

SPAM: Wenn sich die Mailbox des Computers in eine Müllkippe verwandelt

Sie sind verboten und blockieren dennoch die elektronischen Briefkästen vieler Internet-Nutzer: Unerwünscht zugesandte Werbemails. Hinzu kommt die Gefahr durch 0190-Dialer (Selbsteinwahl-Programme), die sich wie Vieren ausbreiten und immense Kosten beim Empfänger verursachen können. E-Mails, die man nicht will und die man auch nicht angefordert hat. Gemeinhin werden solche nicht gewollten Mails als „SPAM“ bezeichnet. Darunter versteht man nach der Definition der EU-Kommission unverlangt zugestellte E-Mails.

Mit 206 Milliarden SPAM-Mails zugemüllt

Die meisten SPAM-Mails sind kommerziell und werden aufgrund der geringen Kosten für den Versender in großen Massen verschickt. Es existieren bereits Programme, die den vollautomatischen Versand von Millionen E-Mails ermöglichen. Experten schätzen, dass sich die Zahl der Werbemails zwischen September 2001 und November 2002 verdoppelt hat. Der deutsche Provider 1&1, der zwei Millionen Postfächer betreut, blockt täglich etwa 300.000 SPAM-Mails. Inoffizielle Schätzungen der Provider gehen davon aus, dass ungefähr ein Drittel des dienstinternen Mailverkehrs mit ungewollten E-Mails belastet ist. Die Marktforschungsfirma Jupiter Media Metrix schätzt, dass Verbraucher im Jahr 2006 mit über 206 Milliarden Junk-E-Mails zugemüllt werden. Das macht im Durchschnitt 1.400 Mails pro Person. Im Jahr 2002 dürfte diese Zahl bei etwa 700 gelegen haben. Allein die Kosten für den Download im Jahr 2003 werden weltweit auf über 12 Mrd. Euro geschätzt. Erste Untersuchungen zeigen auch, dass bereits über 90 Prozent der Verbraucher, die regelmäßig E-Mail nutzen, von SPAMs genervt sind.

Fünf Tipps zum Schutz gegen den täglichen SPAM-Müll

ECO, der Verband der deutschen Internetwirtschaft e.V. schätzt, dass sich 90 Prozent der unerwünschten Werbeflut allein durch technische Filter abblocken lässt.

Tipp 1: Der alternative E-Mail-Account

Der „Spammer“ – so bezeichnet man den Müllversender – sollte gar nicht erst an die im normalen E-Mailverkehr genutzte E-Mail-Adresse herankommen. Für bestimmte Aktivitäten im Internet sollte daher ein alternativer E-Mail-Account eingerichtet werden. Solch eine temporäre Mail-Adresse lässt sich leicht bei einem Freemail-Provider (z.B. Yahoo.de) einrichten und kann jederzeit gelöscht oder verändert werden. Dort kommt dann der SPAM-Müll an und die eigentliche E-Mail-Anschrift bleibt geschützt.

Tipp 2: Der Einsatz von Filterprogrammen

Viele der Standard-E-Mail-Programme wie Pegasus, Eudora, Outlook oder Netscape 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. Aber auch Hilfsprogramme, die die eigene Mailbox überprüfen und unerwünschte Mails löschen, noch bevor die Mailbox geöffnet wird, können installiert werden. Diese Tools gibt es mittlerweile für alle Betriebssysteme. Während einige dieser Tools lediglich die E-Mail-Adresse des Absenders überprüfen, suchen andere Tools den kompletten Nachrichteninhalt nach bestimmten Schlüsselwörtern ab. Wer einen der kostenlosen E-Mail-Dienste wie GMX, Yahoo oder web.de nutzt, kann dort die vorhandenen SPAM-Filter aktivieren.

Tipp 3: Der Eintrag in die Robinsonliste

Der Eintrag in die so genannte Robinsonliste soll den Empfänger vor unerwünschten, absichtlichen oder versehentlichen Werbe- und Rundsendungen schützen. Robinsonlisten gibt es für Faxrund-, Brief-, SMS- und E-Mailsendungen. Einige Fachleute raten allerdings von einem Eintrag ab, da die eigene E-Mail-Anschrift so preisgegeben wird und es wirklich hartnäckigen Spammern egal sein dürfte, ob jemand in der Robinsonliste steht.

Tipp 4: Die SPAM-Mail zurückverfolgen

Eine SPAM-Mail, die es tatsächlich geschafft hat, in die Mailbox zu kommen, niemals direkt beantworten! Denn so wird transparent, welche der E-Mail-Anschriften aktiv genutzt wird und weiterer Müll würde unweigerlich folgen. Auch führt eine direkte Antwort in den wenigsten Fällen zum Erfolg, da die E-Mail-Adressen der Spammer in der Regel gefälscht oder nur kurzfristig für eine Aktion genutzt werden. Weitere Infos, wie sich die wahre Herkunft einer SPAM-Mail herausfinden lässt, erfragt man am besten beim eigenen Internet-Provider. In letzter Zeit werden verstärkt SPAM-Mails verschickt, die für 0190-Faxabrufdienste werben oder Links enthalten, die zur Installation eines 0190-Dialers führen. In diesen Fällen sollte man als SPAM-Opfer versuchen den Netzbetreiber der rechtswidrig beworbenen 0190-Nummer ausfindig zu machen und ihn entsprechend auf den rechtswidrigen Umgang mit der 0190-Nummer aufmerksam machen. Der Netzbetreiber muss den Endbetreiber der 0190-Nummer auf sein rechtswidriges Verhalten hinweisen und ist nach erfolgloser Mahnung zur Sperrung der Nummer verpflichtet. Zuverlässige Hilfe bei der Ermittlung des Netzbetreibers findet sich unter: www.dialer-control.de/0190anbieterliste.php.

Tipp 5: Eine Beschwerde bei eco/ICTF

Die ICTF (Internet Content Task Force) ist ein Arbeitskreis des Internetverbandes, der eine Hotline zur Entgegennahme von Beschwerden von Internet- und Usenetnutzern über rechtswidrige Inhalte betreibt. Die E-Mail-Adresse: hotline@eco.de. Jede Beschwerde sollte den vollständigen „E-Mail-Header“, das sind die auf der E-Mail nicht sichtbaren Detailinformationen über den Absender und den Inhalt der Mail enthalten. Im Outlook-Programm lassen sich die „Header-Infos“ leicht durch einen Klick auf der Menüleiste unter „Ansicht“ und weiter unter „Option“ sichtbar machen. mr

Quelle: ECO Verband der deutschen Internetwirtschaft e.V., Internet: www.eco.de

Antiviren-Software muss sein

Denken Sie auch daran, eine Antiviren-Software auf Ihrem Rechner zu installieren. E-Mails im HTML-Format, also mit allen Formatierungen (Fett, Kursiv, verschiedene Schriftarten etc.) können unter Umständen schon einen aktiven Virus enthalten. Das Problem dabei ist, dass ein Mailprogramm wie z.B. Outlook o.ä. diese HTML-E-Mails entsprechend anzeigen will und somit der schädliche Code (Virus, Trojaner, Dialer etc.) sofort auf dem Rechner ausgeführt wird, obwohl der Datei-Anhang nicht geöffnet wurde. Im besten Fall erkennt das eine Antiviren-Software und befreit die Mail bereits beim Download vom lästigen Anhang.

Wichtig: Die regelmäßige Aktualisierung der Antiviren-Software. Am besten wöchentlich durch einen Download beim Hersteller. mr

Hersteller von Antiviren-Software

Symantec (www.symantec.de)

McAfee (www.mcafee.de)

Sophos (www.sophos.de)

Norman (www.norman.com/de)

Panda (www.panda-software.de)

Weitere Infos zum Thema Viren

www.av-test.de

www.zdnet.de

www.pc-welt.de