

SPAM DRÜBER

**Beim Bekämpfen der lästigen Werbe-Mails helfen
Ihnen unsere Tricks, Gratistools und – Ihr Provider!**



ILLUSTRATION WILLIAM DUKE

• von Gaby Salvisberg

Sspam ist die derzeit am schlimmsten grassierende Form von Netzmissbrauch: Sie erhalten unerwünschte Werbe-Mails von Firmen oder Personen, mit denen Sie nie Kontakt hatten. Ihre E-Mail-Adresse wurde von den Verursachern selbst oder von Datensammlern irgendwo im Internet aufgefunden und einer Datenbank hinzugefügt, die ab diesem Zeitpunkt fleissig unter den Spammern, also Leuten, die Spam verschicken, weiterverkauft wird.

Der PCTip hat dieses Jahr für einmal den Spam nicht gleich entsorgt, sondern fein säuberlich gesammelt. Während der acht Monate bis Ende August bekam die Autorin an ihre Redaktions-Adresse über 1300 «Angebote» der unerfreulichen Art, siehe Grafik «Dramatische Zunahme», rechts. Alles, wirklich alles hätten wir haben können: angefangen bei amerikanischen Green-Cards («USA Green Card Lottery Program»), über Potenz steigernde («Cheapest Viagra Guaranteed») und andere («Breakthrough: Herpes») Wundermittel (inkl. Pfeffersprays), von Börsen- und sonstigen reich machenden Tipps («As seen on National TV!!») bis zu Sicherheitstools aller Art («Das Internet-Sicherheitspaket zum Spitzenpreis!»), und nicht zu vergessen die Unmengen an Geschmacklosigkeiten in Form von Porno-Werbung («Free Nasty Teen Porn!!»). Natürlich hätten wir uns auch CD-ROMs mit E-Mail-Adressen bestellen können («Over 250 Million Email Addresses»), um selbst mit der Spammerei anzufangen.... **Screen 1.**

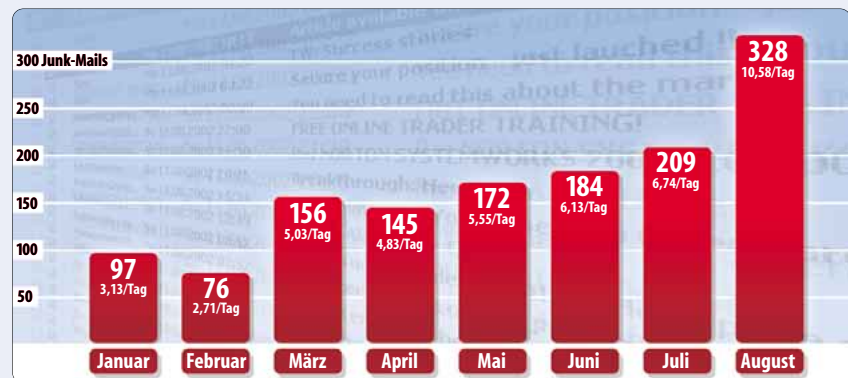
Ein Blick in die Kopfzeilen der Mails zeigt: Der Schund erreichte uns aus der ganzen Welt, vornehmlich aus dem Fernen Osten, Osteuropa, Nord- und Südamerika. Einige spannende Übeltäter sitzen jedoch auch in der Schweiz.

Von	Erhalten	Betreff
Carl Groves	Mo 12.08.2002 10:17	Article available on the hard truth about wireless LAN s...
Sara	Mo 12.08.2002 04:22	FW: Success stories
john	Mo 12.08.2002 03:22	Secure your position - just lauched !!
wayanna_gunn...	Mo 12.08.2002 00:30	You need to read this about the market
investors98290...	So 11.08.2002 22:00	FREE ONLINE TRADER TRAINING!
rgmaio@hotmail...	So 11.08.2002 21:30	Re: NORTON SYSTEMWORKS 2002 BLOWOUT!
Liz Cressente	So 11.08.2002 20:25	Breakthrough: Herpes
Resident-Green...	So 11.08.2002 15:34	Now Online, Get Your American Green Card
telefonsearch.c...	So 11.08.2002 12:39	Super-Aktion für CD-R
forfree@ihcr.de	So 11.08.2002 08:52	Die Besucherzahlen auf Ihrer Homepage sind zu gering?
Management10...	So 11.08.2002 02:52	USA Green Card Lottery Program - Now Online
sicherinsinterne...	So 11.08.2002 02:44	Das Internet-Sicherheitspaket zum Spitzenpreis!
FreeSilver@the...	So 11.08.2002 00:57	Get A Free Silver Bracelet Compliments of TheGreatSm...
vollg@hotmail.c...	Sa 10.08.2002 23:09	Feeling Sluggish You need Extreme Colon Cleanser
breakfree@lux...	Sa 10.08.2002 20:26	A GIANT AWAKES!!
Daniel	Sa 10.08.2002 11:35	Congratulations on Your 6 New Signups
mtg4you54271...	Sa 10.08.2002 06:40	discounted mortgage broker 54271813109766544433
vollg@hotmail.c...	Sa 10.08.2002 03:51	Feeling Sluggish You need Extreme Colon Cleanser
helen_raley@th...	Sa 10.08.2002 02:25	Claritin, Lipitor, Celebrex, Zyan, Viagra from Canada
zast123@hotmail...	Sa 10.08.2002 01:13	Give Away Free CD's - Earn 5K in 30 Days
puff_dime01@y...	Sa 10.08.2002 01:10	..THE TRUTH ABOUT HOW TO GET MORE SALES/LEADS, W...
puff_dime01@y...	Sa 10.08.2002 01:10	..THE TRUTH ABOUT HOW TO GET MORE SALES/LEADS, W...
skan_ac@hotmail...	Fr 09.08.2002 21:06	SYSTEMWORKS CLEARANCE SALE_LIMITED QUANTITIES...

Die Anzahl verschickter Spams nimmt stetig zu.

Spams im PCTip-E-Mail-Postfach

Dramatische Zunahme



Seit Januar 2002 sammelt der PCTip alle Spams, die an seine E-Mail-Adresse geschickt werden. Die monatliche Zunahme ist dramatisch.

Beängstigend: Waren es während des Monats Januar noch knapp 100 unerwünschte Mails, bescherte uns der August mehr als die dreifache Menge, nämlich 328 Stück.

Spam ist unlauter, weil das «Porto», sprich die Kosten für den Versand und die Zustellung, nicht vom Verursacher bezahlt werden, sondern von den Opfern. Zu diesen Opfern gehören die Internet-Provider, deren teure Ressourcen für Millionen von Junk-Mails erhalten müssen. Auch Sie als Benutzer dürfen sich zu Recht als Spam-Opfer sehen, denn erstens müssen Sie direkt oder indirekt fürs Herunterladen der unerwünschten Post bezahlen, zweitens werden Ihre Personendaten (Ihre E-Mail-Adresse) von den Spammern (oft rechtswidrig) missbraucht und drittens ärgern Sie sich über die verlorene (Arbeits-)Zeit.

Ob sich 99 Prozent der Empfänger über ihre Post ärgern, ist einem Spammer allerdings völlig egal, Kollateralschäden aller Art (volle Mail-Boxen, überlastete Mail-Server) werden unbeeindruckt mit einem Schulterzucken abgetan. Das Einzige, was für ihn zählt: Wenn nur eine von tausend Mails eine Bestellung bewirkt, hat sich das Spammen für ihn bereits gelohnt.

Über die Menge von Spam und der verursachten Kosten bei Benutzern und Providern schwirren die unterschiedlichsten Zahlen herum. Zwischen 20 und 70 Prozent der versendeten Mails sollen bereits Junk (Müll) sein und gemäss einer Studie der Europäischen Kommission vom Januar 2001 soll das Herunterladen der Junk-Mails alleine die Benutzer weltweit pro Jahr rund 15 Milliarden Franken kosten; dies ohne die Spesen, welche die Provider selbst tragen müssen oder die der Wirtschaft entstehen – Tendenz natürlich massiv steigend. Spam ist ein globales Problem.

SPAM VERMEIDEN

Ist Ihre Adresse einmal in einer Spam-Datenbank gelandet, gibt es praktisch nichts, das Sie tun könnten, um diese dort wieder herauszubekommen – besonders, wenn es sich um einen ausländischen Adressensammler handelt. Aus diesem Grund sollten Sie sich ein gutes Konzept überlegen, wie Sie vermeiden, dass ein Spammer Ihre Mail-Adresse überhaupt erst in die Finger kriegt.

Sparsam weitergeben: Geizen Sie mit Ihrer Mail-Adresse. Wenn Sie sich für Dienste oder Software registrieren, lesen Sie die Privacy-Informationen der Anbieter. Wird darin eine Weitergabe oder Verwendung der Adressdaten für Werbezwecke nicht explizit ausgeschlossen, dann verweigern Sie die Angabe Ihrer Adresse. Suchen Sie auf Registrations-Seiten auch nach einem allenfalls bereits gesetzten Häkchen, das es der Firma erlaubt, Sie mit «Produktinformationen» zu versorgen.

► **Mehrere Mail-Konten:** Legen Sie sich mindestens drei Mail-Adressen zu. Eine geben Sie nur Ihren Freunden und Bekannten. Die zweite verwenden Sie für Kontakte mit Firmen, zum Beispiel mit Software-Lieferanten oder Online-Shops. Die dritte Adresse ist Ihr «Spam-Magnet», den Sie an Orten einsetzen, die Spammer typischerweise nach frischen Adressen abgrasen, z. B. in Chats, Diskussionsforen, Online-Gästebüchern oder Usenet-Newsgroups. Für solches eignen sich kostenlose Mail-Dienste bestens, zum Beispiel GMX <http://www.gmx.ch/>, Swissinfo <http://www.swissinfo.org/> oder (für unsere Abonnentinnen und Abonnenten) PCTip-Freemail <http://www.pctip.ch/freemail/>.

Noch etwas weiter geht das «Spam-Motel» <http://www.spammotel.com/>. Hier können Sie Mail-Adressen erstellen und verwalten – und auch gleich feststellen, ob Ihre Adresse für Spam missbraucht wird. Ein Beispiel: Firma XY will Ihnen den Lizenz-Key einer online gekauften Software zustellen, darum müssen Sie eine gültige Mail-Adresse bekannt geben. Erstellen Sie per Spam-Motel eigens für diesen Zweck eine Adresse, die Sie für nichts anderes mehr verwenden werden. Versehen Sie die Mail-Adresse mit einem Kommentar («Registrierung bei XY») und lassen Sie Spam-Motel fortan diese Mails an Ihre wirk-

liche Adresse weiterleiten. Sie werden die erwünschte Mail von Firma XY über Ihr normales Mail-Konto empfangen, begleitet von Ihrem Kommentar «Registrierung bei XY». Sollte später aus einer anderen Richtung Spam an diese Adresse verschickt werden, wissen Sie, wer Ihre Adresse weitergegeben hat. Sie können die Adresse jederzeit auch wieder löschen.

Keine Ketten-Mails: Machen Sie nicht mit bei Spielen oder Scherzen, die per Mail von einem Benutzer zum nächsten weitergeleitet werden sollen. Verzichten Sie aufs Weiterleiten von Hoaxes (z. B. Virenwarnungen), da es in diesen Mails oft von Dutzenden oder Hunderten von E-Mail-Adressen wimmelt. Falls Sie eine Mail an viele Personen verschicken wollen, setzen Sie diese Adressen ins Feld BCC (Blind Carbon Copy), so sind die Mail-Adressen nicht für alle Empfänger sichtbar. Kennen Sie jemanden, der Ihnen Mails mit unzähligen sichtbaren Adressen sendet, bitten Sie ihn um mehr Rücksichtnahme. Und verzichten Sie darauf, Mail-Adressen Ihrer Bekannten herauszugeben, z. B. auf Seiten mit Formularen wie «Empfehlen Sie uns einem Freund!».

Bestätigung vermeiden: In HTML-Mails können sich Codes verbergen, die einem Spam-

mer automatisch zurückmelden, welche seiner Spam-Opfer seine Mail gelesen haben. Denn «gelesen» heisst für den Spammer «Adresse gültig». Dies steigert für ihn den Wert Ihrer Adresse, weshalb er Sie bald mit noch mehr Angeboten erfreuen wird. Schalten Sie Lesebestätigungen aus, verwenden Sie ein Mail-Programm, in dem sich auch HTML ausschalten lässt, oder fügen Sie Outlook oder Outlook Express ein Plug-In hinzu, mit dem sich HTML abstellen lässt (siehe auch «Outlook 2002 ohne HTML», S. 37).

Denselben Bestätigungs-Effekt haben oft auch Links innerhalb dieser Mails, unter denen Sie sich angeblich aus der Adressliste austragen können. Manche Spammer denken nicht daran, Sie aus der Datenbank zu entfernen, sondern wissen im Gegenteil jetzt um die Gültigkeit der Adresse.

E-Mail-Adresse verstecken: Die Angaben in diesem Abschnitt sind vor allem für Anwender interessant, die eine eigene Webseite im Internet unterhalten und über entsprechende Vorkenntnisse verfügen.

Adressensammler grasen mit Such-Robotern («Bots») Webseiten ab und speichern die gefundenen Mail-Adressen für spätere Werbezwecke. Wenn Sie eine eigene Webseite haben, prüfen Sie die unten erwähnten Möglichkeiten, um Ihre

Internet

Werbe-Mails

Adresse vor den Sammel-Bots zu verstecken und dabei für die Besucher Ihrer Seite trotzdem erreichbar zu bleiben:

■ **Per Kontakt-Formular:** Verwenden Sie zum Beispiel ein Kontakt-Formular, das Ihnen die Mitteilung der Surfenden über ein CGI-Script übermittelt (siehe PCTip 9/2002, «Ab ins Netz», Box S. 23). Der Nachteil ist, dass ein Besucher die Nachricht nicht über sein Mail-Programm senden kann und deshalb keine Kopie seiner Mitteilung in seinen gesendeten Objekten findet.

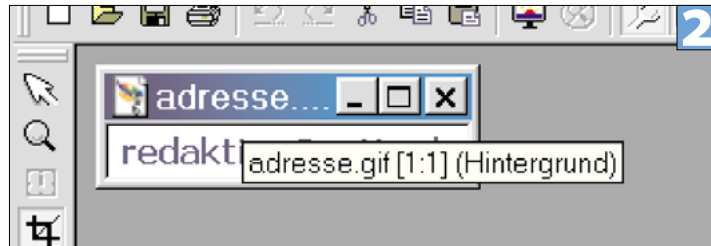
■ **Per Grafik:** Erstellen Sie eine Grafik, in der Ihre Mail-Adresse steht, und fügen Sie diese als Bild in Ihre Webseite ein. Hüten Sie sich davor, diese mit einem «mailto:»-Link zu verknüpfen, sonst steht die Adresse wieder für Bots sichtbar im Quelltext Ihrer Webseite. Nachteile: Die Surfenden müssen Ihre Adresse von Hand abtippen und zweitens schliessen Sie Leute aus, die unterwegs per langsamem/teurem Handy ins Netz gehen und deshalb das Anzeigen von Bildern ausschalten, Screens 2 bis 4.

■ **Als numerischen ASCII-Wert:** Hierbei wird jedes Zeichen als ASCII-Wert (eine Zahl) ausgegeben, was jeder Browser ohne besondere Klümmzüge zurückverwandeln kann. Allerdings besteht die Gefahr, dass Ihnen die Suchroboter trotzdem auf die Schliche kommen. So gehts: Öffnen Sie Ihre Webseite in einem Text-Editor und ersetzen Sie in Ihrem «mailto:»-Link Ihre Mail-Adresse durch die entsprechenden ASCII-Werte. Es gibt online benutzbare (<http://www.suchbuch.de/cgibin/nospam.pl>) und lokal installierbare (<http://pluto.spaceports.com/~mobysw/de/mailto-encrypter.html>, <http://www.awes.com/obfuscator/>) Hilfsmittel, die Ihnen beim Umwandeln Ihrer Mail-Adresse helfen können, Screen 5.

Hintergrund

Dosenfleisch

Eigentlich ist Spam eine Art Dosenfleisch der Firma Hormel Foods Corporation (siehe <http://www.spam.com/>). Durch einen herrlich schrillen Sketch der englischen Kult-Satire-Truppe «Monty Python» (John Cleese, Terry Gilliam, Terry Jones, Graham Chapman, Eric Idle und Michael Palin) wurde das Wort Spam zum Synonym für die lästige Wiederholung von Dingen, die keiner haben will. Der Sketch spielt in einem Restaurant, in dem alles, was einem hungrigen weiblichen Gast (gespielt von Graham Chapman) von der Kellnerin (Terry Jones) angeboten wird, Spam enthält, obwohl sich die verzweifelte Lady vehement gegen den Spam wehrt («I don't want any Spam!», «I don't like Spam!»). Wie man es von diesen «Monty Python's Flying Circus»-Sketches nicht anders kennt, ist es eine Selbstverständlichkeit, dass der Sketch in schrägste Gefilde abdriften muss. So überrascht auch der Wikingerchor nicht, der wie aus dem Nichts auftaucht und anfängt «Spam, Spam, Spam» zu singen. Der Begriff Spam wurde erstmals in Usenet-Newsgruppen mit unerwünschten elektronischen Werbe-Botschaften in Verbindung gebracht und später auf Werbe-Mails ausgedehnt.



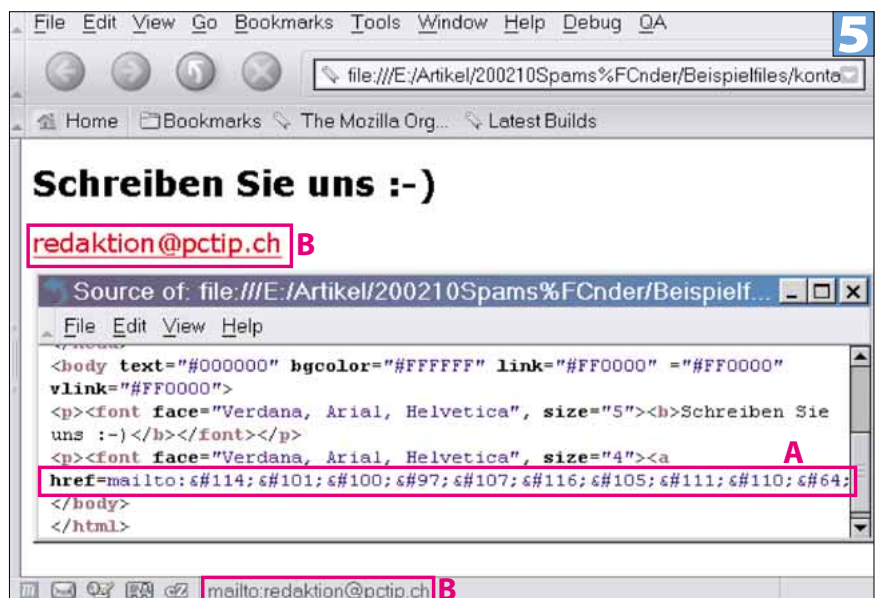
2 Erstellen Sie ein Bild im GIF-Format mit Ihrer Mail-Adresse und fügen Sie es in Ihre Webseite ein. Die Mail-Adresse können nur Ihre Web-Besucher lesen.

```
<!doctype html public "-//W3C//DTD HTML 4.0 //EN">
<html>
<head>
<title>Schreiben Sie uns!</title>
</head>
<body text="#000000" bgcolor="#FFFFFF" link="#FF0000"
alink="#FF0000" vlink="#FF0000">
<p><font face="Verdana, Arial, Helvetica", size="5"><b>Schreiben
Sie uns :-)</b></font></p>
<p></p>
</body>
</html>
```

Hier wird das «Bild» der Mail-Adresse in den Quellcode der Webseite eingefügt.



4 Das Resultat: Die Adresse ist für menschliche Web-Besucher zu lesen, aber nicht für Sammel-Bots.



Im Quelltext steht die Adresse ASCII-codiert (A), aber die Browser Ihrer Web-Besucher wandeln die Adresse um (B).

► ■ **Per JavaScript:** In den Screens 6 und 7 sehen Sie ein einfaches Beispiel, wie sich der E-Mail-Link per JavaScript verstecken lässt. Dies ist recht zuverlässig, denn Sammel-Bots decodieren keine JavaScripts. Ausserdem lassen sich den Variablen («zuerst» und «nachher») erstens problemlos andere Namen verpassen, z.B. «no» und «spam» oder «teil1» und «teil2» und zweitens lässt sich das Script noch verkomplizieren, indem Sie es auf mehrere «var»-Teile erweitern, die sich in der «document.write»-Zeile per Pluszeichen wieder zusammensetzen lassen.

Ein JavaScript-fähiger Browser interpretiert das Script und zeigt beim Surfen den Link zu «mailto:redaktion@pctip.ch» korrekt an. Nachteil: Falls JavaScript im Browser Ihres Web-Besuchers ausgeschaltet ist, wird dieser nichts erkennen.

Verbieten Sie Spam: Machen Sie auf Ihrer Webseite klar (am besten in Deutsch und Englisch), dass Sie keine Spams an eine Ihrer Mail-Adressen haben wollen. Sorgen Sie dafür, dass Ihre Adresse im Telefonbuch ein Sternchen (für «Wünscht keine Werbung») trägt. Beides wird die meisten Spammer zwar nicht von ihrer Tätigkeit abhalten, aber Sie haben etwas in der Hand, falls sich die rechtliche Situation oder die internationalen Antispam-Bemühungen verbessern.



Ein einfaches JavaScript (unten) zeigt einem menschlichen Leser die wahre Mail-Adresse (links), verbirgt sie aber vor den Sammel-Bots.

```
<p><font face="Verdana, Arial, Helvetica", size="5"><b>Schreiben Sie uns :-)</b></font></p>
<p><font face="Verdana, Arial, Helvetica" size="3"><b>
<script language="JavaScript">
<!--
var zuerst = "redaktion";
var nachher = "pctip.ch";
document.write('<a
href=\ "mailto:' +zuerst+'@'+nachher+'\' ">E-Mail-Adresse</a>');
// -->
</script>
</b></font>
</p>
</body>
</html>
```

A blue box with the number '7' is in the top right corner of the code block.

Spam soll sich nicht lohnen: Überlegen Sie es sich genau, ob Sie eine Firma oder Person, die mit unlauteren Methoden wirbt, mit einer Bestellung «belohnen» möchten.

Umstrittene Massnahmen: Bisweilen trifft der spamgeplagte Webbenutzer auf Empfehlungen, die nur bedingt oder gar keinen Erfolg bringen, die das Problem bloss verlagern oder die gar zu weiteren Datensammlungen führen:

■ **Robinsonlisten:** Ganz ähnlich wie die Robinsonliste des Schweizer Direktmarketing-Verbandes (SDV) <http://www.dmverband.ch/files/robinson1.htm> funktioniert auch «e-Robinson» <http://www.robinsonliste.de/>. Die Idee dahinter: Wer keine Werbung per E-Mail möchte, trägt seine Mail-Adresse in die Liste ein. Direktwerber gleichen ihre Daten gegen Gebühr mit der Liste ab und entfernen alle Adressen, die in der Robinsonliste aufgeführt sind. Ein ähnliches Konzept verfolgt PermissionBase <http://www.permissionbase.com/> (siehe auch PCtip-Webnews: <http://www.pctip.ch/webnews/wn/19895.asp>).

Leider kommen aber kritische Benutzer dem Wunsch, in möglichst wenigen Datenbanken aufzutauchen, so keinen Schritt näher. Ausserdem garantiert nichts, dass diese Listen nicht

doch eines Tages in die falschen Hände geraten. Und zu guter Letzt stammt nur ein Bruchteil des weltweiten Spams von Firmen, die ihre Daten mit e-Robinson abgleichen.

■ **Gefälschte Mail-Adressen:** Einige Netz-Benutzer haben sich angewöhnt, in Diskussionsforen, Gästebüchern oder im Usenet falsche E-Mail-Adressen zu verwenden, zum Beispiel «nospam@bla-bla.com» oder «nospam@keinprovider.aetsch», damit Mails an diese Adressen ins «Leere» laufen.

Irrtum! Spam an ungültige Adressen löst sich nicht einfach in Luft auf, sondern landet stets bei unschuldigen anderen Benutzern oder Postmastern. Während verfälschte Adressen in internationalen oder amerikanischen Newsgroups trotzdem üblich sind, stossen sie in den meisten deutschen oder Schweizer Groups (de.gruppenname oder ch.gruppenname) auf Ablehnung. Die Gründe gegen falsche Mail-Adressen werden in Carsten Gerlachs Mini-FAQ (Frequently Asked Questions) <http://www.gerlo.de/falsche-email-adressen.html> ausführlich erklärt. Verwenden Sie für solche Fälle lieber Ihre Spam-Magnet-Adresse.

■ **Zu viele Wegwerf-Adressen:** Auch «Wegwerf»-Adressen, die Sie zum Beispiel mit Spam-Motel (siehe S. 28) verwalten können, haben einen Ha-

ken. Nehmen wir an, ein Spammer liest irgendwo eine Spam-Motel-Adresse auf, die Sie bereits gelöscht haben. Der Effekt wird ein ähnlicher sein, wie wenn Sie eine gefälschte Adresse verwendet hätten. Zudem wird eine Kontaktaufnahme mit Ihnen verunmöglicht, wenn Ihnen jemand zum Beispiel auf Grund eines Forum-Eintrags endlich den längst ersehnten rettenden Tipp schicken möchte. Verwenden Sie also nicht zu viele solche Adressen, werfen Sie diese nicht allzu schnell wieder weg und setzen Sie sie mit Bedacht ein.

SPAM BEKÄMPFEN

Gleich vorneweg: Um Spam langfristig zu bekämpfen, braucht es in erster Linie nicht technische, sondern politische und rechtliche Mittel. Nur auf diesem Weg wird Spam eines Tages in möglichst vielen Ländern verboten. Dies fängt direkt vor unserer Nase an, nämlich in Bern, im Bundeshaus. Kurz- und mittelfristig sind Sie hauptsächlich auf die Mitarbeit der Internet Service Provider (ISP) angewiesen.

Spam-Beschwerde beim ISP: Da der Netzmissbrauch durch Spammer auch den meisten ►

► Providern sauer aufstösst, verbietet praktisch jeder ISP in den Nutzungsbedingungen seinen Kunden den Versand von Spam. Nun kann ein Provider seinen Kunden nicht ständig über die Schulter schauen, um zu sehen, was diese gerade treiben. Deshalb informieren Sie den Provider, ■ bei dem sich der Spammer eingewählt hat, ■ über dessen Mail-Server die unerwünschte Post verschickt wurde, ■ der die Webseite des Spammers hostet, ■ bei dem der Spammer ein Mail-Konto als Drop-Box (Bestell- oder Remove-Adresse) eingerichtet hat.

Solche Informationen finden Sie einfach heraus, wenn Sie den Weg einer E-Mail kennen (siehe «Mail@Wissen», PCtip 6/2002, ab S. 24). Und anhand des Artikels «Mails auf dem Seziertisch», PCtip 7/2002 (ab S. 40), erfahren Sie, wie Sie die Kopfzeilen einer E-Mail lesen und gründlich auf ihre Herkunft analysieren. Beide Artikel stehen als PDF-Dateien in unserem Archiv <http://www.pctip.ch/archiv/2002/> zum Download bereit.

Haben Sie herausgefunden, welche Provider zuständig sind? Dann schreiben Sie eine Mail an die entsprechende Netzmissbrauchs-Abteilung, die meist eine E-Mail-Adresse wie «abuse@providername.ch» trägt («abuse» ist Englisch für «Missbrauch»). Sollten Sie beim Finden der zuständigen Adresse Schwierigkeiten haben, steht Sie vielleicht in der Datenbank der Anti-Netzmissbrauchs-Organisation «abuse.net» <http://www.abuse.net/lookup.phtml>. Tippen Sie den fraglichen Domainnamen (z. B. irgendwas.com) ins «Lookup»-Feld und schauen Sie, ob eine plausible Beschwerde-Adresse resultiert.

Ist die Adresse des Providers gefunden, fügen Sie sowohl den gesamten Header als auch den Werbetext des Spams in Ihre Mail ein, allenfalls den HTML-Quelltext, falls Sie auf diesen zugreifen können. Als Betreff übernehmen Sie jenen der Spam-Mail und fügen vorher noch die Zeichen [UBE] (für «unsolicited bulk e-mail») hinzu, so sieht der Mitarbeiter des Abuse-Desks gleich, dass es sich um eine Spam-Beschwerde handelt. Oberhalb des eingefügten Headers und Mail-Texts erläutern Sie dem Provider kurz, weshalb Sie denken, dass er zuständig sei. Sitzt der Provider in einem Land, dessen Sprache Sie nicht beherrschen, schreiben Sie in Englisch. Ach ja: Bleiben Sie bei diesen Beschwerde-Mails höflich (anfangen mit «Dear Sirs», enden mit «Regards»).

Hier kurze Beispiel-Texte:

I received the UCE/UBE that I attached below (heisst: Ich habe den unten stehenden Spam erhalten).

It looks like the spammer used your internet access services (heisst: Es sieht so aus, als habe der Spammer Ihre Internet-Zugangsdienste benutzt).

8

ORDB

Überprüfen

Dieser Host wird derzeit von ORDB-Benutzern geblockt

Hauptdatenbankstatus 211.147.1.45 211.147.1.45

Look up this host in non-ORDB RBL's (May take a while to load)

Erstmals in ORDB registriert:	2002-07-22 21:34 GMT
Erstmals gemeldet von:	64.81.100.235
Zuletzt positiv überprüft:	2002-07-28 12:00 GMT

Kopfzeilen der relayten Email

Return-Path:
Delivered-To: marvin@groundzero.ordb.org
Received: from 3wins.com (unknown [211.147.1.45])
by groundzero.ordb.org (Postfix) with SMTP id 75CDc5E104

Mit der Black List von ORDB wäre der Spam von dieser IP-Adresse bei uns gar nicht erst angekommen.

It looks like the spammer used your mail server to send this spam (heisst: Es sieht so als, als habe der Spammer Ihren Mail-Server für den Versand dieses Spams benutzt).

Obviously the e-mail account «hier die Mail-Adresse» on your server is used as a drop box (heisst: Offensichtlich wird die E-Mail-Adresse «Adresse» als Drop-Box benutzt).

The advertised web page «hier die Web-Adresse» seems to be hosted on one of your servers (heisst: Die beworbene Webseite «Web-Adresse» scheint auf einem Ihrer Server gehostet zu werden).

Please take appropriate action to stop this net abuse (heisst: Bitte unternehmen Sie geeignete Schritte, um diesen Netzmissbrauch zu stoppen).

Sie können auch auf die Dienste von Spamcop <http://spamcop.net/> zurückgreifen, der automatisch und recht zuverlässig die richtigen Adressen findet und eine Spam-Beschwerde an diese absetzt. Einige Provider (z. B. Bluewin) behandeln die via Spamcop erzeugten Beschwerde-Mails sogar mit Priorität.

Die Provider können nun die beworbene Webseite vom Netz nehmen, das als Drop-Box benutzte Mail-Konto sperren, dem Spammer in Zukunft die Einwahl verweigern oder den verwendeten Mail-Server soweit abdichten, dass er nicht mehr für unerlaubten Massenversand zur Verfügung steht. Wie die Schweizer Provider mit solchen Fällen umgehen, lesen Sie unter «Die Schweizer Internet-Provider», S. 34. Dass die Gegenmassnahmen leider bei internationalem Spam noch nicht überall helfen, zeigt die Webseite von «Spamhaus» <http://www.spamhaus.org/>, die hauptsächlich jene ISPs und Firmen anprangert, die sich regelmässig durch Untätigkeit oder Laxheit auszeichnen, wenns ums Abdichten von Servern oder Verhindern von Spam geht.

Rechtliche Schritte: Sollten Sie von jemandem aus der Schweiz Spam erhalten, verfahren

Sie wie oben erwähnt. Erwägen Sie allenfalls rechtliche Schritte, besonders wenn es sich um illegale Angebote (Lawinen-Systeme, Kinderpornografie handelt, siehe auch <http://www.pctip.ch/topthema/tt/19458.asp>). Da bei Spam meist auch das Schweizer Datenschutzgesetz verletzt wird, lohnt sich auch ein Blick auf den Leitfaden des Eidgenössischen Datenschutzbeauftragten http://www.edsb.ch/d/doku/leitfaeden/pdaten_recht/index.htm.

SPAM FILTERN ODER LÖSCHEN

Das Filtern von unerwünschten Mails ist nicht sehr zuverlässig, denn erstens schlüpft immer noch etwas Spam durch und zweitens bleiben teilweise auch erwünschte Mails im Filter hängen. Und ein weiterer wichtiger Nachteil: Der überflüssige Mail-Verkehr findet trotzdem statt, bis er entweder bei Ihrem Mail-Anbieter oder in Ihrem Mail-Programm im Filter landet.

Das Filtern von Spam ist trotz dieser Nachteile relativ beliebt, weil einerseits niemand durch ► **Bounces** belästigt wird und weil der Spam am Zielort gelöscht oder zumindest von den erwünschten Mails separiert wird. Spam-Filter dämmen zwar die Belästigung etwas ein, stoppen aber nicht die Verursacher.

Für Postmaster: Wer einen eigenen Mail-Server betreibt, kann so genannte Black Lists einsetzen. Hierbei wird die Herkunft der Mails überprüft. Stammt die Mail von einer auf der Black List als «Spamschleuder» gemeldeten IP-Adresse, wird die Mail entsorgt oder nicht angenommen. Die Black Lists von ORDB (Open Relay Database) <http://www.ordb.org/>, Spamhaus <http://www.spamhaus.org/sbl/> und Spamcop <http://spamcop.net/bl.shtml> dürfen Postmaster kostenlos verwenden, **Screen 8**.

Selbst filtern: Wollen Sie als normaler Mail-Benutzer Spam selbst anhand solcher Black Lists filtern, verwenden Sie zum Beispiel jeweils den MailWasher <http://www.mailwasher.net/>, bevor ►

► Sie Ihre Mails vom Server abholen. Dieser zeigt Ihnen Grösse, Absender, Betreff und Datum der Mails an, die auf dem Server liegen, und vergleicht diese mit drei bereits eingetragenen Black Lists. Was nach Spam «riecht», wird entsprechend markiert und zum Löschen oder «Bouncen» vorgeschlagen. Aufs Bouncen sollten Sie eher verzichten, weil die Bounces meist Unschuldige treffen, aber immerhin lässt sich der Spam gleich bequem auf dem Server löschen. Ihr Mail-Programm wird anschliessend nur noch die erwünschten Mails herunterladen, **Screen 9**.

Abgesehen von Freeware-Tools schiessen derzeit auch kostenpflichtige Filter-Programme wie Pilze aus dem Boden, etwa Spam Buster <http://www.contactplus.com/products/spam/spam.htm>, SpamAssassin http://www.deersoft.com/sp_pro.html oder SpamDetective <http://www.emtec.com/spamdetective/index.htm>.

Filtern lassen: Verschiedene Mail-Anbieter und Internet-Provider bieten (teils nur in den kostenpflichtigen Diensten) auch automatische Filter an, die sich auf Wunsch aktivieren lassen. Dies ist zum Beispiel bei Bluewin mit dem HighWay-Abo der Fall, sofern «Mail übers Web» aktiviert ist, oder bei Sunrise mit dem Produkt «Premiumsurf». Am besten erkundigen Sie sich auf der Webseite Ihres Providers.

Gemeinsam filtern: Für Outlook gibt es seit kurzem ein Plug-In (Zusatz) namens SpamNet <http://www.pctip.ch/downloads/dl/21356.asp>. Mit diesem Werkzeug arbeiten Sie mit anderen Benutzern zusammen (Peer-to-Peer). Verschiebt ein SpamNet-Benutzer eine Mail in seinen Spam-Ordner, wird dieselbe Mail, falls sie bei anderen SpamNet-Teilnehmern eintrifft, ebenfalls als Spam taxiert und nach dem Abholen im Spam-Ordner abgelegt. Dies eliminiert den Spam zwar nicht, trennt aber relativ zuverlässig die Spreu vom Weizen.

DIE SCHWEIZER INTERNET-PROVIDER

Der Pctip hat zehn Schweizer und zwei deutsche Internet Service Provider (ISP) gefragt, wie sie

Betriebszeiten), nach **10**

C. Pflichten des Kunden

1. Der Kunde ist für die Informationen (Sprache, Bilder, Klänge, andere Daten) verantwortlich, die er und die mit ihm kommunizierenden Dritten mit seinem Einverständnis durch Bluewin übermitteln oder bearbeiten lassen oder zum Abruf bereithalten. Rechtswidrige Informationen (insbesondere Gewaltdarstellungen, Pornografie, Diskriminierungen, Aufrufe zu Gewalt oder zu Straftaten, Glücksspiele, Verletzung von Urheberrechten, Markenrechten und anderen Immaterialgüterrechten, unverlangte Massensendungen etc.) sowie Belästigungen sind untersagt. Der Kunde anerkennt die Verhaltensregeln, Leistungsbeschreibungen und Nutzungsbestimmungen, welche von Bluewin in geeigneter Weise (insbesondere auf der Bluewin Website oder per E-Mail) mitgeteilt werden. Der Kunde befolgt die [Netiquette](#).
2. Der Kunde ist für die Beschaffung und Einrichtung sämtlicher Anschlüsse, Soft- und Hardware etc. verantwortlich. Bluewin übernimmt keine Garantie, dass die Nutzung der Dienstleistung mit allen Endgeräten und Einstellungen möglich ist. Der Kunde ist für den

Document Done (0.469 secs)

Die Nutzungsbedingungen von Bluewin: Unverlangte Massensendungen sind verboten.

MailWasher version 1.33

File Email Tools Register Help

MailWasher

Contact me Development About me

Check Mail Stop Process Mail Mail Program Tell a Friend

Delete	Bounce	Status	Size	From	Subject	Receiv	Accour
<input type="checkbox"/>	<input type="checkbox"/>	Normal	3.4KB	oxyg	Oxygen3 24h-365d [Integer overflow	07.08.20	PCtip G
<input type="checkbox"/>	<input type="checkbox"/>	Normal	4.2KB	Tren	TREND MICRO WEEKLY NEWS	07.08.20	PCtip G
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Origin blacklisted by DRDB	7.1KB	vollg	Feeling Sluggish You need Extreme	08.08.20	PCtip G
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Origin blacklisted by DRDB	7.1KB	vollg	Feeling Sluggish You need Extreme	08.08.20	PCtip G
<input type="checkbox"/>	<input type="checkbox"/>	Normal	21.3KB	Offic	Microsoft Office Tools on the Web,	08.08.20	PCtip G
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Origin blacklisted by VISI	7.5KB	L.cor	FEEL BETTER RIGHT AWAY! EXT	08.08.20	PCtip G
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Origin blacklisted by DRDB	1.5KB	Barb	look young	08.08.20	PCtip G
<input type="checkbox"/>	<input type="checkbox"/>	Normal	1.3KB	Ernst	V92 Standard	07.08.20	PCtip G
<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	Origin blacklisted by SpamCop	1.7KB	silent	Does snoring keep you awake at nig	08.08.20	PCtip G
<input type="checkbox"/>	<input type="checkbox"/>	Normal	3.1KB	Marc	Abt. EDV, Betriebskosten senken di	08.08.20	PCtip G
<input type="checkbox"/>	<input type="checkbox"/>	Normal	1KB	Hart	ups	08.08.20	PCtip G
<input type="checkbox"/>	<input type="checkbox"/>	Normal	1KB	Bluth	Farian	08.08.20	PCtip G

Mail was last checked 2 minutes ago

MailWasher erkennt den Spam anhand der Black Lists und schlägt Massnahmen vor.

mit Spammern umgehen, wenn sie feststellen, dass einer ihre Systeme missbraucht. Antworten erhielten wir von Bluewin, Cybernet, Green.ch, Init Seven, Internet Pipeline, Profitel, Sunrise, SwissOnline, Ticino.com und von GMX (Deutschland). Deren Antworten zeigen deutlich, dass mit Spammern nicht lange gefackelt wird.

Es wird abgeklemmt! Alle Provider untersagen in ihren Nutzungsbedingungen ganz klar den Versand von Spam, **Screen 10**. Wer sich trotzdem zwecks Spam-Versand bei ihnen einwählt, Spam über den Mail-Server verschickt, bei diesen Providern eine E-Mail-Adresse als Drop-Box betreibt oder eine dort gehostete Webseite per Spam bewirbt, kann sein blaues Wunder erleben. Fast alle klemmen einem Spammer spätestens im Wiederholungsfall (nach entsprechender Ermahnung) die Dienste ab und lösen seine Webseite oder sein Mail-Konto auf. Die meisten ISPs verhindern Missbrauch durch Dritte schon durch technische Vorkehrungen; so ist Mail-Ver-

sand nur eigenen Kunden möglich. **SwissOnline** und **GMX** sperren Mail-Konten sofort, wenn sie vom Missbrauch erfahren. Allerdings wird den Kunden erlaubt, schriftlich zu intervenieren.

Um die Einhaltung ihrer Nutzungsbedingungen durchzusetzen, gehen die Provider unterschiedlich vor. Erhalten die ISPs Kenntnis davon, dass ein Kunde dagegen verstösst, setzen fast alle auf eine entsprechende schriftliche Ermahnung. Einige haben auch durchblicken lassen, dass sie im Extremfall zu rechtlichen Mitteln greifen würden, wozu gemäss unserer Umfrage **Green.ch**, **SwissOnline** und **Sunrise** sogar schon gezwungen waren. Und bei den deutschen Mail-Profis von **GMX** kommt ein Missbrauch unter Umständen teuer: In den Bedingungen wird eine Konventionalstrafe von 5000 Euro angedroht.

Seit einiger Zeit bieten aber immer mehr ISPs einen anonymen Webzugang an, der keine vorgängige Anmeldung erfordert. Um Wiederholungstäter am Missbrauch zu hindern, greifen zum Beispiel **Init Seven**, **Sunrise** und **Ticino.com** in extremen Fällen zum einzigen noch tauglichen Mittel: Sie hindern die Telefonnummer des Spammers an der Einwahl.

Auch Kunden mit eigenen Servern müssen sich vorsehen, wenn sie bei diesen Providern etwa Standleitungen benutzen. Würde über den schlampig konfigurierten Mail-Server (offener Relay) eines Kunden Spam verschickt, wird auch dieser in der Regel vorübergehend gesperrt, bis der Administrator des Kunden das Problem gelöst hat. Alle neun Zugangsprovider geben an, ihre Standleitungs-Kunden aktiv beim Ablichten der Server zu unterstützen.

Zukunftsaussichten: Natürlich wollten wir von den Providern auch wissen, wie ihre Antispam-Bemühungen in der Zukunft aussehen.

Teilrevision des Fernmeldegesetzes

Gesetze kündigen sich an

Einiges zur Spam-Bekämpfung ist von der Teilrevision des Fernmeldegesetzes (FMG) zu erwarten, zu dem interessierte Kreise noch bis zum 15. Oktober 2002 Stellung nehmen können. Weitere Informationen finden Sie auf der Webseite des Bundesamtes für Kommunikation (<http://www.bakom.ch/de/medieninfo/medienmitteilungen/uvek/artikel/00720/>).

Sollte die Revision übernommen werden, müssten Provider gemäss dem FMG-Artikel 45a «mit geeigneten und zumutbaren Massnahmen die Übermittlung von Werbemitteln an Kundinnen und Kunden verhindern, die dazu nicht ihre ausdrückliche Zustimmung gegeben haben oder nicht schon in einer Geschäftsbeziehung mit der Absenderin oder dem Absender der Mitteilung stehen.» Auch steht eine Änderung des Bundesgesetzes gegen den unlauteren Wettbewerb (UWG) in der Vernehmlassungsphase. Neu würde zu Artikel 3 ein Buchstabe «n» hinzukommen: «Unlauter handelt insbesondere, wer (...) Telekommunikationsmittel zu Werbezwecken bei Personen verwendet, die dem nicht ausdrücklich zugestimmt haben und mit denen er oder sie nicht schon in einer Geschäftsbeziehung steht.»

Den Stein ins Rollen brachte die SP-Nationalrätin und Kon-

sumentenschützerin Simonetta Sommaruga, die am 23. Juni 2000 im Nationalrat eine Motion für die Schaffung von Anti-Spam-Gesetzen einreichte. Von ihr wollten wir wissen, inwiefern diese Gesetzesänderungen ihrem Anliegen entgegenkommen. Sommaruga zum FMG-Artikel 45a: «Der Ausdruck «zumutbare Massnahmen» ist ein relativer Begriff und könnte daher zu zurückhaltend ausgelegt werden. Auch müsste geprüft werden, ob ein Provider etwa legitim handelt, falls er für einen Spam-Schutz zusätzlich Geld verlangt.» Den neuen UWG-Artikel würde Simonetta Sommaruga sehr begrüßen: «Es wäre gut und richtig, dies ins UWG aufzunehmen. So hätten eben nicht nur die Betroffenen selbst, sondern auch Verbände (z. B. KonsumentInnenorganisationen) das Recht, gegen Firmen Strafanzeige einzureichen, die Spam verschicken. Solche Anzeigen müssten dann von Annetes wegen verfolgt werden.»

Spam geht oft auch mit einer Verletzung des Datenschutzgesetzes einher. Deshalb wandten wir uns mit ähnlichen Fragen an Philipp Stüssi, Mitarbeiter des Eidgenössischen Datenschutzbeauftragten. Zuerst wollten wir von ihm wissen, wie der FMG-Artikel 45a auszulegen wäre, falls er in der zur Diskussion stehenden Form übernommen würde.

Stüssi: «Die Fernmeldeanbieterinnen allein können ihre Kunden nie gänzlich vor Spam schützen. Es geht hier vor allem darum, dass sie ihre Kunden im Kampf gegen unerwünschte Werbung unterstützen und keinesfalls aktiv an der Verbreitung von Spam mitwirken. Es darf aber daraus selbstverständlich keine Überwachung des Fernmeldeverkehrs der Kunden resultieren.» Offenbar lägen mit dem neuen FMG-Artikel datenschutzrechtliche Bedenken vor, falls etwa die Provider zwecks Spam-Filterung den Mail-Verkehr der Kunden zu stark überwachen und damit übers Ziel hinauschiessen würden. Insofern könnte also nicht nur Spam von der neuen Gesetzgebung betroffen sein, sondern auch die Anti-Spam-Massnahmen.

Natürlich fragten wir ihn auch, wie er als Mitarbeiter des Datenschutzbeauftragten zum geplanten neuen Zusatz zum UWG stehe.

Stüssi: «Hier wird Klarheit geschaffen, dass nur bei Vorliegen einer Einwilligung (Opt-In) oder einer Geschäftsbeziehung Telekommunikationsmittel zu Werbezwecken genutzt werden dürfen. Dies ist aus unserer Sicht eine wesentliche Verbesserung. Jedenfalls gegen Spammer in der Schweiz wird man sich besser wehren können. Für Spam aus dem Ausland sehen wir nach wie vor Probleme.»

Bluewin, Cybernet, Sunrise, SwissOnline und Init Seven wollen ihre technischen Massnahmen weiterhin verbessern oder zusätzliche Filtertechnologien einführen, wobei Letzteres, so gab Fredy Künzler von Init Seven zu bedenken, «eigentlich der falsche Ansatz» sei. Er lege deshalb zusätzlich Wert auf die Mitarbeit in der Antispam-Community, d. h. den Informationsaustausch mit anderen betroffenen Administratoren und Benutzern.

Spammer müssen zudem vielleicht schon bald tief in die Tasche greifen, denn wie uns Bluewin wissen liess, sei die «Umwälzung der durch Spammer entstehenden Kosten auf den Verursacher» eines ihrer Fernziele.

Her mit Gesetzen und Urteilen! «Was fehlt Ihnen am meisten beim Bekämpfen von Spam?» war die Frage, bei der wir erwarteten, dass sich die Schweizer Internet-Provider primär über Mangel an Zeit, Geld oder Perso-

nal beklagen. Doch weit gefehlt! Stattdessen forderten die Provider sehr deutlich mehr Rechtssicherheit in Form von Gesetzen oder brauchbaren gerichtlichen Präzedenz-Urteilen gegen Spammer sowie eine vermehrte Sensibilisierung der Politiker gegen Internet-Missbrauch im Allgemeinen.

Die schwierige internationale Zusammenarbeit gegen Spam war ein Punkt, den **Sunrise** bemängelte. Auch **Cybernet**-Pressesprecher Marco Plüss hielt fest, dass Spamming schneller wachse als die zur Verfügung stehenden (technischen) Mittel und dass eine weltweite Antispam-Organisation eine Notwendigkeit wäre, um Massnahmen und Vorschriften gegen das globale Spam-Problem festzulegen. Nicht zuletzt liege es aber – gemäss Karl Franke von **Ticino.com** – auch an den Benutzern selbst, die Provider auf Verstösse gegen deren Nutzungsbedingungen aufmerksam zu machen. ●