Surfen ? - Mit Sicherheit !

Risiken im Internet

Marc Liesching

WEISSER RING
Gemeinnütziger Verein zur Unterstützung von Kriminalitätsopfern und zur Verhütung von Straftaten e.V.

Angaben zur Person des Autors:

Marc Liesching ist Wissenschaftlicher Mitarbeiter am Institut für Strafrecht, Strafprozessrecht und Kriminologie in Erlangen, Vorsitzender Prüfer der Freiwilligen Selbstkontrolle Fernsehen in Berlin und Jugendschutzbeauftragter für Online-Dienste. Er befasst sich seit Jahren in Publikationen und Vorträgen mit Fragen des Medienrechts, insbesondere im Bereich des Straf- und Jugendschutzrechts.

Verantwortlich für den Inhalt:
Marc Liesching

WEISSER RING
Gemeinnütziger Verein zur Unterstützung von Kriminalitätsopfern
und zur Verhütung von Straftaten e.V.

Gestaltung:
OKINOL! GmbH

Herausgeber:
WEISSER RING e.V.
Weberstraße 16
55130 Mainz

Telefon	0 6131/83 03-0
Telefax	0 6131/83 03 45
Info-Telefon	0 18 03/ 34 34 34 (rund um die Uhr)
e-Mail	info@weisser-ring.de
Internet	www.weisser-ring.de

Informationen zur Arbeit des WEISSEN RINGS erhalten Sie auch bei den rund 2.300 ehrenamtlichen MitarbeiterInnen in den bundesweit 400 Außenstellen des gemeinnützigen Vereins.

2. Auflage 2002

Surfen? - Mit Sicherheit!

Hinweise und Ratschläge

Einführung

Das Internet boomt. In den letzten 12 Jahren gewann das bereits Ende der 60er Jahre in den USA als militärisches Projekt entwickelte Kommunikationssystem stetig an Bedeutung und ist heute aus der Medienlandschaft nicht mehr wegzudenken. Allein in Deutschland nutzten schon Ende 2000 mehr als 20 Mio. Menschen das Internet. Die unüberschaubare Vielfalt der mehr als 210 Mio. Online-Angebote weltweit birgt neben den unbestreitbaren Chancen und Nutzungsmöglichkeiten im Dienstleistungs- und Bildungsbereich zugleich erhebliche Gefahren und Risiken, welche sich zum einen aus den technischen Gegebenheiten des weltumspannenden Computernetzes ergeben. Zum anderen aber hat die rasante Fortentwicklung der Informations- und Kommunikationsdienste die bestehende Rechtslage in vielen Bereichen überholt oder zumindest auf den Prüfstand gestellt. Neue Regelungen, mit denen der Gesetzgeber auf die heutige Situation im weiter wachsenden Multimedia-Bereich reagiert hat, sind noch zum Teil wenig bekannt oder haben sich in der Rechtspraxis noch nicht bewehrt. Die folgenden Anmerkungen sollen daher eine erste Hilfestellung geben und Wegweiser sein im Hinblick auf eine sichere und rechtskonforme Nutzung des Internets.

E-Commerce

Wegweiser und Gefahrenhinweise bezüglich Geschäftsabschlüssen im Internet

In zunehmendem Maße wird das Internet als schnelle und oft kostengünstige Möglichkeit des Bezugs von Waren oder der entgeltlichen Inanspruchnahme von Dienstleistungen bis hin zur umfassenden Rechtsberatung genutzt. Allein in Deutschland wird der daraus erzielte Umsatz für das Jahr 2002 auf 94 Mrd. DM geschätzt. Welche rechtlichen Spielregeln hierbei zu gelten haben, wurde bereits in wesentlichen Grundzügen durch Richtlinien des Europäischen Parlaments und des Rates festgelegt, welche der Gesetzgeber zum Teil schon durch das sog. Informations- und Kommunikationsdienste-Gesetz von 1997 in deutsches Recht umgesetzt hat. Entscheidende Fragen des Electronic-Commerce – wie kommt ein verbindlicher Vertrag im Internet zustande? in welchen Fällen ist ein Vertrag unwirksam? oder welche Verbraucherschutzmöglichkeiten existieren? – lassen sich so im Rahmen der allgemeinen bürgerlich-rechtlichen Bestimmungen mit einiger Klarheit und Rechtssicherheit beantworten.

Vertragsabschluss via Internet

Wann kommt ein Vertrag zustande?

Der Abschluss eines Kauf-, Dienst-, oder Werkvertrages setzt nach den Regeln des Bürgerlichen Gesetzbuches zwei inhaltlich übereinstimmende Erklärungen der Vertragsparteien, nämlich ein Angebot und die Annahme dieses Angebotes voraus. Insoweit gilt auch für den Vertragsschluss via Internet nichts anderes. Allerdings stellt die bloße Präsentation von Waren im World Wide Web zu Verkaufszwecken im Regelfall noch kein rechtlich bindendes Vertragsangebot dar, sondern lädt interessierte Besucher der Web-Site lediglich ein, ihrerseits ein Angebot abzugeben. Also kommt auch durch den Vorgang der Bestellung von Waren oder Dienstleistungen (=Angebot) noch kein

wirksamer Vertrag zustande. Erst wenn die – meist auf elektronischem Wege erfolgende – Bestätigung der Bestellung von Seiten des Waren- oder Dienstleistungsanbieters (=Annahme) dem Kunden zugegangen ist, liegt eine rechtlich bindende Vereinbarung zum Kauf, zur Miete, zur entgeltlichen Erbringung von Dienstleistungen etc. vor. Maßgeblich für die Wirksamkeit ist somit der Eingang der Empfangsbestätigung beim Kunden, also der Zeitpunkt, indem der Kunde die Bestätigungs-email abrufen kann. Also Achtung (!): Kommt ein Vertragsangebot oder eine -annahme wegen eines Datenübermittlungsfehlers beim Empfänger gar nicht oder nur als unleserlicher „Datensalat" an, so kann mangels Zugangs der grundsätzlich empfangsbedürftigen Willenserklärungen schon kein Vertrag vorliegen.

In welchen Fällen sind Verträge unwirksam?

Verstoß gegen ein gesetzliches Verbot

Es gibt eine Reihe von gesetzlichen Gründen, in denen Verträge unwirksam bzw. nichtig sein können. So sind nach § 134 des Bürgerlichen Gesetzbuchs Rechtsgeschäfte grundsätzlich nichtig, wenn sie gegen ein (deutsches) gesetzliches Verbot verstoßen. Insbesondere bei E-Commerce-Geschäften über das Internet kommt hier zum einen der illegale Bezug bzw. die Einfuhr pornographischen Materials in Betracht. Zum anderen kann auch die Bestellung von verschreibungspflichtigen Arzneien ohne Rezept wegen Verstoßes gegen das Arzneimittelgesetz zu keinem wirksamen Vertrag mit entsprechenden Diensteanbietern führen. Darüber hinaus sind Verträge auch dann nichtig, wenn sie „gegen die guten Sitten" verstoßen, was vor allem bei Wuchergeschäften der Fall sein kann.

Anfechtung wegen Irrtums

Unterläuft dem Kunden bei dem elektronischen Bestellvorgang ein Eingabefehler, z. B. Tippfehler oder das versehentliche „Anklicken" einer Ware, die der Kunde gar nicht bestellen wollte, so kann er sein derart gar nicht gewolltes (Kauf-)Angebot wegen Erklärungsirrtums anfechten und so alle Vertragsbindungen nichtig machen. Nach der E-Commerce-Richtlinie der EU soll darüber hinaus in allen Mitgliedstaaten durch Gesetze dafür Sorge getragen werden, dass der Diensteanbieter dem Nutzer angemessene, wirksame und zugängliche technische Mittel zur Verfügung stellt, mit denen er Eingabefeh-

ler vor Abgabe der Bestellung erkennen und korrigieren kann (z. B. „virtueller Warenkorb"). Diese Vorgaben wurden nunmehr durch den neuen § 312e Abs. 1 Nr. 1 des Bürgerlichen Gesetzbuchs (BGB) in nationales Recht umgesetzt. Wird erst bei Zugang der Eingangsbestätigung des E-Commerce-Anbieters die irrtümliche Falscheingabe bemerkt, sollte der Kunde zur Wahrung der Anfechtungsfrist unverzüglich, am besten umgehend via email die Bestellung anfechten.

Formmängel

Bei manchen Rechtsgeschäften schreibt das Gesetz die Schriftform vor. Solche Verträge sind also nach der bisherigen Rechtslage nur bei eigenhändiger, handschriftlicher Unterschrift der Parteien gültig. Das lässt sich aber bei einer bloßen Online-Korrespondenz nicht bewerkstelligen, so dass der freie Geschäftsverkehr im Internet in manchen praktisch bedeutsamen Bereichen wie etwa der Zahlungsabwicklung über das Lastschriftverfahren gestört war. Daher wurden im Mai 2001 die Formvorschriften durch Gesetz an den modernen Rechtsgeschäftsverkehr angepasst. Nunmehr kann die schriftliche Form im Regelfall durch eine elektronische Form ersetzt werden, bei welcher der Aussteller der Erklärung seinen Namen hinzufügen und das Dokument mit einer elektronischen Signatur gemäß den Anforderungen des Signaturgesetzes versehen muss. Voraussetzung ist aber, dass die Beteiligten ausdrücklich oder durch schlüssiges Handeln die Anwendung der elektronischen Form billigen und deshalb mit dem Zugang einer elektronischen Willenserklärung rechnen müssen. Bei bestimmten Verträgen, welche für Privatleute schnell zu „Schuldenfallen" werden können (z. B. Bürgschaften, Verbraucherkreditverträge) ist wegen des gebotenen Übereilungsschutzes nach wie vor nur die Schriftform zulässig.

Verbraucher- und Kundenschutz

Allgemeine Geschäftsbedingungen

Die meisten E-Commerce-Anbieter verwenden für ihre Warenkauf- oder Dienstleistungsverträge sog. Allgemeine Geschäftsbedingungen, in denen durch bestimmte Klauseln der Inhalt des Rechtsgeschäfts näher ausgestaltet

wird (z. B. Lieferbedingungen, Eigentumsvorbehalt, Haftungsbeschränkungen). Für eine wirksame Einbeziehung solcher Bedingungen in einen Vertrag ist ein deutlicher Hinweis erforderlich, der von einem Durchschnittskunden auch bei nur flüchtiger Betrachtung nicht übersehen werden kann (vgl. § 305 des BGB neuer Fassung). Dies ist bei Online-Geschäften jedenfalls dann gewährleistet, wenn im Rahmen vorgefertigter Bestellformulare auf die geltenden Geschäftsbedingungen des Anbieters – etwa durch eine Link-Verweisung – hingewiesen wird. Unbedingt ratsam ist die sorgfältige Lektüre solcher Bedingungen, bevor eine Bestellung getätigt wird, da diese regelmäßig Vertragsmodifikationen zuungunsten des Kunden enthalten.

Neues Verbraucherschutzrecht

Das im Juni 2000 verkündete Gesetz über sog. Fernabsatzverträge und die sodann Anfang 2002 erfolgte Eingliederung der Bestimmungen in das Bürgerliche Gesetzbuch regelt den Verbraucherschutz im E-Commerce-Bereich neu. Es gilt insbesondere für Verträge über Lieferungen von Waren oder Dienstleistungen, die zwischen einem Unternehmer und einem Verbraucher (Also keine Online-Auktionen unter Privatleuten!) ausschließlich über Fernkommunikationsmittel wie dem Internet geschlossen werden. Ausgenommen sind aber u. a. Finanzdienstleistungen, Verträge über Lebensmittel und Gegenstände des täglichen Bedarfs sowie Verträge im Rahmen der Unterbringung, Beförderung oder Lieferung von Speisen (vgl. § 312b Abs. 3 BGB). Nach § 312c Abs. 1 BGB ist bereits bei der Vertragsanbahnung der geschäftliche Zweck und die Identität des Unternehmers kenntlich zu machen. Ein Internet-Angebot muss daher Geschäftszweck, wie z.B. Versandverkauf und Identität des Unternehmers, d.h. also die komplette Angabe der Rechtsform und der Adresse enthalten. Darüber hinaus trifft den Anbieter eine umfassende Informationspflicht, etwa hinsichtlich des zusätzlichen Anfalls von Liefer- und Versandkosten sowie Einzelheiten hinsichtlich der Zahlung und der Lieferung oder Erfüllung.

Widerrufsrecht

Nach der Neuregelung im Bürgerlichen Gesetzbuch kann der Verbraucher grundsätzlich jeden Fernabsatzvertrag innerhalb einer Frist von zwei Wochen widerrufen. Der Widerruf muss keine Begründung enthalten, sondern lediglich den Vertrag so bezeichnen, sodass dieser identifiziert werden kann. Er

kann schriftlich, auf einem anderen dauerhaften Datenträger (z. B. email auf den Server eines Online-Providers, so dass diese vom Anbieter jederzeit abrufbar ist) oder durch Rücksendung der Ware erfolgen. Zur Fristwahrung genügt die rechtzeitige Absendung. Die Frist beginnt mit dem Zeitpunkt, in welchem dem Verbraucher eine deutlich gestaltete Belehrung über sein Widerrufsrecht auf einem dauerhaften Datenträger (z. B. Bestellformular auf der Homepage des Anbieters) zur Verfügung gestellt worden ist und der Anbieter darüber hinaus seiner umfassenden Informationspflicht nach § 312c Abs. 2 BGB genüge getan hat. Die Belehrung muss auch den Namen und die Anschrift des Widerrufsempfängers und einen Hinweis auf den Fristbeginn enthalten. Ein Widerrufsrecht besteht allerdings nicht bei Lieferungen von Audio- oder Videoaufzeichnungen oder von Software, wenn die gelieferten Datenträger bereits vom Verbraucher entsiegelt worden sind. Auch bei der Bestellung von Zeitungen, Zeitschriften und Illustrierten über das Internet kann der Verbraucher nicht widerrufen. Im Übrigen erlischt das Widerrufsrecht spätestens sechs Monate nach Vertragsschluss.

Rückgabe der Bestellware

Der Verbraucher ist bei Widerruf der Bestellung grundsätzlich zur Rückgabe der bestellten Lieferware verpflichtet. Die für die Rücksendung anfallenden Kosten und die Gefahr einer Beschädigung oder Zerstörung der Sache hat im Regelfall freilich nicht der Verbraucher sondern der Anbieter zu tragen. Allerdings kann der Unternehmer die regelmäßigen Rücksendungskosten bei Bestellungen bis zu einem Betrag von 40 Euro durch vertragliche Vereinbarung dem Kunden auferlegen. Auch hier lohnt sich also ein genauer Blick in die allgemeinen Geschäfts- und Lieferbedingungen des Anbieters! Hat der Verbraucher die in seinem Besitz befindliche Ware durch eigenes Verschulden schon beschädigt oder durch Benutzung im Wert gemindert, muss er sich dies bei der Rückerstattung seines Kaufpreises anrechnen lassen. Daher sollte mit angelieferter Ware sorgsam umgegangen werden, gerade wenn sie der Kunde nicht behalten will und gegebenenfalls nach Widerruf an den Verkäufer zurücksenden muss.

Besonderheiten bei Online-Auktionen

Wegen der oft sehr kostengünstig zu erzielenden Schnäppchen erfreuen sich sog. Online- Auktionen großer Beliebtheit. Es gibt bereits eine Reihe von professionellen Auktionatoren, die auf eigene Rechnung handeln oder die im Wege der Kommission Ware für Dritte im eigenen Namen, aber für fremde Rechnung anbieten und dafür eine Provision erhalten. Darüber hinaus können aber auch Privatleute untereinander ihre gebrauchten Gegenstände auf einer gemeinsamen Plattform zur Versteigerung bringen. Der Auktionator betätigt sich hier lediglich als Vermittler zwischen Wareninhaber und Interessenten.

Wann kommt ein Vertrag zustande?

Wem bei einer Versteigerung im Internet die Ware zugesprochen wird, der muss sie auch abnehmen. Mit dem Zuschlag kommt ein rechtlich verbindlicher Vertrag zwischen dem Anbieter und dem Kunden zustande, aus dem auf Zahlung des Kaufpreises geklagt werden kann. Schon in der Freischaltung der Seite mit der entsprechenden Präsentation einer Ware liegt eine rechtsverbindliches Kaufofferte des Anbieters, so dass dieser auch bei einem sehr niederen Zuschlagspreis zur Übereignung der ersteigerten Kaufsache an den Meistbietenden verpflichtet ist. Dies hat der Bundesgerichtshof in seiner Entscheidung vom 7. November 2001 bestätigt. Eine Anfechtung der Angebotserklärung kommt nicht in Betracht!

Widerrufsrecht der Auktionskunden?

Auktionsteilnehmer, die eine bestimmte Sache ersteigert haben, können grundsätzlich das dadurch zustande gekommene rechtlich bindende Geschäft nicht widerrufen! Bei privaten Auktionen fehlt es bereits an dem für das Widerrufsrecht typischen Unternehmer-Verbraucher-Verhältnis. Doch auch bei Versteigerungen professioneller Auktionatoren ist ein Widerruf wegen einer Ausnahmeklausel in § 312d des BGB neuer Fassung nicht möglich. Daher ist bei der vermeintlich lockeren Auktionsatmosphäre Vorsicht geboten: Jedes Mitbieten kann den Abschluss eines zahlungsverpflichtenden Vertrages bedeuten, von dem man nicht mehr ohne weiteres loskommt!

Geldgeschäfte

Im E-Commerce-Geschäft ist die Hauptangst der Verbraucher, dass persönliche Daten und Konto- oder Kreditkarten-Informationen im Zahlungsverkehr an nicht autorisierte Stellen fallen, welche damit persönlichen oder finanziellen Schaden anrichten können. 80 % der deutschen Online-Nutzer ziehen daher beim Internet-Shopping klassische Zahlungswege der Kreditkartenbenutzung vor. Auch nur jeder neunte Deutsche nutzt die Möglichkeit des sog. Online-Bankings.

Zahlungsmöglichkeiten

Klassische Zahlungswege

Die traditionellen Verfahren wie Nachnahme oder Lieferung gegen Rechnung werden von den meisten Online-Kunden bevorzugt. Dies liegt vor allem daran, dass die Ware erst bei oder nach Erhalt bezahlt werden muss. Des weiteren ist der Besteller auch nicht gezwungen, über seine Lieferanschrift hinaus weitere persönliche Daten wie Kreditkarten- oder Kontonummern im Internet preiszugeben. Damit sind die klassischen Zahlungsmethoden wohl die derzeit sichersten im E-Commerce-Bereich. Ein Nachteil ist aber, dass sie sich nicht bei kleineren Geldbeträgen (sog. Micropayments) rentieren. Zudem bieten Händler nicht immer diese herkömmlichen Bezahlungsoptionen an, weil sie bei diesen zunächst in Vorleistung treten müssen und damit das Risiko der Zahlungsunfähigkeit bzw. -unwilligkeit des Online-Kunden tragen. Daher wird bei einigen Angeboten im WWW Vorausbezahlung durch Überweisung verlangt. Darauf sollte man sich allerdings nur dann einlassen, wenn gesicherte Informationen über die Seriosität des Anbieters vorliegen. Mehrfach sind Betrugsfälle in diesem Bereich bekannt geworden, weshalb die unten bei Punkt 5. gegebenen Warnhinweise unbedingt Beachtung finden sollten!

Bezahlung mit Kreditkarte

Bei kreditkartenbasierten Zahlungssystemen wird die Ware über die Kreditkarte abgerechnet. Dazu muss der Kunde neben seinen persönlichen Daten zumeist nur die Kartennummer und das Gültigkeitsdatum eingeben. Der

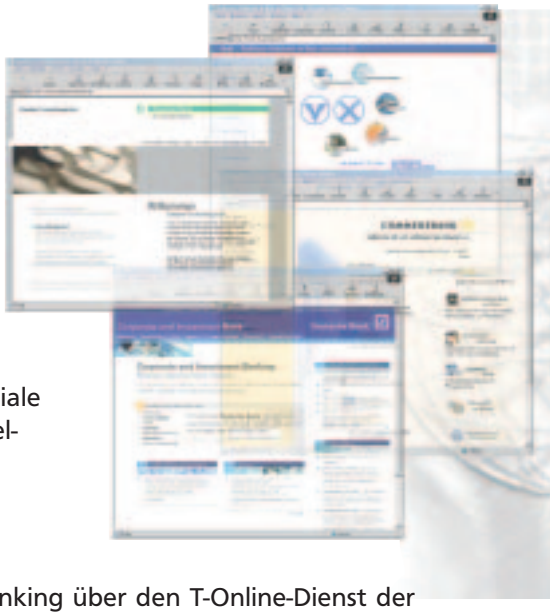
Händler kann das dann einfach akzeptieren oder zusätzlich über eine sog. Clearingstelle abfragen, ob das Kundenkonto überhaupt gedeckt ist. Aufgrund der großen Verbreitung von Kreditkarten verlassen sich auch die meisten Online-Shops auf dieses weltweit verfügbare Zahlungsverfahren. Durch das von Kreditkartenfirmen und Computerunternehmen entwickelte sog. SET (Secure Electronic Transaction) - Verfahren kann sichergestellt werden, dass die gesamte Übermittlung der relevanten Daten verschlüsselt und für Dritte nicht lesbar erfolgen kann. Dennoch werden Kreditkarten-Informationen immer wieder von unberechtigten Dritten ausgespäht und missbraucht. Die aktuelle Rechtslage schützt den Kunden jedoch weitgehend vor Missbrauchsschäden, da die Kreditbank die Beweislast für die tatsächliche Weisung des berechtigten Kartenbesitzers trägt und daher im Regelfall das zu Unrecht beim Kunden eingezogene Geld zurückzahlen muss. Stellt man also bei Überprüfung der Kreditkarten-Abrechnung Unregelmäßigkeiten bzw. tatsächlich nicht veranlasste Einziehungen fest, sollte der Bank möglichst bald nach Erhalt der Abrechnung mitgeteilt werden, dass der Abbuchung mangels berechtigter Anweisung widersprochen wird, da diese von unbefugter Seite veranlasst worden sein muss. Diese Mitteilung kann zunächst mündlich erfolgen, sollte jedoch zusätzlich schriftlich eingereicht werden. Die Bank wird dann den Anbieter bzw. Verkäufer auffordern, die beim Kauf getätigte Legitimation nachzuweisen, also beispielsweise den Kartenbeleg einzusenden. Vermag er das nicht, muss die Bank das Geld an Sie zurück überweisen.

Damit trägt der Verbraucher also auch bei Bezahlung mit Kreditkarte ein noch kalkulierbares, geringes Risiko. Aber Vorsicht: Auch der über seine Kontodeckung hinaus zahlende Karteninhaber kann sich bei Schädigung des Kartenausstellers sogar strafbar machen!

Weitere Zahlungsmöglichkeiten

Eine weitere Zahlungsmodalität ist die dem Geldkartensystem ähnliche sog. elektronische Geldbörse. Der Kunde muss dabei zunächst seine Geldbörse auffüllen, bevor er etwas kaufen kann. Das Auffüllen muss freilich über eine der genannten Zahlungswege erfolgen. Auf dem gleichen Grundmuster basiert die von einzelnen Banken entwickelte Möglichkeit des Bezahlens mit digitalem Geld (z. B. eCash, Cybercash). Bei diesem Verfahren werden Transaktionen über eine Art Ersatzwährung abgewickelt, die nur von autorisierten Firmen in echtes Geld umgetauscht werden kann. Der User kauft hier „elektronische Münzen“ und kann mit diesem virtuellen Geld einkaufen.

Auch wenn diese Methode einen sicheren Zahlungsverkehr gewährleistet, hat sie sich bisher im E-Commerce wegen mangelnder Akzeptanz der Kunden und zu geringem Angebot durch Unternehmer bei weitem noch nicht durchgesetzt.



Online-Banking

Die Vorteile des auch als „Homebanking" bezeichneten Online-Bankings liegen auf der Hand: Direkte Erledigung aller Bank- und Finanzgeschäfte von zu hause bzw. vom Arbeitsplatz, also ohne eine Filiale aufsuchen zu müssen. – Und dies zu regelmäßig kostengünstigen Optionen.

Zwei Verfahren

Die klassische Methode ist das Onlinebanking über den T-Online-Dienst der Deutschen Telekom, über den die meisten Banken ihren Service auch heute noch anbieten. Voraussetzung für eine Nutzung ist neben PC und Modem bzw. ISDN-Karte, dass der Nutzer auch Kunde der Telekom ist und darüber hinaus bei seiner Bank das sog. BTX-Konto freischalten lässt.
Eine zweite Möglichkeit des Online-Bankings ist die (direkte) Abwicklung im Internet, sog. Netbanking. Allerdings gestaltet sich hier das Tätigen von Bankgeschäften wesentlich schwieriger, da der Service aufgrund technischer Gegebenheiten (z. B. Verwenden von sog. Java Appletts) nicht so ausgereift ist wie bei dem T-Online-Verfahren. Zudem müssen bestimmte Hardware-Voraussetzungen (z. B. IBM-Kompatibilität) erfüllt sein.

Wie sicher ist Online-Banking?

Beim T-Online-Verfahren erhält jeder Banking-Kunde eine Zugangsnummer für T-Online, ein dazugehöriges Passwort sowie eine Persönliche Identifikations-Nummer (PIN). Ebenso wie bei der EC-Karten-Geheimnummer ist es unbedingt ratsam, die Daten keiner dritten Person weiterzugeben. Versucht ein Unbefugter über seinen T-Online-Anschluss und mit dem Wissen einer

fremden Kontonummer die PIN durch mehrmalige Eingabe zu erraten, sperrt der Rechner das Online-Konto bei der dritten Falscheingabe. Als weitere Sicherheitsbarriere werden bei jeder kontobelastenden Aktion des Kunden einmalige Transaktionsnummern (TAN) verwandt, welche diesem zuvor von der Bank in einer Liste übersendet werden. Damit ist das T-Online-Banking die derzeit sicherste Form, Bankgeschäfte direkt über die Datenautobahn zu tätigen. Allerdings sei nochmals nachdrücklich darauf hingewiesen: Die persönlichen Zugangsdaten sollten unbedingt geheimgehalten werden. Insbesondere ist von einer Speicherung der Codes auf dem eigenen PC-Rechner abzuraten, um ungebetenen „Gästen" kein allzu leichtes Spiel zu gewähren.

Auch bei Netbanking wird ein Schutzsystem mit PINs und TANs verwandt. Allerdings stellt das Internet gegenüber dem T-Online-System wegen seiner dezentralen Struktur und der globalen Vernetzung einen höheren, da nicht hinreichend kalkulierbaren Risikofaktor dar.

Power-Shopping

Eine besondere Form des Online-Vertriebs von Waren stellt die Möglichkeit der Kunden dar, virtuelle Einkaufsgemeinschaften zu bilden, bei denen mit steigender Zahl der Käufer bzw. der nachgefragten Stückzahl der Kaufpreis nach festgelegten Stufen sinkt. So kann die „Shopping Community" durch Nachfragesteigerung den Ausgangskaufpreis einer angebotenen Ware erheblich mindern. Allerdings verstieß diese Vertriebsform gegen das bis vor kurzem geltende deutsche Rabattgesetz und war deshalb jedenfalls unzulässig. Doch auch nun ist die Rechtslage unklar, da im Falle des „Power Shopping" auch ein Verstoß gegen Wettbewerbsvorschriften in Betracht kommt. Daher ist zumindest bezüglich des Geschäftsverkehrs mit deutschen Anbietern, für die die einschlägigen nationalen gesetzlichen Bestimmungen gelten, eine Beteiligung an virtuellen Einkaufsgemeinschaften nicht ratsam, da es an einer rechtlichen Grundlage für die getätigten Kaufgeschäfte fehlen kann.

Vorsicht vor Betrug und Missbrauch! – Warnhinweise

Aufgrund der Anonymität des Geschäftsverkehrs im Internet ist ein hundertprozentiger Schutz vor Missbrauch und Betrug durch einzelne Anbieter kaum möglich. Um so dringender ist auf bestimmte Sicherheitsvorkehrungen hinzuweisen und um so genauer muss der E-Commerce-Kunde bestimmte Warnsignale wahrnehmen und beachten!

Angaben des Anbieters

In erster Linie sollte beim Online-Einkauf darauf geachtet werden, dass der Anbieter seiner umfassenden Pflicht zur Angabe des geschäftlichen Zweckes und die Identität des Unternehmens nachkommt. Insbesondere sollte sich der Kunde vor der Tätigung einer Bestellung vergewissern, an wen er sich im Falle einer Nicht-, Fehl- oder Schlechtlieferung oder im Falle eines Widerrufs der Bestellung wenden kann. Nicht ausreichend ist dabei die bloße Angabe einer email-Kontaktadresse auf der Homepage des Anbieters. Nur die genaue Anschrift sowie die eingeräumte Möglichkeit telefonischer Rückfragen gewährt hinreichende Sicherheit für die Wahrung späterer Rechte und bürgt für eine gewisse Seriosität des Unternehmens. Wer ganz sicher gehen will, sollte sich vor der Online-Bestellung auf anderem Wege über den Anbieter kundig machen (z. B. Berichte Dritter über den Anbieter, telefonische Nachfrage, Bekanntheit des Unternehmens).

Zahlung per Vorauskasse

Bietet das Shopping-Unternehmen lediglich die Möglichkeit der Vorauszahlung durch Überweisung an, muss dies noch nicht bedeuten, dass der Kunde über den Tisch gezogen wird. Allerdings sind vereinzelt Betrugsfälle publik geworden, in denen der Anbieter von vornherein ohne die Absicht der tatsächlichen Auslieferung Waren bzw. Dienstleistungen angeboten und die

gutgläubige Kundschaft um den vorausbezahlten Kaufpreisbetrag „geprellt“ hat. Daher lohnt sich ein vergleichender Blick mit Hilfe sog. Suchmaschinen, ob nicht gegebenenfalls andere Online-Anbieter das gleiche Produkt zu günstigeren Zahlungsmodalitäten feilbieten. Ist man indes zur Zahlung per Vorauskasse bereit, gilt die eingangs genannte Obliegenheit in besonderem Maße: Vorab umfassende Informationen über den Anbieter einholen! Zum Zahlungsmissbrauch durch sog. „0190-Nummern“ siehe Seite 18.

Warnhinweise in Geschäftsbedingungen

Üblicherweise werden auch beim Geschäftsverkehr im Internet allgemeine Geschäftsbedingungen verwandt, die einzelne Konditionen der Lieferung, Bestellung, Kostentragung oder Haftung behandeln und in den Kauf- oder Dienstleistungsvertrag mit einbezogen werden. Fehlen solche Bedingungen ganz, kann dies ein erster Warnhinweis für fehlende Seriosität des Anbieters sein. Denn: wer auf die Ausbedingung bestimmter Haftungs- und Lieferungsmodalitäten verzichtet, hat möglicherweise gar nicht die Absicht, zu liefern! Sind Geschäftsbedingungen seitens des Unternehmers vorhanden, sind diese genau zu studieren. Finden sich darin nämlich Klauseln, welche den bestellenden Kunden in unverhältnismäßiger oder gar ungesetzlicher Weise übervorteilen (z. B. „vollständiger Haftungsausschluss“, „kein Anspruch auf Lieferung“, „Widerruf und Rückgewähr ausgeschlossen“), sollte von einer Bestellung in jedem Fall abgesehen werden, auch wenn sich der Unternehmer im Konfliktfall auf die Klauseln aus rechtlichen Gründen nicht berufen könnte.

Ausländische Anbieter

Die Bestellung von Waren bei ausländischen Anbietern erhöht die Risiken des Missbrauchs und des Betrugs im Bereich des Geschäftsverkehrs. Zunächst ist die rechtliche Grundlage, auf der Käufe oder Dienstverträge getätigt werden, nicht auf den ersten Blick klar, da nach dem sog. Herkunftslandsprinzip deutsches Recht zumeist nicht zur Anwendung gelangen wird. Bieten die den E-Commerce betreffenden Richtlinien der Europäischen Gemeinschaft auch eine Gewähr dafür, dass innerhalb der EU ein Verbraucher- und Kundenschutz in vergleichbarem Umfange gewährt wird, so ist dessen praktische Durchsetzung schwieriger. Letzteres gilt erst recht für Geschäfte mit Anbietern aus nichteuropäischen Staaten. Daher kann sich gegebenenfalls ein vergleichender Blick auf inländische Angebote lohnen.

Unzulässige Daten-Manipulationen

Viren und sog „Trojaner“

Spätestens seit der verheerenden Ausbreitung des Virus „I Love You“ dürfte den meisten Internet-Nutzern die Gefahr der Veränderung und Vernichtung eigener Daten durch sog. Viren, Makroviren oder „Würmern“ bekannt sein. Diese gelangen zumeist durch unkontrolliertes Öffnen von Mails mit Anhängen in Form von Programmen bzw. Word- oder Excel-Dokumenten auf den eigenen Datenrechner. Auch CD´s, Disketten oder andere Datenträger können Viren enthalten. Eine besonders „heimtückische“ Sonderform sind sog. „Trojanische Pferde“. Das sind Programme, die eine schädliche Funktion beinhalten (z. B. gezieltes Ausspähen von persönlichen Daten), sich aber hinter einem durchaus brauchbaren Programm verbergen. Wird das Programm installiert, kann es oft Monate dauern, bis ein Anwender bemerkt, dass sich schädliches Programm auf seinem System befindet.

Wirksamer Schutz vor Viren?

Da Viren lediglich von außen und fast immer durch (unbewusste) Mithilfe des Nutzers auf den eigenen PC gelangen, sind einige Schutzmaßnahmen möglich und für einen sicheren Datenverkehr auch erforderlich. Allerdings kann ein nahezu hundertprozentiger Schutz nur dadurch erreicht werden, dass man überhaupt keine neuen Programme oder Daten auf den Rechner gelangen lässt. Zunächst sollte jeder Anwender auf seinem Rechner einen Virenscanner installiert haben und diesen mit aktuellen Signaturen „updaten", um Virenprogramme frühzeitig zu erkennen und Schäden zu vermeiden. Im übrigen ist es ratsam, keine Anhänge aus unbekannten Quellen zu öffnen und nicht identifizierbare e-Mails am besten bereits auf dem Server zu löschen. Beim Herunterladen von Software – etwa aus dem Internet – ist Vorabinformation über die Seriosität der Quelle empfehlenswert. Schließlich sollte beim Empfang von Excel- und Worddokumenten darauf geachtet werden, dass diese mit einem nicht makrofähigen Viewer geöffnet werden.

Wirksamer Schutz vor Trojanern?

Im Grunde gelten hier die selben Schutzhinweise wie bei Viren. Allerdings können nicht alle Virenscanner Trojaner erkennen oder sind hierzu nur in begrenztem Umfang in der Lage. Empfehlenswert sind indes die Anti-Viren-Programme „AntiViralToolkitPro" (AVP), zu finden unter: http://www.avp.at, oder „Mc Afee", zu finden unter: http://www.nai.com. Darüber hinaus können sog. „Anti-Trojaner-Programme", welche während Online-Sitzungen aktiviert sind, Infizierungen mit diesen ungebetenen „Haustieren" sehr oft verhindern. Ob sich auf dem eigenen PC bereits ein Trojanisches Pferd befindet, kann anhand folgender Anomalien erkannt werden: Wird Windows während einer Arbeitssitzung einfach beendet oder heruntergefahren, ist die Taskleiste plötzlich nicht mehr sichtbar, sind die Maustasten plötzlich vertauscht, verändern sich die Farben des Systems, schließt sich das CD-Laufwerk von allein, oder finden während einer Online-Sitzung unmotivierte Übertragungen statt, ohne dass neue Seiten geladen werden, dann besteht der dringende Verdacht einer Infektion mit einem Trojaner. Weitere Informationen sind etwa unter http://www.trojaner-info.de erhältlich.

Sogenannte „0190-Dialer“

Neben den bereits dargestellten Zahlungsmöglichkeiten kann der Kunde auch anonym per Telefonabrechnung bezahlen, indem die Online-Verbindung über eine 0190-Servicenummer aufgebaut wird. Hierfür werden dem Interessenten sog. Dialer zum Download und zur Installation angeboten.

Besondere Missbrauchsgefahr

Beim Herunterladen des Dialers besteht die bereits oben im allgemeinen erläuterte Gefahr, sich einen „Virus“ oder ein „Trojanisches Pferd“ einzufangen. Daneben legen aber auch einige Dialer-Programme entsprechende Eintragungen im System an. Diese Eintragungen bewirken den automatischen Start einer 0190-Verbindung bei jedem Neustart des Windows-Systems. Eine weitere Missbrauchsvariante besteht darin, dass die ohnehin neu angelegte DFÜ (Datenfernübertragung)-Verbindung als Standardverbindung definiert wird. Gibt der User eine Internetadresse in seinen Browser ein, so schaltet sich die definierte DFÜ-Verbindung zwischen, so dass während der gesamten Internet-Sitzungen eine 0190-Verbindung besteht. Zuweilen verschweigen einige Anbieter auch bewusst die entstehenden Kosten bei der Präsentation Ihrer Waren und Dienstleistungen und geben lediglich vor, dass es sich bei dem herunterzuladenden Dialer-Programm nur um eine zusätzliche Software handele, die zur Nutzung des Angebots erforderlich sei.

Ist Schutz gegen 0190-Abrechnungen möglich?

Grundsätzlich ist wegen der gerade erläuterten hohen Missbrauchsgefahr eine Zahlung über das Dialersystem nicht empfehlenswert, so dass bei fehlenden Zahlungsalternativen auf die Wahrnehmung entsprechender Angebote verzichtet werden sollte. Allerdings ist auch denkbar, dass sich beim Besuch einer Web-Site ein Dialer-Programm selbständig auf dem heimischen PC installiert. Daher bietet sich zur Gewährleistung eines hundertprozentigen Schutzes eine komplette Sperrung aller 0190-Verbindungen durch die Telefongesellschaft an. Die Deutsche Telekom offeriert gegen eine einmalige Gebühr seinen Kunden, die Einwahl zu 0190-Diensten von einem Anschluss aus komplett sperren zu lassen. Weitere Informationen zum Thema „0190-Nummern“ lassen sich unter http://www.livetraum-exchange.de/dialer finden.

Rechtswidrige Inhalte im Internet

Mehr als nur ein Randbereich im Internet ist die Verbreitung illegaler Inhalte wie insbesondere Pornographie und Gewaltdarstellungen. Sie stellt neben rechts- bzw. linksextremistischen Online-Angeboten die größte Gefahr für Kinder und Jugendliche dar und nimmt sowohl Eltern als auch andere erwachsene Anwender im Hinblick auf eine sichere Nutzung in die Pflicht. Daneben hat jeder User in sog. „Community-Bereichen" wie Chats oder Foren die Bestimmungen der allgemeinen Äußerungsdelikte zu beachten.

Pornographie und Gewalt im Internet

Sexualität beinhaltende Angebote

Das Strafgesetzbuch verbietet das „Zugänglichmachen" von pornographischen Inhalten an Kinder und Jugendliche. Da im WWW grundsätzlich jeder Zugriff auf bereitgehaltene Dienste hat, ist also das unverschlüsselte bzw. uncodierte Anbieten sexueller Darstellungen mit Pornographiecharakter unzulässig und mit Strafe bedroht. Selbst Zugangsbeschränkungen wie „Adult Check" oder „X-Check" werden von den Strafverfolgungsbehörden bislang nicht als ausreichend angesehen, um die Strafdrohung abzuwenden.

Allerdings ist nicht jede erotographische Darstellung schon Pornographie. Solche liegt nach der Rechtsprechung erst dann vor, wenn das Sexuelle grob aufdringlich und anreisserisch in den Vordergrund gerückt wird. Der Nutzer bzw. Betrachter solcher Angebote macht sich grundsätzlich nicht strafbar. Allerdings ist die Rechtslage und insbesondere die Praxis der Staatsanwaltschaften noch unklar. Denn § 184 Abs. 1 Nr. 4 Strafgesetzbuch verbietet die Einfuhr pornographischen Materials im Wege des Versandhandels. Ob hierunter auch der private Endverbraucher fällt, ist umstritten. Jedenfalls muss derjenige, der einschlägiges Material (z. B. Videokassetten) online aus dem Ausland bestellt, unter Umständen damit rechnen, unerwartete Bekanntschaft mit dem örtlich zuständigen Staatsanwalt zu machen.

Generell verboten ist darüber hinaus die sog. „harte Pornographie", also solche, welche Gewalttätigkeiten, den sexuellen Missbrauch von Kindern oder sexuelle Handlungen von Menschen mit Tieren (Sodomie) zum Gegenstand haben. Im Falle der Kinderpornographie ist bereits der Besitz (Herunterladen auf den eigenen Rechner) strafbar. Finden Anwender im Internet derartige Inhalte, oder besteht lediglich der Verdacht, solche Darstellungen bei weiterer Recherche zu finden, sollten unverzüglich die Strafverfolgungsbehörden, das Bundeskriminalamt (info@bka.de) oder die länderübergreifende Kontrollstelle „jugendschutz.net" (info@jugendschutz.net) informiert werden.

Gewalt beinhaltende Angebote

Nicht nur das Verbreiten an Minderjährige, sondern vielmehr jedes Zugänglichmachen von Gewaltdarstellungen im Sinne des § 131 Strafgesetzbuch ist verboten. Davon werden aber nur sehr wenige, extreme Medieninhalte erfasst, welche grausame oder sonst unmenschliche Gewalttätigkeiten gegen Menschen in einer Art schildern, die eine Verherrlichung oder Verharmlosung solcher Gewalttätigkeiten ausdrückt oder die das Grausame oder Unmenschliche des Vorgangs in einer die Menschenwürde verletzenden Weise darstellt. Aber auch unterhalb dieser Schwelle liegende gewaltbeinhaltende Online-Angebote können nach dem Gesetz über die Verbreitung jugendgefährdender Schriften und Medieninhalte unzulässig sein, insbesondere wenn sie auf dem Index stehen. Vor allem bei Online-Auktionen werden von privater Seite zuweilen indizierte Medien (z. B. Horrorvideos) zum Kauf angeboten. Dies ist stets strafbar, und zwar auch dann, wenn der private Anbieter von der Indizierung gar nichts wusste, sich aber hätte informieren können und müssen!

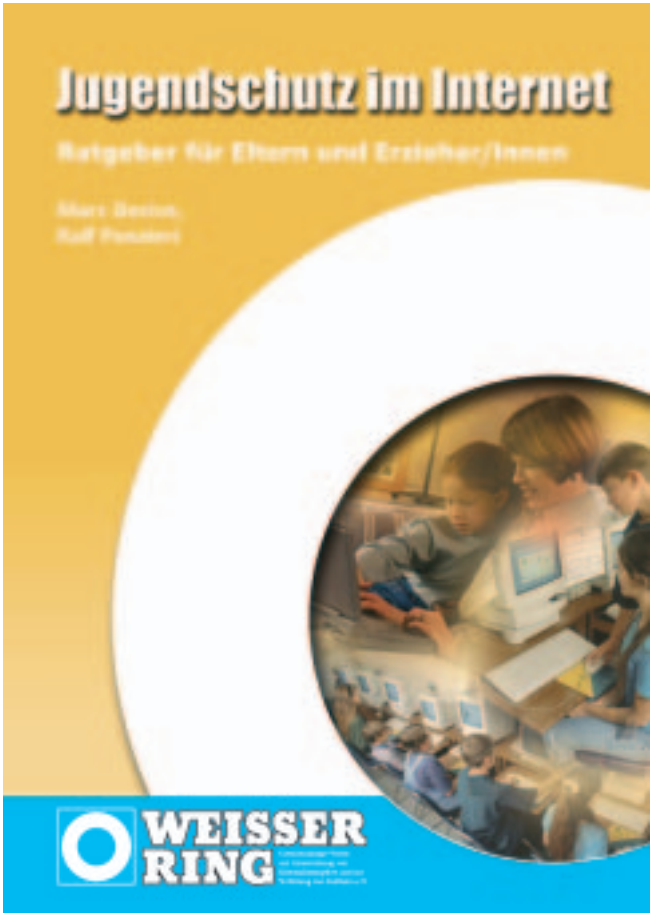
Extremistische Online-Angebote

Nach Schätzungen des Bundesamtes für Verfassungsschutz ist die Zahl der von deutschen Rechtsextremisten betriebenen Homepages von 1999 insgesamt 330 auf ca. 800 im März 2000 angestiegen. In geringerem Umfange sind auch linksextremistische Bestrebungen im Internet beobachtbar. Das WWW dient den einschlägigen Kreisen als Forum für Aufrufe zur Gewalt, die Verbreitung sog. „Todeslisten" mit den persönlichen Daten Andersdenkender sowie die Störung demokratischer Diskussionsforen im Internet. Strafbar ist darüber hinaus das Verbreiten von Propagandamitteln verfassungswidriger Organisationen, wovon die Rechtsprechung allerdings in kaum nachvollziehbarer Weise vorkonstitutionelle Schriften (das sind solche, die vor Gründung der BRD verfasst wurden) wie Hitlers „Mein Kampf" ausklammert. Indes ist das öffentliche Verwenden (im Internet) verfassungsfeindlicher Kennzeichen wie etwa das Hakenkreuz oder Grußformen wie „Heil Hitler" bei Strafe verboten. Eine Ausnahme gilt für die Berichterstattung über Zeitgeschehen, die staatsbürgerliche Aufklärung über geschichtliche Vorgänge oder ähnliche Zwecke.

Schließlich kann wegen Volksverhetzung bestraft werden, wer zum Hass gegen Bevölkerungsteile aufstachelt, zu Gewalt- oder Willkürmaßnahmen gegen sie auffordert oder die Menschenwürde anderer dadurch angreift, dass er Minderheiten beschimpft oder verleumdet. Ein im Gesetz zurecht besonders hervorgehobenes Verbot ist das öffentliche Billigen, Leugnen oder Verharmlosen des Holocausts. Im Hinblick auf semantische Umgehungsversuche vieler rechtsextremer Online-Anbieter wird hierunter auch schon das bloße In-Frage-Stellen des Holocausts oder hiermit im Zusammenhang stehender Verbrechen der Nationalsozialisten fallen. Werden derartige Inhalte im Internet aufgefunden, sollte umgehend eine Information der zuständigen Strafverfolgungsbehörden, des Amtes für Verfassungsschutz (bfvinfo@verfassungsschutz.de) oder der länderübergreifenden Kontrollstelle „jugendschutz.net" (info@jugendschutz.net) erfolgen.

Jugendschutz im Internet

Über die genannten rechtswidrigen Inhalte hinaus sind eine Reihe weiterer unzulässiger, insbesondere jugendgefährdender Medieninhalte im Internet auffindbar. Auch diese sind zumeist unzulässig oder unterliegen zumindest Verbreitungsbeschränkungen, die der Anbieter im Hinblick auf den Schutz von Kindern und Jugendlichen beachten muss. Für nähere Informationen sei auf die Broschüre des Weissen Rings zum Thema „Jugendschutz im Internet“ verwiesen.



Hinweise für private und gewerbliche Anbieter

Immer mehr Internet-Anwender beschränken sich nicht nur auf die gleichsam „passive" Rezeption von Medieninhalten, sondern nehmen gestalterisch daran teil, indem sie entweder ihre eigene Homepage gestalten oder auch nur in sog. „Community-Bereichen" wie Chatrooms, Foren oder Online-Gästebüchern ihre „Spuren" hinterlassen. Daher werden im folgenden noch einige Hinweise für Anbieter oder Verwender eigener Inhalte gegeben, die für die rechtskonforme Online-Nutzung unerlässlich oder/und hilfreich sind.

Welche Domain-Namen sind zulässig?

Wer zuerst kommt, malt zuerst?

Wer seine eigene private oder gewerbliche „homepage" erstellen und im Internet bereithalten will, braucht hierfür zunächst eine Internetadresse (sog. Domainname), unter der die angebotenen Inhalte abgerufen werden können. Solche Domainnamen werden für die Top-Level-Domain „.de" von der

Denic e.G. vergeben. Die Denic vergibt einen freien Namen grundsätzlich an denjenigen, der ihn zuerst anmeldet. Eine rechtliche Prüfung nimmt die Denic dabei abgesehen von Extremfällen wie grob anstößigen, beleidigenden oder sonst offensichtlich rechtswidrigen Namen grundsätzlich nicht vor. Wer bei der Anmeldung kostspielige Gerichtsverfahren mit anderen Namensinhabern vermeiden will, muss daher selbst eine rechtliche Prüfung der angemeldeten Domain vornehmen. Dabei sind verschiedene Gesichtspunkte zu beachten.

Kollision mit anderen Namensrechten

Einerseits darf der Name keine älteren Namensrechte verletzen. Dies ist z.B. der Fall, wenn der Name mit einer eingetragenen oder bekannten Marke oder einem älteren Unternehmensnamen identisch ist, oder damit verwechselt werden kann. Auch sonstige Namensrechte (z.B. von Städten und Gemeinden) sind bei der Anmeldung einer Domain zu beachten. Da das Internet kein rechtsfreier Raum ist, kann jeder Inhaber eines älteren Namensrechts gegen die Anmeldung einer Domain gerichtlich vorgehen, die mit seinem Namen verwechselbar ist, oder seinen guten Ruf ausbeutet oder beschädigt. Auf der anderen Seite muss der Anmelder auch das allgemeine Wettbewerbsrecht beachten. Zwar ist die Anmeldung von allgemeinen Gattungsbezeichnungen inzwischen unproblematisch, doch darf ein Domainname nicht irreführend sein. D.h. er darf bei den Lesern keine falsche Vorstellungen über den Inhalt der Internetseiten oder das Unternehmen wecken, das sich unter der Domain präsentiert.

Nähere Informationen zur Anmeldung von Domains finden sich im Internet unter www.denic.de. (Entsprechendes gilt für die Top-Level-Domain „.com". Dazu finden sich Informationen unter www.icann.org.) In Zweifelsfällen empfiehlt es sich jedoch dringend, einen erfahrenen Anwalt zu Rate zu ziehen.

Verantwortlichkeit für eigene und fremde Inhalte

Anbieter sind für eigene Inhalte stets im Rahmen der gesetzlichen Bestimmungen verantwortlich. Insofern ergeben sich keine Besonderheiten gegenüber der Verbreitung durch andere Medien oder öffentlichen Äußerungen.

Halten Internet-Nutzer hingegen fremde Inhalte zur Nutzung bereit, kann sich hieraus eine rechtliche Verantwortlichkeit nur ergeben, wenn sie von diesen fremden Inhalten Kenntnis haben und es ihnen technisch möglich und zumutbar ist, deren Nutzung zu verhindern. Dies ist etwa bei dem Anbieten sog. Foren oder Gästebüchern der Fall, welche dem anonymen Nutzer die Möglichkeit geben, eigene Texte, Bilddateien oder Links auf die Plattform des Anbieters zu stellen. Auch wenn es demnach für den Anbieter besser ist, fremde Inhalte auf seiner Website gar nicht zu sichten und damit nicht zu „kennen", empfiehlt sich aus Gründen der Rechtssicherheit eine gelegentliche, zumindest stichprobenhafte Kontrolle. Da für die meisten Anbieter ohnehin die Pflicht zur Bestellung eines Jugendschutzbeauftragten besteht, kann dieser mit regelmäßigen Sichtungen betraut werden.

Wird zu fremden Inhalten lediglich der Zugang vermittelt, so kann der Anbieter für diese Inhalte überhaupt nicht haftbar gemacht werden. Dies ist in erster Linie bei sog. Access-Providern der Fall. Hingegen ist bei dem Setzen von Hyperlinks auf andere Internetseiten die Rechtslage unklar. Für den Anbieter ist es jedenfalls ratsam, sich neben dem Hinweis auf die eigene Verantwortung des fremden Site-Betreibers zusätzlich in aller Deutlichkeit von fremden Inhalten zu distanzieren.

Pflicht zur Bestellung eines Jugendschutzbeauftragten

Anbieter, welche gewerbsmäßig Online-Angebote zur Nutzung bereithalten, sind gesetzlich verpflichtet, einen Jugendschutzbeauftragten zu bestellen, wenn die Angebote jugendgefährdende Inhalte enthalten können und allgemein angeboten werden. Die Bestellpflicht trifft also auch jeden seriösen Website- bzw. Homepage-Besitzer, der Chatrooms, Foren oder Gästebücher bereithält, da auch hier jugendgefährdende Materialien eingestellt werden „können". Kommt der Anbieter seiner Bestellpflicht nicht nach, kann dies als Ordnungswidrigkeit mit erheblichen Bußgeldern geahndet werden.

Der Beauftragte soll als Ansprechpartner für Nutzer und Berater des Anbieters fungieren und muss daher fachlich hinreichend qualifiziert sein. Nicht ausreichend ist die bloße formale Selbstbestellung, etwa um Kosten zu sparen. Andererseits muss auch nicht zusätzlich Personal eingestellt werden. Es reicht die kostengünstigere, externe Beauftragung, welche etwa von

www.jugendschutzbeauftragter.net angeboten wird. Zudem besteht die Möglichkeit, dass eine Organisation der freiwilligen Selbstkontrolle, wie z. B. www.fsm.de, zur Wahrnehmung der Aufgaben des Jugendschutzbeauftragten verpflichtet wird. Allerdings ist bislang umstritten, ob die sog. FSM ihren gesetzlichen Aufgaben hinreichend gerecht wird. Die Bestellung bzw. Delegation verursacht in jedem Falle Kosten, die aber durch Preisvergleich niedrig gehalten werden können. Teurer ist allerdings stets die Bezahlung von Bußgeldern, die nach dem Gesetz bis zu einer Höhe von 1 Mio. DM verhängt werden können!

Zum Inhalt:

Die weitgehende Anonymität des Datentransfers im Internet birgt erhebliche Gefahren und Risiken.

Wie sicher ist E-Commerce? Welche Möglichkeiten hat der Verbraucher? Ist Schutz vor Betrügern oder Hackern möglich? Was kann man gegen Computer-Viren tun? Können Kinder sicher surfen? Was muss ich bei der eigenen Homepage beachten? Die Broschüre gibt erste Antworten und dient als Leitfaden für sicheres Surfen im Internet.

Marc Liesching

WEISSER RING
Gemeinnütziger Verein zur Unterstützung von Kriminalitätsopfern und zur Verhütung von Straftaten e.V.

Infotelefon:
01803 - 34 34 34