Spam wirksam bekämpfen

Christian Schneider

I. Einleitung

1. Was ist Spam?

Welcher E-Mail-Benutzer hat nicht schon offenbar massenweise ausgesandte, nicht angeforderte Nachrichten von Fremden oder unbekannten Firmen erhalten, in denen zweifelhafte Angebote beworben werden? Diese nennt man *„Junk-Mails"* oder *„Spam"*. In den meisten Fällen sind sie auf Englisch und werden ungelesen gelöscht. Solche Massenmails auszusenden, nennt man *„spammen"* bzw. *„spamming"*.

Spammen kann man nicht nur mit Mails, sondern auch durch massenweises Senden von unerwünschten Artikeln in eine Unzahl von Newsgroups; man kann durch übertrieben häufige Anmeldung der Webpage Suchmaschinen mit dem Ziel spammen, bei der Suche nach der Seite auf vordere Ränge in der Liste der Suchergebnisse zu gelangen usw. Auch das Versenden von unsinnigen bzw. falschen Botschaften, z.B. über nicht existente Viren (Hoax) oder zu vordergründig karitativen Zwecken mit der Bitte um Weiterleitung an möglichst viele Personen, ist Spam in Form von Kettenbriefen.

Spam hat also die Merkmale der vermuteten Unerwünschtheit und Belästigung des weitaus größten Teils der Empfänger, des massenweisen Auftretens eines identischen Inhalts, der unproduktiven Belastung von Netz- und Computersystemen, der Unverhältnismäßigkeit zwischen Gesamtaufwand und Nutzen, Nichtachtung der Arbeitszeit anderer und vieles mehr; kurz des Missbrauchs der Freizügigkeit des Internet.

Dieser Artikel behandelt Spam nur in Form der unerwünschten Werbemails. Hier unterscheidet man unter anderem noch genauer zwischen:

- UBE - *Unsolicited Bulk E-Mail*: Wird ohne Anforderung an eine riesige Anzahl von Empfängern ausgesendet. Diese Form ruft allerdings nicht zum Kauf von Produkten oder zum Besuch einer kommerziellen Webseite auf, im Gegensatz zum:
- UCE - *Unsolicited Commerical E-Mail*, das den weitaus größten Teils des Spams ausmacht.
- MLM - *Multilevel Marketing*, welches phänomenale Profite durch Kauf und Verkauf diverser Produkte an möglichst viele Abnehmer verspricht. Dies ist verwandt mit:
- MMF - *Make Money Fast*, einer Aufforderung zur Teilnahme an in den meisten Ländern verbotenen Pyramidenspielen. [1]

Das Wort Spam hat eine ungeklärte Entstehung. Es soll von angeblich wenig geschmackvollem Büchsenfleisch kommen, welches im englischen Sprachraum „Spam" (*Spiced Pork and Ham*)[2] genannt wird. SPAM in Großbuchstaben ist außerdem ein eingetragenes Markenzeichen und Produkt der Firma Hormel, die aber nichts mit Spam in Form unerwünschter Mail zu tun hat[3]. Auch soll ein Monty-Python-Sketch, in dem das Wort häufig vorkommt, der Namensgeber sein.[4]

2. Rechtliches

Spammen verstößt in jedem Fall gegen die *Netiquette*, die allgemein akzeptierten Regeln für den fairen Internetgebrauch:

Bitte verschicken Sie keine unerwünschten Werbe-E-Mails an irgendwelche E-Mail-Adressen, die Ihnen in die Hände fielen. In Österreich ist das explizit verboten.[5]

Seit Sommer 1999 ist in einer Novelle des österreichischen Telekommunikationsgesetzes (BGBl. I Nr. 188/1999) geregelt, dass „die Zusendung einer elektronischen Post als Massensendung oder zu Werbezwecken der vorherigen – jederzeitig widerruflichen – Zustimmung des Empfängers bedarf. Jeder Verstoß ist mit Geldstrafe bis zu 500.000 ÖS sanktioniert."[6]

In der BRD ist Spammen ebenso verboten. Der Deutsche Multimedia-Verband http://www.ec-infosite.de/ bemerkt auf seiner Webseite:

Im Unterschied zur postalischen Werbung ist die Zusendung unerbetener E-Mail-Werbung nicht erst mit Eintragung des Empfängers in eine Robinson-Liste unzulässig, sondern verstößt nach gegenwärtiger Rechtsprechung bereits dann gegen § 1 UWG (Gesetz gegen den unlauteren Wettbewerb), § 823 Abs. 1 BGB (Schadensersatz wegen unerlaubter Handlung), wenn Werbe-Emails ohne Aufforderung des Empfängers an diesen versandt werden. Dem Adressaten unerbetener Emailwerbung steht daher gegen den Absender ein Unterlassungsanspruch zu.

Auch die Schweizer Lauterkeitskommission verurteilte im November 2001 Spamming als aggressive und unlautere Werbemethode. Die meisten Angebote seien überteuert und von minderwertiger bzw. zweifelhafter Qualität, wurde festgestellt.[7]

An einer gesamteuropäischen Gesetzesregelung wird gearbeitet, eine sogenannte „Opt-In-Lösung" scheint sich abzuzeichnen, was bedeutet, dass Empfänger von Werbemails vorher ausdrücklich hierzu ihre Zustimmung geben müssen:

The European Parliament has decided to accept the Council's Common Position which would require senders of advertisements by "electronic mail" to have the recipient's prior consent. "Electronic mail" is defined broadly enough so as to include text messaging systems based on mobile telephony in addition to email.

The 'opt-in' requirement for electronic mail will be in Article 13, Paragraph 1 of the new Directive concerning the processing of personal data and the protection of privacy in the electronic communications sector which will enter into force following its publication in the Official Journal. The Directive will guide the enactment of legislation throughout the European Economic Area, which includes the 15 EU Member States and European Free Trade Association members Norway, Iceland, and Liechtenstein. EU Members Austria, Denmark, Finland, Germany, Greece, and Italy as well as EFTA member Norway had already implemented 'opt-in' in their national legislation.[8]

Darüber hinaus haben alle seriösen ISP (Internet-Service-Provider) in den Geschäftsbedingungen Klauseln, die jede Art von Missbrauch verbieten:

Im Falle der strafgesetzwidrigen Nutzung, bei offensichtlicher Verwendung der Dienste in missbräuchlicher, belästigender oder schädigender Absicht iSd TKG ist tele.ring berechtigt, den Dienst vorübergehend, bis zu einer endgültigen Klärung der Sachlage, zu sperren.

Die Dienste des Kunden werden gesperrt, und er muss für eine eventuelle Wiedereinschaltung die Kosten übernehmen.[9]

Viele ISP verbieten auch das Anpreisen von Spamdiensten und -programmen auf den Webseiten ihrer Kunden.

Clause: Internet Abuse. HostPro will always take the appropriate action when Internet abuse is brought to our attention. Customer shall not abuse Internet resources including, but not limited to, allowing spamming by third parties to promote a web site hosted by HostPro; offering for sale or otherwise enabling access to (i) warez or (ii) software products that facilitate the sending of unsolicited e-mail or facilitate the assembling of multiple e-mail addresses ("spamware").[10]

II. Bewertung des Spammens

1. Kontroversielle Ansichten

Schnell, billig, exakt, zuverlässig, bequem – das ist E-Mail und dadurch in kürzester Zeit zu einer der beliebtesten Kommunikationsmöglichkeiten überhaupt geworden. Räumliche Entfernungen spielen keine Rolle. Man prognostiziert für das Jahr 2006 das Versenden von 60 Milliarden E-Mails täglich[11]. So gesehen, wäre es ein einfaches und kostengünstiges Werbemedium. Ein Text kann an unbeschränkt viele Empfänger versendet werden.

Vergessen darf man auch nicht, dass das Internet nicht zuletzt auf Grund von hohen Werbeeinnahmen relativ kostengünstig betrieben werden kann. So ist es zu einem weit verbreiteten Vorurteil gekommen, dass „im Internet alles gratis" zu haben sei. Viele Informationen werden auf werbefinanziert betriebenen Webseiten kostenfrei angeboten. Kostenfreie Programme sind werbefinanziert

(Adware). „Ohne Spam, Trick-Banner und Pop-ups wäre das Internet längst kostenpflichtiges Ödland“[12].

Bis 2006 sollen einer Prognose zufolge 67% der Europäer Internetanwender sein und 147 Milliarden Euro mittels E-Commerce umgesetzt werden. Schon jetzt werden in Österreich jeden Tag 25 Millionen E-Mails und SMS versendet. Die Kommunikationswelt wurde durch das Internet unvergleichlich verändert, obwohl es erst am Anfang der Entwicklung steht und mit dem Entwicklungsstand des Fernsehens in den Fünfziger Jahren verglichen wird.[13]

2. Universität vs. Kommerz

Internet, WWW und E-Mail sind aus wissenschaftlich-universitären, von öffentlichen Stellen finanzierten Netzwerken entstanden[14]. Das Internet ist von „educated people“ für „educated people“ geschaffen worden. Mit der Öffnung für die Allgemeinheit und durch seine nachfolgende rasante Verbreitung spiegeln die Benützer aber immer mehr die Zustände unserer realen Gesellschaft wider. So wird schon 1997 bemerkt:

Auch die Kommerzialisierung des Internet, vor der man sich noch 1994 gefürchtet hat [...], hat mittlerweile stattgefunden und die Furcht vor einer Kommerzialisierung ist einem Zusammenleben gewichen.[15]

Allerdings ist vom akademischen Geist noch immer viel zu spüren, vielleicht weniger im WWW, aber doch am meisten in den Newsgroups. Hier ist jegliche Form von kommerziellen Beiträgen verfemt, und auf sie wird im Allgemeinen sehr allergisch reagiert. Auch beim Medium E-Mail will sich der User grundsätzlich nicht mit uninteressanter Werbung beschäftigen müssen, da sie ein „Störungsrauschen“ in seinem Gedankenaustausch in wichtigen und interessanten Briefwechseln darstellen. Vielfach war und ist das E-Mail ein Wissens- und Wissenschaftsvermittler, bei dem sich unangemessene Inhalte negativ und ablenkend auswirken. Wenn man sich mit einem wissenschaftlichen oder sonstigen Problem intensiv mit Anderen auseinandersetzt, ist jegliche Unterbrechung besonders unangenehm. Daher die weitgehende Ablehnung kommerzieller Inhalte in E-Mail und Usenet.

3. Warum also Spam bekämpfen?

Ich habe schon festgestellt, dass Spammen kein Kavaliersdelikt ist. Und das hat einleuchtende Gründe. Nirgendwo kann es ohne Folgen bleiben, dass ein einzelner mit geringstem Aufwand Hunderttausende schädigen kann, und es gibt ein krasses Missverhältnis zwischen dem Aufwand des Schädigers und dem Schaden für die Internetgemeinde und die Empfänger.

Spam kostet wertvolle Bandbreite, Server werden überlastet, Mitarbeiter müssen Spam-Beschwerden behandeln[16], Spamming muss zurückverfolgt und ausgeforscht werden, und der Empfänger zahlt zusätzliche Onlinegebühr für den Download der Nachrichten und verschwendet seine Zeit für das Sortieren wichtiger und unerwünschter Mail: unnötige Kosten von Zeit, Geld und Arbeitskraft. Die verschiedenen Methoden der Spam-Abwehr verursachen ebenfalls einen nicht unbeträchtlichen Aufwand.

Insgesamt gesehen dürfte sich Spamming unter dem Strich für die Allgemeinheit nicht rechnen, unter Umständen aber für den Übeltäter. So ist eine Rücklaufquote von 0,1% einer Spamaktion schon ein durchschlagender Erfolg[17]. 99,9% hingegen werden geschädigt.

Die Kosten für den Versender von Werbemails sind mindestens um den Faktor 1000 niedriger als bei konventionellen Marketingmethoden, um 10.000 DM kann man 30 Millionen Werbemails versenden[18]. So ist nicht zu verwundern, dass im Zeitraum von September 2001 bis März 2002 eine Verdoppelung des Spamaufkommens beobachtet werden konnte mit einem Schaden von schätzungsweise 10 Milliarden Euro im Jahr weltweit[19].

Auch der immaterielle Schaden ist beträchtlich:

There are psychological costs as well; frustration and annoyance mounts with each spam message polluting one's inbox.[20]

Vint Cerf, der „Vater des Internet“, schreibt:

Spamming is the scourge of electronic-mail and newsgroups on the Internet. It can seriously interfere with the operation of public services, to say nothing of the effect it may have on any individual's e-mail mail system. ... Spammers are, in effect, taking resources away from users and service suppliers without compensation and without authorization.[21]

Spam ist also zu einem ernsten Problem geworden, und dringender Handlungsbedarf ist geboten. Ich vergleiche Spam mit dem Virenproblem der vergangenen Jahrzehnte. Dabei ist Spam kontraproduktiv und ruiniert schlussendlich das Image der beworbenen Produkte und des Absenders!

III. Technische Voraussetzungen

1. Die Methoden der Spammer

Um Spam wirksam vermeiden bzw. abwehren zu können, muss man einen Exkurs auf die Gegenseite wagen und sich mit den Methoden der Spammer auseinandersetzen. Deren Vorgangsweise zerfällt technisch in drei Schritte: Mail-Adressen sammeln, Spam versenden und Resultate auswerten.

An E-Mail-Adressen heranzukommen ist nicht schwer. Es ist ja gerade Sinn dieser Adressen, dass sie veröffentlicht werden, damit dann jedermann mit dem Eigner in Kontakt treten kann. Veröffentlicht werden sie im Allgemeinen auf der eigenen Homepage, in Newsgroup-Artikeln, im Chat usw. Auch fordern manche Webpages für Zusatzdienste das Eingeben der Mailadresse. Und genau aus diesen Quellen versorgen sich Spammer mit dem wertvollen Gut, allerdings meist nicht händisch. Es gibt Spezialprogramme, die automatisiert das Internet nach Mailadressen durchsuchen, sogenannte „Harvester“ (Erntemaschinen):

Power Email Harvester is the most powerful, easiest to use bulk email software on the market today. Power Email Harvester is the only bulk email software available that can build an emailing list and send bulk email to each email address at the same time! And the program is so simple to use. It can be mastered in 5 minutes.

Power Email Harvester works by checking the validity of every possible address within parameters that you set for it. It then creates a list, in alphabetical order no less, of all valid email addresses within the specified range. You can have the program send a message to that address while it is extracting, save the list to use later, or both![22]

Scheut man den Aufwand, kann man Adressen bei spezialisierten Händlern auch kaufen, und zwar in unterschiedlichen Qualitäten und Preisen. Entweder man entscheidet sich für billige Massenware – *zig Millionen Adressen sind kein Problem – oder man bevorzugt sozusagen „handverlesene“ Qualität: beispielsweise Adressen, die nachweislich existieren, in Betrieb sind, deren Besitzer antworten und sich nicht über den Spam beschweren:

We never release any of our CD's until it passes our "very high standards" test.

Here's how we prepare our email lists.

ABSOLUTELY NO DUPLICATES. Contains over 15 million different addresses! So you don't waste time emailing the same customer twice.

No computer generated addresses. All addresses were collected from real live people!

No GOV, US, EDU, ORG or MIL addresses. Also all known addresses from ISPs of the States of Washington, Virginia or California have been removed. So you won't get in trouble emailing official organizations or emailing states where email marketing is banned.

[...]

All internet addresses have been grouped by domain name to provide the fastest possible delivery times, then randomized within the domain to eliminate the possibility of providers blocking you from sending alphabetical lists.

Addresses include AOL, CompuServe, Prodigy, Delphi, Genie, Mcimail, and miscellaneous from the internet, so you have a cross section of email addresses to send.

Addresses collected right up to the time of production. Very very fresh! So you won't be sending to any out of date email addresses.

We also use a special filter file to remove the list of known complainers to email advertising people that have requested to be removed from future mailings and people that just overall should not be emailed an advertisement.

We use a filter list of 1,800+ words/phrases to clean even more, like spam or webmaster.

We sorted the list into easy to manage packages of 100,000 addresses in a simple text (txt), this format is compatible with of all the Bulk Email software available today and makes it easier for you to send.

All domains have been verified as valid, so you aren't sending emails to domain which don't exist.

[...]

We sell the following packages: -

- *15 Million Email Addresses - $120.00*

- *10 Million Email Addresses - $90.00*
- *5 Million Email Addresses - $70.00*
- *1 Million Email Addresses - $50.00*
- *100,000 Email Addresses - $35.00*[23]

Auch zum Versenden der Massenmails gibt es eine Anzahl von Spezialprogrammen, die – aus naheliegenden Gründen – Fälschungen in die versendeten Nachrichten einbauen, um die Herkunft des Spams zu verschleiern und die Rückverfolgung somit zu erschweren. Sie nützen verschiedene Schwachstellen des SMTP (*Simple Mail Transfer Protocol*), mit dem Mail übers Internet versendet wird, aus:

Express Mail Server - Turns your personal Computer into an actual Bulk Email Server! Completely bypass your ISP's email server and send out your email originating from your personal computer, directly into your recipients mail box! Mail is delivered instantaneously! This incredible mail engine actually hand delivers the message from your computer into the recipient's mailbox, no delay, message literally travels right to its destination. Guaranteed delivery! Every single last one of your messages gets delivered! Message goes directly from your computer to your recipient. Automatically inserts recipients name in the body or your letter for a dramatic increase in responses. Verifies every single address before sending! Puts all bad addresses in a bad address file (practically eliminates undeliverables!).

Express mail will send up to 80,000 messages per hour with a 28.8 modem (even faster with ISDN and T1) and every single message will be individually placed in your recipients' mailbox instantaneously! Randomizing option allows you to break through any filters. This is a necessity to get mail through some ISP filters. Create your messages in the built-in word processor. It has everything you need including spell check and color! This registered version has a value of $299 but it yours' free to send your emails. It is one of the best packages on the market![24]

Wie erwähnt, ist ein tatsächlicher Rücklauf von einem Promille schon ein großer Erfolg. Immerhin funktionieren die Mailadressen der Absender, und die Mails werden tatsächlich gelesen. Auch unhöfliche Antworten bzw. Beschwerden sind daher gerne von Spammern als Qualitätsmerkmal gesehen!

2. Technische Schwächen

E-Mail gibt es schon seit 1972. Ray Tomlinson schrieb die Programme *Readmail*, um Nachrichten zu empfangen, und *Sendmsg* war das andere Teilprogramm, um senden zu können. Auf ihn geht auch das „Klammeraffen"-Zeichen @ zurück.[25]

Das noch heute benützte SMTP, das Transportprotokoll von gesendeten Mails übers Netz, geht auf das Jahr 1982 zurück. Bis zu diesem Zeitpunkt wurde das FTP (*File Transfer Protocol*) benutzt, und mit der Umstellung des Internet auf TCP/IP, das ebenfalls bis heute benützt wird, stellte man den Mailverkehr auf SMTP um, welches von Jon Postel entwickelt worden war. Im selben Jahr wurde der Begriff „Internet" geprägt.[26]

Wir sehen also, die Technik, die hinter unseren E-Mails steckt, stammt noch aus der „Steinzeit" der Computer, und damals war der Kreis der Internetbenutzer ein elitärer von Universitäten, Wissenschaftsinstituten, Regierungs- und militärischen Stellen der USA. So konnte man damals mit den Schwachstellen des SMTP leben.

Und davon gibt es viele. Um eine Mail über einen beliebigen SMTP-Server im Netz an beliebig viele Empfänger zu senden, muss grundsätzlich kein Passwort angegeben werden (*Open Relay*), die Absenderadresse wird nicht verifiziert, und eine Verfälschung ist daher problemlos möglich; der Übertragungsmechanismus ist simpel und kann leicht manipuliert werden, und die Mail kann auf jedem Rechner, der am Übertragungs- und Weiterleitungsweg beteiligt ist, im Klartext eingesehen werden.[27]

```
telnet smtp.ccc.at 25
220 exdb01.ccc.at Microsoft ESMTP MAIL Service, Version:
5.0.2195.5329 ready at Sat, 28 Sep 2002 09:50:33 +0200
HELO
250 exdb01.ccc.at Hello [212.95.24.226]
MAIL FROM: <webmaster@pigeontoestudio.com>
250 2.1.0 webmaster@pigeontoestudio.com....Sender OK
RCPT TO: <schneider@gmx.at>
550 5.7.1 Unable to relay for schneider@gmx.at
```

Um den Prozess genauer zu verstehen, kann man sich mit Telnet[28] in einen Mailserver einloggen und direkt auf der Kommandozeile Mail schreiben[29].

Um den Transportweg einer Mail zu dokumentieren, fügt jeder beteiligte Server im Header, dem für den User im Allgemeinen unsichtbaren Teil der Nachricht, „Received-Zeilen" ein. Diese sind relativ leicht zu fälschen.

3. Das Open-Relay-Problem

Wie wir in Punkt 2 dieses Kapitels gesehen haben, funktioniert der Mailversand praktisch anonym und über jeden Server. Das ist allerdings heute nicht mehr so, da jeder seriöse ISP seine Mailserver sicherer konfiguriert. Zum Beispiel darf nur von der eigenen Einwahlverbindung des Kunden gesendet werden. Oder zuerst muss der Kunde seine Post abholen, dabei wird ja das Passwort verifiziert, und nach dieser Identifikation hat seine IP-Adresse erst Sendeerlaubnis (SMTP after POP). Auch „SMTP-Auth", vor dem Senden wird ein Passwort abgefragt, ist möglich.

Für Spammer, die ja anonym versenden wollen, ist dies kein geeignetes Verfahren mehr, da sie ja sogleich erkannt und vom Provider blockiert, gekündigt und mit Schadenersatzzahlungen bzw. sogar Gerichtsverfahren konfrontiert werden. Daher suchen sie sich gezielt schlecht konfigurierte Server aus, die von jedem Mail annehmen, die Open Relays[30].

Ein richtig konfigurierter Server lehnt fremde Mails ab. Das sieht dann wie auf dem obigen Bild aus: Pech gehabt!

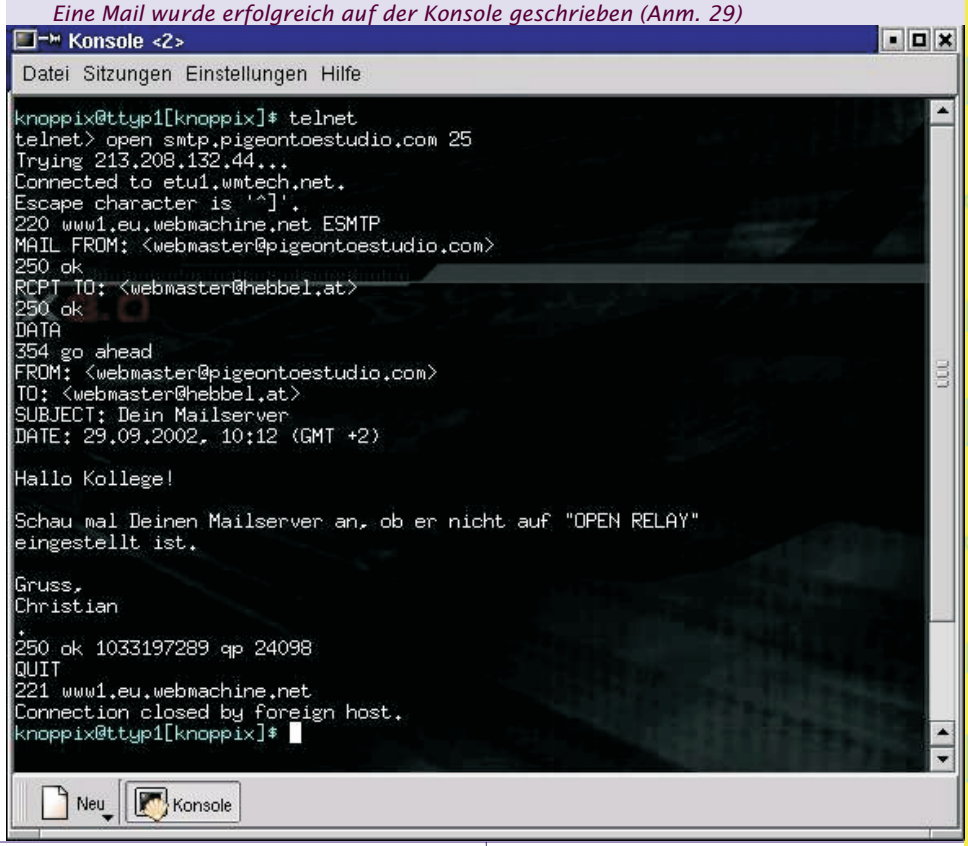
Dennoch ist eine Rückverfolgung möglich, da viele Mailserver, auch die von Webmail-Diensten, die IP-Adresse des Computers des Absenders speichern und in die Mail-Header einfügen. Doch manche tun nicht einmal dies[31], und dann ist der Spammer nur äußerst schwierig über die Logdateien des Mailservers, wenn überhaupt, ausfindig zu machen.

IV. Spam abwehren

1. Vorbeugende Maßnahmen

Kaum einem wird einfallen, sich das Telefonbuch zur Hand zu nehmen und einen Fremden aufs Geratewohl anzurufen. Bei E-Mail ist das anders. Meist werden Fremde auf Postings in Newsgroups oder beim Betrachten derer Internetseiten angeschrieben, da hier viel mehr Informationen über den Betreffenden vorhanden

Eine Mail wurde erfolgreich auf der Konsole geschrieben (Anm. 29)



sind. Im Gegensatz zum überraschenden Telefonanruf oder auch normalen Brief werden solche E-Mails adäquaten Inhalts nicht als Belästigung empfunden.

Es ist ganz wesentlich einfacher, eine Webseite zu erstellen oder seine Meinung in einem Diskussionsforum darzustellen, als etwa ein Buch zu schreiben, um eine breite Öffentlichkeit anzusprechen[32]. Die Mailadresse hat also den Zweck, veröffentlicht zu werden, und so kann sie auch missbraucht werden. Sie haben nur die Wahl, entweder anonym zu bleiben oder in Kontakt mit der Internet-Gemeinschaft zu treten. Selbst das Verheimlichen der Mailadresse nützt nicht viel, da sie oft „erraten" werden kann.

Sie können sich aber mindestens zwei Mailadressen besorgen, z.B. bei einem der zahlreichen Freemail-Dienste. Die persönliche wird nur an Freunde weiter gegeben, die öffentliche wird publiziert. Das hat allerdings den Nachteil, dass Sie zwei Konten verwalten, abrufen und durchsehen müssen, und das bedeutet Mehraufwand. Dennoch ist diese Methode empfehlenswert, da viele Freemail-Anbieter schon Filterregeln für eingehende Mails anbieten, die pauschal und individuell konfigurierbar sind[33].

Wenn Sie in Diskussionsforen Artikel veröffentlichen, wird Ihre Mailadresse damit automatisch öffentlich gemacht, ebenso, wenn sie auf Ihrer persönlichen Homepage als Kontaktmöglichkeit aufscheint. Dazu genügt schon ein `mailto:`-Link, den Harvester erkennen! Geben Sie auch in Chats nie Ihre Mailadresse an.

Geben Sie Ihre Mailadresse nur mit Verstand weiter und tragen Sie diese nicht auf Internetseiten unbekannter bzw. zweifelhafter Unternehmen ein. Abonnieren Sie keine Newsletter, die Sie nicht unbedingt brauchen.

Anworten Sie nicht auf Spam! Dadurch weiß der Übeltäter, dass Sie die Werbemail gelesen haben, und Sie erhalten noch mehr Mails. Klicken Sie daher auch nie auf einen *„Unsubscribe"*-Link.

Wenn möglich, öffnen Sie keine Spam-Mail. Manche HTML-Mails laden Grafiken aus dem Internet, und auch so kann durch den Spammer verifiziert werden, dass die betreffende Mail gerade Sie angesehen haben. Auf dem gleichen Wege kann sogar schädlicher Code auf Ihren Computer geladen werden, etwa Dialer, bei denen der Download trotz Druck auf „Abbrechen" durchgeführt wird[34]. Klicken Sie daher auch auf keinen Fall auf einen Link in der Mail!

Löschen Sie daher Spam-Mail wenn möglich direkt vom Server und laden Sie diese erst gar nicht auf Ihren Computer.

Kaufen Sie nie etwas von Spammern. Diese werben nur, um Geld zu machen, und so unterstützen Sie diese noch. Und wer will schon zweifelhafte Geschäftskontakte knüpfen? Der Firmensitz ist meist in einem fernen Land, so dass man rechtlich gar nicht vorgehen kann, wenn Probleme in der Geschäftsbeziehung auftreten.

Beschweren Sie sich bei Ihrem Provider und bei dem des Absenders, wenn Sie diesen ausgeforscht haben. Machen Sie Spam zu deren Problemen![35]

2. Auf Providerseite

Um anonyme Mailversendung zu unterbinden, muss der entsprechende Mailserver richtig konfiguriert sein. Ein Open Relay ist unakzeptabel. Er soll nur Mails mit richtiger Absenderangabe oder aus dem eigenen Netzwerk annehmen, eine weitere Möglichkeit ist SMTP after POP, wie schon beschrieben. Die Zahl der Empfänger kann limitiert werden, so dass der Spammer nur beschränkten Schaden anrichten kann.

Auch auf der Empfängerseite kann es sich kein seriöser ISP leisten, nichts gegen Missbrauch zu tun. tele.ring z.B. blockiert die IP-Adresse des Mailservers, über den gespammt wird, ein Script am Mailserver entfernt Spam, wenn in großem Ausmaß gespammt wird, Unterlassung wird gefordert und bei Wiederholung rechtlich dagegen vorgegangen[36]. E-Tel akzeptiert u.a. nur Mails, die nicht von Offenen Relays laut ORDB[37] oder von bekannten Spammern laut der Realtime Blackhole List (RBL)[38]stammen[39]. Viele unerwünschte Mails gelangen so erst gar nicht in die Mailboxen der Kunden. RBL und ORDB sind Datenbanken potenzieller Spamquellen, die laufend am neuesten Stadt gehalten werden und auf den Mailservern der ISP, die diese implementiert haben, Massenmails ausfiltern.

Wirkungsvoll ist das Einrichten einer *Teergrube*. Sie verlangsamt künstlich den Mailempfang von Spam, sodass sich die Übertragung zeitlich derart hinzieht, dass sie für den Versender uninteressant wird. Der normale Mailverkehr wird nicht behindert[40].

Es gibt auch kommerzielle Spamfilter, die Administratoren und Provider einsetzen können wie z.B. Brightmail[41], das auch noch Viren ausfiltert. Erkennung und Analyse von Spam wird in Echtzeit an den Kunden übermittelt, so dass die Filterregeln meist noch vor Eintreffen der Spambomben entsprechend am neuesten Stand sind.

3. Was der Endkunde tun kann

Die naheliegendste Möglichkeit ist, unerwünschte Mails, die ja fast immer an Absenderangabe und Betreff im Mailprogramm leicht zu erkennen sind, einfach ungelesen zu löschen. Doch damit wird das Problem nicht kleiner.

Ein schon schwierigeres Unterfangen ist es, Ausschusslisten und Filterregeln im Mailprogramm zu führen. Hierbei besteht zumindest bei unerfahrenen Anwendern die Gefahr, durch unbedachte Einträge auch erwünschte Mails auszufiltern. Daher muss der aussortierte Spam doch durchgesehen werden.

Auch Freemail-Dienste haben meist umfangreiche und gut durchdachte Filterregeln implementiert, auch benutzerdefinierte, die man mit der entsprechenden Erfahrung gut einstellen kann (siehe Anmerkung 33). So gelangen sie erst gar nicht auf die Festplatte bzw. müssen nicht erst heruntergeladen werden. Der Absender erhält eine entsprechende Fehlermeldung.

Wenn möglich, sollte man sich unbedingt beschweren. Dies setzt jedoch etwas Erfahrung und technisches Verständnis voraus.

V. Richtig beschweren

1. Die Header-Zeilen

Wie bereits erwähnt, lässt sich der Transportweg jeder Mail im Internet im Allgemeinen zurückverfolgen. Dazu dient ein an sich unsichtbarer Teil der Nachricht, der sogenannte Header. In den meisten Mailprogrammen und bei vielen Webmail-Diensten kann man sich diesen anzeigen lassen – in Outlook Express etwa, wenn man auf die fragliche Mail klickt und „Eigenschaften – Details – Quelltext" aufruft. Dies ist bei jedem Programm unterschiedlich. [42]

Weiters muss man die so sichtbar gemachten Header-Zeilen richtig interpretieren und verstehen. Dies soll an einem Beispiel demonstriert werden[43]:

Interessant für die Nachforschung des Providers des Absenders sind nur die Zeilen, die mit *Received:* beginnen. Jeder am Transport beteiligte Server trägt diese Informationen aufsteigend in den Header der Mail ein, daher beginnt man von unten nach oben zu lesen. In der untersten Header-Zeile ist eine Nummer nach dem Schema von vier Zahlenblöcken, die mit Punkten voneinander getrennt sind, angegeben. Das ist die IP-Adresse des Senders, die nur sehr schwer oder gar nicht gefälscht werden kann, in diesem Fall 66.238.52.25. Alle anderen Angaben können leicht manipuliert werden und haben daher keinen Wert.

Header einer Spam-Mail

```
Return-Path: <sexgirl6931@hotmail.com>
Delivered-To: <Ihre_Mailadresse@provider.at>
Received: (qmail 2530 invoked from network); 20 Sep 2002 15:32:04 -0000
Received: from unknown (HELO hotmail.com) ([66.238.52.25]) (envelope-sender <sexgirl6931@hotmail.com>) by anubis.provider.at
(qmail-ldap-1.03) with SMTP for <Ihre_Mailadresse@provider.at >; 20 Sep 2002 17:32:01 +0200
From: "Angelina Jolie" <sexgirl6931@hotmail.com>
To: Ihre_Mailadresse@provider.at
Date: Friday, September 20, 2002 8:33 AM
Subject: Re: !!!Shocking Angelina Jolie Movie Clip, Strange Sex Ritual, Caught on tape!!!
```

2. Die Whois-Abfrage

Mit der IP-Adresse kann man dann eine sogenannte *Whois-Abfrage* machen. Es gibt mehrere Möglichkeiten hierzu, am leichtesten geht es bei einem webbasierten Service, der ähnlich wie eine Suchmaschine arbeitet, z.B. Arin (http://www.arin.net/whois/). Das Resultat sieht dass in etwa so aus:

Manche Spezialprogramme fügen gefälschte Headerzeilen ein, so dass man mit Hausverstand vorgehen und sich nach oben durcharbeiten muss, bis man den verantwortlichen Provider gefunden hat. Wenig plausibel sind etwa Domains international bekannter Firmen oder Internetorganisationen.

3. Die Beschwerde

In diesem Fall schreibt man seine Beschwerde an hostmaster@concentric.net. Zusätzlich kann man eine Kopie der Mail an abuse@hotmail.com senden für den Fall, dass die Absenderadresse nicht gefälscht ist. Bei wiederholter Belästigung durch eine Domain kann man auch seinen eigenen Provider benachrichtigen, dieser sperrt die auffällige Domain dann vielleicht, und man erhält von dort keine Mails mehr. Im Allgemeinen ist die richtige Beschwerdeadresse nach dem Schema abuse@provider.com aufgebaut.

Man leitet die unveränderte Nachricht mit dem unveränderten Betreff mit Forward weiter. Die Beschwerde sollte auf Englisch verfasst sein und in etwa so aussehen:

Dear Sirs/Ladies, I have received this spam mail. It comes probably from one of your users. Please take the appropriate action.

Yours, …

Dann fügt man die vollen, unveränderten Header in die Beschwerdemail ein. Das ist sehr wichtig, da sonst die Beschwerde nicht behandelt werden kann! Die Mail sollte man grundsätzlich als Nur-Text-Nachricht senden. Man muss unbedingt höflich bleiben, weil der zuständige Administrator fast nie etwas mit der Belästigung zu tun hat. Er ist auf keinen Fall der Absender!

Ist in der Originalmail ein Link zu einer Webseite eingebaut, so sollte man sich auch beim Hosting-Provider der Webseite auf analoge Art beschweren, damit diese entfernt wird. Der Link muss unverändert mit angegeben werden!

Ein Klick auf *„Remove me“* oder ähnlich bzw. eine Beschwerde an den Absender der Mail wird mit ziemlicher Sicherheit nichts fruchten und ist, wie oben beschrieben wurde, meist kontraproduktiv. Es wäre allerdings möglich, dass sich jemand – unabsichtlich oder mit Vorsatz – in eine durchaus seriöse Mailingliste mit Ihrer Adresse eingetragen hat. Dann ist natürlich die Unsubscribe-Information zu befolgen bzw. der Listenadministrator zu benachrichtigen. Hier ist also viel Hausverstand und Erfahrung nötig!

Für viele Anwender ist die dargestellte Prozedur zu mühevoll, obwohl man hierdurch sein Spam-Aufkommen meinen Erfahrungen nach deutlich reduzieren kann. Man kann sich diese Vorgänge mit einem Antispamprogramm deutlich erleichtern.

```
Search results for: 66.238.52.25

OrgName:    XO Communications
OrgID:      XOXO
NetRange:   66.236.0.0 - 66.239.255.255
CIDR:       66.236.0.0/14
NetName:    XOX1-BLK-2
NetHandle:  NET-66-236-0-0-1
Parent:     NET-66-0-0-0-0
NetType:    Direct Allocation
NameServer: NAMESERVER1.CONCENTRIC.NET
NameServer: NAMESERVER2.CONCENTRIC.NET
NameServer: NAMESERVER3.CONCENTRIC.NET
NameServer: NAMESERVER.CONCENTRIC.NET
Comment:    ADDRESSES WITHIN THIS BLOCK ARE NON-PORTABLE
RegDate:    2002-02-20
Updated:    2002-07-09
TechHandle: DIA-ORG-ARIN
TechName:   DNS and IP ADMIN
TechPhone:  +1-408-817-2800
TechEmail:  hostmaster@concentric.net
# ARIN Whois database, last updated 2002-09-22 19:05
# Enter ? for additional hints on searching ARIN's Whois database.
```

Whois-Abfrage für 66.238.52.25

VI. AntiSpamWare 2.1

1. Beschreibung

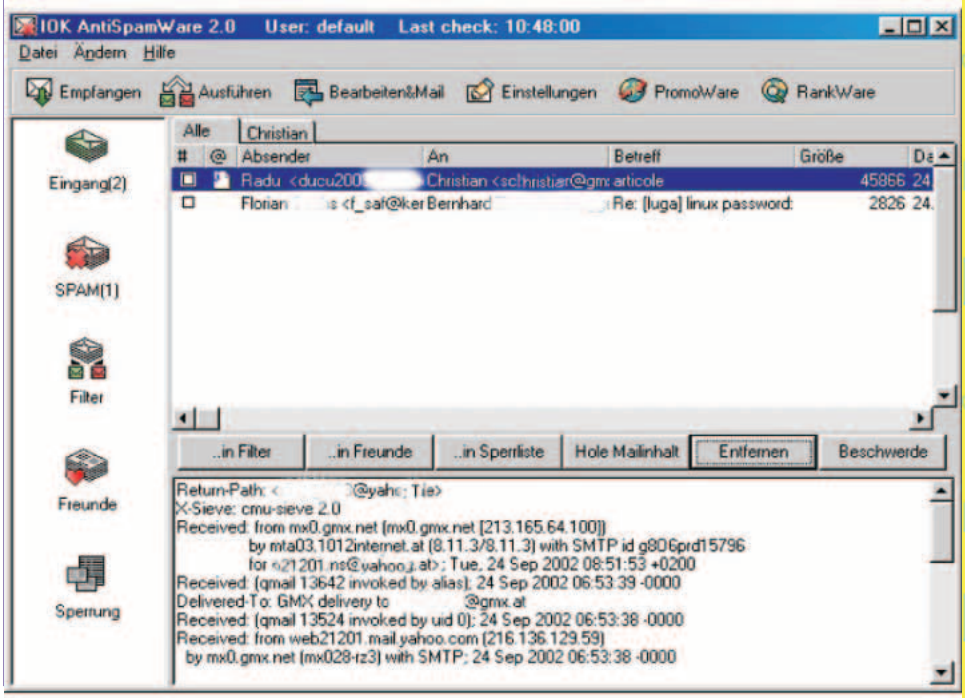
Dieses mir vorliegende, einfach zu bedienende, aber doch mächtige Programm wird von der Firma IOK[44] hergestellt und vertrieben. Es läuft auf allen Windows-Plattformen von 95 bis XP, prüft alle eingehenden Mails auf POP3, IMAP4-, AOL- und Hotmail-Konten, und man kann bei der Installation zwischen verschiedenen Sprachen (deutsch, englisch, französisch, spanisch) wählen. Die Lizenz kostet 29 Euro, eine 30-Tage-Testversion ist gratis.

Es besteht die Möglichkeit, Mails direkt am Server zu löschen, ohne sie auf die eigene Festplatte zu laden. Verschiedene mitgelieferte typische Filterregeln, die man als Benutzer noch ergänzen und verändern kann, verschieben schon viele unerwünschte Mails in den Spam-Ordner des Programms. Man kann effektiv vortäuschen, die eigene Mailadresse sei nicht existent und entsprechende Fehlermeldungen an die Spammer verschicken. Auch die in den Mailheadern vorkommenden IP-Adressen können sehr schnell und einfach zurückverfolgt werden; es findet die zuständigen Beschwerdeadressen der Provider heraus, an die dann automatisch eine Beschwerde gesendet werden kann. Es unterstützt mehrere Benutzerprofile und Mailkonten und vieles mehr.[45]

2. Grundlegende Bedienung

Die Installation verläuft Windows-typisch unkompliziert und selbsterklärend. Beim ersten Aufruf des Programms wird ein passwortgeschütztes Benutzerprofil festgelegt, welches bei jedem Start ausgewählt werden kann. Ist man alleiniger Benutzer des Computers, kann auch „Auto-Login“ festgelegt werden, sodass das Programm dann unmittelbar startet, ohne ein Passwort abzufragen. Die Konfi-

Screenshot AntiSpamWare



guration verläuft analog der eines E-Mail-Programms und sollte auch Unerfahrenen keine Hürden bereiten.

Bei bestehender Internet-Verbindung muss zuerst AntiSpamWare gestartet werden, nicht das Mailprogramm, da ja sonst die Mails heruntergeladen sind und nicht mehr auf dem Mailserver bearbeitet werden können.

Man drückt in AntiSpamWare auf „Empfangen“, und die Mails samt Header, aber ohne Body (den eigentlichen Text) und ohne Dateianhänge werden heruntergeladen. Angezeigt werden: HTML bzw. Dateianhang, Absender, An, Betreff, Größe, Datum, Organisation, und im unteren Fenster die Header. Den eigentlichen Nachrichtentext kann man sich im Zweifelsfall mit „Hole Mailinhalt“ anzeigen lassen. Spam-Mails werden meist gleich in den Ordner „Spam“ verschoben. Mails, die man empfangen möchte, lässt man unangetastet!

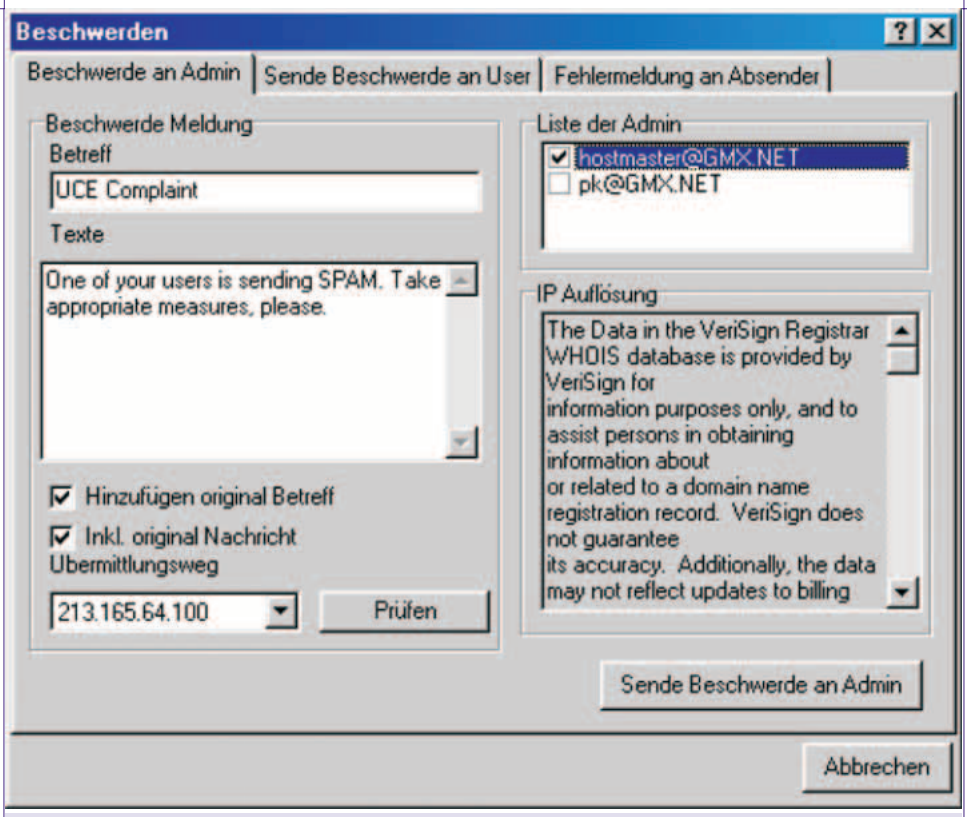
Nun kann man auf eine Mail klicken und „...in Filter“, „...in Freunde“, „...in Sperrliste“, „Entfernen“ oder „Beschwerde“ wählen. Durch Entfernen wird die Mail in den Spam-Ordner verschoben. Die Beschwerde-Prozedur wird im nächsten Kapitel behandelt. Wichtig ist, dass man dann alle im Spam-Ordner befindlichen Mails mit dem Klick auf „Ausführen“ direkt vom Mailserver löscht; dieser Klick darf nicht vergessen werden! Auch Mails mit zu großen Attachements können so entfernt werden, sodass sie nicht zeitaufwändig geladen werden müssen.

Hat man nur mehr erwünschte Mails im Eingang und hat alle unerwünschten Nachrichten entsprechend bearbeitet, schließt man das Programm und kann mit dem eigentlichen Mailprogramm alle Mails herunterladen.

3. Die Beschwerdefunktionen

Durch den Klick auf „Beschwerde“ bei einer markierten Spam-Mail hat man die Möglichkeit, sich beim zuständigen Admin des Internet-Providers des Spammers zu beschweren, an den Absender eine Beschwerde zu richten oder eine Fehlermeldung an den Absender vorzutäuschen. Folgendes Fenster öffnet sich hierzu, und man wählt den entsprechenden Tabellenreiter:

Bei der Beschwerde an den Admin muss man zuerst mit einem Klick auf „Prüfen“ die IP-Adresse des Absenders auflösen. In der Liste der Admin erscheint gleich automatisch die zuständige Adresse, an die gleich mit „Sende Beschwerde an Admin“ eine automatisch generierte Nachricht geschickt werden kann. Im Drop-Down-Menü links sind alle im Header der Spam-Mail enthaltenen IP-Adressen aufgelistet, so dass man erst prüfen muss, ob das Resultat plausibel ist, bevor man sich beschwert. Oft muss man mehrere IP-Adressen auf Resultate hin prüfen. Wie im Kapitel V.2 dargelegt, muss man eine Plausibilitätsprüfung durchführen und selbst entscheiden, bei wem man sich beschwert.



Beschwerdefenster AntiSpamWare

So eine automatisch generierte Reklamationsmail sieht in etwa wie unten dargestellt aus:

Analog dazu verläuft die Beschwerde an den User. Aus oben dargestellten Gründen ist diese aber in den meisten Fällen nicht zielführend, und man sollte diese Möglichkeit genau prüfen, bevor man davon Gebrauch macht. Dieser erhält in etwa folgende Nachricht: (siehe Darstellung auf der nächsten Seite)

Der Spammer kann so mit gewisser Wahrscheinlichkeit getäuscht werden und wird eventuell die betroffene Mailadresse aus der Verteilerdatei löschen.

Insgesamt kann bei Ausschöpfung der vielfältigen Möglichkeiten dieses Programms Spam wirksam eingedämmt werden.

VII. Schlussbemerkung

Spam ist nicht nur lästig, er wirkt sich immer hinderlicher auf die Kommunikation aus. Jeder Netzteilnehmer sollte, indem er aktiv etwas gegen diese Erscheinung tut, beitragen, dass das Internet das interessanteste Kommunikationsmedium bleibt.

Die Gesetzesgebung hat richtig reagiert und E-Mail-Werbung geregelt; eine weltweite Lösung ist anzustreben. Man könnte vorschreiben, dass Massenmails mit einem bestimmten, von Filtern leicht zu erkennenden Merkmal versehen werden müssen, so dass jeder entscheiden kann, ob er sie empfangen will oder nicht.

ISP sind gefordert, zum Schutz ihrer Kunden wirksam gegen Spam anzugehen, einfache und billige Möglichkeiten gibt

Automatisch versendete Beschwerde an den Provider des Spammers

```
One of your users is sending SPAM. Take appropriate measures, please.
-- Below this line is a copy of the message.
Return-Path: <b.49f.1dd310f7@offers.makemoneyfast.com>
X-Sieve: cmu-sieve 2.0
Received: from mx0.dmx.net (mx0.dmx.net [213.165.64.104])
     by mta04.1012internet.at (8.11.3/8.11.3) with SMTP id g8NKVcu25326
     for <Ihre_Mail@ihrprovider.at>; Mon, 23 Sep 2002 22:31:38 +0200
Received: (qmail 12046 invoked by alias); 23 Sep 2002 20:32:22 -0000
Delivered-To: DMX delivery to schneider@dmx.at
Received: (qmail 11843 invoked by uid 0); 23 Sep 2002 20:32:20 -0000
Received: from offers.makemoneyfast.com (66.7.132.48)
  by mx0.dmx.net (mx005-rz3) with SMTP; 23 Sep 2002 20:32:20 -0000
Date: Mon, 23 Sep 2002 13:32:12 -0700 (PDT)
Message-ID: <fSA3DxOdA=3d8f7a4c@offers.makemoneyfast.com>
To: schneider@dmx.at
From: "Makemoneyfast" <news@offers.makemoneyfast.com>
Subject: Makemoneyfast Newsletter for September 2002
X-Accept-Language: en
MIME-Version: 1.0
Content-Type: multipart/mixed;
 boundary="————fSA3DxOdA=00"
X-Resent-By: Forwarder <forwarder@dmx.at>
X-Resent-For: schneider@dmx.at
X-Resent-To: Ihre_Mail@ihrprovider.at
```

es, wie in Kapitel IV.2 beschrieben, genug. Je besser die Ausfilterung, umso zufriedener sind die zahlenden Kunden, die sonst Mailadresse und Provider wechseln.

Duldung durch den User ist der falsche Weg, etwa kommentarloses Löschen bzw. aufwändiger Wechsel der E-Mail-Adresse oder strikte Geheimhaltung.[46] Ich ziehe offene Kommunikation dem Verstecken in Anonymität vor und habe mit der Veröffentlichung meiner Mailadresse überwiegend gute Erfahrungen gemacht. – Ich hoffe, praktikable Wege aufgezeigt zu haben, wie man sich wehren kann. Fragen Sie Ihren Provider, wie er gegen Spam vorgeht, und wechseln Sie diesen bei unzureichender Beantwortung Ihrer Fragen!

Ein zukunftsweisender Schritt sind Antispamprogramme, von denen noch viel zu erwarten ist. In nächster Zeit werden sie zum Standard auf jedem Rechner werden.

```
You have sent the attached unsolicited e-mail to my e-mail account.
I do not wish to receive such messages in the future.
Please remove my name from your lists immediately.
-- Below this line is a copy of the message. […]
```

Wirkungsvoll ist es, eine Fehlermeldung an den Absender zu richten. Dadurch wird vorgetäuscht, dass die eigene E-Mail-Adresse nicht existiert:

```
The original message was received at 30.09.02 13:37:07
   —— The following addresses had permanent fatal errors ——
<axxxxxxx@mail.telering.at>
   —— Transcript of session follows ——
... while talking to mail.telering.at:
>> RCPT To:<axxxxxxx@mail.telering.at>
<< 550 <axxxxxxx@mail.telering.at>... User unknown
550 <axxxxxxx@mail.telering.at>... User unknown
-- Below this line is a copy of the message.
[…]
```

Beschwerde bzw. Fehlermeldung an den Absender des Spams, automatisch generiert von AntiSpamWare

Download Antispamware 1.1

http://webstadt.lion.cc/athen/510020/ASW.zip

Endnoten: Links und Inhalt entsprechen dem Stand von Ende September 2002. Da das Internet raschem Wandel unterworfen ist, kann die Richtigkeit der Angaben nicht gewährt werden. Aus diesem Grund wurden häufig wörtliche Zitate eingebaut.

1 Vgl. Stargate http://help.stargate.net/spam_security/spam/spam.html Siehe auch http://www.acronymfinder.com

2 Vgl. Wolf Hosbach: Spammer im Visier. So arbeiten Massenmailer. - In: PC-Magazin 10/2002, Poing (BRD), S. 142. http://www. pc-magazin.de

3 Vgl. Zentraler Informatikdienst der Universität Wien http://www.univie.ac.at/ZID/faq/was_tun_gegen_spam.html bzw. http://www.spam.com und http://www.spam.com/ci/ci_in.htm

4 Vgl. Hosbach S. 142. Der Text des Sketches ist unter http://www.ironworks.com/comedy/python/spam.htm veröffentlicht. Vgl. auch http://skater.priv.at/~andy/spam.html: „Spam ist eigentlich ein Dosenfleisch. Aber in einem Monty Python-Sketch wurde das Wort Spam sehr oft wiederholt. Und Spam-Mails sind normalerweise ähnliche Texte, die immer wieder versendet werden. Daher der Name Spam."

5 Netiquette: http://www.akis.at/service/mailnetiquette.html

6 Gerhard Laga http://www.laga.at; http://www.laga.at/Doks/spam-kurz.html. Gesetzestext bei http://www.wienerzeitung.at/aktuell/2001/antispam/austria.htm bzw. http://www.kronegger.at/recht/norm/tkg101.htm

7 Vgl. Quintessenz http://www.quintessenz.at; http://www.quintessenz.at/archiv/msg01829.html

8 Spamhaus http://www.spamhaus.org, Link: Europe Outlaws Spam.

9 Allgemeine Geschäftsbedingungen tele.ring http://www.telering.at

10 Bei Spamhaus http://www.spamhaus.org/aups.html. HostPro, Inc http://www.hostpro.net

11 ORF-Teletext vom 27. September 2002, Seite 108: 2006: 60 MRD E-MAILS TÄGLICH *Glaubt man einer aktuellen IDC-Studie, so wird sich die weltweite Anzahl der E-Mails bis 2006 verdoppeln. Zurzeit wird der tägliche weltweite E-Mail-Verkehr mit rund 30 Mrd beziffert.*

12 Heiko Mergard: Spam für alle! - In: PC Professionell 10/2002, München, S. 7. http://www.pcpro.de

13 Vgl. Alwin Schönberger: Weltmacht WWW. - In: Profil Nr. 29, 15. Juli 2002, S. 93 ff.

14 Vgl. Katie Hafner, Matthew Lyon: Arpa Kadabra oder Die Geschichte des Internet. - dpunkt: Heidelberg, ²2000. Tim Berners-Lee: Der Web-Report. - Econ: München, 1999.

15 Helmut Wimmer: Zur Konvergenz von Technologie und Denken. Hypertext und Internet. - Diplomarbeit, Wien, 1997. S. 117.

16 Spambeschwerden sind die häufigsten Beschwerden, die ISP bearbeiten müssen. Vgl. Spamhaus, Startseite.

17 Vgl. Roland Kissling: Webpromotion. - Ohne Ortsangabe, 1998. Teildatei Newsgroups.doc aus webpromotion.zip, heruntergeladen von der Seite http://wald.heim.at/schwarzwald/520257. Die Schlussfolgerung auch dort: „Sie sollten auf diese Form der Werbung besser gänzlich verzichten!!"

18 Vgl. ECO - Verband der deutschen Internetwirtschaft e.V. http://www.eco.de, Pressemitteilung eco-Verband gegen unerwünschte Massenmails (1999).

19 Hosbach, S. 142.

20 Stargate http://help.stargate.net/spam_security/spam/spam.html

21 zit. b. Cauce http://www.cauce.org, http://www.cauce.org/about/problem.shtml

22 Gefunden bei Spamhaus: http://www.iemailworld.com/ Hosted at 218.5.72.52 by chinanet.cn.net since Apr 9 2002 Siehe auch Astalavista http://astalavista.box.sk/ - Suche nach bulk mail.

23 Gefunden bei Spamhaus: http://www.millionsofemails.com/ Hosted at 202.98.123.88 by cninfo.net (China) since Apr 19 2002.

24 Gefunden bei Spamhaus: http://www.emailsgalore.com/ Hosted at 202.98.123.88 by cninfo.net since Jan 13 2002.

25 vgl. Hafner, Lyon. S. 226 ff.

26 vgl. Hafner, Lyon. S. 298. Schönberger S. 93. Wimmer S. 135; RFC 822.

27 vgl. Othmar Kyas: Internet professionell. Technische Grundlagen und praktische Nutzung. - Thomson: Bonn u.a., 1996. S. 137 f.

28 Das auch schon seit 1974 existiert! Vgl. Schönberger S. 93.

29 Versuchen Sie's mit diesen Angaben nicht, Ihre IP-Adresse wird sofort blockiert werden! Thanks to Gus & Lou http://www.pigeontoestudio.com

30 Vgl. Open Relay Database http://www.ordb.org. Dort auch Testmöglichkeit, ob ein Server auf Open Relay eingestellt ist.

31 z.B. habe ich am 29. 09. 2002 von http://mail.md eine Mail an mich geschrieben und meine IP-Adresse nirgends in den Headern gefunden!

32 Vgl. Wimmer, S. 122.

33 Laut Mitteilung auf meine Anfrage von GMX Abuse, http://www.gmx.net: Schutz vor Werbemails aus großen Domains, Schutz vor Mailbomben, individuelle Aufnahme von unerwünschten Mails bestimmter Absender oder ganzen Domains in eine Ausschlussliste usw.

34 Vgl. Dialerhilfe http://www.dialerhilfe.de, dubiose Dialer. Dialer sind Programme, die sich zu sehr stark erhöhten Kosten ins Internet einwählen, meist um Porno- oder Warez-Seiten anzuzeigen.

35 In absoluten Einzelfällen machen Provider mit den Spammern gemeinsame Sache. Es kam schon vor, dass Usern auf eine Beschwerde hin Viren geschickt wurden! Vgl. Computerbetrug http://www.computerbetrug.de Link E-Mail - Spam.

36 Laut Auskunft tele.ring Telekom Service GmbH Wien, Abteilung Öffentlichkeitsarbeit, http://www.telering.at, info@telering.co.at

37 Open Relay Database, vgl. Anm. 30. Diese Organisation führt eine Liste von bekannten Open-Relay-Servern. Link: FAQ - How do I use ORDB to protect my mailserver?

38 RBL http://mail-abuse.org/rbl/ Link: How to use bringt Informationen zu deren Gebrauch für Administratoren.

39 Vgl. Etel http://www.etel.at, http://www.ins.at/AntiSPAM.htm

40 Nähere Informationen bei http://www.iks-jena.de/mitarb/lutz/usenet/teergrube.html; Suchmaschinen: Teergrube (das Wort hat auch in den englischen Sprachraum Einzug gefunden).

41 Vgl. Hosbach, S. 142. Brightmail http://www.brightmail.com, Link: ISP.

42 Übersicht über die Headeranzeige bei gebräuchlichen Mailprogrammen auf http://mailbox.univie.ac.at/header.html

43 Quelle: Spamhaus. Die Header wurden vom Autor verändert.

44 IOK Internet Services GmbH & Co. KG, Konrad-Zuse-Weg 15, D-33415 Verl, http://www.antispamware.de

45 Vgl. Presseaussendungen IOK; Michael Rupp: Schluss mit Werbung. – In: PC-Magazin 10/2002. S. 181.

46 Wer sich verstecken will, braucht keinen Internetanschluss.