



## Volles Postfach

So wehren Sie Spam-Mails erfolgreich ab

Heute besteht bereits etwa die Hälfte aller E-Mails aus Spam. Gegen die meist im Ausland sitzenden Spammer ist zwar kein Kraut gewachsen, aber die Spam-Flut lässt sich bereits mit einfachen Mitteln zumindest halbwegs eindämmen. Wir zeigen Ihnen, wie die Spammer vorgehen und was Sie dagegen tun können

Der Schaden, der allein den Unternehmen durch Spam-Mails entsteht, ist beträchtlich, denn neben dem Aufwand für Datenleitungen und Hardware geht durch die Bearbeitung der Werbenachrichten kostbare Arbeitszeit verloren. Eine Studie geht davon aus, dass den Firmen durch Spam alleine in den USA Kosten von 10 Milliarden US-Dollar entstehen. Dabei sind nach Ansicht des Experten Steve Linford vom Spamhaus Project ([www.spamhaus.org](http://www.spamhaus.org)) gerade einmal 150 spezialisierte „Dienstleister“ für 90 Prozent aller Werbe-Mails verantwortlich. Offenbar können sich also die Spammer über Auftragsmangel nicht beklagen.

Auf den ersten Blick erscheint es kaum vorstellbar, dass Händler den Vertriebsweg „Spam“ wählen, denn welcher Mail-Empfänger ist schon so dumm, die häufig mit reißerischen Slogans aufgemachten Mails zu lesen und dann den beworbenen Unsinn auch noch zu bestellen? Im Gegensatz zum konventionellen Vertrieb kalkulieren Spammer allerdings in größeren Dimen-

sionen, denn sie haben bis zu 250 Millionen Mailadressen in ihrer Datenbank und können innerhalb von Minuten Hunderttausende Mails verschicken. Abgerechnet wird mit dem Produktanbieter entweder auf Fallbasis oder über eine Provision pro initiiertem Verkauf. Etwa 0,75 Prozent aller Werbemails werden tatsächlich gelesen, wovon ein Bruchteil schließlich zur Geschäftsanbahnung führt. Angesichts der geringen Kosten reichen bereits wenige dutzend Verkäufe für den Spammer aus, um in die Gewinnzone zu gelangen. Das Online-Magazin Wired

hatte vor einigen Monaten aufgrund der Schlampigkeit eines Spammers Zugriff auf die Bestellliste für ein dubioses Medikament ([www.wired.com/news/business/0,1367,59907,00.html](http://www.wired.com/news/business/0,1367,59907,00.html)). Laut Wired kamen für das 50 US-Dollar teure Mittel rund 6.000 Bestellungen im Gesamtwert von rund einer halben Million Dollar zusammen.

### Spam aus deutschen Landen

In Deutschland gibt es dagegen gute Chancen, gegen Spammer oder deren Auftraggeber vorzugehen, wenn einer der beiden hierzulande ansässig ist. Bevor Sie allerdings die unerwünschten Mails einer Firma ins Visier nehmen, sollten Sie zuerst überlegen, ob Sie nicht selbst Auslöser dafür sind. Seriöse Internetunternehmen wie Yahoo geben einem bei der Anmeldung zu ihren Diensten die Möglichkeit, sich über Abhakboxen gegen Werbezusendungen auszusprechen. Andere Dienste, zum Beispiel GMX, finanzieren ihr kostenloses Angebot durch Werbemails und der Anwender erklärt sich mit deren Zustimmung bei seiner Anmeldung einverstanden. Es muss selbstverständlich trotzdem möglich sein, die Werbemails loszuwerden, sei es durch einen Abmeldelink in der Mail, ein Formular auf der Homepage oder durch Kündigung des Dienstes.

Illegal sind auf jeden Fall Praktiken, bei denen jeder, der eine Supportanfrage an ein Unternehmen richtet, einen Online-Einkauf tätigt oder seine Mailadresse irgendwo hinterlegt – dazu gehört natürlich auch die eigene Homepage – automatisch in Werbeverteilern landet. All-

Rainer Gievers/ms

Connection No.	Email Address	Right
Connection 1	cgp@hotmail.com	42
Connection 2	cgr@hotmail.com	54
Connection 3	cgd@hotmail.com	44
Connection 4	cge@hotmail.com	56
Connection 5	cgf@hotmail.com	54
Connection 6	cgg@hotmail.com	53
Connection 7	cgh@hotmail.com	44
Connection 8	cgi@hotmail.com	48
Connection 9	cij@hotmail.com	45
Connection 10	cjk@hotmail.com	44
Connection 11	ckl@hotmail.com	53
Connection 12	ckm@hotmail.com	50
Connection 13	ckn@hotmail.com	43
Connection 14	cko@hotmail.com	47
Connection 15	ckp@hotmail.com	58
Connection 16	ckq@hotmail.com	53
Connection 17	ckr@hotmail.com	38
Connection 18	cks@hotmail.com	55
Connection 19	ckt@hotmail.com	45
Connection 20	cku@hotmail.com	49
Connection 21	ckv@hotmail.com	46

**Power Email Harvester sucht nicht Webseiten nach gültigen Mailadressen ab, sondern probiert einfach selbst erzeugte Mailadressen aus. Besonders beliebte Opfer sind dabei die Nutzer von Freemail-Diensten**

gemeine Geschäftsbedingungen, die Werbemails ohne Einverständnis des Empfängers für zulässig erklären, sind darüber hinaus wettbewerbswidrig. Unzulässig ist auch die Weitergabe von Kundendaten und damit der Mailadressen von einem Unternehmen zum anderen, ohne dass der Kunde zugestimmt hat. Reagiert ein deutscher Spammer nicht auf Aufforderungen, den Spam-Versand zu unterlassen, hilft es eventuell, die Mitverursacher zu kontaktieren. Kommt die Spam-Mail über einen deutschen E-Mail-Provider

### Spam international

Gegen Spam aus dem Ausland lässt sich kaum etwas tun, zumal die Absenderadressen meist gefälscht sind. Auf keinen Fall sollte man auf die Mails antworten oder auf eventuell eingebettete Abmelde links klicken, denn damit bestätigt man nur, dass die eigene Mailadresse korrekt ist. Es ist allerdings immer einen Versuch wert, sich beim Mail-Provider oder im Falle einer angegebener Freehoster-Website, beim Hostler zu beschweren. In die so genannten Robinson-

**Datenschutzrechte**

Die Microsoft Corporation tritt als Datenverwaltungsstelle für Microsoft .NET Passport auf. Dort werden bestimmte persönliche Informationen zu Ihrem .NET Passport-Konto erfasst und verarbeitet. Unser Standort befindet sich in One Microsoft Way, Redmond, Washington 98052 USA.

Wir erfassen und verarbeiten diese Daten (1) zur Authentifizierung von Benutzern und (2) zur Vereinfachung der Registrierung bei Partnersites, die gemäß den Datenschutzerklärungen Ihre persönlichen Informationen benötigen. Außerdem erfassen und verarbeiten wir bestimmte Informationen zum Netzwerkverkehr, um die Sicherheit zu erhöhen und Kundensupport für Ihr .NET Passport-Konto bereitstellen zu können. Soweit es das anwendbare Gesetz nicht anders vorschreibt, werden diese Informationen nach spätestens 90 Tagen gelöscht.

Unter [www.passport.net](http://www.passport.net) können Sie sich für ein .NET Passport-Konto registrieren. Sie müssen hierzu lediglich Ihre E-Mail-Adresse und ein Kennwort angeben. Wenn Sie diese Informationen nicht angeben, wird kein .NET Passport-Konto für Sie eingerichtet. Sie können sich ebenso bei den Partnersites für ein .NET Passport-Konto anmelden, diese benötigen jedoch unter Umständen weitere persönliche Daten von Ihnen. Wenn Sie diese Informationen nicht angeben, erhalten Sie auf diesen Sites kein .NET Passport-Konto, und Sie können sich nicht über .NET Passport anmelden. Wenn Sie sich auf einer Partnersite bei .NET Passport registrieren, werden Ihre persönlichen Informationen bei der Registrierung für diese Website zugänglich.

Wir geben einige persönliche Daten an die Partnersites weiter. Dies ist jedoch nur der Fall, wenn Sie sich bei der Website anmelden. Sie können Ihre Einwilligung für bestimmte Informationen abgeben, so dass nur die von Ihnen angegebenen persönlichen Informationen weitergegeben werden. Wenn Sie bei der Registrierung für ein .NET Passport-Konto ein E-Mail-Konto erhalten haben, stellen wir Ihre persönlichen Daten mit Ihrem .NET Passport-Profil der Partnersite zur Verfügung, die die E-Mail-Adresse ausgegeben hat. Wir geben Ihre E-Mail-Adresse auch an Partnersites weiter, die diese

Seriöse Unternehmen, zum Beispiel Hotmail ([www.hotmail.de](http://www.hotmail.de)), informieren ausführlich darüber, was sie mit den gespeicherten Mailadressen machen. Der Anwender kann dann selbst bestimmen, ob Dritte Zugriff auf seine Mailadresse erhalten dürfen

oder Freehoster, benachrichtigen Sie diesen. Wie Sie den Inhalt der E-Mail-Header analysieren, erfahren Sie im Kasten „Spammer entlarven“. Die meisten Provider haben dafür extra eine Support-Mail im Format [abuse@providername.de](mailto:abuse@providername.de) eingerichtet. Eine Klage oder auch nur die Einschaltung eines Rechtsanwalts dürfte sich dagegen nur in harten Fällen lohnen, da die Richter nicht immer im Sinne des Geschädigten entscheiden. Eine Übersicht deutscher Urteile hat unter anderem der Spammer-Hammer ([www.spammer-hammer.de](http://www.spammer-hammer.de)) zusammengestellt. Die rechtliche Vorgehensweise mit Abmahnung und Klage erläutert beispielsweise die Kanzlei Schweizer ([www.kanzlei-prof-schweizer.de/bibliothek/content/01742](http://www.kanzlei-prof-schweizer.de/bibliothek/content/01742)).

Listen, die Adressen von Anwendern sammeln, die keine Werbemails wünschen, sollten Sie sich dagegen nicht eintragen, denn für die skrupellosen Spammer sind solche Listen eine große Versuchung. Einige internationale Robinson-Listen werden zudem nachweislich von Spammern betrieben.

### Mailadressen-Sammler

An die Mailadressen kommen die Spammer auf verschiedenen Wegen. So werden Programme angeboten, die einfach alle möglichen Mailadressen zufällig oder aus Wörterbüchern erzeugen und dann durch einen Connect mit dem Mail-Server auf Gültigkeit überprüfen. Besonders betroffen von den so genannten Mail-Harvestern („Erntemaschinen“) sind große Free-mail- und Internetprovider, denn

## Tip

### Adressen-Sammler aufgedeckt

Ein kleines PHP-Skript hilft dabei, den Mailadressen-Sammlern auf die Finger zu schauen. Einzige Voraussetzung ist eine noch ungenutzte Domain auf Ihrer Website, die Sie statt „domain.de“ im Skript verwenden.

Legen Sie nachfolgende Seite zum Beispiel als „test.php3“ an und verlinken Sie von Ihrer Webseite darauf:

```
<html><body>
<h1><a href="mailto:<?php echo $REMOTE_ADDR; echo '_on_'; echo date('j_m_y_G!'); echo '@domain.de'; ?>">E-Mail</a></h1>
</body></html>
```

Die dynamisch erzeugten Mailadressen, zum Beispiel „192.168.1.11\_on\_6\_08\_03\_1036@domain.de“ enthalten die IP des Mail-Harvesters sowie seine Besuchszeit. Weil der erste Teil der Mail veränderlich ist, müssen Sie für die betreffende Domain Ihrer Website konfigurieren, dass alle Mails angenommen werden. In Ihrem Mail-Client oder bei Ihrem Provider müssen Sie zudem den Spamschutz für die Testdomain deaktivieren.

dort gibt es mehrere Millionen potenzielle Opfer. Gegen die Mail-Harvester kann man sich relativ einfach durch eine möglichst lange Mailadresse schützen, denn die Programme probieren nur kurze Zeichenketten aus. Die Wahrscheinlichkeit, dass ein internationaler Mail-Anbieter wie Yahoo.com oder Hotmail.com von Harvestern besucht wird, ist zudem wesentlich höher als bei deutschen Providern.

Eine weitere Methode der Adressensammlung sind Harvester, die systematisch Webseiten nach Mailadressen durchsuchen. Sind die „mailto“-Links in Webseiten mit ei-

nem Namen versehen, kann der Spammer später sogar seine Opfer mit Namen ansprechen, wodurch seine Mails häufiger gelesen werden. Betroffen sind von den Web-Harvestern nicht nur Anwender mit eigener Homepage, sondern auch Nutzer von Gästebüchern, Diskussionsforen oder Newsgroups. Wenn Sie unbedingt Ihre Mailadresse angeben müssen, machen Sie sie durch Bearbeitung unbrauchbar, zum Beispiel, indem Sie sie als „name at domain.de“, „name domain.de“ oder „nameK EINS PAM@domain.de“ ausschreiben. Alternativ nutzen Sie einfach eine zweite, öffentliche Mailadresse, die Sie ab und zu wechseln.

**Spam Goes Down The Hole**

**Create a spamhole without having an account...**

Your favorite name:   
 Your Email Address:   
 Type 'yes' (no quotes) in this box if you have read and agree to the spamhole.com User Agreement:  yes  
 Keep this spamhole active for  hours  
 Please  the Information

**Use your passworded account to create a spamhole...**  
 (click here to get a passworded account)

Your Favorite Name:   
 Your Email Address:   
 Your Password:   
 Type 'yes' (no quotes) in this box if you have read and agree to the spamhole.com User Agreement:   
 Keep this spamhole active for  hours  
 Please  the Information

Something not working? Drop a mail here.

Schnell eingerichtet und effektiv: Temporäre Mailadressen bei Spamhole ([www.spamhole.com](http://www.spamhole.com)), die Mails an Ihren Mail-Account weiterleiten und sich nach maximal 72 Stunden deaktivieren

Tipp

Spammer entlarven

Zwar ist der Absender von Werbemails häufig falsch, nicht verfälschen lässt sich allerdings die IP des zur Einlieferung genutzten Mail-Servers, die sich im Mail-Header befindet. Der vollständige Header wird bei fast allen Mail-Programmen erst nach Aufruf von „Zeige Header“ oder Ähnlichem angezeigt.

Beispiel-Header:

```
Return-path: <mvitra6wO@123india.com>
Envelope-to: info@gicom.de
Delivery-date: Tue, 05 Aug 2003 14:12:56 +0200
Received: from [203.237.105.19] (helo=123india.com)
  by mxng01.kundenserver.de with smtp (Exim 3.35 #1)
  id 19kOgj-00027g-00
  for info@gicom.de; Tue, 05 Aug 2003 14:12:48 +0200
Received: from unknown (201.2.24.127)
  by 123india.com with ESMTP (Exim 4.05) id CwhjDysbPff
  for <info@gicom.de>; Tue, 5 Aug 2003 06:09:37 -0500
Message-Id: <iHVkKvowWxi7.snw4nBr0VcRf@123india.com>
From: mvitra6wO@123india.com
Date: Tue, 5 Aug 2003 06:09:37 -0500
Subject: ksw Powerful DVD copy software. zxfun Now you can save your
  favorite movies.
To: info@gicom.de
X-Mailer: The Bat! (v1.51) Personal
MIME-Version: 1.0
Content-Type: text/plain;
Content-Transfer-Encoding: 8bit
X-PMFLAGS: 34078848 0 1 P54750.CNM
```

Interessant für uns sind die Received-Zeilen, die von unten nach oben die Route vom Sender zum Empfänger angeben. Korrekte Received-Zeilen weisen wie eine Kette von einem Server zum nächsten, im Beispiel-Header von 201.2.24.127 nach 123india.com und dann von 123india.com nach mxng01.kundenserver.de. Auch Uhrzeit und Datum in den Received-Zeilen liefern wertvolle Informationen, denn normalerweise benötigt die Mail von einer Received-Station bis zur nächsten nur wenige Minuten. Im Beispiel-Header soll die Einlieferung bei 123india.com um „06:09:37 -0500“, das heißt um 01:09:37 Uhr nach UTC (Coordinated Universal Time, früher „Greenwich Mean Time“) stattgefunden haben, während der Mail-Server mxng01.kundenserver.de die Nachricht um „14:12:56 +0200“, also 16:12:56 Uhr erhalten hat. Es ist also eine deutliche Zeitdifferenz zu erkennen, die manchmal auf eine Überlastung oder eine falsch gesetzte Uhr des entsprechenden Servers zurückzuführen ist. Häufiger handelt es sich aber um gefälschte Received-Zeilen, die vom Spammer eingefügt wurden, um die Rückverfolgung zu erschweren. Klarheit liefert ein Whois auf die beteiligten Server, wie ihn unter anderem [www.whois-service.de](http://www.whois-service.de) anbietet. Es zeigt sich dann, dass die Zeile „Received: from unknown (201.2.24.127)“ gefälscht ist, denn die IP 201.2.24.127 ist überhaupt nicht vergeben. Der Spammer sitzt also mit hoher Wahrscheinlichkeit hinter 203.237.105.19. Das Whois liefert auch gleich eine abuse-Mailadresse, an die Sie Ihre Beschwerde – selbstverständlich zusammen mit der vollständigen Werbemail inklusive Header – schicken können.

Empfehlung: Einiges an Detektivarbeit nimmt Ihnen die Spamcop-Website ab, die für den Header und die in der Mailnachricht enthaltenen Webadressen die zuständigen Spam-Meldestellen ermittelt. Häufig liefert der Dienst auch einen Hinweis, dass eine Spammer-Website bereits einmal aufgefallen ist. Melden Sie sich bei Spamcop unter [www.spamcop.net/anonsignup.shtml](http://www.spamcop.net/anonsignup.shtml) an. Der Rest ist selbst erklärend.

Einen effektiven Schutz vor Harvestern bietet zurzeit die Verwendung von HTML-Code im „mailto“-Link, zum Beispiel

```
<a href="mailto:me&#64;provider&#46;de">
  me&#64;provider&#46;de</a>
name&#64;provider&#46;de</a>
was gleichbedeutend zu <a href="mailto:name@pro
  vider.de">name@pro
  vider.de</a>
```

Noch raffinierter ist das Einbetten der Mailadresse in JavaScript, das von Harvestern nicht auswertbar ist. Dazu bietet Hiveware unter [www.hiveware.com/enkoder\\_form.php](http://www.hiveware.com/enkoder_form.php) einen entsprechenden Konverter an, dessen Ergebnis man in seine Webseiten einfügt. Unbequem für jemanden, der Ihnen etwas senden will, ist dagegen die Textgrafik-Methode, bei der Sie die Mailadresse in ein Bild einfügen, das in den Seiten eingebunden wird. Derzeit ist noch kein Mail-Harvester bekannt, der Texte per OCR aus Bildern extrahieren könnte.

Weil die Spammer immer wieder aufrüsten, werden die angegebenen Tricks irgendwann einmal überlistet werden. Absolute Ruhe vor Spammern haben Sie als Website-Besitzer wohl nur, wenn Sie keine Mailadressen auf Ihren Webseiten angeben und

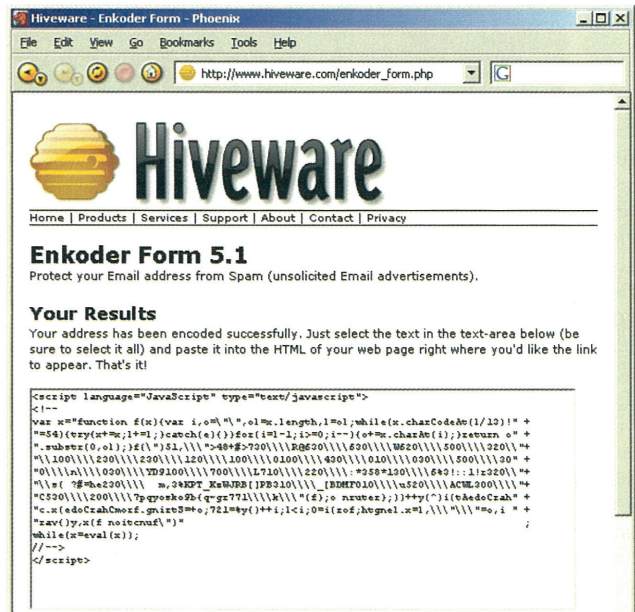
stattdessen ein CGI-Formular verwenden, über das der Besucher Kontakt mit Ihnen aufnehmen kann.

Wenn Sie wissen möchten, welche Mail-Harvester sich so auf Ihrer Homepage herumtreiben, können Sie sich eine kleine Spam-Falle bauen. Das Skript dafür finden Sie im Kasten „Adressen-Sammler aufgedeckt“.

Müssen Sie einmal eine Mailadresse angeben, kann zudem eine temporäre Mailadresse sehr nützlich sein, wie sie von Spamhole ([www.spamhole.com](http://www.spamhole.com)) angeboten wird. Alle Nachrichten an die temporäre Mailadresse werden an Ihren eigentlichen Mail-Account weitergeleitet. Nach maximal 72 Stunden deaktiviert sich die Spamhole-Mailadresse automatisch wieder.

Mail-Filter der Provider

GMX und Web.de Freemail haben im Spam ein Argument für ihre Dienste entdeckt und bieten schon seit einiger Zeit entsprechende Filter an. Das System von Freemail ist dreistufig angelegt und lässt nur Mails durch, deren Absender im Freemail-Adressbuch stehen. Dagegen landen unter anderem über



Hiveware bietet unter der Webadresse [www.hiveware.com/enkoder\\_form.php](http://www.hiveware.com/enkoder_form.php) einen raffinierten Konverter an, um aus einer E-Mailadresse verständliches JavaScript-Kauderwelsch zu erzeugen. Das JavaScript baut man in die eigenen Webseiten ein, woraufhin deren Besucher eine normale E-Mailadresse sehen, die von Mail-Harvestern aber nicht auswertbar ist

**Stopping Spambots: A Spambot Trap**  
Using Linux, Apache, mod\_perl, Perl, MySQL, ipchains and Embperl

Copyright © 2003 by Neil Gunton  
Last updated: Sun Jun 22 09:35:16 2003 CDT

This document describes my experiences with spambots on my websites, and the techniques I have developed to stop them dead. I assume the reader has basic familiarity with [Linux](#), [Apache](#), [mod\\_perl](#), [Perl](#), [MySQL](#) and firewall rules using [ipchains](#) - each of these topics could fill a book, so I won't talk about installation or basic configuration. I will, however, provide full scripts and instructions on using these within the context of these tools. If you'd like some basic pointers on getting set up using these tools, then you could take a look at my short series of three [Linux Network Howto](#) articles.

2002-04-12: I've had a lot of feedback since the original slashdot [article](#) - thanks to all those people who have written with some really great ideas for alternative ways to foil the spambots. I've tried to incorporate some of these into the document, and also to give credit to people by name where it's due. Thanks again!

2002-04-26: There's a new [update](#) on how the spambots seem to be "evolving" to avoid traps.

**Unzählige Webseiten beschäftigen sich mit der Abwehr von Mail-Verstärkern. Eine der umfangreichsten wird von Neil Gunton unter [www.neilgunton.com/spambot\\_trap](http://www.neilgunton.com/spambot_trap) betrieben. Dort finden Sie auch viele nützliche Skripte zum Thema**

Empfangsfrequenz, Header- und Inhaltsanalyse sowie Absender-IP als Spam identifizierte Nachrichten automatisch im „Unerwünscht“-Mailordner. Ist der Spam-Filter einmal unschlüssig, werden die Mails dagegen im „Unbekannt“-Ordner abgelegt. Der Mail-Absender erhält dann eine Nachricht mit Bitte um Eintrag in das Freemail-Adressbuch des Empfängers. Nutzer eines Freemail-Accounts, die ihre Nachrichten per Mail-Client abrufen, erhalten täglich eine Übersicht der Betreffs der ausgefilterten Nachrichten. In der

Praxis hat der Freemail-Nutzer tatsächlich ein fast spamfreies Postfach, das dahinter liegende System ist aber nicht unproblematisch: Außenstehende, die häufiger Freemail-Nutzer ansprechen, dürften es über kurz oder lang als Zumutung empfinden, sich jedesmal in ein Adressbuch eintragen zu müssen. Der Empfänger kann mit einem Mausklick allerdings auch selbst Absenderadressen in sein Adressbuch aufnehmen und der Absender wird darüber benachrichtigt. Falls gewünscht, kann der Spam-Schutz auch deakti-

SpamCop version 1.3.3 (c) Julian Haight, Joel Martin 1998-2003 All Rights Reserved

Saved email:  
This page may be saved for future reference:  
<http://spamcop.net/sc?id=2141908222f28098d1d7d9aaf346110321c6c1e20az>  
[Skip to Reports](#)

Parsing header:

Received: from [217.172.161.6] (helo=isis28.plussserver.de) by mxng11.kundenserver.de with esmtp (Exim 3.35 #1) id 19kcri-0003of-00 for bille@gievers.de; Thu, 07 Aug 2003 06:59:06 +0200  
no from  
Possible spammer: 217.172.161.6  
Received line accepted

Received: by isis28.plussserver.de (Postfix, from userid 0) id 15B5E235B05; Thu, 7 Aug 2003 06:57:01 +0200 (CEST)  
no ip found in received line  
Ignored

Tracking message source: 217.172.161.6:  
Routing details for 217.172.161.6:  
[refresh/show](#) Cached whois for 217.172.161.6: npe@netfabrik.de hostmaster@intergenia.de  
Using abuse net on hostmaster@intergenia.de  
abuse net intergenia.de = service@plussserver.de, postmaster@plussserver.de  
Using best contacts service@plussserver.de, postmaster@plussserver.de  
217.172.161.6 not listed in dnsbl.njabl.org  
217.172.161.6 not listed in dnsbl.njabl.org  
217.172.161.6 not listed in proxies.blackholes.easynet.nl

**Spamcop.Net identifiziert anhand eines E-Mail-Headers, den man in das Formular einfügt, den Ursprung einer E-Mail. Falls gewünscht, wird dem zuständigen Provider auch gleich eine automatisch generierte Beschwerde-Nachricht geschickt**

viert werden. Man darf dann selbst Filterregeln anlegen, um zum Beispiel abhängig von Betreff oder Absender eine Nachricht als Spam zu behandeln.

Der Spamschutz von GMX lässt dem Nutzer im Vergleich zu Web.de Freemail mehr Filtermöglichkeiten, benötigt dafür aber einiges an Einarbeitungszeit. Verdächtige Nachrichten sortiert das System in einen Spamverdacht-Ordner ein und GMX-Nutzer, die einen Mail-Client verwenden, bekommen täglich eine Liste mit den Be-

mit dem GMX-Antispam-System länger auseinander setzt, erzielt gute Ergebnisse.

#### Programme gegen Spam

Außerhalb der Mail-Provider werden zahlreiche kommerzielle und kostenlose Anti-Spam-Lösungen angeboten, die vom externen Mail-Proxy über lokale Server-Lösungen bis hin zur Desktop-Software reichen. Im Desktop-Bereich wird unterschieden zwischen lokalen Proxys, die sich zwischen Mail-Account und Mail-Client schalten, und Spam-Filtern, die auf

FreeMail von WEB.DE - Phoenix

Unbekannt - 5 Nachrichten

Posteingang (102/53) Unbekannt (5/5) Unerwünscht (14/14) zum Patent angemeldet

So funktioniert der Drei-Wege Spam-Schutz - Spam-Schutz Fragen  
 Diesen Ordner nicht per POP3 abholen - Spam-Schutz einstellen Ordner verwaltet

Von	Betreff	Spam?
V3-MitgliederService <bounceme@blaster.tier1mail.com> <jenny@web.de> <gievers@web.de>	Sondernews: Gutscheine enthal... have hundreds of lenders help...	kein Spam kein Spam kein Spam
"Claudio Morton" <v42bog76ilee@mad.servicom.es>	get paid to preview movie trai...	kein Spam
"Sandra" <sandra.m1981@webtv.net> <Thaddeus Welch <khdfkrybmn2f@excite.com>	Re: unser treffen vjrfs h... "I Want To Satisfy My L..."	kein Spam kein Spam

Spamwahrscheinlichkeit: über 75% 75% - 26% 25% - 1%

**Im „Unbekannt“-Ordner landen bei Web.de Freemail alle Mails, die nicht eindeutig als Spam identifiziert wurden. Der Nutzer kann sie dann selbst per Mausklick als „Spam“ oder „kein Spam“ einordnen. Über 90 Prozent an Spam landen schon vorab im „Unerwünscht“-Ordner**

treffs der ausgefilterten Mails. GMX analysiert Nachrichten anhand von bis zu sieben verschiedenen Kriterien, wobei auf Wunsch statt der Einsortierung in den Spamverdacht-Ordner auch eine Annahmeverweigerung möglich ist. Neben der vom Anwender erstellten Whitelist und Blacklist mit erwünschten beziehungsweise unerwünschten Empfängern nutzt GMX eine Liste mit Spamverdächtigen Servern sowie eine Liste mit Absendern, die für Werbemails bekannt sind. Weitere Filter sind ein Mail-Header-Analyser und ein Blocker für Absender-Adressen großer Mail-Anbieter, die über einen anderen Provider verschickt wurden. Neben dem Spam-Filter-System bietet GMX auch eine sehr leistungsfähige, vom Anwender verwaltbare Filterung, um Nachrichten unter anderem nach Betreff, Absender und Größe in die Ordner einzusortieren. Wer sich

dem Mail-Account vor dem Nachrichtenabruf die Werbung entfernen. Eine Ausnahmestellung nimmt Mozilla-Mail ein, denn der vom Mozilla-Projekt entwickelte Mail-Client besitzt bereits einen eigenen eingebauten Spam-Filter. Eine umfangreiche Liste der Spam-Killer finden Sie übrigens unter <http://spam.links.port5.com/filter-client-win.htm>. Empfehlenswert sind unter anderem die kostenlosen Programme Mailwasher ([www.mailwasher.net](http://www.mailwasher.net)) und K9 ([www.keir.net](http://www.keir.net)).

#### Fazit

Wer die Datensammlungsmethoden der Spammer kennt, kann bereits viel gegen die unerwünschten Werbenachrichten tun. Häufig reduziert schon der Wechsel auf eine längere Mailadresse die Werbeflut erheblich. Spam-Filter sind da nur noch der Punkt auf dem berühmten i-Tüpfelchen. ■