



e-f@cts

Informationen
zum E-Business

Innovationspolitik, Informationsgesellschaft, Telekommunikation

Schwerpunkt

Jeder, der eine E-Mail-Adresse besitzt, kennt das Problem: Spam! Was ist Spam? Wie ist die Rechtslage? Wie kann man Spam vermeiden oder Spammer verfolgen?

► ab Seite 1

Fakten & Zahlen



► ab Seite 3

E-Business-ABC

Administrator, DNS-Adresse, Domain, Hostprovider, IP-Adresse, Mail-Header

► ab Seite 5

Praxis & Technik

Praxisleitfaden für erwünschtes Online-Direktmarketing

► Seite 6



Kommunikation und Spam

Jeder, der eine E-Mail Adresse besitzt, kennt das Problem: Regelmäßig kommen unerwünschte E-Mails, die für Produkte oder Dienstleistungen werben. Gemeinhin werden solche Mails als „Spam“ bezeichnet. Man spricht auch von „Junk Mail“, „Bulk Mail“ oder UCE (Unsolicited Commercial E-Mail).

Spam-Aufkommen angestiegen

Seit Januar 2006 ist das Spam-Aufkommen erneut gestiegen. In Deutschland sind 56,9 Prozent aller eingehenden Mails Spam-Nachrichten (Quelle: messagelabs.com). Zudem kommt es nunmehr verstärkt zum Einsatz von Trojanern, mit deren Hilfe Angreifer fremde Computer ferngesteuert für den Spam-Versand zweckfremden können. Im Jahr 2006 wurden mehr als 90 Prozent aller Spam-Mails von solchen infizierten Computern, sog. Zombie-Pcs verschickt (Quelle: sophos.de).

Zunahme von Image-Spam

Ende 2005 tauchte ein neues Spam-Verfahren auf – das sog. Image-Spam. Hierbei werden Werbebotschaften in unterschiedliche Arten von Bildern integriert, um dadurch die Spam-Filter zu überlisten. Zugleich führt dies zum starken Anstieg der Größe der Spam-Mails, was die Überlastung und Verstopfung der E-Mail Konten zur Folge haben kann.

Spam-Kosten bei Providern und Empfängern

Massenmails sind für den Absender kostengünstig. Wenn er eine Nachricht an 100.000 E-Mail-Adressen schickt, entstehen bei ihm nur minimale Kosten. Es gibt Programme, die den vollautomatischen Versand von Millionen von E-Mails ermöglichen. Der größte Teil fällt bei Providern und Empfängern an. Der Server des Providers muss die Liste der 100.000 Mailadressen abarbeiten. Den privaten Empfänger kostet der Spamdowload vor allem Zeit und Speicherkapazität sowie Entgelt für die Onlineverbindung.

Kommunikation und Spam



Inhalt

Schwerpunkt

Jeder, der eine E-Mail-Adresse besitzt, kennt das Problem: Spam! Was ist Spam? Wie ist die Rechtslage? Wie kann man Spam vermeiden oder Spammer verfolgen?

► ab Seite 1

Fakten & Zahlen



► ab Seite 3

E-Business-ABC

Administrator, DNS-Adresse, Domain, Hostprovider, IP-Adresse, Mail-Header

► ab Seite 5

Praxis & Technik

Praxisleitfaden für erwünschtes Online-Direktmarketing

► Seite 6

Spam vermeiden

Es ist effektiver, Spam zu vermeiden als zu bekämpfen. Es gibt eine ganze Reihe von Möglichkeiten, die Zahl der Spam-Mails zu reduzieren:

Alternativer E-Mail-Account

Zunächst sollte man dafür sorgen, dass Spammer erst gar nicht an die im normalen E-Mail-Verkehr genutzte E-Mail-Adresse herankommen. Internetnutzer, die ihre Identität bei Teilnahme an Gewinnspielen, bei der Registrierung von Online-Diensten oder beim Schreiben in Newsgroups häufiger preisgeben, riskieren, dass ihr Mail-Briefkasten mit lästigen Werbebriefen überfüllt wird. Denn gerade die Newsgroups sind bei Spammern äußerst beliebte „Jagdreviere“. Darum sollte man sich für bestimmte Internetaktivitäten alternative E-Mail-Accounts einrichten. Solche zusätzlichen und ggf. nur temporären Mail-Adressen gibt es günstig oder sogar kostenlos bei Freemail-Providern (z. B. web.de, gmx.de, yahoo usw.).

Einsetzen von Filterprogrammen

Viele der Standard-E-Mail-Programme sind mittlerweile in der Lage, alle empfangenen E-Mails nach bestimmten Adressen zu filtern und Nachrichten einer bestimmten E-Mail-Adresse oder von einer bestimmten Domain (z. B. @sexversand.de) zu blockieren. Dafür muss man als Nutzer die betreffenden Adressen in die Rubrik eingeben. Beispiel Outlook: unter „Aktionen/Junk-E-Mail/Zur Liste der Junk-E-Mail-Versender hinzufügen“.

Außerdem gibt es zahlreiche externe Hilfsprogramme für alle Betriebssysteme, die die eigene Mailbox überprüfen und unerwünschte E-Mails löschen oder in einem gesonderten Bereich des Postfachs speichern, noch bevor man die Mailbox zum Lesen öffnet.

Mail-Adressen kodieren

Um Spam zu vermeiden, kann man auf der eigenen Internetseite E-Mail-Adressen nicht in der üblichen Form angeben, sondern eine Kodierung im ASCII-Format benutzen. Während auf der für Internetnutzer sichtbaren Oberfläche der Webseite die E-Mail-Adresse in ihrer norma-

len Form erscheint, wird sie im Rahmen des Quelltextes ausschließlich durch die ASCII-Zeichenfolge abgebildet. Da die Adressen-Suchprogramme der Spam-Versender lediglich den Quelltext einer Internetseite durchsuchen und den ASCII-Code auch nicht in die ursprüngliche Mail-Adresse zurück übersetzen können, ist Ihre E-Mail-Adresse somit wirksam geschützt. Aus der Mail-Adresse info@bmwi.bund.de würde im Quelltext: `info@bmwa.bund.de`.

Mail-Adressen kodieren können Sie mit einem entsprechenden Encoder unter www.wbwip.com/wbw/emailencoder.html.

Spam zurückverfolgen

Hat es doch einmal eine Spam-Mail durch alle Filter in die eigene Mailbox geschafft, so können Sie diese E-Mail nicht nur einfach löschen, sondern versuchen, den Absender ausfindig zu machen, um gegen ihn vorzugehen. Nicht immer lohnt sich jedoch der Aufwand, da viele Spammer aus dem Ausland kommen und es häufig schwierig ist, sie dort zu verfolgen.

Um Spammer zu ermitteln, sollten Sie die folgenden Hinweise beachten:

► Bei offensichtlich nicht seriösen Firmen, insbesondere bei Aktien- und Medikamenten-Spam, sollten Sie auf die Werbe-E-Mail nicht antworten, auch wenn mittlerweile fast alle dieser Werbenachrichten mit Zeilen wie „For removal from any future mailings, just send a blank e-mail to...“, (Wenn wir Sie aus unserem Verteiler streichen sollen, senden Sie eine leere E-Mail an...) enden.

Eine Antwort auf eine Spam-Mail würde dem Spammer ggf. nur deutlich zeigen, welche Mail-Adresse Sie nutzen. Weitere Spam-Mails würden unweigerlich folgen.

► Darüber hinaus führen direkte Antworten in vielen Fällen nicht zum Erfolg (also zum Spammer), da deren E-Mail-Adressen in der Regel gefälscht sind. Oder aber der Spammer hat einen der von vielen Providern kostenlos angebotenen E-Mail-Accounts für nur eine Aktion oder nur kurzfristig genutzt.



► Es empfiehlt sich vielmehr, die wahre Herkunft der meistens gefälschten Spam-Mail festzustellen und dann die Spam-Mail an den Administrator des Servers weiterzuleiten. Dafür muss man den so genannten Mail-Header ermitteln. Wie man Mail-Header für die gängigen Mail-Programme heraus bekommt, ist hier genau beschrieben: th-h.de/faq/headerfaq.php3#headerzeigen.

Mail-Provider benachrichtigen

Wenn Sie über den E-Mail-Header den Provider, über den Spam verschickt wurde, ermittelt haben, können Sie unter www.openrbl.org mittels Eingabe der IP-Adresse oder DNS-Adresse (s. S. 5 und 6, E-Business ABC) des Providers erfahren, ob der Server in einem größeren Netzwerk arbeitet. Hierhin sollten Sie dann Ihre Beschwerde richten. Fast alle Provider-Administratoren

Rufnummern-Spam

Beim Rufnummern-Spam werden gezielt Rufnummern und vor allem so genannte Mehrwertdiensterufnummern (z. B. 0190-Nummern) beworben. Dafür nutzen einige Anbieter nicht nur das Internet, sondern auch andere Medien wie Telefax, SMS oder so genannte Ping-Anrufe. Bei letzteren erhält ein Teilnehmer einen kurzen Anruf, der ausreicht, um die Rufnummer zu hinterlassen. Diese – meist kostspielige Mehrwertdiensterufnummer – erscheint in der Liste der versäumten Anrufe. Ruft der Teilnehmer zurück, fallen oft über- teuerte Gebühren an.

Um gegen Rufnummern-Spam vorzu- gehen, können Teilnehmer, die eine uner- wünschte Werbung mit einer Rufnummer erhalten, sich telefonisch oder per E-Mail an die Bundesnetzagentur wenden. Dort wird der Fall schnell geprüft.

Auf den Internetseiten der Bundesnetz- agentur sind bereits Hunderte von Spam- Nummern aufgelistet. Die Konsequenzen für den Anbieter: von einer Abmahnung bis hin zu einer Abschaltung der Rufnum- mer und einem Bußgeld bis zu 100.000 €.

haben zu diesem Zweck mittlerweile spezielle E-Mail-Adressen (z. B. abuse@provider.com) ein- gerichtet. Im Zweifelsfalle funktioniert meist auch die Anschrift postmaster@provider.de. Dabei ist es sehr wichtig, dem Administrator die komplette Spam-Mail inklusive des gesamten Headers zu senden und damit niemals länger als etwa drei Tage zu warten. Sonst wird eine Bearbeitung erheblich schwieriger. Unter Um- ständen erfährt ein Administrator erst auf diese Weise, dass sein Mail-Server zur Verteilung der Spam-Mails missbraucht wurde.

Werbekunden-Provider benachrichtigen

Man kann als Spam-Opfer seine Beschwerde auch an den Provider des Werbenden richten (= Hostprovider). Dies ist aber nur dann sinn- voll, wenn der Versender der Spam-Mail und derInhaber der in der Mail angegebenen Web- seite identisch sind. Die meisten dieser Host- provider haben in ihren Allgemeinen Geschäfts- bedingungen Klauseln, die Spam-Aktionen ver- bieten. Betreibt ein Kunde dennoch Spamming, kann der Hostprovider seinen Vertrag kündi- gen. Den Hostprovider der beworbenen Seite ermitteln Sie am schnellsten über die so genann- ten Whois-Abfragen. Dabei müssen Sie hier die vollständige URL der fraglichen Web-seite ein- geben. Bei de-Domains kann man eine solche Abfrage über die Denic-Datenbank starten (www.denic.de/de/whois/index.jsp). Für com-, net- oder org-Domains empfehlen sich z. B. die Whois-Dienste von www.networksolutions.com, www.lund1.com oder www.united-domains.de.

Über Spam beschwerden: Anti-Spam-Bündnis

Sie können (und sollten) sich über Spam und Spammer beschweren. Zu diesem Zweck haben sich der Verband der deutschen Internetwirt- schaft e.V. (eco), die Verbraucherzentrale Bun- desverband, die Zentrale zur Bekämpfung unlauteren Wettbewerbs e.V. und die Bundes- netzagentur zu einem Bündnis zusammenge- schlossen, um gemeinsam gegen Spammer vor- zugehen.

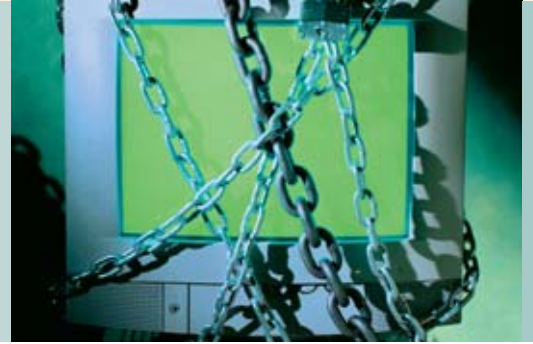
Sie können sich bei Erhalt von E-Mail-Spam an folgende Stellen wenden:

► **Verband der deutschen Internetwirt- schaft e.V. (eco)**

In Deutschland liegt der Anteil der unerwünschten E-Mail- Werbung bei ca. 56,9 Prozent.

Quelle: messagelabs.com

Kommunikation und Spam



Viele Spammer kommen aus dem Ausland, und es ist häufig schwierig, sie dort zu verfolgen.

Internet: www.internet-beschwerdestelle.de
 Hotline: hotline@eco.de
 E-Mail: allgemeiner-spam@internet-beschwerdestelle.de, besonderer-spam@internet-beschwerdestelle.de

► **Verbraucherzentrale Bundesverband**

Internet: www.vzbv.de
 E-Mail: beschwerdestelle@spam.vzbv.de

► **Zentrale zur Bekämpfung unlauteren Wettbewerbs e.V.**

Internet: www.wettbewerbszentrale.de
 E-Mail: mail@wettbewerbszentrale.de

Alle Eingänge werden geprüft und bearbeitet. Jede Beschwerde muss den vollständigen E-Mail-Header und den Inhalt der Spam-Mail enthalten, damit die verantwortlichen Personen schnell und zuverlässig ermittelt werden können.

nen. Darüber hinaus werden Informationen an Partner-Hotlines und Antispam-Organisationen im Ausland weitergeleitet. Die Erfahrung hat gezeigt, dass dadurch die Spam-Belästigung spürbar reduziert werden kann.

Wenn in der Werbe-E-Mail deutsche Telefonnummern beworben werden und bei klassischem Rufnummernspam kann man sich zudem an die Bundesnetzagentur wenden.

Internet: www.bundesnetzagentur.de.

So werden Ihre E-Mails nicht als Spam blockiert

Damit ihre Kunden weniger belästigt werden, richten immer mehr Provider Spam-Filter ein, die einen Großteil unerwünschter Werbung blockieren. Diese Spam-Filter sieben aber irrtümlich auch angeforderte Mails oder Newsletter aus. In Deutschland sperren Provider derzeit 10 bis 20 Prozent der angeforderten Newsletter zu Unrecht als vermeintliche Spam-Mails. Dabei können Versender einiges dafür tun, damit ihrer Mail und ihrem Newsletter dieses Schicksal erspart bleibt. Hier die wichtigsten Tipps:

Keine unangeforderten E-Mails versenden

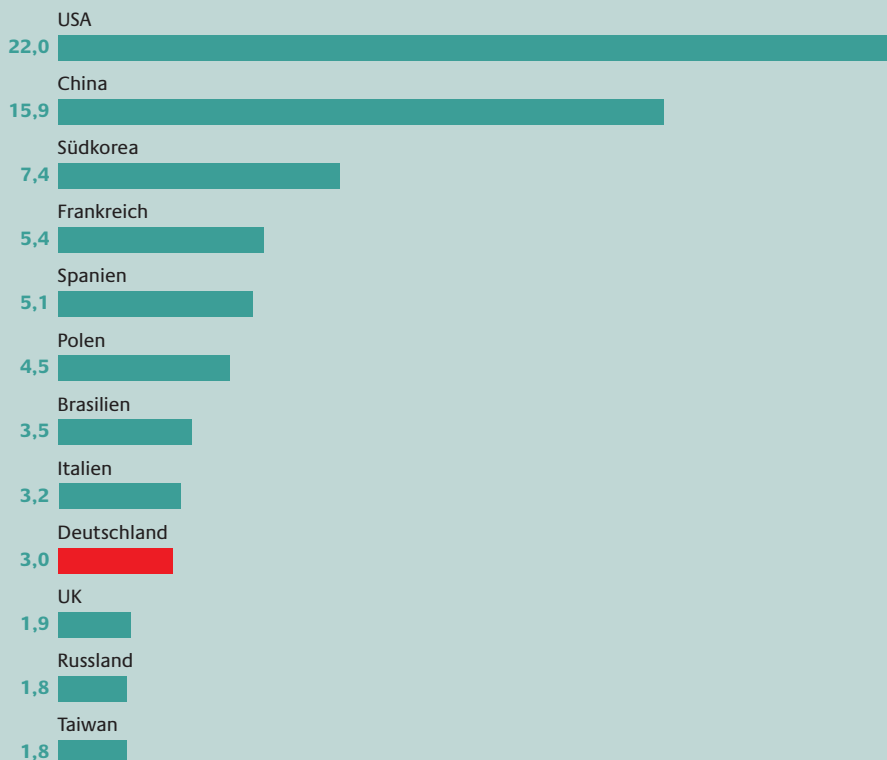
Stellen Sie organisatorisch wie technisch sicher, dass niemand gegen seinen Willen E-Mails von Ihnen zugesandt bekommt. Sorgen Sie auch dafür, dass die E-Mail-Empfänger, bei denen Sie die Einwilligung einholen, auf ihr Widerspruchsrecht (Kündigungs- bzw. Abbestellmöglichkeit) hingewiesen werden. Mangelnde Sorgfalt führt zu Beschwerden durch Ihren Provider und der Einschätzung, dass es sich um Spam handelt.

Seriöse Absenderadresse handhaben

Nicht nur die Adresse des Adressaten, auch die des Absenders sagt viel über die zu erwartende Qualität des E-Mail-Inhalts aus. E-Mail-Marketing-Aktionen, die aus organisatorischen Gründen nicht von einer persönlichen Absenderadresse verschickt werden sollen, werden eher zugestellt, wenn sie aus vollständigen Wort- oder Namenskombinationen bestehen, z. B. newsletter@company.de oder Tom.Mustermann@company.de.

Herkunft von Spam-Mails

2006 – Angaben in %



Quelle: Messagelabs 2006



Keine Reizworte in der Betreffzeile und im Text wählen

Spam-Filter reagieren allergisch auf bestimmte Reizworte, Zeichen, Slogans, Abkürzungen oder gar leere Betreffzeilen. E-Mails, die gut ankommen sollen, sollten Sie mit einer eindeutig informativen Wortwahl formulieren. Die in Spam-Filtern aktiven Wortlisten sorgen für eine sofortige Kennzeichnung der Mail als Spam, wenn verdächtige Worte einfach oder mehrfach vorkommen.

Betreffzeilen wie „Gewinnen Sie jetzt“ oder „500 Prozent in nur 4 Wochen“ werden als Spam markiert oder eliminiert. Zu vermeiden sind Floskeln wie z. B. „Super-Sonder-Special-Angebot“ und Abkürzungen wie XXL, Betreffzeilen mit Ausrufungszeichen und GROSS-BUCHSTABEN. Generell sollten Sie auf mehrfache Sonderzeichen verzichten. Am besten orientieren Sie sich an den typischen seriösen Wort- und Stilelementen eines klassischen Geschäftsbriefs.

E-Mail-Anhang mit Bedacht wählen

Spam-Filter identifizieren und vermuten mittlerweile Spam in allen möglichen Anhang-Formaten (doc, jpg usw.). Auch bei der Versendung von Dateien, die eigene Programmierbefehle enthalten (so genannte exe-Dateien), ist Zurückhaltung geboten. Ausnahme: das Adobe Portable Document Format (pdf). Versender seriöser Informationen sollten daher Newsletter oder ähnliches als pdf-File anhängen.

HTML-Darstellung vermeiden

Spammer haben eine Vorliebe für HTML-formatierte E-Mails (z. B. zur Darstellung von Grafiken). Daher sollten Sie bewusst darauf verzichten und Ihre E-Mails als „Plain Text“ formatieren (evtl. mit Hyperlinks auf HTML-Webseiten).

Keinen Anlass zu Beschwerden geben

Durch Spam belästigte E-Mail-Empfänger können sich bei ihrem Provider beschweren. Beschwerden sind für Provider der zuverlässigste

Fortsetzung auf Seite 7

E-Business-ABC

Administrator

Er hat meistens erweiterte Rechte in komplexeren Internetauftritten. Er kann z. B. auf Webseiten, in Mailboxen oder Online-Foren Beiträge löschen oder Benutzer sperren.

DNS-Adresse

Die DNS-Adresse ist der Domain-Name (z. B. www.bmw.de) zu der eine bestimmte IP-Adresse gehört. Der Domain Name Server, auch als DNS-Server bezeichnet, ist ein Rechner, der Listen mit IP-Adressen (= Nummern) und deren dazu gehörige Domain-Adressen verwaltet.

Spam: Die Rechtslage

Die Versendung von unerwünschten E-Mails mit besonders schädlichen Inhalten ist in der Regel strafbar. Dies gilt z. B. für

- ▶ Spam-Mails mit pornographischen Inhalten, wenn diese auch an Minderjährige gesandt werden
- ▶ E-Mails mit betrügerischem Inhalt
- ▶ E-Mails, mit denen der Versender versucht, durch Vortäuschen einer anderen Identität an Passwörter und Zugangsdaten von Bankkonten zu gelangen („Phishing-Mails“)
- ▶ E-Mails, die Computerviren oder -würmer enthalten

Auch bei an sich „legalem Inhalt“ ist das Zusenden elektronischer Post mit Werbecharakter (Spamming) in Deutschland gemäß § 7 Absatz 2 Nr. 3 UWG grundsätzlich unzulässig, wenn der Adressat der Zusendung zuvor nicht zugestimmt hat. Erlaubt sind Werbe-mails nur mit der ausdrücklichen vorherigen Einwilligung der Empfänger (Opt-in). Der Absender sollte aber nachweisen können, dass eine Einwilligung wirklich vom Empfänger stammt. Erlaubt sind Werbemails auch dann, wenn ein Unternehmer im Zusammenhang mit dem Verkauf einer Ware oder Dienstleistung von einem Kunden dessen Mail-Adresse erhalten hat und sie dann für eigene ähnliche Waren oder Dienstleistungen verwendet. Erlaubt ist dies aber nur, solange der Kunde der Verwendung nicht widersprochen hat und bei jeder Verwendung klar und deutlich darauf hingewiesen wird, dass er der Verwendung jederzeit widersprechen kann.

Liegt ein Verstoß vor, so können Wettbewerber und anerkannte Klageverbände gerichtlich Unterlassung und Schadenersatz verlangen. Zudem besteht ein Gewinnabschöpfungsanspruch.

Das am 01.03.2007 in Kraft getretenen Telemediengesetz soll ebenfalls einen verbesserten Schutz vor irreführenden Angaben bei E-Mail-Werbung schaffen. Charakter und Herkunft einer E-Mail-Werbung müssen sich künftig bereits aus Kopf- und Betreffzeile der Nachricht ergeben. Der Empfänger soll frei entscheiden können, wie er mit der E-Mail umgeht ohne sie zuerst öffnen zu müssen. Zuwiderhandlungen können mit einem Bußgeld bis zu 50.000 € belegt werden.

Praxis-Leitfaden für erwünschtes Online-Direktmarketing

Dieser Leitfaden enthält die wichtigsten Punkte, die Sie bei der praktischen Umsetzung der „Richtlinie für erwünschtes Online-Direktmarketing“ beachten sollten. Er zeigt außerdem, wie die Richtlinie nicht ausreichend umgesetzt wäre.

Quelle: Verband der Deutschen Internetwirtschaft e.V. (eco) 2002; www.eco.de

E-Business-ABC

Domain

Die weltweit eindeutige Adresse einer Internetpräsenz. Beispiel: www.bmw.de. Der letzte Teil des Domainnamens (Top-Level-Domain) kennzeichnet meist das Land (de für Deutschland). Die so genannten generischen Domains bezeichnen die Art der Internetpräsenz (z. B. com für kommerziell, org für Organisationen).

Hostprovider

Provider des Hosts. Host = Englisch für Gastgeber: Ein Computer, der im Internet oder in einem anderen Netzwerk die Daten oder Dienste für angeschlossene Rechner bereitstellt und auf den permanent zugegriffen werden kann.

IP-Adresse

Nummer, die jedem Computer zugeordnet wird, um die Kommunikation zwischen Nutzern im Internet zu ermöglichen.

Mail-Header

Teil einer E-Mail, die Informationen über Inhalt, Absender und Sendedatum liefert.

Newsgrup

Diskussionsforum oder „Schwarzes Brett“ zu bestimmten Themen im Internet. Hier kann man nach Neuigkeiten „stöbern“, Fragen stellen und – wenn man „eingreifen“ will, Fragen beantworten.

Permission Marketing

Hier wird die Zustimmung des Empfängers zum Erhalt der E-Mail eingeholt.

Anforderung

1. Verständliche Erklärungen
Erklärungen in verständlichen Worten

2. Nur angeforderte Werbung
Interessenten erhalten nur explizit selbst angeforderte Werbung

2.1 Adressherkunft

2.2 Anbieterkennzeichnung

2.3 Online-Anforderung

2.4 Bestätigung

3. Adressverwendung transparent
Adressen werden nur zum angegebenen Zweck verwendet

4. Empfänger können abbestellen
Empfänger können sich selbst vom Verteiler streichen

5. Hinweis auf Abbestellfunktion
Jede Nachricht enthält Hinweis auf Kündigungsmöglichkeit

6. Keine Adressweitergabe
Adresse wird nicht ohne Zustimmung weitergegeben

7. Datenschutzerklärung
Umgang mit persönlichen Daten wird in einer Datenschutzerklärung erläutert

Praktische Umsetzung

Eindeutige und einfache Formulierung

Opt-In: Versand nur nach vorab eingeholter Zustimmung des Empfängers

Hyperlink auf Homepage in jeder Botschaft
Homepage: Hyperlink auf Impressum

Datensparsamkeit:
nur abfragen was notwendig ist
Anonymen und pseudonymen Bezug ermöglichen

Umgehende Bestätigung des Bezugs regelmäßiger Informationen

Hinweis auf Umfang, Inhalt und Frequenz der Zusendungen vor der Datenerhebung

Bequemes Abbestellen per Web-Formular, E-Mail, SMS oder Telefon Bestätigung der Abmeldung

Verständliche Beschreibung des Abbestellvorgangs

Adressweitergabe/Verwendung nur für die Erbringung der Kernleistung
Hinweis auf das Land, in dem die Datenverarbeitung stattfindet

Hinweis auf Datenschutzrichtlinie des Unternehmens vor der Dateneingabe
Verweis auf Datenschutzrichtlinie durch Hyperlink

Unzureichende Lösung

Wesentliches im Kleingedruckten

E-Mail-Adressen aus Webverzeichnissen und Bestandsdaten ohne Einwilligung
Opt-Out: unaufgeforderter Versand mit gleichzeitiger Abbestellfunktion

Keine Anschrift
Kein Vertretungsberechtigter
Versteckte Anbieterkennzeichnung

Pflichtfelder bei der Angabe des Namens
Leistung nur gegen Übermittlung der Daten: Koppelungsverbot, wenn der Diensteanbieter eine Monopolstellung innehat

Fehlende Bestätigung der Anmeldung

Vorangeklickte Zustimmungsfelder zur Weiterverwendung von Daten

Keine Abbestellfunktion
Nichtselbständige Ausführung

Adressweitergabe zu Marketingzwecken ohne explizite Zustimmung

Hinweis auf AGB
Hinweis erst NACH Dateneingabe
Hinweis auf Verwendung der Daten nur innerhalb der eigenen Firmengruppe



Fortsetzung von Seite 5

Indikator bei der Einschätzung, ob es sich um unerwünschte Werbung handelt. Bei zertifizierten (Massen-)Versendern (certified sender alliance) können Beschwerden beim Verband der Deutschen Internetwirtschaft e.V. (eco) zu einer Rüge bzw. einem vorübergehenden oder dauerhaften Ausschluss aus der weißen Liste führen (s. „Vertrauenswürdigen Mailserver nutzen“).

Rückläufer aus dem Verteiler nehmen

Wenn Sie Adressen regelmäßig anschreiben und nicht zustellbare Rückläufer aus dem Verteiler löschen, so reduziert sich Ihre Fehler-Rückläufferrate. Diese Rückläufferrate ist für Provider und Spam-Filter ein wichtiger Indikator bei der Einschätzung, ob es sich um Spam handelt. Mögliche Folge: Kündigung des Vertrags.

Vertrauenswürdigen Mailserver nutzen

Wenn über einen Mailserver nur seriöse E-Mails versandt werden, steigt dessen Reputation. Wird gespamt, landet der Mailserver auf schwarzen Listen. Verpflichtet sich der Mailserverbetreiber gegenüber den Providern, selbst gegen Spam vorzugehen, besteht die Chance, auf eine positive weiße Liste zu kommen. Versenden Sie deshalb nur über vertrauenswürdige Mailserver, die eventuell in einer solchen Whitelist stehen. Ein Zentralregister, in dem Sie feststellen können, ob z. B. ein Provider auf einer schwarzen Liste steht, finden Sie unter www.senderbase.org (IPNummer des „verdächtigen“ Providers eingeben). Für seriöse gewerbliche Massenversender hat der Verband der deutschen Internetwirtschaft e.V. (eco) eine Whitelist

Informationen zu Spam

- ▶ BMWi: www.bmwi.de (s. Technologie und Information, Informationsgesellschaft)
- ▶ Verbraucherzentrale Bundesverband: www.vzbv.de
- ▶ Verband der deutschen Internetwirtschaft e.V. (eco): www.eco.de
- ▶ Zentrale zur Bekämpfung unlauteren Wettbewerbs e. V.: www.wettbewerbszentrale.de

geschaffen, die nur zertifizierte Massenversender enthält: unter www.eco.de/whitelist.

Spam-Assassin-Test

Der einfachste Weg, die eigene E-Mail auf mögliche Spam-Klassifikation zu prüfen, ist der Spam-Assassin-Test. Unter www.lyris.com/contentchecker/ sowie unter www.heise.de/ix/nixspam/spamtest/ können Sie Ihre Mail testen.

Selbstverpflichtung der Initiative „Richtlinie für erwünschtes Online-Direktmarketing“

Die Initiative „Richtlinie für erwünschtes Online-Direktmarketing“ setzt sich dafür ein, dass Unternehmen nur noch E-Mails versenden, wenn diese ausdrücklich vom Empfänger erwünscht sind („Permission Marketing“). Die Richtlinie erläutert detailliert, wie erwünschtes Online-Marketing praktisch umgesetzt werden kann. Konkret verpflichten sich die angeschlossenen Unternehmen, die in der Richtlinie genannten sieben Regeln einzuhalten:

Die sieben Regeln für erwünschtes Online-Direktmarketing

1. Erklärungen in verständlichen Worten

Ziel des so genannten Permission Marketing ist der Aufbau einer vertrauensvollen, gleichberechtigten Kundenbeziehung. Um dieses Vertrauen aufzubauen, verpflichten sich Unternehmen zu einer klaren, verständlichen Sprache, damit das Vertrauen nicht durch Missverständnisse belastet wird, die bei deutlicherer Erläuterung vermeidbar gewesen wären.

2. Interessenten erhalten nur selbst angeforderte Werbung

Interessenten erhalten nur Informationen, die sie vorher explizit angefordert haben. Sie bestimmen selbst, über welches Ausgabemedium (E-Mail, SMS, Telefon) sie Informationen erhalten möchten. Die Anforderung regelmäßiger elektronischer Informationsdienste wird bestätigt, wobei mit der Bestätigung auch die Möglichkeit zu einer sofortigen Kündigung des An-

E-Business-ABC

Phishing

Phishing (= Password fishing) zielt darauf, von Internet-Nutzern persönliche Daten zu „fischen“. Beim Phishing werden Massenmails verschickt, die vorgeben, z. B. von einer Bank zu stammen. Die Mails enthalten stattdessen Links auf (betrügerische) Internetseiten. Der Adressat gibt z. B. auf dieser vermeintlichen Bank-Internetseite seine PIN und TAN ein. Damit können die Täter dann von der „echten“ Internetseite der Bank Geld vom Konto des Getäuschten abheben.

URL

Komplette Adresse einer Internetseite.

Phishing-Sites

Anteil in %



Quelle: www.antiphishing.org 2006

Kommunikation und Spam



Impressum

Herausgeber:

Bundesministerium für Wirtschaft und Technologie (BMWi)
Öffentlichkeitsarbeit
11019 Berlin
info@bmwi.bund.de
www.bmwi.de

Redaktion:

Bernd Geisen, Regine Hebestreit,
PID Arbeiten für Wissenschaft und Öffentlichkeit GbR
Menzenberg 9, 53604 Bad Honnef
Tel.: 02224 90034-0, Fax: 02224 90034-1
info@pid-net.de

Mitarbeiter dieser Ausgabe:

Markus Goss
GROUP Technologies
Sven Karge
Verband der Deutschen
Internetwirtschaft e.V. (eco)
Ben Schlüßler
Kompetenzzentrum EC-SH, Kiel
Torsten Schwartz
Dr. Schwartz Consulting, Waghäusel

Gestaltung und Produktion:

PRpetuum GmbH, München

Bildnachweis:

MEV, Photodisc

Druck:

Druckpunkt Offset GmbH, Bergheim

Auflage: 10.000

Schwerpunkt der nächsten Ausgabe:

„Kunden finden im Internet“

Wenn Sie dazu Fragen oder Anregungen haben oder Fragen zu anderen Themen der e-f@cts, wenden Sie sich bitte an:

Bernd Geisen, Regine Hebestreit
PID Arbeiten für Wissenschaft und Öffentlichkeit GbR

gebots gegeben wird. Für den Empfänger muss erkennbar sein, von welchem Anbieter er Informationen erhält. Anbieter sollten weitgehend individualisierte Inhalte anbieten und nicht nur Massenversand von Standardnachrichten betreiben.

3. Adressen werden nur zum angegebenen Zweck verwendet

Die Verwendung der von Interessenten angegebenen Adresse geschieht ausschließlich zu dem Zweck, der vorab mitgeteilt wurde. Beispielsweise erhält niemand telefonische Produktangebote, wenn vorher die Telefonnummer ausdrücklich nur für den Fall von Rückfragen im Zusammenhang mit einer Bestellung gegeben wurde. Gleiches gilt für E-Mail-Adressen.

4. Empfänger können sich selbst vom Verteiler streichen

Empfänger können jederzeit den Informationsservice abbestellen und erhalten dann mit schnellstmöglicher Wirkung keine weiteren Informationen mehr zugesandt. Die Abbestellfunktion sollte möglichst bequem realisierbar sein und keine vermeidbare Hemmschwelle darstellen. Eventuell kann die Kündigung noch einmal bestätigt werden.

5. Jede Nachricht enthält Hinweis auf Kündigungsmöglichkeit

Um die Entscheidung zum probeweisen Bezug von Botschaften möglichst leicht zu machen, sollte dieser Bezug jederzeit bequem wieder zu beenden sein. Dazu enthält jede Botschaft einen Hinweis auf die schnellstmöglich wirksame Kündigungsmöglichkeit.

6. Adresse wird nicht ohne Zustimmung weitergegeben

Die eventuelle Weitergabe von Kundenadressen sollte nur auf ausdrücklichen Wunsch von Interessenten stattfinden. Die Erlaubnis hierzu ist durch eine eindeutige Handlung der Interessenten zu erteilen und muss auch deutlich kommuniziert werden.

7. Umgang mit persönlichen Daten wird in einer Datenschutzrichtlinie erläutert

Der Nutzer ist möglichst umfassend über die Verarbeitung von Bestands- und Nutzungsdaten zu unterrichten.

Internationale Zusammenarbeit bei der Spam-Bekämpfung

Unerwünschte E-Mails machen an der Landesgrenze nicht halt. 95 Prozent aller Spam-Mails stammen aus dem Ausland. Spam kann daher nur durch enge internationale Kooperation wirksam bekämpft werden.

EU: Die Europäische Kommission hat ein Anti-Spam Kontakt Netzwerk (Contact Network on Spam-Authorities - CNSA) eingerichtet. Im Mittelpunkt steht die Zusammenarbeit beim Austausch von grenzüberschreitenden Spam-Beschwerden. Deutsche Kontaktstellen im Rahmen dieser Kooperation sind die Spam-Hotline des Verbands der deutschen Internetwirtschaft e.V. (eco), für Rufnummernspam die Beschwerdestelle der Bundesnetzagentur (s. S.3, „Über Spam beschwerden“).

OECD: Die Anti-Spam-Task Force der Organisation für wirtschaftliche Zusammenarbeit und Entwicklung (OECD) hat ein sog. „Anti-Spam-Toolkit“ erarbeitet, in dem verschiedene Ansätze gegen Spam zusammengefasst sind.
www.oecd.org

ITU: Die Internationale Fernmeldeunion (ITU) hat vereinbart, das Thema Spam auch im Rahmen der „Internet-Governance“ zu behandeln. Auch hier ist das BMWi in die laufenden Arbeiten eingebunden.
www.itu.int/home

FTC: Das BMWi unterstützt die Operation-Spam-Zombie der US Federal Trade Commission. Bei der Operation handelt es sich um eine weltweite Aufklärungskampagne der FTC mit dem Ziel, Internet Service Providern und Netzwerkbetreibern Möglichkeiten aufzuzeigen, die Versendung von Spam über „Zombie-Rechner“ zu verhindern. Bei „Zombie-Rechnern“ handelt es sich meist um gewöhnliche PCs, die Spam-Versender mit Hilfe von Viren und Trojanern ohne Wissen des Eigentümers für die Versendung von Spam-Mails missbrauchen.
www.ftc.gov