Müll-Abfuhr

Der Mailmüll hat ein unerträgliches Ausmass erreicht. Lesen Sie alles über dessen Ursachen und wie Sie sich wehren können.

ILLUSTRATION TOM HÜBSCHER, TNT-GRAPHICS

von Gaby Salvisberg

Vor gut anderthalb Jahren veröffentlichte der PCtipp schon einmal einen ausführlichen Artikel zum Thema Spam (PCtipp 10/2002). Damals wagte es die Schreibende doch tatsächlich, sich über lächerliche zehn Spammails pro Tag zu beklagen. «Nur» zehn pro Tag, das wäre heute wie Weihnachten. Zum Vergleich: Im Januar 2004 landeten im E-Mail-Postfach der Redaktion täglich rund 134 Spams, im Februar waren es dann schon über 180 – an jedem einzelnen Tag inklusive Wochenenden. Die Anzahl der unerwünschten Werbemails hat sich somit seit Oktober 2002 *verachtzehnfacht*!

Lesen Sie im nächsten Abschnitt, was Spam überhaupt ist und wo es herkommt. Auf Seite 27 erfahren Sie, warum auch Sie mit den verhassten Werbebotschaften belästigt werden. In Sachen Spam-Bekämpfung werden den Benutzern manchmal auch Märchen aufgetischt. Lesen Sie auf Seite 28, was bestimmt *nicht* gegen Spam hilft oder sogar schadet. Weil Spam nervt, zeigen wir Ihnen ab Seite 29, wie Sie die Spam-Plage am besten filtern. Und nicht zuletzt haben es jetzt auch die Politiker gehört, dass in dieser Hinsicht endlich etwas passieren muss: Mehr oder weniger griffige Antispam-Gesetze schiessen von West nach Ost und von Nord nach Süd in immer mehr Ländern wie Pilze aus dem Boden. Nur in unserer sonst so geordneten Schweiz tut man sich damit schwer. Auf Seite 31 berichten wir über den aktuellen Stand des geplanten Antispam-Gesetzes.

Was ist Spam?

Die britische Komikertruppe «Monty Python» brachte das Wort «Spam» (sprich «spähm») in den Siebzigerjahren erstmals in Zusammenhang mit hartnäckigen Angeboten, als in deren berühmtem Wikinger-Sketch einem Gast nichts als Spam (spiced ham, gewürztes Dosenfleisch) aufgedrängt wurde, siehe auch Box «Spam oder SPAM?», unten.

HINTERGRUND

Spam oder SPAM?

Die Hormel Foods Corporation, die amerikanische Herstellerin der Dosenfleisch-Marke SPAM, hat nichts dagegen, wenn das Wort «Spam» für unerwünschte Werbemails herhalten muss (www.spam.com/ci/ci_in.htm). Aber sie legt Wert darauf, dass «SPAM» in vier Grossbuchstaben immer das Fleischprodukt in der Dose bezeichnet. Handelt es sich aber um Werbemails, dann wird gebeten, Spam in Kleinbuchstaben zu schreiben. Fürs deutsche Spam mit einem Grossbuchstaben am Anfang wird wohl eine Ausnahme gemacht.

Das ist Spam, also eine Werbemail, und nicht SPAM (Dosenfleisch)

In Fachkreisen wird statt von Spam eher von UBE bzw. UCE gesprochen, was ausgeschrieben «Unsolicited Bulk E-Mails» und «Unsolicited Commercial E-Mails» bedeutet. Es handelt sich also um unerwünschte Massen- bzw. kommerzielle E-Mails. Als UCE gelten mit Abstand die meisten Spam-Exemplare, da es darin um Geld geht. Eher als UBE gilt jede andere Art von Massenmails, wie z. B. Polit-Spam im Vorfeld von Wahlen und Abstimmungen oder das exzessive Verbreiten von Hoaxes (Scherzmails) und Verschwörungstheorien an Personen, die das nicht wünschen.

Kein Spam ist es hingegen, wenn Sie von einer Firma, deren Kunde Sie sind, hie und da Mails bekommen, genauso wenig wie der Newsletter, den Sie abonniert haben. Wollen Sie diese E-Mails nicht mehr erhalten, tragen Sie sich aus dem Newsletter aus oder bitten Sie die Firma, Ihre Adresse zu streichen. Bei manchen Newsletters ist dies nicht möglich, da der Newsletter-Empfang Teil eines genutzten Angebots ist. Wer zum Beispiel nur die kostenlosen Dienste des deutschen Mailanbieters GMX nutzt, muss den GMX-Newsletter plus Online-Werbung wohl oder übel hinnehmen.

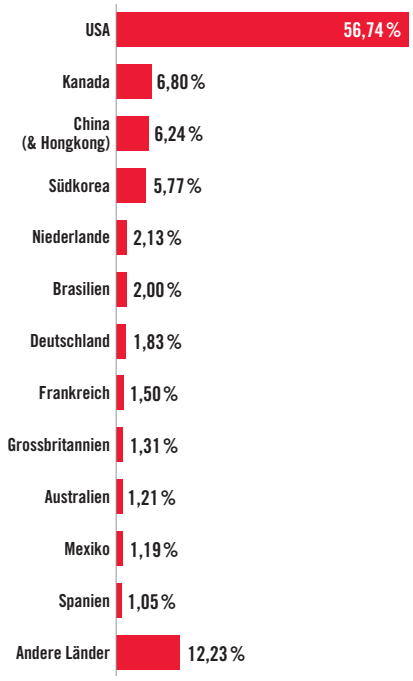
Woher kommt all der Müll? Die eigentlichen Verursacher des Spams sind nur schwer ausfindig zu machen, da sie sich gut zu verstecken wissen. Gemäss einer Hitliste, die der britische Sicherheits-Software-Hersteller Sophos im Februar veröffentlichte (www.sophos.com/spaminfo/articles/dirtydozen.html), werden fast 57 Prozent aller Spammails durch PCs verschickt, die in den USA stehen, siehe Grafik rechts.

Das muss nicht zwingend bedeuten, dass dort auch die meisten Spammer sitzen. Vielmehr ist diese Zahl dem Umstand anzulasten, dass in den USA relativ viele PCs per Breitband-Anschluss am Internet hängen. Unzählige dieser PCs haben sich einen Wurm oder Trojaner eingefangen, der die PCs ohne Wissen ihrer Besitzer in fernbedienbare Spam-Schleudern verwandelt.

HERKUNFT

USA als Hauptsünder

Gemäss einer «Hitliste», die der britische Sicherheits-Software-Hersteller Sophos Ende Februar veröffentlichte (www.sophos.com/spaminfo/articles/dirtydozen.html), werden fast 57 Prozent aller Spammails durch PCs verschickt, die in den USA stehen.



Die Hersteller von Antiviren-Software hegen auf Grund der Bauweise neuerer Würmer einen schlimmen Verdacht: Spammer und Virenschreiber stecken zunehmend unter einer Decke. Das Vorgehen der unheiligen Allianz können Sie sich etwa so vorstellen: Virenschreiber setzen Würmer wie z. B. Sobig oder Bagle in Umlauf. Diese öffnen in der Internetverbindung der befallenen PCs eine Hintertür. Anschliessend greifen Spammer mit den geeigneten Hilfsmitteln auf die befallenen PCs zu und missbrauchen diese dazu, Spam an beliebig viele Empfänger zu schicken.

Das deutsche Computermagazin c't wies vor kurzem nach, dass es im Untergrund des Netzes Personen gibt, die Listen mit tausenden von IP-Adressen solcher offenen PCs vermieten. Dies ist für Virenschreiber und Cracker eine Einnahmequelle, während die Spammer durch den Missbrauch jener meist privat genutzten PCs die wahre Herkunft des Spams bequem verschleiern können.

Der Dumme in diesem üblen Spiel ist nicht nur der Anwender, der am Ende Spam bekommt, sondern vielmehr jener, dessen PC missbraucht wird: Er ist es, dessen Internetverbindung vom Provider gekappt wird, sofern sich andere Personen über den Spam von seiner verwurmten Kiste beschweren. Wobei das noch das kleinere Übel ist; denn er wird es auch sein, an dessen Tür die Ermittlungsbeamten zuerst klopfen, wenn über seinen PC nicht nur gewöhnliche Spammails, sondern auch illegale Inhalte verbreitet werden.

Warum gerade Ihre Adresse?

Etwas treibt vielen Anwendern die Sorgenfalten auf die Stirn: Kaum ist bei einem Provider ein neues Mailkonto eröffnet, trifft schon die erste Spammail ein, obwohl man doch die neue Adresse noch gar nicht öffentlich benutzt hat. Wie kann so etwas passieren?

Verkauft Ihr Provider etwa die Adressen seiner Kunden? Kaum! Wenn schon am ersten Tag eine wahre Spam- oder Virenflut über Ihr Konto hereinbricht, dann hat das oft eine ganz andere, banale Ursache: Sie haben sich vermutlich eine Adresse geschnappt, die zuvor einem anderen Benutzer gehörte und von diesem aufgegeben wurde. Je früher ein Provider eine solche Adresse wieder zur Registrierung freigibt, desto grösser ist die Gefahr, dass man Spam vom Vorbesitzer erbt. Mit diesem Risiko müssen Sie leider leben.

Adressernte beim Mailserver: Eine der am häufigsten eingesetzten Methoden von Spammern und Adresssammlern nennt sich SMTP-Harvesting (engl. to harvest, ernten). Der SMTP-Server ist der Computer, der beim Provider die Mails für die spätere Verteilung in die eigenen Postfächer oder an externe Server entgegennimmt. Ein SMTP-Harvesting-Programm nutzt nun die typische Kommunikation aus, die auch bei einem normalen Mailversand zwischen den beteiligten Computern stattfindet. Stellen Sie sich diese Kommunikation etwa wie ein Gespräch vor:
Harvester: «Hallo Server, ich habe Post für 'aaa'.»
Server: «Verschwinde. Habe kein solches Konto.»
Harvester: «Hallo Server, ich habe Post für 'aab'.»
Server: «OK, Konto gibts, her mit der Mail.»
Harvester: «Ätsch, habs mir anders überlegt.»

Ohne wirklich eine Mail an «aab@server.ch» verschickt zu haben, weiss das perfide Harvesting-Tool schon, dass die Adresse «aab» auf diesem Server existiert. Solche Ernte-Programme probie- ▶

HINTERGRUND

Typische Antispam-Filtermethoden

Filtermethoden wie diese finden Sie in vielen verschiedenen Antispam-Lösungen, siehe Seite 29.

■ **Bayes Textmuster-Profiler:** Dieses Filterkonzept will herausfinden, welche Inhalte Sie haben möchten. Weil jeder Benutzer andere Vorlieben hat, lässt sich dieser Filter trainieren. Hierfür reicht es meist, in Ihrem Mailprogramm oder im Online-Filter des Providers eine unerwünschte Mail als Spam zu kennzeichnen.

■ **Blacklist:** Eine Liste mit unerwünschten Absenderadressen oder Absender-Domains. Was von da kommt, wird gefiltert.

■ **DNS-Blacklist:** Ständig aktualisierte Listen von Servern, die viel Spam verschicken. Was von da kommt, wird automatisch gefiltert oder sogar beim Eintreffen ganz einfach abgelehnt.

■ **Open-Relay-Datenbanken:** Ständig aktualisierte Listen von ungeschützten Mailservern («open relays»), von denen ausser Spam nichts zu erwarten ist. Was von diesen Servern kommt, wird abgelehnt oder gefiltert.

■ **Regular Expressions (RegEx):** Spammails enthalten oft typische, sich wiederholende Merkmale, Ausdrücke oder Zeichen wie z. B. «alles gratis», «click here to remove», «Viagra», «$$$» oder eine Häufung von GROSSSCHRIFT und bestimmten Satzzeichen, z. B. «!!!». Ein RegEx-Filter vergibt nun für jedes Merkmal Spam-Punkte. Überschreitet eine Mail eine bestimmte Punktzahl, wird sie (meist zu Recht) als Spam betrachtet und eliminiert.

■ **Whitelist:** Das Gegenteil einer Blacklist. Was mit einer Absenderadresse oder Absender-Domain daherkommt, die auf einer Whitelist steht, umgeht alle anderen Filterprüfungen und gilt somit automatisch als erwünschte Mail.

ren alle möglichen Zeichenkombinationen durch, die vor dem @-Zeichen stehen können, z. B. auch Vornamen/Nachnamen-Kombinationen.

So kitzeln sie aus einem Server innert weniger Stunden automatisch tausende von gültigen Adressen – auch solche, die nie öffentlich verwendet wurden. Als Anwender können Sie gegen diese Adressdiebe rein gar nichts tun. Die Provider versuchen, die Attacken mit technischen Mitteln zu erschweren, leider jedoch mit mässigem Erfolg. Da diese Sammelmethode mit legitimen Kommunikationselementen arbeitet, würden zu strenge Einschränkungen auch gewöhnliche, echte Mails abschmettern. Über einen solchen Fall berichteten wir im Januar 2004, siehe WEBCODE **26354**.

Foren, Websites, Usenet: Sehr gerne stürzen sich Spammer und Adresssammler auf alles, was sich mit einem @-Zeichen öffentlich blicken lässt. Das können Adressen in Diskussionsforen sein, aber auch in Online-Gästebüchern, öffentlichen Verzeichnissen (z. B. von ICQ, AOL), Webseiten und Usenet-Newsgroups. Auch hier kennt der Spammer Programme, die das Sammeln der Adressen automatisch für ihn erledigen. Verhindern können Sie das nur, indem Sie Ihre Adresse schlicht nicht veröffentlichen oder für solche Zwecke die Adresse eines eigens angelegten Alternativkontos angeben. Erstellen Sie ein solches Konto bei einem Freemail-Provider (z. B. GMX, Hotmail oder Swissinfo.org) und filtern Sie dieses beim Abholen der Mails, siehe auch «Filtern», Seite 29.

Kauf von Maildatenbanken: Wenn der Spammer die Adressen nicht selbst sammeln will, kauft er sie eben bei jemandem, der diese Arbeit schon erledigt hat. Hat ein Adresssammler Ihre Adresse einmal in die Finger bekommen, können Sie davon ausgehen, dass Sie früher oder später mehr als nur ein Spammer mit seinem Müll eindeckt.

Was sicher nicht hilft

Über Spam und Spam-Bekämpfung wird viel geschrieben, leider auch viel Falsches. Wir haben uns mal in der «Märchenabteilung» umgehört.

Antwort an Spammer: Das Zurückmailen einer geharnischten Antwort an den Spammer ist völlig zwecklos, weil die Absenderadresse für gewöhnlich nicht dem Spammer gehört: Entweder existiert die Adresse gar nicht oder sie gehört einem unschuldigen anderen Spam-Opfer. Die Absenderadresse einer Mail lässt sich leider beliebig fälschen.

An Provider weiterleiten: In der Tagespresse liest man gelegentlich einen Tipp wie «Leiten Sie Spam an Ihren Provider weiter.» Eine solche Empfehlung ist Unsinn. Ihr eigener Internetprovider kann normalerweise genauso wenig für den Spam wie Sie. Und er kann dem Spammer auch nicht die Leitung kappen; es sei denn, der Spammer wäre zufälligerweise auch ein Kunde Ihres Providers.

Der «Remove»-Link: In vielen Spammails ist ein Link angegeben, den man benutzen solle, um die Mails abzubestellen. Sollen Sie da wirklich draufklicken, um sich aus der Spam-Datenbank auszutragen?

Entscheiden Sie selbst: Die meisten Spammer sind freche Lügner. Die belügen Sie über die Qualität und Wirkung der Produkte, machen Ihnen falsche Gewinnversprechungen, verwenden falsche Absenderadressen, verstecken im HTML-Quellcode dubiose Links unter offiziell aussehenden Adressen und behaupten oft auch noch, Sie hätten die Informationen selbst angefordert. Und da wollen Sie einem Spammer glauben, wenn er vorgibt, er würde Ihre Adresse löschen? Eben.

Es mag zwar Ausnahmen geben, aber das Gros der Spammer wird etwas ganz anderes tun, als Ihre Adresse zu löschen: Mit einem Klick auf den «Remove»-Link bestätigen Sie ihm, dass Sie sein Spam bekommen haben und Ihre Adresse somit gültig ist. Ihre Adresse gewinnt für ihn an Wert, mit dem Resultat, dass er Sie noch häufiger mit Spam überschüttet oder dass er die Adresse umso teurer an seine Spammer-Kumpels verkauft.

«Kauf mich!»: Auf keinen Fall sollten Sie etwas bei einem Spammer kaufen, egal, wie interessant sein Produkt auf den ersten Blick in der Werbemail aussehen mag. Jeder einzelne Franken, den Sie einem Spammer überlassen, bestärkt ihn in seinem belästigenden Treiben. Sollten Sie das Produkt unbedingt haben wollen, dann suchen Sie eine andere Bezugsquelle. Vielfach werden Sie beim Vergleich der Preise oder Produktbeschreibungen sogar merken, dass Sie beim Spammer zu viel bezahlt hätten oder dass sein Produkt nicht das ist, was er Ihnen weismachen wollte.

Filtern

Spam kann an verschiedenen Stellen und nach verschiedenen Kriterien ausgefiltert werden. Das Filtern ist allerdings ein zweischneidiges Schwert. Erstens können erwünschte Mails im Filter hängen bleiben. Zweitens wird das eigentliche Problem nicht gelöst: Spam wird trotzdem verschickt, Sie haben damit bloss etwas weniger Arbeit. Und dem Verursacher ist es wurst, ob 50 Prozent seines Mülls ungelesen entsorgt wird. Trotzdem ist es nicht von der Hand zu weisen: Spam-Filter sparen Zeit.

Filter des Providers: Immer mehr Internetprovider bieten eigene Spam-Filter an, die direkt in den Postfächern auf dem Mailserver arbeiten. Ist das bei Ihrem Mailprovider der Fall, können Sie den Spam-Filter für Ihr Mailkonto selbst verwalten. Je nachdem, welche Einstellungen Sie gewählt haben, werden als Spam erkannte Mails schon bei der Ankunft auf dem Server ohne Ihr Zutun sofort entsorgt oder in einen Spam-Ordner verschoben.

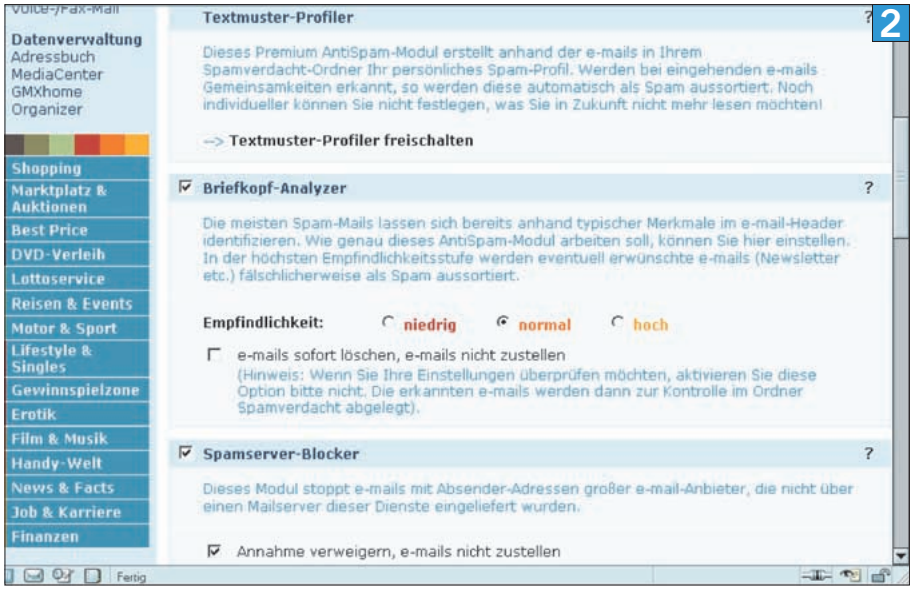
Surfen Sie auf die Webseite Ihres Mailproviders und melden Sie sich dort mit Ihrem Mailbenutzernamen und dem zugehörigen Kennwort an. Es präsentiert sich eine Übersicht, das so genannte Web-Interface zu Ihrem Mailkonto, wie zum Beispiel beim Provider GMX, Screen 1.

Halten Sie darin nach einem Link wie SPAMFILTER oder SPAMSCHUTZ Ausschau und klicken Sie ihn an. Nun haben Sie meist verschiedene Optionen zur Verfügung, die Sie nach Ihren Wünschen einstellen können, Screen 2. Normalerweise finden Sie zu allen Einstellungen auch eine genauere Beschreibung in Form einer Hilfe (hier jeweils das Fragezeichen) oder noch präziser einstellbare Optionen.

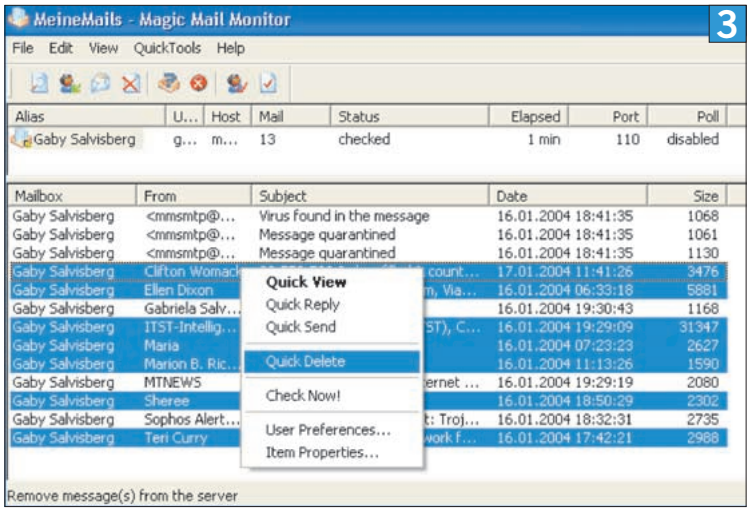
Die meisten Spam-Filter arbeiten nach ähnlichen Prinzipien, egal, ob es sich um den Filter Ihres Providers handelt, um jenen Ihres Mailprogramms oder um ein zusätzlich installiertes Filter-Programm wie zum Beispiel SpamPal. Lesen Sie in der Box «Typische Antispam-Filtermethoden», S. 27, welche Begriffe was bedeuten.

Falls Sie den Spam-Filter Ihres Providers einsetzen, bedenken Sie: Wenn Sie Spam nicht aus Ihrem Konto entfernen, sondern online in einen Spam-Ordner verschieben lassen, verbrauchen die Müllmails wertvollen Speicherplatz. Sie müssen deshalb hie und da das Web-Interface des Providers aufsuchen und den Spam-Ordner leeren. Dies kann je nach Provider und Internetverbindung eine ziemlich langwierige Sache sein.

Ein Web-Interface wie dieses finden Sie bei vielen Mailprovidern



Über Ankreuzen der gewünschten Optionen steuern Sie die Einstellungen



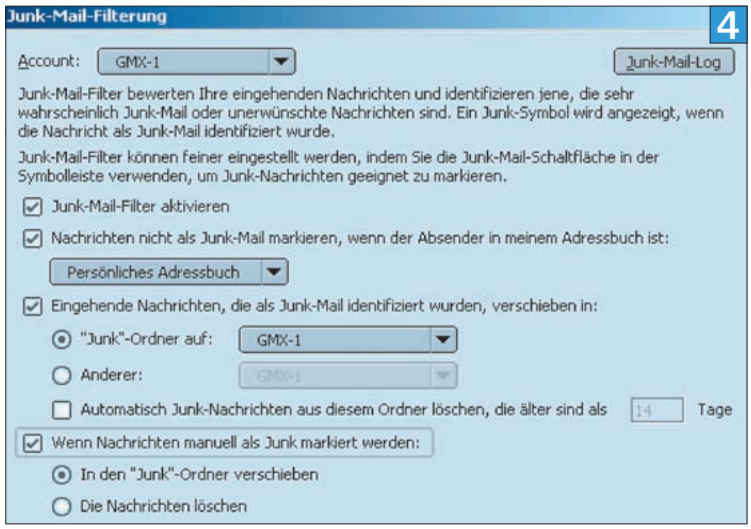
Mit dem Magic Mail Monitor räumen Sie Spammails im Nu weg

Fernlöschen per Hilfs-Programm: Es gibt Software, mit der Sie den Inhalt Ihres Postfachs, das beim Provider liegt, direkt anschauen können. Absender, Betreffzeilen und Grösse der Mails werden angezeigt. So entsorgen Sie lästige Mails mit wenigen Mausklicks gleich im Dutzend, bevor Sie diese mit Ihrem regulären Mailprogramm herunterladen. Der Magic Mail Monitor ist ein solches «Fernlösch-Programm», Screen 3. Details über dieses praktische Freeware-Programm lasen Sie im PCtipp 3/2004, «Blick ins Postfach», S. 48. Diesen Artikel finden Sie auch im Online-Archiv unter www.pctipp.ch mit WEB-CODE **pdf040348**. ▶

Filter im Mailprogramm: Einige Mailprogramme, unter anderen auch Outlook 2003, haben einen integrierten Spam-Filter, der Mails, die wie Spam aussehen, nach dem Herunterladen direkt in einen Spam-Ordner oder in den Papierkorb verschiebt. Solche Filter sind meist lernfähig: Sie können ihm beibringen, was für Sie Spam ist. Über einen brauchbaren Filter verfügen die Programme Mozilla Mail und Mozilla Thunderbird.

Um ihn einzuschalten, gehen Sie zum Menü TOOLS/JUNK-MAIL-FILTER und setzen ein Häkchen bei «Junk-Mail-Filter aktivieren». Sollen die als Spam erkannten Mails aus dem Weg bzw. aus dem Posteingang geräumt werden, setzen Sie ebenfalls Häkchen bei «Eingehende Nachrichten, die als Junk-Mail identifiziert wurden, verschieben in» und «Wenn Nachrichten manuell als Junk markiert werden». Wählen Sie bei beiden Optionen als Verschiebeziel den «Junk»-Ordner aus, dann wird ein solcher nach dem bestätigenden Klick auf OK automatisch erstellt, Screen 4.

Von nun an wird Spam automatisch in den «Junk»-Ordner verschoben. Wurde eine Spammail übersehen oder eine erwünschte Mail fälschlicherweise als Junk taxiert, bringen Sie Mozilla durch den Klick auf die JUNK- bzw. KEIN JUNK-Schaltflächen Vernunft bei.



Aktivieren Sie in Mozilla Mail oder Thunderbird die Junk-Mail-Optionen

Filtern per Zusatz-Programm: Fehlt Ihrem Mailprogramm ein brauchbarer Filter, übergeben Sie diese Aufgabe einem Zusatz-Programm, das sich quasi zwischen Ihr Mailprogramm und Ihr Online-Postfach setzt und die Mails nach typischen Filtermethoden (siehe Box S. 27) filtert bzw. gegebenenfalls als Spam markiert. Und mit Ihrem Mailprogramm erledigen Sie den Rest, indem Sie die als Spam markierten Mails mit einer einfachen Sortierregel entweder in einem Spam-Ordner oder direkt im Papierkorb versenken. Ein sehr guter und recht zuverlässiger Spam-Markierer ist die Freeware SpamPal, WEBCODE 23312. Voraussetzung ist, dass Ihr Mailkonto auf einem so genannten POP3-Server liegt, was z. B. bei Hotmail nur gegen Bezahlung der Fall ist.

Bereiten Sie zuerst die Mailprogramm-Einstellungen vor: Lassen Sie sich darin die EIGENSCHAFTEN Ihres Mailkontos anzeigen (meist via EXTRAS/KONTEN). Unter SERVER steht Ihr POP3-

Servername (z. B. «pop.provider.net»). Notieren Sie sich diesen und ändern Sie ihn zu «localhost» (ohne Anführungszeichen). Bei den Anmeldeinformationen finden Sie Ihren Benutzernamen. Hängen Sie diesem ein «@» an (auch wenn er schon ein @ enthält) und fügen Sie dahinter den vorhin durch «localhost» ersetzten POP3-Server an, damit Ihr Benutzername z. B. «alter-benutzername@pop3.provider.net» lautet, Screen 5.

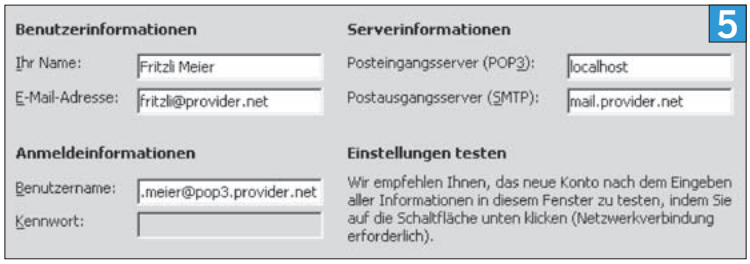
Laden Sie nun SpamPal herunter und starten Sie die Installation durch einen Doppelklick auf die Datei spampal.exe. Wählen Sie Ihre Sprache, akzeptieren Sie die Lizenzvereinbarung und klicken Sie sich per WEITER durch die Installation. Sobald ein lila Schirmchen im Systemtray (in der Systemleiste unten rechts) auftaucht, klicken Sie mit Rechts darauf und wählen OPTIONEN. Klicken Sie MAIL-MARKIERUNG an und stellen Sie Folgendes ein: Das Kästchen «Markiere die Betreff-Zeilen von Spam» muss ausgewählt sein und im zugehörigen Feld soll «**SPAM**» stehen, Screen 6.

Ab sofort markiert SpamPal alle Mails, die er für Spam hält, im Betreff mit «**SPAM**». Was jetzt kommt, kann jedes halbwegs moderne Mailprogramm: Erstellen Sie in Ihrem Posteingang einen separaten Ordner namens «Spam». Richten Sie in Ihrem Mailprogramm eine einfache Filterregel ein. Dies bewerkstelligen Sie z. B. unter Outlook mit dem REGEL-ASSISTENTEN im Menü EXTRAS und bei Outlook Express via EXTRAS/REGELN/E-MAIL. Verwenden Sie diese Kriterien: «Nach Erhalt einer Nachricht mit **SPAM** im Betreff, diese in den Ordner 'Spam' verschieben.»

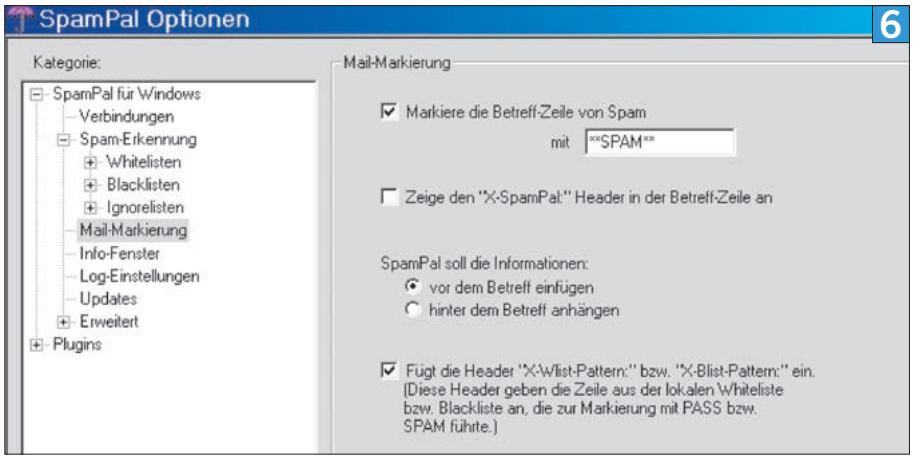
In den OPTIONEN von SpamPal finden Filterprofis übrigens viele zusätzliche Einstellungen, um den Filter weiter zu optimieren, Screen 7. Hier die fünf wichtigsten:

- Sollte SpamPal die Mail eines erwünschten Absenders fälschlicherweise immer wieder als Spam markieren, setzen Sie diesen Absender auf die «Whitelisten», Screen 7 **A**.
- Standardmässig sind nicht alle Blacklists aktiviert. Wenn Sie besonders scharf filtern möchten, schalten Sie unter «Allgemeine Blacklisten» **B** noch die eine oder andere zusätzlich ein, zum Beispiel jene von «SPEWS» und «SpamCop».
- Sofern Sie aus bestimmten Spam-trächtigen Ländern wie z. B. China oder Korea keine erwünschten Nachrichten erwarten, können Sie die Mails von dort via «Länder» **C** gleich gesamthaft in den Filter stecken.
- Via «Updates» **D** bestimmen Sie, wie oft SpamPal nach Updates des Programms selbst oder der DNSBL-Blacklists suchen soll.
- Unter «Plugins» **E** finden Sie die leistungsfähigen Inhaltsfilter «RegExFilter» und «URLBody». Der erste erkennt typische Spam-Ausdrücke und der zweite prüft die im Spam enthaltenen Web-Links darauf, ob diese auf einer Blacklist stehen.

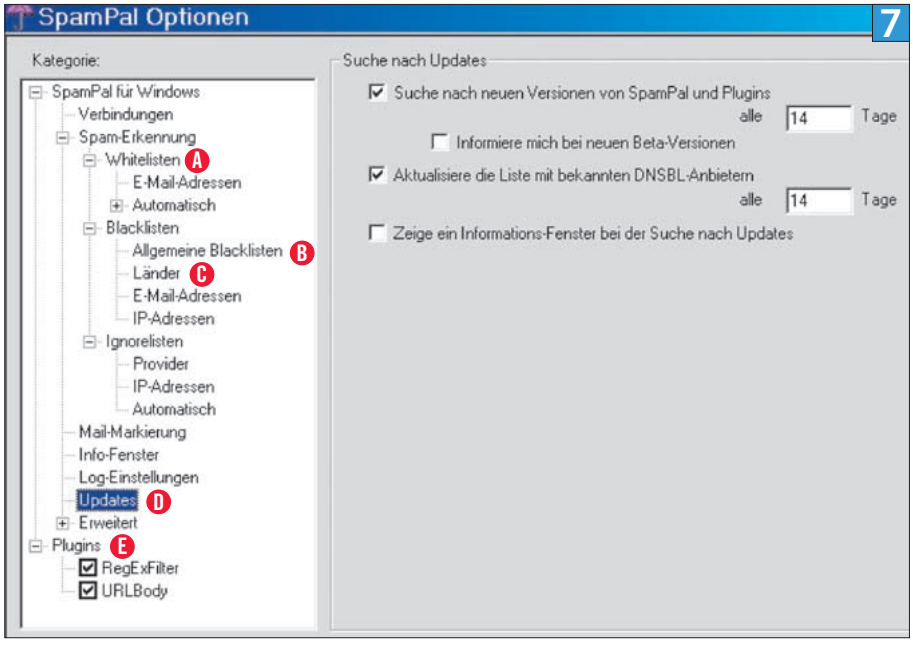
Tipps: Setzen Sie den Spam-Filter mit Bedacht ein. Benutzen Sie ihn nicht zum direkten Löschen von Spammails, sondern lediglich zum Markieren und Aussortieren. So trennen Sie schon mal die gröbste Spreu vom Weizen. Bevor Sie die aussortierten Mails komplett löschen, überfliegen Sie die Absender und Betreffzeilen. Das gibt Ihnen die Chance, einen «false positive» (falsch als Spam erkannte Mail) aus dem Eimer zu fischen.



Ihre Kontoeinstellungen (hier Outlook 2002) sind jetzt bereit für SpamPal



SpamPal soll Spam-Betreffzeilen mit dieser Zeichenfolge versehen



Stöbern Sie ruhig mal in diesen Einstellungsmöglichkeiten

Rechtliches

Der Bundesrat schmiedete bis im Sommer 2002 an einer Revision des Fernmeldegesetzes (FMG), das neben anderen Punkten auch neue Gesetzesartikel enthält, die Spam verbieten. Nach einer Vernehmlassungsphase, die bis Ende Oktober 2002 dauerte, und nach dem Sichten und Zusammenfassen der Ergebnisse verabschiedete der Bundesrat im November 2003 seine Botschaft zur Änderung des Fernmeldegesetzes an die Adresse der zuständigen «Kommission für Verkehr und Fernmeldewesen» (KVF).

Im Februar 2004 empfahl diese Kommission dem Nationalrat, auf den Entwurf *nicht* einzutreten. Der Grund war die ebenfalls im FMG-Revisionsentwurf enthaltene Entbündelung der «letzten Meile» des Telefonfestnetzes, die einer Mehrzahl der Kommissionsmitglieder in dieser Form nicht gefiel. Schon drohte, zusammen mit der Entbündelung auch das weitgehend unbestrittene Spam-Verbot bachab zu gehen. Am 18. März 2004 beschloss hingegen der Nationalrat, auf die geplante FMG-Revision einzutreten. Man darf jetzt wieder hoffen, dass Spam in ein oder zwei Jahren in der Schweiz verboten sein wird. ■