Arbeitskreis Vertrauen & Sicherheit

Leitfaden E-Mail-Werbung für Online-Shops

Dieser Leitfaden soll Online-Shopbetreibern Grundlagen für eine erfolgreiche Vermarktung ihrer Angebote per E-Mail vermitteln, damit ihre E-Mail-Werbung nicht in den Spam-Ordnern der User und Provider landet.

Inhaltsverzeichnis

1. Einleitung

E-Mail-Werbung – der Weg zum Kunden ist schwer

40 Prozent aller E-Mails werden heute als Spam-Mails bezeichnet. Weltweit werden geschätzte 12.4 Milliarden E-Mails verschickt – und das täglich! Für die E-Commerce Branche geht es längst nicht mehr nur um die entstandenen Kosten, sondern um das Vertrauen der Kunden. Aber wie können sich Online-Shops und Internet Service Provider effektiv gegen die Einordnung erlaubnisbasierter Werbeemails als „SPAM"-Mails wehren? Ein Beitrag des Arbeitskreises Sicherheit und Vertrauen der Fachgruppe E-Commerce im BVDW.

Viele Internet Service Provider (ISP) suchen nach einer Lösung, um ihre Kunden vor Massen-E-Mails zu schützen. Deshalb setzen sie Spam-Filter ein, um eine Vorauswahl der Mails zu treffen. Nachrichten, die dabei als unerwünschte Werbe-E-Mails eingeordnet werden, landen häufig im Spamverdacht-Ordner oder bleiben gänzlich an SPAM-Filtern hängen. Laut eigenen Angaben sortiert z. B. AOL jeden Tag 780 Millionen derartiger Mails aus. Trotzdem erhält die entsprechende Abteilung ungefähr vier Millionen Beschwerden über Spam-Mails pro Tag!

Wegen der Ungenauigkeit der Filterverfahren kann es dabei leider passieren, dass seriöse E-Mails fälschlicherweise als Spam markiert werden, sog. „False Positives". Eine Studie von Assurancesys.com ergab, dass ISPs in den USA im Durchschnitt 15% der seriösen E-Mails als unzulässige Werbung aussortierten. Dadurch wird das seriöse E-Mail-Marketing erschwert [absolit].

Diese Umstände stellen die Betreiber von Online-Shops vor die Frage, welche Maßnahmen er treffen kann, damit seine legale und erlaubnisbasierte Werbung den Kunden erreicht. Zum einen sind dabei rechtliche und zum anderen technische Maßnahmen zu beachten.

2. Rechtliche Maßnahmen

Werbe-E-Mails sind heutzutage weit verbreitet und ein einfaches, kostengünstiges Werbemittel. Wenn sie allerdings im Spam-Ordner landen, können sie einen Imageschaden und zudem erhebliche Kosten für das werbende Unternehmen in Form von Schadensersatz und Anwaltshonoraren verursachen. Daher sollten die Folgenden sieben grundlegenden rechtliche Anforderungen an Werbemails beachtet werden.

- Anforderung 1:

  In Deutschland findet das sog. „Opt-In-Prinzip" Anwendung. Dieses besagt, dass sich der Versender elektronischer Werbung vor Versand der Werbung das Einverständnis des Adressaten zum Erhalt der Werbung einholen muss. Eine „Generaleinwilligung" zum Erhalt von Werbung, noch dazu vielleicht versteckt in Allgemeinen Geschäfts- oder Teilnahmebedingungen, reicht nicht aus. Ferner gilt das Gebot der Datensparsamkeit. Das bedeutet, es dürfen nur die Daten erhoben werden, die für die Erbringung der Leistung des Anbieters erforderlich sind.

  Die Zusendung von Werbemails darf also grundsätzlich nur erfolgen, wenn der Empfänger dies ausdrücklich gewünscht hat. Wenn Sie einen eigenen Newsletterverteiler aufbauen, sollten Sie Adressen ausschließlich über das sog. „Double-Opt-In-Verfahren" erheben. Hier wird ein Benutzer nur eingetragen, wenn er eine an ihn gesendete Anmelde-E-Mail zurücksendet bzw. einen Freischaltungslink aktiviert und dadurch bestätigt, dass die Anmeldung durch ihn erfolgte und er in die Verwendung seiner E-Mail-Adresse einwilligt. Das sog. „Confirmed-Opt-In-Verfahren", bei dem der Nutzer zumindest eine Bestätigung per E-Mail über die Aufnahme seiner E-Mail-Adresse in den Verteiler erhält, wird überwiegend auch akzeptiert. Ein einfaches Anmeldeformular ist hingegen nicht ausreichend, denn das werbende Unternehmen trifft im Streitfall die Beweislast, dass der Empfänger dem Erhalt der Email vorher zugestimmt hat. Ohne entsprechende Logfiles oder Datenbankeinträge können Sie im Zweifel nicht beweisen, dass die Anmeldung durch den Benutzer selbst erfolgte.

  Um zu verhindern, dass eine E-Mailadresse nicht vom wirklichen Empfänger in ihre Mailingliste eingetragen wird, ist also vor der ersten Zusendung einer Werbemail eine Bestätigungs-Anfrage (Double Opt-In – E-Mail) an den Empfänger zu richten, ob er sich tatsächlich für den Empfang von werbenden Mails angemeldet hat bzw. in den Verteiler aufgenommen werden will. Es empfiehlt sich hier, dass der Empfänger noch mal eine aktive Handlung, wie das Klicken auf einen Bestätigungs-Link, durchzuführen hat, bevor die Zusendung der Mail erfolgt (Double Opt-In). Bei dieser Bestätigungsmail darf jedoch kein werbender Inhalt enthalten sein, da ansonsten ein von einem Dritten eingetragener Empfänger, rechtliche Ansprüche geltend machen kann.

- Anforderung 2:

  Die Zusendung von Werbe-Mails ist auch – jedoch nur unter sehr engen Voraussetzungen – zulässig. Dies ist nur möglich, wenn der Werbende die E-Mailadresse beim Verkauf einer Ware oder Dienstleistung erhalten hat. Die Werbung darf sich allerdings nur auf seine eigenen Produkte bezieht und diese müssen ähnlich dem Produkt sein, dass der Kunde ursprünglich erworben hat.

  Über diesen Weg kann zum Beispiel nicht - ohne die unter Anforderung 1 beschriebene Einwilligungshandlung - für Schuhe geworben werden, wenn die E-Mailadresse beim Kauf eines Buches erhalten wurde. Weiterhin darf der Kunde der Verwendung seiner E-Mailadresse nicht widersprochen haben. Daher muss er bei der Angabe seiner E-Mailadresse auf die beabsichtigte Kundeninformation hingewiesen werden und es muss ihm die Möglichkeit des Widerspruchs gegeben werden. Aus Gründen des Datenschutzes empfiehlt es sich jedoch, dass auch hier der Kunde seine Zustimmung durch das Setzen eines Häkchens (Opt-In) aktiv erteilen sollte.

- Anforderung 3:

  Der Werbende muss in einem eventuellen Prozess nachweisen, dass sich der Empfänger tatsächlich in die Verteilerliste eingetragen hat. Hierzu reicht es nach einer neuen Gerichtsentscheidung des AG Hamburg (Az. 6 C 404/06) nicht aus, wenn lediglich das unter 1. oder 2. beschriebene Verfahren angewandt wird. Es muss vielmehr individuell jede einzelne Eintragung in den E-Mailverteiler protokolliert werden, so dass dies später individuell belegbar und nachvollziehbar ist.

- Anforderung 4:

  Bei der Versendung der E-Mails muss darauf geachtet werden, dass die E-Mailadressen korrekt geschrieben sind und nicht aus Versehen durch einen Schreibfehler jemand anderes unerwünscht die E-Mail bekommt. Zudem muss sichergestellt sein, dass die E-Mailadressen der Empfänger nicht missbraucht werden können. Daher dürfen Werbemails nur als Blindkopien versandt werden und auf keinen Fall alle E-Mailadressen für alle Empfänger sichtbar sein. Dies würde dem Datenschutzrecht widersprechen und kann zu einem erheblichen Vertrauensverlust für das werbende Unternehmen führen.

- Anforderung 5:

  Der Versender muss für den Empfänger als Absender der Werbemail nach § 6 Abs. 2 TMG, welches seit dem 01.03.2007 gilt, erkennbar sein. Hierzu ist erforderlich, dass der Versender im Header in der Absenderzeile aufgeführt wird. Darüber hinaus darf der kommerzielle Charakter der Mail nicht verschleiert

werden. Im Betreff sollte konkret der Anlass der Mail benannt werden wie beispielsweise: Weihnachtangebot von XY.

- Anforderung 6:

  Der Werbetreibende muss in seiner E-Mail zudem seinen vollständigen Namen (Vor- und Zuname), sofern er eine juristische Person ist (wie zum Beispiel eine GmbH) sämtliche Vertretungsberechtigte, seine Anschrift (kein Postfach), eine E-Mailadresse sowie eine Telefonnummer, seine Handelsregisternummer und bei welchem Handelsregister er eingetragen ist sowie seine Umsatzsteueridentifikationsnummer angeben. Diese Angaben entsprechen insoweit den Daten, die auch als Anbieterkennzeichnung auf einer Homepage unter Kontakt oder Impressum angegeben sein müssen. Die oben angegeben Anforderungen sind hier auf typische Online-Shopbetreiber zugeschnitten.

- Anforderung 7:

  Der Empfänger muss jederzeit die Möglichkeit haben, seine E-Mailadresse aus dem Verteiler zu entfernen. Hierauf muss er auch in jeder E-Mail hingewiesen werden. Es empfiehlt sich zudem, den Empfänger bereits bei Anmeldung für den E-Mailversand hierauf hinzuweisen.

Diese Anforderungen sollen einen kurzen Überblick über die wichtigsten Anforderungen an E-Mailwerbung verschaffen und helfen, die offensichtlichsten Fehler zu vermeiden. Natürlich kann hier nicht jeder juristische Fallstrick behandelt werden und daher kann dieser Überblick grundsätzlich nicht den professionellen Rat eines spezialisierten Anwalts ersetzen. Dieser sollte auch aufgesucht werden, wenn Sie eine Abmahnung erhalten, die Abgabe einer Unterlassungserklärung gefordert wird oder sie gar verklagt werden.

3. Technische Maßnahmen

Auf den ersten Blick hat der Betreiber auf technischer Ebene nicht sehr viele Möglichkeiten zu verhindern, dass seine E-Mails als Spam gekennzeichnet werden oder die IP-Adresse seines Mailservers in die entsprechende Blacklists aufgenommen wird. Diese Entscheidung fällt der „empfangende" Provider, auf den der Betreiber des Shops keinen direkten Einfluss hat.

Eine Strategie verbleibt Ihnen jedoch: Ein Spam-Filter ordnet Nachrichten nach bestimmten Kennzeichen als Spam oder Nicht-Spam ein. Dabei wird vor allem nach Merkmalen gesucht, die in der Vergangenheit häufig bei Spam-Aktionen aufgetreten sind. Durch eine möglichst weitgehende Differenzierung der eigenen Nachrichten von typischen Spam-Mails steigert der Betreiber eines Online-Shops die Wahrscheinlichkeit, dass seine E-Mails als Nicht-Spam eingestuft und daher an den Empfänger ausgeliefert werden. Folgende Merkmale erhöhen beispielsweise die Wahrscheinlichkeit, dass eine Nachricht als Spam eingestuft wird:

- Bestimmte Schlüsselworte im Subject oder Mail-Body, z. B. free, $$$, cash, money, do not reply, lottery, opportunity, urgent
- „Undisclosed recipients" im To-Header
- Nur Grossbuchstaben im Subject
- Betreffzeile in englischer Sprache
- Verwendung von „Re:" im Subject ohne zitierten Text (einer beantworteten Nachricht) im Mail-Body
- HTML-Inhalt, mit Referenzen auf externe Bilder, mit IP-Adressen statt vollqualifizierten Servernamen, mit roter Farbe (#FF0000)
- Verwendung von asiatischen Zeichensätzen
- Versendung von einem Dialup-Rechner (d.h. aus einem Netz, dass typischerweise von Privatpersonen zur Verbindung in das Internet verwendet wird)
- Versendung von einem Mailserver, der nicht korrekt im DNS eingetragen ist, zum Beispiel wenn der IP-Adresse des Mailservers im DNS kein Name zugeordnet ist
- Versendung aus einer bestimmten Region, z. B. Lateinamerika
- Eintrag eines Reply-To-Headers, der mit dem From-Header übereinstimmt
- Keine Verwendung eines echten Namens im To-Header (z. B. wird „peter@domain.org" eher als Spam erkannt, als „Peter Hausmann <peter@domain.org>"
- Verwendung von Ziffern im From-Header („service0021@domain.de")
- Verwendung von „Multipart" zur Nachrichtenkodierung, es ist aber nur ein Part vorhanden

Im Folgenden sollen einige Lösungen exemplarisch vorgestellt werden, die ISPs für den Schutz ihrer Kunden gegen unerwünschte Mails verwenden [Bleich 05] [Topf 05] [BSI 05].

- Bei **White- und Blacklist-Verfahren** werden IP-Adressen oder Absenderadressen, die zu einer Versendung berechtigt sind (Whitelist) bzw. nicht berechtigt sind (Blacklist) explizit in eine Liste des ISPs eingetragen. Dadurch dass E-Mail-Adressen einfach zu verfälschen sind, um der Sperrung durch eine Blacklist zu entgehen, wird heute eher das Konzept der Whitelisten genutzt. In diesen Whitelisten werden Versender aufgenommen, die nachweisen können, dass die von Ihnen versendeten E-Mails auf der Erlaubnis der Empfänger basieren (sog. Permission Marketing). So lassen sich Versender von legitimen Massen-E-Mails eintragen, damit ihre Nachrichten nicht automatisch aussortiert werden. Über die Certified Sender Alliance (CSA) haben sich mittlerweile viele seriöse Emailversender und ISPs zusammengeschlossen und ein übergreifendes Whitelist-Projekt ins Leben gerufen, das die Zustellung von erlaubnisbasierten Werbeemails sicherstellen soll.
- Beim **Greylisting-Verfahren** wird jede E-Mail beim ersten Zustellversuch mit einem temporären Fehler abgelehnt. Im Normalfall probieren die Mailserver dann etwas später eine weitere Zustellung, die dann angenommen wird. Dieses Vorgehen ist für den Versender etwas aufwendiger und ressourcenintensiver, so dass Spammer dadurch abgeschreckt werden und meist nach dem ersten Versuch keine weitere Zustellung probieren. Bei Verwendung dieses Systems hat der Mail-Service-Provider vor Nutzung der E-Mail-Adresse seines Kunden diesen nach § 93 TKG darauf hinzuweisen, dass seine E-Mail-Adresse für das Greylisting Verfahren genutzt wird.[Stadler 05]
- Beim **IP-Blacklisting mit DNS-Eintrag** werden schwarze Listen von IP-Adressen von Rechnern geführt, von denen keine E-Mails angenommen werden sollen. Versucht ein Rechner, der auf einer schwarzen Liste ist, Mails einzuliefern, bricht der Mailserver des Providers die Annahme ab, bevor die Nachricht übertragen wird. Der absendende Server erfährt von der Blockade durch eine Fehlermeldung. Wenn aber ein legitimer Mailversender hinter diese Adresse steckt, wird er diese Fehlermeldung in Form einer Mail an den Provider rückmelden. Der Empfänger kann nicht erreicht werden, bis der Provider die IP-Adresse des Absenders wieder zulässt. Wie IP-Adressen auf schwarze Listen kommen, ist von Provider zu Provider verschieden. Manche nutzen DNS-Blacklists von unabhängigen Firmen und Organisationen oder interne Listen.
- Beim **IP-Blacklist-Verfahren mit Frequenzanalyse** wird gezählt, wie viele Nachrichten in einem Zeitraum vom gleichen Rechner kommen. So kann z. B. ein Server, der plötzlich tausende Nachrichten verschickt, als verdächtig gekennzeichnet und auf eine interne schwarze Liste eingetragen werden. Dabei werden auch andere Kriterien, wie die Anzahl der bekannten und unbekannten

Empfängeradressen registriert, da Spammer oft fehlerhafte Adressen nutzen und somit Fehlermeldungen als Antwort zurückkommen.

- Hinter dem **Sender-Permitted-From-Verfahren** (auch "Sender Policy Framework"), wie es etwa von MSN (Hotmail) genutzt wird, steckt die Idee, dass der Empfänger überprüfen kann, ob die Nachricht auch wirklich vom angegebenen Absender kommt. Dafür wird eine Ergänzung der Einträge von E-Mail-Servern im Domain Name System (DNS) vorgenommen. Dadurch kann ein empfangender Server kontrollieren, ob die Absenderangaben in der Mail mit denen im DNS übereinstimmen. Bei der Lieferung einer E-Mail wird im DNS nachgesehen, ob der jeweilige versendende Server überhaupt dazu berechtigt ist, für diese Domain E-Mails zu verschicken. Teilnehmende Provider veröffentlichen im DNS welche Mailserver E-Mail aus ihren Domains versenden dürfen.
- Beim **DomainKeys-Verfahren** wird zu jedem E-Mail-Header, der das versendende System durchläuft, eine Prüfsumme erstellt. Dazu erzeugt der Betreiber eines MTA (Mail Transfer Agent) ein Schlüsselpaar (privaten und öffentlichen Schlüssel). Der Provider erstellt eine elektronische Signatur mit seinem privaten Schlüssel und fügt sie dem Header zu. Mit dem öffentlichen Schlüssel des Provider ist dann der Empfangsserver in der Lage zu überprüfen, ob die E-Mail von der im E-Mail-Kopf angegebene Adresse kommt und kann sie akzeptieren oder zurückweisen.
- Das **MTAmark-Verfahren.** Hier werden IP-Adressen oder ganze Blöcke von Internet Providern als IP-Adressen markiert, aus denen dann E-Mails versandt werden dürfen oder nicht. Dazu wird im DNS ein entsprechender Eintrag vorgenommen. Unterstützt der Empfänger ebenfalls das MTAmark-Verfahren, kann er diesen Eintrag abfragen und die Annahme der E-Mails von solchen Rechnern erlauben oder verweigern.

4. Fazit

Diese Zusammenstellung soll die unterschiedlichen Möglichkeiten aufzeigen, die Provider verwenden, um das Problem der Spam-Mails zu entschärfen. Die meisten Provider nutzen eine Kombination von unterschiedlichen Verfahren. Manche von diesen Methoden wie MTAmark oder DomainKeys sind noch nicht oder nur teilweise umgesetzt. Weiterhin ist damit zu rechnen, dass Spammer immer wieder neue Wege finden werden, um auch diese Maßnahmen zu umgehen.

Zum guten Ton für Online-Shop-Betreiber gehört es, dass die E-Mails personalisiert (mit Anrede) verschickt werden und für den einzelnen Leser nicht erkennbar ist, wer diese Mail ebenfalls erhalten hat. Als weitere Maßnahme können sich die Betreiber bemühen, in Whitelists der verschiedenen Provider eingetragen zu werden oder einen Versanddienstleister nutzen, der Mitglied der CSA ist.
Einige Versanddienstleister bieten in Ihren Lösungen auch schon SPAM-Tests vor der Versendung der geplanten Werbeemail an. Darüber kann der Shopbetreiber dann testen, ob seine Werbeemail als SPAM betrachtet werden könnte und entsprechende Änderungen vornehmen.

5. Literatur

absolit (2003): Spam bedroht seriöses eMail-Marketing, http://www.ecin.de/marketing/emailspam/

Bundesamt für Sicherheit und Informationstechnik (2005): Antispam-Strategien - Unerwünschte E-Mails erkennen und abwehren http://www.bsi.de/presse/pressinf/120505antispam.htm

Bleich, Holger (2004): Säuberungsmaßnahmen - Absender-Authentifizierung zum Schutz vor Spam und Betrug, c't 19/2004, S. 134

Stadler, Tobias (2005): Schutz vor Spam durch Greylisting, DuD 2005, S. 348

Topf, Jochen (2005): Ausgesiebt - Wie Mail-Provider gegen Spam vorgehen, c't 11/2005, S. 188

6. Autoren:

Rechtsanwalt Gerd M. Fuchs, Justiziar des BVDW, fuchs@bvdw.org

Dipl.-Inform. Anastasia Meletiadou, Institut für Wirtschafts- und Verwaltungsinformatik, Universität Koblenz-Landau, nancy@uni-koblenz.de.

Ass. Jur. Markus Sacher, Universität Kassel, Projektgruppe verfassungsverträgliche Technikgestaltung (provet), m.sacher@uni-kassel.de.