

**Spam** oder  
*wenn sich die Mailbox in eine Müllkippe verwandelt.*  
**7 Tipps was Sie dagegen tun können!**

# 1. Allgemeines, Zahlen und Fakten

Jeder, der eine E-Mail Adresse besitzt, kennt das Problem: Regelmäßig kommen E-Mails herein, die für Produkte und/oder Dienstleistungen werben, die einen nicht interessieren. E-Mails, die man eigentlich nicht will und noch viel weniger angefordert hat. Gemeinhin werden solche unverlangten Mails als „**Spam**“ bezeichnet. Unter „Spam“ versteht man also unverlangt zugestellte E-Mails. Man spricht auch von „Junk Mail“, „Bulk Mail“ oder UCE (Unsolicited Commercial E-Mail).

Die meisten Spam-E-Mails sind kommerziell und werden aufgrund der geringen Kosten für den Versender **in großen Massen** verschickt (100.000 und mehr). Einer Schätzung der Europäischen Kommission vom 22.01.2004 zufolge bestehen heutzutage über 50 % des weltweiten E-Mail-Aufkommens aus SPAM. Nach einer Statistik von Brightmail/Symantec, Hersteller von Spam-Filtern für Provider, belief sich der weltweite Anteil von Spam im Juni 2004 auf 65 %. Laut einer Prognose der Anti-Spam-Organisation Spamhaus soll der Spam-Anteil im Jahr 2006 bis zu 95 % am Gesamtaufkommen betragen. Allein Microsoft blockt täglich 3,2 Milliarden Spam-E-Mails an Hotmail-Accounts<sup>1)</sup>.

Die meisten unerwünschten Massen-E-Mails kommen nach der jüngsten Auswertung des britischen Antivirensoftware-Herstellers Sophos nach wie vor aus den USA und aus China. Im zweiten Quartal des Jahres 2006 sind 23,2 % des elektronischen Mülls aus den USA verschickt worden, aus China 20 %. Aus Deutschland sind ca. 2,5 % der Massen-E-Mails gekommen. Nach Kontinenten gelistet führt Asien (42,8 Prozent) vor Nordamerika (25,6 Prozent) und Europa (25 Prozent) das Spam-Länderranking an.

Die meisten Spam-E-Mails stammten von so genannten **Zombie-PCs**. Dabei handelt es sich um Rechner, die von Virenschreibern gezielt mit Schadcodes infiziert und danach für den Versand der Spam-E-Mails genutzt werden. Diese Rechner werden zu fernsteuerbaren Netzwerken, sog. Botnetze, aus kommunizierenden Rechnern (Bots), konsolidiert. Die Netze führen sodann Anweisungen des Netzbeherrschers aus, ohne auf dem einzelnen Rechner Schaden anzurichten. Ohne dass der jeweils betroffene Nutzer dies bemerkt, können die Rechner für Spam-

Verbreitung, DDoS Attacken, usw. verwendet werden. Bei Programmierern werden solche Schädlinge von professionellen Spammern in Auftrag gegeben. In Ländern, in denen die Rechtsverfolgung von Spamming sich sehr schwierig gestaltet, werden oft auch Spam-Server genutzt, deren Betreiber sich – zumeist gegen ein erhöhtes Entgelt – beschwerderesistent geben (sog. „**bulletproof**“ Server). Als weiterer Trend zeigt sich, dass es immer mehr „Pump-and-Dump“-Kampagnen gibt, mit denen Spam-Versender versuchen, die Aktienkurse durch falsche Informationen bewusst in die Höhe zu treiben und so an schnelles Geld zu kommen. Auch sind Werbe-Mails auf dem Vormarsch, bei denen die Versender Bilder verwenden, um Filter zu umgehen, die auf die Analyse der Text-Inhalte ausgerichtet sind.

Um an E-Mail-Adressen zu gelangen, benutzen die Spam-Versender verschiedene Methoden. In den meisten Fällen werden die Adressen – zumeist automatisiert durch sog. **Harvester** (Ernter)-Programme – im Internet ausgelesen („geerntet“), also auf Internet-Präsenzen, in Newsgroups oder in Chats. Auch aus Adressbüchern von E-Mail-Clients kann die E-Mail-Adresse durch Viren-infizierte Rechner den Spammern zum Opfer fallen. Sehr verbreitet ist auch die rechtswidrige Verwendung zunächst rechtmäßig erhobener Daten. Beispiele sind die Übermittlung von personenbezogenen Daten an Dritte ohne entsprechenden Rechtfertigungsgrund (Vermietung von E-Mail-Adressen zur werblichen Nutzung, Weitergabe der Daten an „Partnerunternehmen“, etc.), oder die zweckfremde Verwendung personenbezogener Daten (etwa durch werbliche Verwendung von ausschließlich bspw. zum Zwecke der Teilnahme an einem Gewinnspiel oder zum Abschluss eines Vertrages erhobener Daten). Häufig wird die Einwilligung des Adresseninhabers erschlichen (versteckte Zustimmung des Betroffenen zur werblichen Verwendung seiner Daten in Allgemeinen Geschäftsbedingungen oder in Teilnahmebedingungen) oder „abgepresst“ (die Einwilligung zur werbenden Nutzung der E-Mail-Adresse wird als zwingende Bedingung für die Erlangung eines wirtschaftlichen Vorteils für den Betroffenen dargestellt).

<sup>1)</sup> Lt. Aussage des Herrn David Finn, Direktor der Microsoft-Abteilung „Digital Integrity and Internet Safety“, auf dem 3. Deutschen Anti-Spam Kongress am 7./8. Sep. 2005 in Köln, organisiert vom Verband der deutschen Internetwirtschaft (eco).

Die durch Spam verursachten **Produktivitätsverluste** bei Unternehmen im Europäischen Wirtschaftsraum beliefen sich nach Angaben der Europäischen Kommission im Jahre 2002 auf 2,5 Milliarden EUR. Der größte Teil dieser Kosten wird allerdings nicht von den Spambetreibenden, sondern von den Empfängern und den Providern getragen. Möglich macht dies die Eigenheit des SMTP-Protokolls (mit welchem E-Mails versandt werden), welches ermöglicht, dass der Versender von E-Mails den Text der Spam-Mail zusammen mit einer Liste von hunderten oder gar tausenden E-Mail-

Adressen schicken kann und der Mailserver dann diese Liste abarbeitet. Der Spammer trägt somit nur einen Bruchteil der anfallenden Kosten. Darüber hinaus existieren Programme, die den vollautomatischen Versand von Millionen von E-Mails ermöglichen. Dementsprechend muss der Spammer nur das Programm starten und kann dann einer anderen Tätigkeit nachgehen, während sein Programm hunderttausende von Internetnutzern belästigt.

## 2. Die Rechtslage

### 2.1 Die Rechtslage in Deutschland

Das Versenden von Werbe-E-Mails ohne die vorherige Einwilligung des Empfängers (Spam) ist in Deutschland rechtswidrig (**OPT-IN-Prinzip**). Es stellt – nach mittlerweile gefestigter Rechtsprechung – einen Eingriff in die Privatsphäre bei natürlichen Personen und bei Gewerbetreibenden einen Eingriff in den eingerichteten und ausgeübten Gewerbebetrieb dar. Dem Empfänger einer Spam-Mail steht demnach gemäß §§ 1004, 823 Abs. 1 BGB analog ein Unterlassungsanspruch und ggf. auch einen Schadensersatzanspruch gegen den Versender zu.

Im Rahmen der im Juli 2004 in Kraft getretenen Novellierung des **Gesetzes gegen den unlauteren Wettbewerb (UWG)** hat der Gesetzgeber in Umsetzung von Art. 13 Abs. 1 der **Datenschutzrichtlinie 2002/58/EG** auch die Wettbewerbswidrigkeit von Spam-Werbung<sup>2)</sup> unmissverständlich zum Ausdruck gebracht. Nach § 7 Abs. 2 Nr. 3 UWG stellt die Werbung per E-Mail ohne die vorherige Einwilligung des Adressaten eine unzumutbare Belästigung dar und ist demzufolge unzulässig. Dies gilt unabhängig davon, ob der Empfänger eine Privatperson oder ein Gewerbetreibender ist. Das vermutete Einverständnis des Empfängers im Rahmen einer bestehenden Kundenbeziehung bzw. bei Gleichartigkeit des beworbenen Produkts und des Tätigkeitsfeldes des Empfängers, wie es als Rechtfertigungsgrund vor Inkrafttreten des neuen UWG bestand, ist nunmehr nicht mehr von Bedeutung.

Für das Direktmarketing per E-Mail im Rahmen einer bestehenden Kundenbeziehung sieht das Gesetz in § 7 Abs. 3 UWG eine Ausnahme vom OPT-IN-Prinzip, nämlich ein **„Qualifiziertes OPT-OUT-Prinzip“**<sup>3)</sup> vor. Danach darf im Rahmen einer Kunden- bzw. Geschäftsbeziehung auch ohne die ausdrückliche Einwilligung der Adressaten an diese Werbung versandt werden. Der Versender kommt jedoch nur dann in den Genuss dieser Erleichterung, wenn die nachfolgenden vier Voraussetzungen von ihm kumulativ erfüllt wurden:

- (1) der Versender hat die E-Mail-Adresse des Empfängers im Zusammenhang mit dem Verkauf einer Ware oder Dienstleistung von dem Kunden direkt erhalten;
- (2) der Unternehmer verwendet die Adresse zur Direktwerbung für eigene und ähnliche Waren oder Dienstleistungen;
- (3) der Kunde hat der Verwendung nicht widersprochen sowie
- (4) er wurde bei der Erhebung der Adresse und bei jeder Verwendung klar und deutlich darauf hingewiesen, dass er der Verwendung seiner E-Mail-Adresse zu Marketingzwecke jederzeit widersprechen kann, ohne dass für den Widerspruch andere als Übermittlungskosten nach den Basistarifen entstehen.

<sup>2)</sup> Der BGH hatte mit Urteil vom 11. März 2004 (Az. I ZR 81/01) bereits zum alten UWG entschieden, dass die unerbetene Zusendung von Werbung enthaltenden E-Mails gegen die guten Sitten im Wettbewerb verstößt und eine unzumutbare Belästigung darstellt.

<sup>3)</sup> Von einigen Autoren wird sinngemäß auch die Bezeichnung „Soft-OPT-IN“ benutzt.

§ 7 Abs. 3 UWG gewährt also den werbenden Unternehmen eine spürbare wettbewerbsrechtliche Erleichterung bei der Nutzung der E-Mail-Adressen ihrer Kunden bzw. Geschäftspartnern für Zwecke der Werbung.

Nach der Rechtsprechung wird bereits in der einmalig un- verlangten Zusendung von Werbung per E-Mail eine Rechtsverletzung gesehen (**LG Berlin, 16 O 201/98; LG Traunstein, 2 HKO 3755/97**). Nach Ansicht des LG München I (**Urteil vom 05.11.2002, Az.: 33 O 17030/02** sowie **Urteil vom 15.04.2003, Az.: 33 O 5791/03**) haftet sogar derjenige als **Mitstörer**, der dem Spammer bestimmte Versendefunktionen (**E-Cards, Newsletter**) zur Verfügung stellt. Nach Auffassung des Kammergericht Berlin trägt der Newsletterbetreiber die Beweislast für ein behauptetes Einverständnis des Empfängers: (**KG Berlin: Beschluss vom 08.01.2002, LG Berlin: Beschluss vom 19.09.2002**). Das Landgericht Leipzig hat mit **Urteil vom 13.11.2003 (Az. 12 S 2595/03)** ein vorinstanzliches **Urteil des Amtsgerichts Leipzig (AZ 02 C 8566/02)** bestätigt, wonach der Betreiber eines Erotik-**Subdomain-Services** für unerwünschte Werbe-E-Mails haftet, in denen für die auf den Subdomains abgelegten Seiten geworben wird. Abgesehen von der Rechtswidrigkeit, die auf dem Umstand des un- verlangten Zusendens der Spam-Mails beruht, machen sich einige Spammer durch das Verschicken von Massen-Mails auch strafbar, indem sie für **Pornographieangebote** werben oder pornographische Schriften (Fotos, Filme etc.) als Anhang der Spam-Mails an nichts ahnende E-Mail-Nutzer gelangen lassen. Die Strafbarkeit ergibt sich in solchen Fällen aus § 184 Abs. 1 Nr. 5 bzw. Nr. 6 des Strafgesetzbuches (StGB). Das Versenden von **Phishing-E-Mails**, mit denen die Versender versuchen, sich Informationen wie Kreditkartennummern, Kennwörter, Kontoinformationen oder andere persönliche Daten von Online-Banking-Kunden zu erschleichen, dürfte ebenfalls unter dem Gesichtspunkt des Betruges bzw. des Computerbetruges gemäß § 263 bzw. § 263 a StGB strafbar sein. Eine einschlägige Rechtsprechung hierzu liegt bislang noch nicht vor.

Darüber hinaus können auch solche E-Mails, die **Viren oder Würmer** transportieren, wegen Ausspähen von Daten (§ 202a StGB) bzw. Datenveränderung und Computersabotage (§§ 303a oder 303b StGB) **strafbar** sein. Die Straftatbestände der Datenveränderung und der Computersabotage oder die Störung öffentlicher Telekommunikationsanlagen (§ 317 StGB) kommen auch dann in Betracht wenn die massenhafte Versendung von Werbe-E-Mails den Zusam-

menbruch von Vermittlungsrechnern oder Empfängerpostfächern verursacht.

## 2.2. Die Rechtslage nach EU-Recht

Der EU-Gesetzgeber folgt dem „**Opt-in-Prinzip**“. Dies kommt unmissverständlich in Art. 13 Abs. 1 der **Datenschutzrichtlinie 2002/58/EG** zum Ausdruck. Nahezu alle EU-Länder haben bereits die Anti-Spam-Bestimmungen der Datenschutzrichtlinie ins nationale Recht umgesetzt bzw. stehen unmittelbar davor, die entsprechenden Gesetzgebungsverfahren zu beenden. Verschiedene **internationale Anti-Spam-Projekte**, insbesondere innerhalb der EU, sind unten, unter Ziffer 4 dieses Artikels vorgestellt.

## 2.3. Die Rechtslage in den USA, China und Australien

In den USA gilt seit dem 01. Januar 2004 das Gesetz **Controlling the Assault of Non-Solicited Pornography and Marketing Act of 2003** als erstes einheitliches Anti-Spam-Gesetz auf US-Bundesebene. Nach dem so genannten „**Can-Spam Akt 2003**“ ist unerwünschte Werbung per Email nicht grundsätzlich verboten; es wird im Unterschied zu der Rechtslage in der EU das so genannte „**Opt-Out-Prinzip**“ favorisiert, wonach die vorherige, ausdrückliche Einwilligung des Empfängers nicht erforderlich ist. Die Werber müssen sich allerdings an einige Spielregeln halten. Als illegal im Sinne des vorgenannten Gesetzes gelten alle Werbe-E-Mails, die

- ▶ unter einer gefälschten Absender-E-Mail-Adresse versandt werden,
- ▶ nicht eindeutig als Werbung in der Betreffzeile markiert sind,
- ▶ keine für den Empfänger leicht erkennbare Abbestellmöglichkeit enthalten und/oder
- ▶ den Hinweis nicht enthalten, wie der Absender postalisch zu erreichen ist.

Ferner gelten besondere Kennzeichnungsregelungen zur Identifikation von E-Mails mit sexuellem Inhalt. E-Mails mit solchem sexuellen Bezug müssen einheitlich mit einer Kennzeichnung versehen werden, die die Federal Trade Commission (us-amerikanische Wettbewerbsbehörde – FTC) vorschreibt.

Für Verstöße gegen die vorgenannten Regeln sieht das Gesetz Haftstrafen von bis zu fünf Jahren und erhebliche Geldstrafen in Millionenhöhe vor. Gegen Spammer klagen dürfen allerdings nur Internet-Provider oder staatliche Stellen.

In **Australien** gilt seit 2003 ebenfalls ein **Anti-Spam-Gesetz**, das ein rigides Vorgehen gegen Spam-Versender ermöglicht. Das Gesetz sieht Strafen von bis zu 1,1 Millionen australischer Dollar (650.000 Euro) für uneinsichtige Versender unverlangter Werbebotschaften vor. Privatpersonen können mit bis zu 220.000 Dollar belangt werden. Das Gesetz beruht entsprechend der Rechtslage in der EU auf dem „**Opt-IN-Prinzip**“. Zudem müssen die Werbe-Mails klare Hinweise enthalten, wie man den künftigen Empfang unterbinden kann. Software, mit der E-Mail-Adressen automatisch eingesammelt werden können, ist nach dem Gesetz verboten.

Die **Volksrepublik China**, die mit einem Anteil von 20 Prozent am weltweiten Aufkommen unerwünschter E-Mails als zweitgrößte Spam-Quelle nach den USA gilt, hat **noch keine Anti-Spam-Gesetze** verabschiedet. Dennoch hat sich die Volksrepublik im Juli 2005 dem **London Action Plan on Spam Enforcement Collaboration** angeschlossen. Ziel der Londoner Gruppe ist die international koordinierte Zusammenarbeit von Regulierungsbehörden, Daten- und Verbraucherschützern gegen Spam und daraus resultierende Probleme wie Online-Betrug und Computer-Viren. Mehr Informationen zum London Action Plan sowie weiteren internationalen Anti-Spam-Projekten finden sich unten, unter Ziffer 4 dieses Artikels.

## 3. Vorgehensmöglichkeiten gegen Spam – 7 Tipps

Die effektivste Vorgehensweise gegen Spam ist es zu versuchen, Spam-E-Mails bereits im Vorfeld zu vermeiden. Es gibt eine Reihe von Möglichkeiten, die Zahl der Spam-Mails, die in der eigenen Mailbox ankommen, zu reduzieren:

### 3.1. Alternativer E-Mail-Account

Es sollte zunächst dafür gesorgt werden, dass die Spammer erst gar nicht an die im normalen E-Mail-Verkehr genutzte E-Mail-Adresse herankommen. Internet Benutzer, die häufiger Ihre Identität bei Teilnahme an Gewinnspielen, beim Ausfüllen von Anmeldeformularen oder beim Schreiben in Newsgroups preisgeben, riskieren, dass ihre Mail-Inbox mit lästigen Werbebriefen überfüllt wird, da insbesondere die Newsgroups eine bei Spammern und Adressensammlern äußerst beliebte „Recherchemöglichkeit“ darstellen. Daher ist das Einrichten von alternativen E-Mail-Accounts für bestimmte Internetaktivitäten besonders zu empfehlen. Solch eine temporäre E-Mail-Adresse lässt sich leicht bei einem Freemail-Provider (z.B. GMX, WEB.de, Hotmail, AOL, etc.) einrichten.

### 3.2. Vorsichtiger Umgang mit den E-Mail-Adressen

E-Mail-Adressen, die nicht nur temporär für einen bestimmten Zweck angelegt wurden, sollten nach Möglichkeit nicht in der Öffentlichkeit in der Weise verwendet werden, dass sie für jedermann abrufbar sind. So empfiehlt es sich etwa, auf einer Internet-Präsenz die Kontakt-E-Mail-Adresse nicht im Klartext, sondern etwa in Form eines kleinen Bildes,

oder zumindest unter Verwendung von Leerzeichen oder dem Ausdruck „[at]“ statt „@“ darzustellen. Ein automatisiertes Auslesen wird damit erheblich erschwert.

### 3.3. Einsetzen von Filterprogrammen

Viele der Standard-E-Mail-Programme wie Eudora®, Outlook®, TheBat® oder Mozilla® sind mittlerweile in der Lage, alle empfangenen E-Mails nach bestimmten Adressen zu filtern und Nachrichten einer bestimmten E-Mail-Adresse oder ganzen Domain zu blockieren. Verfügt Ihr E-Mail-Programm dennoch über keine Filtermöglichkeiten, gibt es zahlreiche Hilfsprogramme, die die eigene Mailbox überprüfen können und unerwünschte E-Mails löschen, noch bevor man die Mailbox zum Lesen öffnet. „AntiSpamWare“, „SpamEater Pro“, „SpamFlush“, „SpamKiller“, „SuperSpamKiller Pro“ oder „SPAMfighter“ sind nur einige der zahlreichen Tools, die mittlerweile für alle Betriebssysteme erhältlich sind. Eine Liste mit vielen – auch kostenlosen – Anti-Spam-Anwendungen mit den entsprechenden Download-Links finden Sie am Ende dieses Artikels. Wer einen der kostenlosen E-Mail-Dienste wie etwa GMX oder WEB.de nutzt, kann die dort vorhandenen Spam-Filter aktivieren.

### 3.4. Robinsonliste

Der Eintrag in die so genannte Robinsonliste soll den Empfänger vor unerwünschten, absichtlichen oder versehentlichen Werbe- und Rundsendungen schützen. Robinsonlisten gibt es für Faxrundsendungen, Briefsendungen, SMS- und

E-Mailsendungen gleichermaßen. Eine Übersicht über die verschiedenen Robinsonlisten und entsprechenden Kontaktmöglichkeiten zu den verantwortlichen Stellen findet sich auf der **Website des Bundesdatenschutzbeauftragten**. Einige Fachleute raten allerdings von der Eintragung in Robinsonlisten ab, da man dadurch seine private E-Mail-Adresse preisgibt und es den wirklich hartnäckigen Spammern egal sein dürfte, ob jemand in einer Robinsonliste steht.

### 3.5. Spam zurückverfolgen

Hat es doch einmal eine Spam-E-Mail trotz aller Abwehrmaßnahmen in die eigene Mailbox geschafft, und man möchte diese E-Mail nicht nur einfach löschen, sondern versuchen, den Absender ausfindig zu machen, gilt es, einige Hinweise zu beachten.

Zunächst sollte der Text einer Spam-E-Mail nur mit einem E-Mail-Client gelesen werden, der so eingestellt ist, dass er die Nachrichten nicht im HTML-Format anzeigt, zumindest aber Bilder nicht automatisch nachlädt, da andernfalls der Versender eine Nachricht über das Öffnen seiner E-Mail und damit über die Gültigkeit der angeschriebenen E-Mail-Adresse erhält. Dies multipliziert den Wert einer solchen Adresse für die Spammer und mündet in einer weiteren Zunahme des Eingangs von rechtswidrigen Werbenachrichten.

Des Weiteren sollte niemals direkt auf eine Spam-E-Mail geantwortet werden auch wenn mittlerweile fast alle dieser Werbenachrichten den Empfänger mit Zeilen wie „For removal from any future mailings, just send a blank e-mail to...“ dazu auffordern. Viele Spammer setzen Tools zum Versenden der E-Mails ein, die mögliche Empfängeradressen entweder aus einer Datenbank lesen, oder diese völlig automatisch erzeugen. Eine Antwort auf eine E-Mail würde dem Spammer also zeigen, welche Adressen gültig sind und auch aktiv genutzt werden. Weitere Spam-E-Mails würden unweigerlich folgen. Darüber hinaus werden direkte Antworten in vielen Fällen nicht zum Erfolg (also zum Spammer) führen, da deren E-Mail-Adressen in der Regel gefälscht sind, bzw. der Spammer einen der von vielen Providern kostenlos angebotenen E-Mail-Accounts benutzt hat, den er nur für eine Aktion oder nur kurzfristig nutzt.

Es empfiehlt sich vielmehr anhand des E-Mail-Headers die wahre Herkunft der meistens gefälschten Spam-E-Mail festzustellen und dann die Spam-E-Mail an den Administrator

des Servers weiterzuleiten, der als Spam-Relay dient. Ein guter Beitrag, wie man E-Mails zurückverfolgt, findet sich unter <http://th-h.de/faq/headerfaq.php3#headerzeilen>. Wenn über den E-Mail-Header der Provider, über den der Spam verschickt wurde, ermittelt ist, kann man über <http://openrbl.org> mittels Eingabe der IP- oder DNS-Adresse des Providers erfahren, ob der Server in einem größeren Netzwerk agiert, an welches man dann seine Beschwerde richtet. Viele Administratoren haben zu diesem Zweck mittlerweile spezielle E-Mail-Adressen (z.B. `abuse@provider.com`) eingerichtet. Die Adresse `postmaster@...` sollte aber in jedem Fall funktionieren. Dabei ist es sehr wichtig, dem Administrator die komplette Spam-E-Mail inklusive des gesamten Headers zu senden und damit niemals länger als ca. 1 Woche zu warten, da eine Bearbeitung sonst erheblich erschwert wird. Unter Umständen erfährt ein Administrator erst auf diese Weise, dass sein Mail-Server zur Verteilung der Spam-E-Mails missbraucht wurde. Man kann als Spam-Opfer seine Beschwerde auch an den Hostprovider der mittels Spam beworbenen Web-Seite richten, deren Besitzer in den meisten Fällen auch der tatsächliche Spammer bzw. Spam-Auftraggeber ist. Die meisten Hostprovider haben in ihren Allgemeinen Geschäftsbedingungen bestimmte Klauseln, wonach Spam-Aktionen verboten werden und zur Vertragskündigung führen können. Die Ermittlung des Hostproviders der beworbenen Seite erfolgt am schnellsten über die sogenannten Whois-Abfragen, indem man die vollständigen URL der fraglichen Web-Seite eingibt. Für `com.`, `net.` oder `org.` Domains empfehlen sich die Whois-Dienste von **Hexillion**. Bei `de.`-Domains kann man eine Abfrage über die **Denic-Datenbank** durchführen. Den wahren Spammer oder Auftraggeber der Spam-Aktion ausfindig zu machen, um auch gegen ihn vorzugehen und gegebenenfalls gerichtliche Schritte einzuleiten, ist in der Regel aussichtslos. Voraussetzung dafür wäre die zweifelsfreie Identifizierung des Versenders der E-Mail bzw. des dafür Verantwortlichen. Es muss der vollständige Name bzw. die Firma mit vollständiger Adresse ermittelt werden. Das ist häufig leider nicht oder nur schwer möglich, da die Verursacher regelmäßig gefälschte Absender-Adressen und/oder freie Mail-Server benutzen. Sollte es aber dennoch gelingen, die Identität des Spammers festzustellen, hat man als Spam-Opfer nach der bereits oben geschilderten Rechtslage die Möglichkeit, gegen den Spammer eine strafbewehrte Unterlassungserklärung zu erwirken und gegebenenfalls ihn auf Schadensersatz zu verklagen (wobei letzteres nur Sinn machen dürfte, wenn der Spammer in Deutschland sitzt).

### 3.6. Sonderfall „0900-Dialer“

Einige der Spam-E-Mails enthalten Werbung für (0)900-Faxabruf-Dienste oder Links, die zu der Installation eines (0)900-Dialers führen. Dem Empfänger einer solchen Spam-E-Mail in der eine (0)900er-Rufnummer - die (0)900er-Rufnummern haben zum 31. Dezember 2005 die alten (0)190er-Rufnummern vollständig abgelöst - beworben wird, stehen gemäß §§ 40, 43a, 43b des Telekommunikationsgesetzes (TKG) unter gewissen Voraussetzungen weitere Auskunfts- Unterlassungs- sowie Schadensersatzansprüche zu. In diesen Fällen sollte man als Spam-Opfer versuchen, den Netzbetreiber der rechtswidrig beworbenen (0)900er-Rufnummer ausfindig und ihn auf den rechtswidrigen Umgang mit der Mehrwertdiensterrufnummer aufmerksam zu machen. Hilfestellung zur Ermittlung des (0)900er-Netzbetreibers bieten die kostenlosen **Datenbanken der Bundesnetzagentur (BNetzA)**. Dort findet man auch weitere zahlreiche Informationen und Tipps betreffend die Reaktionsmöglichkeiten bei Rufnummernmissbrauch durch Spam.

### 3.7. Beschwerdestellen

Deutschsprachige Spam-E-Mails können auch als Beschwerde an die Internet-Beschwerdestelle des Verbandes der deutschen Internetwirtschaft eco e.V. unter [www.internet-beschwerdestelle.de](http://www.internet-beschwerdestelle.de), die der eco-Verband zusammen mit der Freiwilligen Selbstkontrolle Multimediadienstanbieter (FSM) mit der Unterstützung der Europäischen Kommission im Rahmen des Programms „Safer Internet plus“ (2005–2008) betreibt, weitergeleitet werden. Beschwerden können per E-Mail unter Beifügung der vollständigen Spam-E-Mail und dem Original-Mail-Header unter der nachfolgenden Adresse eingereicht werden: [spam@internet-beschwerdestelle.de](mailto:spam@internet-beschwerdestelle.de)

Wie man den Header einer E-Mail mit dem jeweilig genutzten E-Mail-Programm anzeigen lassen kann, wird etwa unter <http://th-h.de/faq/headerfaq.php3#headerzeigen> beschrieben. Nach dem Eingang einer solchen Beschwerde werden seitens der Beschwerdestelle des eco-Verbandes die oben beschriebenen Maßnahmen ergriffen. Darüber hinaus werden die erforderlichen Informationen mit Kooperationspartnern zwecks weitergehender Verfolgung kommuniziert. Zu den Kooperationspartnern des eco-Verbandes gehören in Sachen Spam-Verfolgung unter anderem der **Bundesverband der Verbraucherzentralen (vzbv)** und der **Zentrale zur Bekämpfung unlauteren Wettbewerbs (WBZ)**. Mit diesen zwei Organisationen hat sich der eco-Verband im

März 2005 zu einem Aktionsbündnis zur Bekämpfung von deutschen Spam-E-Mails zusammengeschlossen und geht hierzulande rechtlich gegen Spam-Versender vor.

Spam-E-Mails können als Beschwerden auch unmittelbar an die vorgenannten Kooperationspartner unter Beifügung der vollständigen Spam-E-Mail und dem Original-Mail-Header (Informationen hierzu auf <http://th-h.de/faq/headerfaq.php3#headerzeigen>) unter den nachfolgenden Adressen eingereicht werden:

- ▶ [beschwerdestelle@vzbv.de](mailto:beschwerdestelle@vzbv.de) (Verbraucherzentrale Bundesverband (vzbv))
- ▶ [mail@wettbewerbszentrale.de](mailto:mail@wettbewerbszentrale.de) (Zentrale zur Bekämpfung unlauteren Wettbewerbs (WBZ))

Auf europäischer und internationaler Ebene kooperiert die Beschwerdestelle des Verbandes der deutschen Internetwirtschaft eco e.V. mit Microsoft EMEA sowie dem Netzwerk der behördlichen Spam-Beschwerdestellen CNSA sowie mit der U.S.-amerikanischen Federal Trade Commission (FTC).

Spam-E-Mails, die Mehrwertdiensterrufnummern (z.B. (0)190er/(0)900er Nummern) bzw. Dialer-Programme dem Empfänger „vermitteln“, können als Beschwerden an die Bundesnetzagentur (BNetzA) – [www.bundesnetzagentur.de](http://www.bundesnetzagentur.de) – weitergeleitet werden. Die entsprechenden Online-Beschwerdeformulare finden sich zum Abruf unter: [http://www.bundesnetzagentur.de/enid/819c39880bda6c4748efe0ae49cb8804,0/Verbraucher/Dialer\\_-\\_Spam\\_-\\_Rufnummernmissbrauch\\_xy.html](http://www.bundesnetzagentur.de/enid/819c39880bda6c4748efe0ae49cb8804,0/Verbraucher/Dialer_-_Spam_-_Rufnummernmissbrauch_xy.html).

## 4. Wichtige Anti-Spam-Projekte

### 4.1 SpotSpam

Die **europäische Spam-Datenbank „SpotSpam“** soll den grenzüberschreitenden Datenaustausch sowie die wasser-dichte gerichtliche Verwertbarkeit der gesammelten Beweise bei der rechtlichen Inanspruchnahme von Spammern unterstützen.

Beschwerden werden von nationalen Spamboxen direkt in die in Kürze aufgesetzte Datenbank weitergeleitet. Der eco-Verband koordiniert das von der Europäischen Kommission im Rahmen des Safer Internet Action Plans geförderten Projekt. Microsoft EMEA ist Mitinitiator und Industriepartner. Technologiepartner ist die Registrierstelle für .pl-Domains **Research and Academic Computer Network (NASK)**.

### 4.2 Contact Network of Spam Enforcement Authorities (CNSA)

Die internationale Vernetzung der Spammer-Szene ist auch der Grund der Gründung des EU-Behördennetzwerkes **Contact Network of Spam Authorities (CNSA)**.

Im Rahmen dieses Netzwerkes haben bislang 14 Mitgliedsstaaten der EU ein Verfahren zum Austausch von Beschwerden über Spam-E-Mails offiziell akzeptiert. Das im Dezember 2004 im Rahmen der Arbeit des CNSA verabschiedete Verfahren wird die **grenzübergreifende Verfolgung von Versendern von Spam-E-Mails** erleichtern. Es fordert die nationalen Behörden auf, Beschwerden wegen unerwünschter Werbe-Mail, die von den europäischen Kollegen an sie weitergereicht werden, entsprechend ihrem jeweiligen nationalen Recht zu verfolgen. Mit von der Partie sind Deutschland, Österreich, Belgien, Zypern, Tschechien, Dänemark, Frankreich, Griechenland, Irland, Italien, Litauen, Malta, die Niederlande, Spanien und seit neuestem Großbritannien. Auf deutscher Seite wurden vom zuständigen Bundesministerium für Wirtschaft und Technologie zwei Kontaktstellen für Beschwerden angemeldet, nämlich der eco - Verband der deutschen Internetwirtschaft e.V. ([www.eco.de](http://www.eco.de)) sowie für Rufnummern-Spam die Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post und Eisenbahnen, (BNetzA, [www.bundesnetzagentur.de](http://www.bundesnetzagentur.de)).

### 4.3 London Action Plan

Insgesamt mehr als 40 Vertreter aus 27 Ländern wirken seit Oktober 2004 zusammen bei den Aktivitäten des **London Action Plan on Spam Enforcement Collaboration**. Ziel der Londoner Gruppe ist die international **koordinierte Zusammenarbeit von Regulierungsbehörden**, Daten- und Verbraucherschützern gegen Spam und daraus resultierende Probleme wie Online-Betrug und Computer-Viren.

Die US-amerikanische Handelskommission (**Federal Trade Commission**) ist federführend in diesem Projekt; der Betreiber der ersten Anti-Spam-Hotline in Deutschland, der eco-Verband, vertritt die Interessen der deutschen Internetwirtschaft aus deutscher Seite. Die Volksrepublik China, die mit einem Anteil von 20 Prozent am weltweiten Aufkommen unerwünschter E-Mails als zweitgrößte Spam-Quelle nach den USA gilt, hat sich im Juli 2005 dem London Action Plan angeschlossen.

### 4.4 Arbeitsgruppe MAAWG

Die **Messaging Anti-Abuse Working Group (MAAWG)** stellt eine **Arbeitsgruppe von Kommunikations- und Technologieunternehmen** dar, die mehr als 500 Millionen Abonnenten vertreten und sich für die Lösung der Probleme von Spam-Mails, Virusattacken und anderen Formen von Missbrauch im Bereich Messaging und Content engagieren.

### 4.5 Organisation für wirtschaftliche Zusammenarbeit und Entwicklung (OECD)

Die OECD-Länder haben im Jahr 2004 eine Arbeitsgruppe eingesetzt, um die Anstrengungen der Regierungen, der Wirtschaft und Zivilgesellschaft im Kampf gegen Spam zu ordnen und eine umfassende und strategische Antwort auf die durch Spam hervorgerufenen Probleme zu finden.

Die sog. **OECD Task Force** veröffentlichte im April 2006 einen „**Anti-Spam-Toolkit**“ ([http://www.oecd-antis spam.org/article.php3?id\\_article=230](http://www.oecd-antis spam.org/article.php3?id_article=230)) vor. Der Anti-Spam „Werkzeugkasten“ listet gesetzgeberische Maßnahmen, Anti-Spam-Techniken und die Notwendigkeiten der Zusammenarbeit zwischen Industrie und öffentlicher Hand und zwischen internationalen Regierungen auf.

## 5. Eigene Werbung per E-Mail

### 5.1 Richtlinien und Selbstverpflichtungsmaßnahmen

Wer selbst per E-Mail auf sich aufmerksam machen möchte, sollte eine Reihe von wichtigen Voraussetzungen beachten.

Der **Arbeitskreis Online-Marketing des eco-Verbandes** hat sich dem Thema gewidmet und Richtlinien verfasst, die als pdf-Datei unter [http://www.eco.de/servlet/PB/show/1075685/Richtlinie\\_OM\\_121.pdf](http://www.eco.de/servlet/PB/show/1075685/Richtlinie_OM_121.pdf) eingesehen werden können.

Darüber hinaus haben sich die Mitglieder des **Deutschen Direktmarketing Verbandes (DDV)** durch einen **Ehrenkodex** im Rahmen der Selbstregulierung auf die Einhaltung definierter Qualitätsstandards verpflichtet. Der Ehrenkodex regelt wichtige Grundprinzipien wie das Erheben von Adressen und das Einholen der Erlaubnis, eMails zuzustellen, die Behandlung des Widerrufs dieser Erlaubnis, die Absenderkennzeichnung, den Ausschluss der Adressweitergabe, das Führen einer betriebsinternen Blacklist und die Bearbeitung von Bounces. Die dort niedergelegten Regeln lassen sich als eine Art „Check-Liste“ für die Rechtmäßigkeit der eigenen E-Mail-Werbung anwenden.

### 5.2 Certified Senders Alliance (CSA)

Die praktische Umsetzung vom rechtmäßigen E-Mail-Marketing bildet auch den Schwerpunkt des Positivlistenprojektes „**Certified Senders Alliance**“ (CSA), das seit September 2004 vom eco-Verband und dem DDV in Kooperation betrieben wird. Da viele Direktvermarkter beklagen, dass durch die ständige Verschärfung von Filtermaßnahmen bei den Providern auch ihre legitimen Werbeaussendungen die Adressaten nicht mehr erreichen würden, hat sich das Positivlistenprojekt zum Ziel gestellt, eine Grundlage für die **zuverlässige Zustellung von rechtmäßiger E-Mail-Werbung** zu schaffen. Dies wird dadurch erreicht, dass gewerbliche Massenversender nach einem streng definierten Katalog von Qualitätskriterien zertifiziert und auf eine zentrale Positivliste (Whitelist) gesetzt werden, auf die die großen Provider zugreifen. Eine zentralisierte Positivliste bildet mithin nicht nur einen „Spamfence“, sondern auch eine Schnittstelle zwischen Massenversendern und den Internet Service Providern, die die Qualität des Mediums „E-Mail“ verbessert und vor allem sicherstellt, dass wirklich erwünschte Mails seriöser Absender (in beide Richtungen) problemlos ihr Ziel erreichen, ohne dass sich der Absender vor einer negativen Klassifizierung seiner E-Mail fürchten muss.

## 6. Einige hilfreiche URLs zum Thema „Spam“

### Deutschsprachige URLs:

- ▶ Viele Tipps, Infos und zusätzliche Links unter: <http://www.antispam.de/>
- ▶ Online-Download der Studie des Bundesamts für Sicherheit in der Informationstechnik (BSI) – „Antispam – Strategien/Unerwünschte E-Mails erkennen und abwehren“: <http://www.bsi.de/literat/studien/antispam/antispam.pdf>
- ▶ Umfangreiche Urteilssammlung sowie weitere hilfreiche Informationen unter: <http://www.recht-im-internet.de/themen/spam/index.htm>
- ▶ Deutschsprachiges Usenetforum de.admin.net-abuse.mail.
- ▶ E-Mail-Header lesen und verstehen: <http://th-h.de/faq/headerfaq.php3>
- ▶ Spam-FAQ: <http://antispam.talky.de/>
- ▶ Spam – Ursache, Auswirkungen und Bekämpfung: <ftp://ftp.belwue.de/pub/doc/spamvortrag/index.html>
- ▶ Verbrauchertipps beim Dialer-Missbrauch unter <http://www.dialerschutz.de/home.php>, sowie auf den Seiten der Bundesnetzagentur (BNetzA) unter <http://www.bundesnetzagentur.de>
- ▶ Informationen zu Schneeballmails, Pyramidenspielen und Kettenbriefen im Internet: <http://www.detta.de/Schneeballsysteme.htm>
- ▶ Spam-Filter für UNIX-Users: <http://www.belwue.de/wwwservices/hilfestellungen/spamblock.html>
- ▶ Informationen zu der Rechtslage in Österreich: <http://www.internet4jurists.at/e-mail/oe1a.htm>
- ▶ Hinweise auf die Rechtslage in der Schweiz: <http://spam.trash.net/>

### Englischsprachige URLs:

- ▶ „SpotSpam“ – the european Spam-database (<http://www.spotspam.org/>)
- ▶ FTC's site on spam-email: <http://www.ftc.gov/spam/>
- ▶ OECD – „Anti-Spam-Toolkit“: <http://www.oecd-antis spam.org/>
- ▶ The LONDON ACTION PLAN on International Spam Enforcement Cooperation: <http://www.londonaction-plan.org> (Dokumente auch in französischer und russischer Sprache)
- ▶ The Messaging Anti-Abuse Working Group (MAAWG): <http://www.maawg.org/home>
- ▶ Anti-spam project in China: <http://www.isc.org.cn/20020417/ca327764.htm>
- ▶ Fight spam on the Internet: <http://spam.abuse.net/>
- ▶ Network Abuse Clearinghouse: <http://www.abuse.net/>
- ▶ List of All Known DNS-based Spam Databases: <http://www.declude.com/JunkMail/Support/ip4r.htm>
- ▶ Junk e-mail and spam: <http://www.ecofuture.org/jmemail.html>
- ▶ Death to spam: <http://www.mindworkshop.com/alchemy/nospam.html>
- ▶ A tool for tracking down junk e-mailers: <http://www.toppoint.de/~zoc/gspam.html>

## 7. Filter-Software gegen Spamming

- ▶ Diverse Windows Anti-Spam Tools 1: (<http://www.tucows.com/>), kostenlos
- ▶ Diverse Windows Anti-Spam Tools 2 ([email.about.com/cs/winspamreviews](http://email.about.com/cs/winspamreviews)), kostenlos
- ▶ AntiSpamWare ([www.antis spamware.de](http://www.antis spamware.de))
- ▶ eXpurgate ([www.eleven.de](http://www.eleven.de))
- ▶ K9 ([keir.net/k9.html](http://keir.net/k9.html)), kostenlos
- ▶ Mailshield Desktop ([www.lyris.com](http://www.lyris.com))
- ▶ Mailwasher Pro ([www.mailwasher.net](http://www.mailwasher.net)), kostenlos
- ▶ Mozilla ([www.mozilla.org](http://www.mozilla.org)), kostenlos
- ▶ Heise iX-Magazin ([www.heise.de/ix/nixspam](http://www.heise.de/ix/nixspam))
- ▶ No Spam Today (<http://www.nospamtoday.com/>)
- ▶ Pac Spam light ([www.heitho.de](http://www.heitho.de))
- ▶ Spamagent ([www.spytech-web.com](http://www.spytech-web.com))
- ▶ Spam Assassin ([spamassassin.org](http://spamassassin.org)), kostenlos
- ▶ Spambully für Outlook ([www.spambully.com](http://www.spambully.com)), kostenlos
- ▶ SpamEater Pro (<http://www.hms.com/download.asp>), kostenlos
- ▶ Spamihilator ([www.spamihilator.com](http://www.spamihilator.com)), kostenlos
- ▶ SpamKiller ([www.spamkiller.com](http://www.spamkiller.com))
- ▶ SpamPal (<http://www.spampal.de/pmwiki/pmwiki.php>), kostenlos
- ▶ SuperSpamKiller Pro ([www.superspamkiller.de](http://www.superspamkiller.de))
- ▶ The Spam Bouncer (Linux) ([www.spambouncer.org](http://www.spambouncer.org)), kostenlos
- ▶ Werbeblocker für UNIX und Windows: <http://www.junkbuster.com/>, kostenlos
- ▶ Securepoint Spam Filter (<http://www.securepoint.de>)
- ▶ Ad Nuker Popup Blocker & Spam (<http://www.zdnet.de/downloads/prg/e/f/de0EEF-wc.html>), kostenlos
- ▶ Pegasus Mail 4.41 mit Bayes-Spam-Filter ([http://www.pmail.com/downloads\\_maine\\_t.htm](http://www.pmail.com/downloads_maine_t.htm)), kostenlos
- ▶ SPAMfighter ([http://www.spamfighter.com/Lang\\_DE/Product\\_Info.asp](http://www.spamfighter.com/Lang_DE/Product_Info.asp)), kostenlos