen Inhalte im Sinne von § 5 Abs. 2 TDG wird bei grob fahrlässiger Unkenntnis angenommen. Dies entspricht der Vorgabe durch die E-Commerce-Richtlinie und deren Umsetzung durch den Entwurf des „Gesetzes über rechtliche Rahmenbedingungen für den elektronischen Geschäftsverkehr"[15]

Das Zugangverschaffen gemäß § 5 Abs. 3 TDG ist ein Haftungsprivileg. Die Vorschrift schließt die Verantwortlichkeit der Diensteanbieter für fremde Inhalte aus, zu denen sie lediglich den Zugang verschaffen. Suchmaschinen sind der typische Fall für dieses Zugangverschaffen. Die Gründe für diesen Haftungsausschluss der „Access Provider" sind technischer und rechtspolitischer Art. Technisch ist eine Kontrolle der Daten in weltweiten Netzen nicht möglich. Rechtspolitisch ist eine Kontrolle des internationalen Datenverkehrs nicht wünschenswert, denn dies bedeutete die Kontrolle persönlicher Daten, die durch das Datenschutzrecht und das Fernmeldegeheimnis geschützt werden.[16] In der deutschen Rechtsprechung ist das Haftungsprivileg des Zugangverschaffens nur in einem Fall hochgradiger Konzernabhängigkeit angenommen worden.[17] Deshalb muss im Ergebnis davon ausgegangen werden, dass fremde Inhalte die Verantwortlichkeit des Website-Inhabers nach § 5 Abs. 2 TDG begründen.

5.3.4 Die Verantwortlichkeit für Links

Das Internet lebt von Links: Mit dem Hyperlink wird auf eine Homepage verwiesen, der Deeplink zielt unter Umgehung der Homepage direkt auf die Web Site mit der gesuchten Information, der Inlinelink lässt den Nutzer nicht erkennen, dass die Information von einer anderen Web Site stammt.

Der Hyperlink führt nicht zu einem Haftungsprivileg nach § 5 Abs. 3 TDG. Denn der Hyperlink vermittelt nicht „lediglich den Zugang zur Nutzung" im Sinne einer unterschiedslosen und unkontrollierbaren technischen Durchleitung von Daten vergleichbar einer Suchmaschine.[18] Wenn dieses Haftungsprivileg nicht gilt, dann ist der Hyperlink als Bereithalten fremder Inhalte nach § 5 Abs. 2 TDG zu bewerten und ist der verlinkende Website-Inhaber im Falle positiver Kenntnis und grob fahrlässiger Unkenntnis für den rechtswidrigen und fehlerhaften Inhalt verantwortlich.

Bei Deeplinks soll es auf den Eindruck ankommen, der beim durchschnittlichen Nutzer hervorgerufen wird. Ergibt sich aus der Anbieterkennung, dass ein fremder Inhalt bereitgehalten wird, so spricht dies für das Bereithalten fremder Inhalte nach § 5 Abs. 2 TDG.[19]

Der Inlinelink, der den Nutzer nicht erkennen lässt, dass er auf eine andere Web Site weiter verzweigt wird, wird als Bereithalten eines eigenen Inhalts gemäß § 5 Abs. 1 TDG gewertet. Der Inhaber der Web Site macht sich in diesem Falle den fremden Inhalt zu eigen. Er ist damit für diesen Inhalt wie für eigenen Inhalt verantwortlich und haftet für ihn nach allgemeinen Gesetzen.[20]

Die Verantwortlichkeit für die kaskadenartige Entwicklung der Links von Web Site zu Web Site ist eine offene Rechtsfrage. Es soll evident sein, dass für Inhalte, die sich aus der kaskaden-

[13] *Sieber, Verantwortlichkeit im Internet, S. 141.*
[14] *LG München I Urteil vom 30.3.2000, MMR 2000, 431.*
[15] *Der Entwurf ist verfügbar unter http://www iukdg.de.*
[16] *Sieber, Verantwortlichkeit im Internet, S. 142.*
[17] *LG München I Urteil vom 17.11.1999, MMR 2000, 171.*
[18] *So Waldenberger, MMR 1998, 124, 128; Plaß, WRP 2000, 599, 608; Koch, MMR 1999, 704, 706; Spindler, NJW, 1997, 3193, 3198.*
[19] *So Plaß, WRP 2000, 599, 609.*
[20] *So LG Lübeck, U.v.24.11.1998, MMR 1999, 686 = CR 1999, 650 f.; Schack, MMR 2001, 9, 16. Spindler, NJW 1997, 3193, 3197 f.; zum Beleidigungsschutz bei Inlinelinks: LG Hamburg, CR 1998, 565 ff. und die Anmerkung von Bettinger/Freytag, CR 1998 545 ff.*

artigen Entwicklung der Links ergeben, nicht gehaftet werden soll.[21] Mit dem Rechtsgedanken der adäquaten Kausalität könnte die Beschränkung der Verantwortlichkeit für rechtswidrige Inhalte auf die verlinkte Web Site begründet werden.

An dieser Rechtslage wird sich in Zukunft nichts ändern. Die E-Commerce-Richtlinie sieht keine Regelung für Links vor. Damit wird auch die Umsetzung der E-Commerce-Richtlinie durch das „EGG-Gesetz über rechtliche Rahmenbedingungen des elektronischen Geschäftsverkehrs" keine Regelung für die Verantwortlichkeit von Links bieten.[22] Es bleibt damit bei der Verantwortlichkeit für die Inhalte von Links.

Im Ergebnis führt das Linking zur Verantwortlichkeit für den Inhalt. Dieses Risiko kann durch Vereinbarungen zwischen den Inhabern der beiden Web Sites, die verlinkt sind, reduziert werden. Dies bietet sich vor allem in bestehenden gesellschaftsrechtlichen Vertragsbeziehungen, wie Konzernen, an. Bestandteil sollten jedenfalls die folgenden Regeln sein:

- Die Verantwortung für den Inhalt der Links wird von dem Inhaber der verlinkten Web Site getragen.
- Der Inhaber der verlinkten Web Site verpflichtet sich, in regelmäßigen wöchentlichen/monatlichen Abständen den Inhalt auf seine Richtigkeit zu kontrollieren.
- Werden Fehler festgestellt, so werden diese von dem Inhaber der verlinkten Web Site unverzüglich berichtigt.

5.3.5 Ausschluss der Verantwortlichkeit durch Disclaimer

Im Verhältnis vom Web Site-Inhaber zum Nutzer wird versucht, die Haftung durch so genannte „Disclaimer" auszuschließen. Die Grenzen für Disclaimer sind durch die Anforderungen des „Gesetzes über Allgemeine Geschäftsbedingungen" eng gezogen. Eine Orientierung in der Diskussion um den Umgang mit Allgemeinen Geschäftsbedingungen auf der Website bietet jedenfalls der Grundsatz, dass der Nutzer nicht zu benachteiligen ist. Dies verlangt auch das eigene Interesse: Riskante Inhalte, die zu einem Schaden des Nutzers führen, machen die Website uninteressant. Deshalb sollte in dem Disclaimer auf die Mühen um richtige Inhalte hingewiesen werden und auf das spezifische Risiko im Netz, dass sich Inhalte ändern können.

5.4 Fazit: Der Sorgfaltsmaßstab des KonTra-Gesetzes

Das „Gesetz zur Kontrolle und Transparenz im Unternehmensbereich (KonTraG)" vom 27. April 1998[23] verpflichtet den Vorstand einer Aktiengesellschaft, „geeignete Maßnahmen zu treffen, insbesondere ein Überwachungssystem einzurichten, damit den Fortbestand der Gesellschaft gefährdende Entwicklungen früh erkannt werden."[24] Es handelt sich um eine gesetzliche Hervorhebung der allgemeinen Leitungsaufgabe des Vorstandes gemäß § 76 AktG, zu der auch die Organisation gehört. Die Verletzung dieser Organisationspflicht kann zur Schadensersatzpflicht führen, § 93 Abs. 2 AktG. Die konkrete Ausformung der Pflicht ist von Bedingungen, wie der Größe, Branche, Struktur und dem Kapitalmarktzugang des jeweiligen Unternehmens abhängig. Mit der Pflicht des Vorstandes, ein Überwachungssystem einzuführen, korrespondieren die erweiterten Pflichten des Abschlussprüfers. Der Abschlussprüfer ist verpflichtet, diese Maßnahmen zu beurteilen und hierüber dem Aufsichtsrat zu berichten. Dabei hat der Abschlussprüfer zu beurteilen, ob das vom Vorstand einzurichtende Überwachungssystem seine Aufgaben erfüllen kann, § 317 Abs. 4 HGB.[25] Das Ergebnis dieser Prüfung ist in einem besonderen Teil des Prüfungsberichts darzustellen. Hierbei ist darauf einzugehen, ob Maßnahmen erforderlich sind, um das interne Überwachungs-

[21] Schack, MMR 2001, 9, 15; Sieber, MMR-Beil. 2/1999, S. 15, 18.
[22] Bröhl, MMR 2001, 67,71.
[23] BGBl. Teil I S.786-794.
[24] § 91 Abs. 2 AktG eingeführt durch Artikel 1 Nr. 9 KonTraG.
[25] § 317 Abs. 4 HGB eingeführt durch Artikel 2 Nr. 6 KonTraG.
[26] Eingeführt in das HGB durch Artikel 2 Nr. 9 KonTraG.

system zu verbessern, § 321 Abs. 4 HGB.[26] In das GmbH-Gesetz sind entsprechende Regelungen nicht aufgenommen worden. Es wird davon ausgegangen, dass für Gesellschaften mit beschränkter Haftung je nach ihrer Größe, nichts anderes gilt und die Neuregelung Ausstrahlungswirkung auf den Pflichtenrahmen der Geschäftsführer auch anderer Gesellschaftsformen hat.[27] Diese Rechtspflicht, den Fortbestand eines Unternehmens zu sichern, besteht auch für die elektronische Kommunikation eines Unternehmens und seine Präsenz im Internet. Die gegebenen Maßnahmen sind die elektronische Signatur im Interesse der Rechts- und Beweissicherheit der elektronischen Kommunikation und die Kontrolle des Website-Inhalts auf Fehlerlosigkeit und Rechtmäßigkeit. Jedenfalls sind die Verwendung elektronischer Signaturen und ein Qualitätssicherheitssystem für Website-Inhalte Kriterien für die Risikominimierung der Internetpräsenz.

[27] *Begründung des Regierungsentwurfs zu § 91 Abs. 2 AktG in Ernst/Seibert/Stuckert, KonTraG Textausgabe, S. 53.43*

6. Referenten

Herr Jörg Roth absolvierte nach dem ersten juristischen Staatsexamen eine Ausbildung zum Fachjuristen Wirtschaft und Informatik. Anschließend arbeitete er bei zwei führenden EDV-Schulungsunternehmen als EDV-Referent und Schulungsleiter. 1997 machte sich Herr Roth selbstständig und ist seit dieser Zeit Leiter des Unternehmens JRC Training im Bereich IT-Training und Support. Schwerpunkte seiner Tätigkeiten sind die umfassende Integration von Office-Anwendungen, Internet und Back-Office.

Herr Prof. Dr. Thomas Hoeren ist seit April 1997 Universitätsprofessor an der Westfälischen Wilhelms-Universität in Münster. Er hat Rechtswissenschaften an den Universitäten Münster, Tübingen und London studiert und arbeitete nach Staatsexamina, Promotion und Habilitation zunächst an der Heinrich-Heine-Universität in Düsseldorf. Seit April 1996 ist Herr Professor Hoeren auch Richter am OLG Düsseldorf, seit 1998 Mitherausgeber der Zeitschrift „Multimedia und Recht". Er ist Autor zahlreicher Veröffentlichungen, insbesondere in den Gebieten Informations-, Telekommunikations- sowie Medienrecht.

Herr Christoph J. Nießen arbeitete nach dem Studium der Wirtschaftswissenschaften mehrere Jahre als Kundenbetreuer der Abteilung Wohnungswirtschaft der Funk-Gruppe in Berlin. Danach war er Mitarbeiter des Vertriebes in der AON Jauch & Hübener Gruppe in Hamburg. Seit April 2000 ist Herr Nießen Account Manager bei der Marsh GmbH in Hamburg und dort sowohl für nationale als auch für internationale Kunden im Vertrieb zuständig. Außerdem ist er für Verbandsarbeit und Public Relations verantwortlich.

Herr Dr. Ivo Geis ist Rechtsanwalt in der Hamburger Kanzlei Ortner, Geis, Dobinsky und arbeitet speziell im Recht der Informationstechnologie. Er engagiert sich für die Lösung von Rechtsfragen der Informationstechnologie und ist Leiter des Arbeitskreises „Rechtsfragen der digitalen Kommunikation" der Arbeitsgemeinschaft für wirtschaftliche Verwaltung e.V. Herr Dr. Geis ist Vorsitzender der Hamburger Datenschutzgesellschaft und Verfasser zahlreicher Aufsätze zum Thema „elektronische Kommunikation im Geschäftsverkehr".

Bisher erschienen:

Nr.1
M. Rehfeld, N.A. Sittaro, E. Wehking
Psychische Folgeschäden
Ein Problem in der Unfall- und
Haftpflichtversicherung

Nr.2
J. Brollowski, A. Kelb, H. Lemcke, E. Wehking
E+S Rück Fachtagung
Haftpflichtschaden
und Psyche

Erschienen im Februar 2002

Herausgeber:

E+S Rückversicherungs-AG
Karl-Wiechert-Allee 50
30625 Hannover

Tel. 05 11/56 04-0
Fax 05 11/56 04-11 88
www.es-rueck.de

Autoren:
Dr. Ivo Geis
Prof. Dr. Thomas Hoeren
Christoph Nießen
Jörg Roth

Ansprechpartner:
Jörg-Christian Deister
Tel. 05 11/56 04-13 69
joerg-christian.deister@hannover-re.com
oder
Andreas Kelb
Tel. 05 11/56 04-13 00
andreas.kelb@hannover-re.com