by Katja and Guido Socher
<katja/at/linuxfocus.org
guido/at/linuxfocus.org>

About the authors:

Katja ist die deutsche Editorin von LinuxFocus. Sie mag Tux, Film & Fotografie und das Meer. Ihre Homepage befindet sich hier.

Guido ist ein langjähriger Linuxfan und er mag Linux, weil es einem Wahlmöglichkeiten und Freiheiten gibt. Man kann Lösungen nach seinen eigenen Bedürfnissen wählen und entwickeln.

Kampf dem Spam

Abstract:

Spam in deiner Post? Spam E−mail wächst mit einer alarmierenden Geschwindigkeit und ist ein großes Problem für fast jeden.
In diesem Artikel werden wir erklären, was man gegen diese Plage tun kann.

Was ist Spam−Email?

Spam−mail hat viele Namen. Einige nennen sie UCE (Unsolicited commercial email, nicht erbetene Werbemail), andere nennen sie einfach Unwanted E−mail (unerwünschte Email), aber alle diese Namen sagen nicht wirklich, was es ist. Wenn du (noch) keine Spammail bekommst, dann schau dir diese Sammlung von Spam−mail (spam_samples.html) an. Es ist eine zufällige Auswahl von Spammail, die in ein paar Tagen gesammelt wurde. Lies die Mails durch und du wirst schnell verstehen, daß es nichts mit Kommerz oder Business zu tun hat. Diese Spammer sind Kriminelle. Kein(e) seriöse(r) Geschäftsmann/frau würde Millionen von Leuten verärgern und beleidigen, nur um ein paar "Idioten" zu finden, die ihnen ihre "Tricks" abkaufen.

Es ist ein häufiges Mißverständnis von Leuten, die das Internet nicht so oft benutzt haben, zu glauben, daß dieser Typ von Werbung mit Informationen verglichen werden kann, die sie von Zeit zu Zeit von ihrem örtlichen Supermarkt erhalten. Produkte, die über Spam−mails verkauft werden, sind oft illegal oder überhaupt keine Produkte. Sie sind Tricks, um an dein Geld zu kommen.

Wieviel?

Spammer bekommen deine Emailadresse von Webseiten, newsgroups oder Domaineinträgen (wenn du eine eigene Domain hast). Es gibt Leute, die Roboter benutzen, um Adressen zu extrahieren, sie auf CDs brennen und dann sehr billig an andere Spammer verkaufen. Wenn du heute deine Emailadresse in Klartext auf deine Homepage schreibst, so daß solche Programme sie extrahieren können, dann hast du in ein wenigen Monaten ein großes Problem und kannst es nicht stoppen. Das Problem wächst jeden Tag!

1998 lag der Prozentsatz von Spammail, die an LinuxFocus geschickt wurde, bei unter 10%. Im November 2002 sah die Statistik wie folgt aus:

Unser Server bekommt ca. 4075 Mails pro Woche. 3273 davon sind Spam!
=> 80% aller Mail ist Spam.

D.h. 80% der Kapazität des Mailservers und 80% der Netzwerkbandbreite ist für etwas, das niemand will.

Von diesen 3273 Spammails stammen ungefähr 40% aus Amerika (vor allem Kanada, US, Mexiko) und ca. 30% aus Asien (vor allem Korea, China, Taiwan).

Was macht man mit Spam?

Wenn du dir die Spam−mails anschaust, wird dir auffallen, daß beinahe alle die Möglichkeit bieten, sich aus der Liste entfernen zu lassen. Mach das nicht! Du hast es mit Kriminellen zu tun! Kein Spammer hat etwas davon, wenn er eine saubere remove Liste unterhält. Warum fügen sie dennoch diese Möglichkeit hinzu? Die Antwort ist einfach. Es macht einen viel besseren Eindruck auf den Leser und ist ein ausgezeichnetes statistisches Werkzeug. Die Spammer können sofort überprüfen, daß ihre Emails ankommen. In anderen Worten, du bestätigst den Erhalt der Email!

Es gibt auch ein einfaches technisches Problem mit der Idee einer remove list. LinuxFocus ist keine besonders große Seite, aber wir würden eine Person Vollzeit brauchen, um 3273 Spam mails pro Woche abzumelden und dann müßte diese Person eine Mail pro Minute schaffen. Jeder Spammer benutzt eine andere Methode, es wäre eine idiotische Aufgabe und kann nicht funktionieren. Remove lists sind Unsinn und helfen nur den Spammern.

Das einzig richtige, was du tun kannst, ist: lösche sie.

Software, um Spam zu handhaben

Es gibt viele verschiedene Optionen, um Spam auszufiltern und dies ist gut, weil es so für die Spammer schwieriger ist, sie zu umgehen. Es ist jedoch ein Wettrüsten. Die Werkzeuge, um Spam herauszufiltern werden weiter entwickelt, aber die Spammer verbessern ihre Methoden ebenfalls.

Es gibt zwei Arten von Filtern:

1. Überprüfungen direkt im MTA (Message Transfer Agent=Mail server). Hier kann man normalerweise die Email zurückweisen. D.h. du speicherst die Email noch nicht einmal. Du schickst eine Fehlermeldung zurück, sobald du während des Empfangs der Email erkennst, daß es sich um Spam handelt. Typische Werkzeuge dieser Art sind IP basierende Blocklisten und mail header checks. Falls du keinen eigenen Mailserver hast, muss das bei deinem Provider geschehen.

2. Filtern nach dem Empfang der Mail. In diesem Fall ist die Email erfolgreich geliefert worden und wird später aussortiert.

Wir diskutieren jetzt die verschiedenen Möglichkeiten im Detail, alle haben Vor− und Nachteile. Die beste Lösung, um alle Spam loszuwerden, ist, mehrere verschiedene Werkzeuge zu benutzen.

Zurückweisen von Email direkt beim MTA

Wenn du deine Mail direkt am Mailserver während des Empfangs zurückweist, dann kann der Spammer einen Fehlercode zurückbekommen und weiß, daß diese Adresse nicht funktioniert. Wenn er einer dieser "CD−Hersteller" ist, dann nimmt er die Adresse vielleicht heraus. Es kann Netzwerkbandbreite sparen, da du nicht die vollständige Nachricht erhältst. Du kannst den Fehlercode zurückschicken, sobald du herausfindest, daß dies Spam ist.

Um dies zu tun, brauchst du einen guten und flexiblen MTA. Leider sind die beiden am weitesten verbreiteten Server, Sendmail und der von Bill Gates nicht sehr gut für diese Aufgabe geeignet. Zwei sehr gute Alternativen sind Postfix und Exim. Wenn du deinen Server nicht ändern kannst, dann kannst du einen smtp proxy wie messagewall vor den Server (smtp = Simple Mail Transfer Protocol, das Internet mail protocol) setzen.

Wir diskutieren jetzt einige übliche Filtertechniken und erklären, wie sie arbeiten. Wir werden nicht beschreiben, wie man sie genau für jeden MTA konfiguriert. Es würde den Artikel zu lang machen. Stattdessen empfehlen wir, die Dokumentation, die mit dem MTA, den du installier hast dabei ist, zu lesen. Postfix und Exim sind gut dokumentiert.

- Echtzeit−Blocklisten:
  Dies sind auf DNS basierende Listen. Man vergleicht die IP Adresse des Mailservers, der an deinen Server Mail schicken will, gegen eine schwarze Liste von bekannten Spammern. Übliche Listen sind www.spamhaus.org oder ordb.org. Es gibt auch ein Werkzeug namens blq (siehe Referenzen), um per Hand solche Blocklisten zu durchsuchen und zu testen, ob eine bestimmte IP Adresse gelistet ist. Du solltest jedoch nicht zu viel erwarten und die Listen sorgfältig auswählen, da es auch welche gibt, die ganze IP−Bereiche einfach blocken, weil ein Spammer einmal eine dialup Verbindung von diesem ISP gewählt hat. Wir persönlich würden zumindest ordb.org benutzen, um Post von schlecht verwalteten Servern fernzuhalten.
  Die Erfahrung zeigt, daß diese Listen ca. 1−3% der Spammail blocken.

- 8 Bit Zeichen in der Subjektzeile:
  Ungefähr 30% aller Spam stammt heute aus China, Taiwan oder anderen asiatischen Ländern. Wenn du sicher bist, daß du Chinesisch nicht lesen kannst, dann kannst du Mail ablehnen, die viele 8 bit Zeichen (nicht ASCII) im Subjekt enthält. Einige MTAs haben eine eigene Konfigurationsoption dafür, aber du kannst auch reguläre Ausdrücke für den Header benutzen:

  /^Subject:.*[^ −~][^ −~][^ −~][^ −~]/

  Dies weist Emails zurück, die mehr als vier aufeinanderfolgende Zeichen in der Subjektzeile haben, die sich nicht im ASCII Bereich zwischen Leerzeichen und Tilde befinden. Wenn du dich mit regulären Ausdrücken nicht auskennst, lerne sie, du wirst sie brauchen (Siehe LinuxFocusartikel 53). Beide, exim and postfix, können mit Perls regulärer Ausdrucksunterstützung kompiliert werden (siehe www.pcre.org). Perl hat die mächtigsten regulären Ausdrücke.
  Diese Methode ist ganz gut und hält 20−30% der Spammail ab.

- Listen mit "From" Adressen von bekannten Spammern:
  Vergiß es. Dies funktionierte im Jahr 1997. Heutige Spammer benutzen gefälschte Adressen oder Adressen von unschuldigen Leuten.

- Zurückweisen von Nicht FQDN (Fully Qualified Domain Name) Sendern und unbekannten Senderdomains:
  Einige Spammer benutzen nicht existierende Adressen im "From". Es ist nicht möglich, die gesamte Adresse zu prüfen, aber man kann den hostname/domain Teil davon durch Suchen nach einem DNS Server überprüfen.
  Dies hält 10−15% der Spam ab und du willst diese Emails sowieso nicht, da du auf sie nicht antworten könntest, selbst wenn es kein Spam wäre.

- Die IP Adresse hat keinen PTR Eintrag im DNS:
  Dies überprüft, ob die IP Adresse, von der du die Mail bekommst, rückwärts in einen Domainnamen aufglöst werden kann. Dies ist eine sehr mächtige Option und hält eine Menge Mail ab. Wir würden sie nicht empfehlen! Dies testet nicht, ob der Systemadministrator des Mailservers gut ist, sondern ob er einen guten Backbone Provider hat. ISPs kaufen IP Adressen von ihren Backbone Providern und diese kaufen sie von größeren Backbone Providern. Alle involvierten Backbone Provider und ISPs müssen ihre DNS korrekt konfiguriert haben, damit die ganze Kette funktioniert. Wenn jemand dazwischen einen Fehler macht oder es nicht konfigurieren will, funktioniert es nicht. Es sagt nichts über den individuellen Mailserver am Ende der Kette.

- Verlange HELO Befehl:
  Wenn 2 MTAs (Mailserver) miteinander reden (via smtp), dann sagen sie zuerst, wer sie sind (z.B. mail.linuxfocus.org). Einige Spamsoftware macht das nicht. Dies hält 1−5% der Spam ab.

- Verlange HELO Befehl und weise unbekannte Server zurück:
  Du nimmst den Namen, den du im HELO Befehl bekommst und gehst zum DNS und überprüfst, ob dies ein korrekt registrierter Server ist. Dies ist sehr gut, da ein Spammer, der nur eine temporäre Dialup Verbindung benutzt, normlerweise keinen gültigen DNS Eintrag dafür konfiguriert.
  Dies blockt ca 70−80% aller Spam, weist aber auch legitime Mail zurück, die von Seiten mit mehreren Mailservern kommt, wo ein schlampiger Systemadministrator vergessen hat, die hostnames aller Server in den DNS zu schreiben.

Einige MTAs haben sogar noch mehr Optionen, aber die obigen sind die gängigen, die in einem guten MTA vorhanden sind. Der Vorteil all dieser Überprüfungen ist, daß sie nicht CPU intensiv sind. Du brauchst normalerweise deine Mailserverhardware nicht erneuern, wenn du diese Überprüfungen benutzen willst.

Filtern von schon empfangener Mail

Die folgenden Techniken werden normalerweise auf die vollständige Mail angewandt und der Mailserver, der die Mail schickt, bemerkt nicht, daß die Email nicht geliefert wurde. Dies bedeutet auch, daß ein legitimer Sender keinen Mißerfolgsbericht erhält. Die Nachricht verschwindet einfach.
Dies ist allerdings nicht 100% richtig, da es von den Filtermöglichkeiten des Mailservers abhängt. Exim ist sehr flexibel und erlaubt es dir, eigene Filter für Nachrichten zu schreiben.

- SpamAssassin (http://spamassassin.org/):
  Dies ist ein Spamfilter, der in Perl geschrieben wurde. Er benutzt sorgfältig mit Hand geschriebene Regeln und weist bestimmte Punkte zu typischen Spamsätzen wie "strong buy", "you receive this mail because", "Viagra", "limited time offer".... Wenn diese Punkte einen bestimmten Level überschritten

haben, wird die Mail zu Spam erklärt. Das Problem mit diesem Filter ist, daß er sehr schwer ist in Bezug auf Speicher und CPU Leistung. Du wirst wahrscheinlich deine Mailserverhardware erneuern müssen, besonders, wenn der Server schon 2–3 Jahre alt ist. Wir würden nicht empfehlen, ihn direkt auf dem Mailserver zu benutzen. Spamassassin kommt mit einem spamd Programm (spamd=spam daemon + spamc=Client zum Verbinden zum Daemon), was die startup Zeit von spamassassin sowie den CPU Verbrauch reduziert, aber es ist immer noch eine ressourcenfressende Applikation.

Um die Mail zu filtern, mußt du eine .procmailrc Datei (und .forward) ähnlich zu dieser erzeugen:

```
# The condition line ensures that only messages smaller than 50 kB
# (50 * 1024 = 56000 bytes) are processed by SpamAssassin. Most spam
# isn't bigger than a few k and working with big messages can bring
# SpamAssassin to its knees. If you want to run SpamAssassin without
# the spamc/spamd programs then replace spamc by spamassassin.
:0fW:
* < 56000
| /usr/bin/spamc
# All mail tagged as spam (e.g. with a score higher than the set threshold)
# is moved to the file "spam-mail" (replace with /dev/null to discard all
# spam mail).
:0:
* ^X-Spam-Status: Yes
spam-mail
```

Die Installation ist einfach und spamassassin filtert über 90% aller Spam.

- procmail (http://www.procmail.org):
  Procmail ist kein eigener Spamfilter, aber du kannst es dazu benutzen, dir selbst einen zu schreiben. Procmail ist auch sehr leichtgewichtig, solange man die Anzahl von Regeln auf einem vernünftigen Maß hält (z.B. weniger als 10). Um es zu benutzen, erzeugst du eine .forward Datei in deinem home–directory und fügst dort die folgende Zeile hinzu:

  ```
  "| exec /usr/bin/procmail"
  ```

  Einige Leute empfehlen
  "|IFS=' ' && exec /usr/bin/procmail"
  zu benutzen, aber dies erzeugt neue Probleme mit einem extra erzeugten Prozess, der nicht mehr unter der Kontrolle des Mailservers läuft. Sichere Mailserver wie postfix oder exim haben keine Probleme mit der .forward Datei, wie sie oben gezeigt wurde.

  Procmail ist besonders nützlich in einer Umgebung, wo du normalerweise nur in einer geschlossenen Gruppe kommunizierst. Z.B. für Leute in einem Unternehmen, wo die meiste Email von Kollegen und einigen bekannten Freunden kommen sollte. Hier ist ein Beispiel für "mycompany.com":

  ```
  # .procmailrc file.
  # search on header for friends:
  :0 H:
  * ^From.*(joe|paul|dina)
  /var/spool/mail/guido

  # search on header for mails which are not coming from
  # inside mycompany.com and save them to maybespam
  :0 H:
  * !^From.*(@[^\@]*mycompany\.com)
  /home/guido/maybespam

  # explicit default rule
  ```

```
:0:
/var/spool/mail/guido
```

Dies macht es sehr viel einfacher, Spam zu löschen und du findest die häßliche Spam nicht zwischen deiner normalen Mail.

Procmail ist sehr flexibel und kann auch für andere Aufgaben benutzt werden. Hier ist ein total anderes Beispiel:
Procmail kommt mit einem "reply to sender" Programm namens formail. Dies kann z.B. genutzt werden, um eine Nachricht zurück an die Leute zu schicken. Eine große Plage sind diese Emails, die Worddokumente enthalten. Wenn du ein Linuxentwickler bist, der Email zum Austausch von Informationen über deine Projekte oder Linux im allgemeinen benutzt, dann bist du sicher nicht an Leuten interessiert, die Text in ein Worddokument schreiben und es an ihre Emails anhängen. Viren können auf diese Weise leicht übertragen werden. Sie infizieren Linux normalerweise nicht, aber es ist generell eine schlechte Idee, MS−Word zum Verschicken von Texten an andere Leute zu verwenden, da es verlangt, daß MS Word mit derselben Version auf der Empfängerseite vorhanden ist, um den Text zu lesen. Es gibt offene Formate wie RTF oder HTML, die keine Viren verbreiten, plattformunabhängig sind und kein solches Versionsproblem haben.

```
# Promail script to
# reject word documents. Reject the mail, but do not reply to
# error messages "From MAILER-DAEMON"
# If you use ":0 Bc" instead of ":0 B" then you will still get the mail
:0 H
* !^From.*DAEMON
{
  # The mime messages with word documents look like this in the body
  # of the message:
  #------=_NextPart_000_000C_01C291BE.83569AE0
  #Content-Type: application/msword;
  #        name="some file.doc"
  #Content-Transfer-Encoding: base64
  #Content-Disposition: attachment;
  #        filename="real file.doc"
  :0 B
  * ^Content-Type:.*msword
  | (formail -r ; cat /home/guido/reject-text-msword ) | $SENDMAIL -t
}

# explicit default rule
:0:
/var/spool/mail/guido
```

Die Textdatei /home/guido/reject−text−msword sollte einen Text enthalten, daß msword Dokumente Viren verbreiten können und den Sender bitten, das Dokument z.B. im RTF Format zu schicken.

Wie man procmail benutzt und was alle diese seltsamen Buchstaben in der Konfigurationsdatei bedeuten, ist gut in der "procmailrc" man page erklärt.

- bogofilter (http://www.tuxedo.org/~esr/bogofilter):
  Bogofilter ist ein Bayesianischer Spamfilter. Es ist vollständig in C geschrieben und ist sehr schnell (verglichen mit SpamAssassin). Ein Bayesianischer Filter ist ein statistischer Filter, den du zuerst trainieren mußt, zu lernen, was Spam ist und was kein Spam ist. Du brauchst ca. 100 Trainingseinheiten (sortiert nach Spam und Nicht−Spam) bis der Filter effizient bei neuen Nachrichten funktioniert.

  Bogofilter ist schnell, aber er funktioniert nicht vom ersten Tag an wie SpamAssassin. Nach einer

Weile ist er so wirkungsvoll wie SpamAssassin und filtert über 90% aller Spam.

- razor (http://razor.sf.net/):
  Dies ist ein verteiltes, auf Zusammenarbeit beruhendes Spamentdeckungssystem. Prüfsummen von bekannten Spamnachrichten werden in einer Datenbank gespeichert. Wenn du eine neue Mail bekommst, berechnest du die Prüfsumme und überprüfst sie mit den Prüfsummen in der zentralen Datenbank. Wenn die Prüfsumme übereinstimmt, kannst du die Mail als Spam löschen. razor funktioniert, weil bestimmte Emailaccounts über das Internet verbreitet wurden mit dem einzigen Zweck, sie in die Adressenlisten aller Spammer zu bekommen. Diese Accounts fangen nur Spam und keine normale Mail. Zusätzlich kann man natürlich Mails an razor schicken, um es als Spam zu markieren. Es besteht eine gute Chance, daß die Mails schon als Spam bekannt sind, bevor sie in deiner Mailbox ankommen. Das System filtert ca. 80% der Spam. razor hat eine Charakteristik, die keiner der anderen post processing und Filtertechniken besitzt: razor entdeckt fast keine falschen Positiven. D.h. die Anzahl von Mails, die nicht Spam sind, aber dennoch als Spam deklariert werden, ist mit razor sehr niedrig.

Es gibt noch viel mehr mögliche Lösungen, um gegen Spam zu kämpfen. Wir glauben, daß das obige die wichtigsten von ihnen abdeckt.

Die beste Lösung ist, Überprüfungen im MTA als eine erste Stufe zu benutzen und dann die verbleibende Spam in einer zweiten Stufe mit einem post−processing Filter zu filtern.

HTML mails

Eine besonders gefährliche Form von Email sind Spammails in HTML Format.

Die meisten Spammer benutzen die "Abmelde−Möglichkeit (unsubscribe possibility)", um zu sehen, wieviele ihrer Mails ankommen. HTML formatierte Mail bietet eine viel bessere Form an Feedback: Bilder. Du kannst dieses System mit den Besucherzählern, die man auf manchen Webseiten findet, vergleichen. Der Spammer kann genau sehen, wann und wieviele Mails gelesen werden. Wenn du die Spam aufmerksam studierst, wirst du sehen, daß in manchen Fällen der URL für enthaltene Bilder eine Sequenznummer enthält: Der Spammer kann genau sehen, wer zu welcher Zeit die Mail anschaut. Eine unglaubliche Sicherheitslücke.

Moderne Mailleseprogramme zeigen keine Bilder an, die irgenwo von einer URL heruntergeladen werden. Jedoch gibt es kaum einen modernen und sicheren HTML mail reader. Kmail und die neueste Version von mozilla mail bieten die Möglichkeit, Bilder von externen Sourcen abzuschalten. Die meisten anderen Programme generieren nette Statistiken für die Spammer.

Die Lösung? Benutze kein html−fähiges Emailprogrammm oder lade die Mail zuerst nur herunter und lies sie erst, wenn du nicht mehr mit dem Internet verbunden bist.

Wo kommt die Spam her?

Traue niemals der Senderadresse im "From" Feld einer Spammail. Dies sind entweder nicht existierende Benutzer oder unschuldige Leute. Es ist sehr selten, daß dies die Mailadresse des Spammers ist. Wenn du wissen willst, wo die Mail herkommt, mußt du den vollständigen Header anschauen:

```
...

Received: from msn.com (dsl-200-67-219-28.prodigy.net.mx [200.67.219.28])
        by mailserver.of.your.isp (8.12.1) with SMTP id gB2BYuYs006793;
        Mon, 2 Dec 2002 12:35:06 +0100 (MET)
Received: from unknown (HELO rly-xl05.dohuya.com) (120.210.149.87)
```

```
by symail.kustanai.co.kr with QMQP; Mon, 02 Dec 2002 04:34:43
```

Hier schickt ein unbekannter Host mit der IP Adresse 120.210.149.87, der vorgibt rly−xl05.dohuya.com zu sein, die Mail zu symail.kustanai.co.kr. symail.kustanai.co.kr schickt diese Nachricht weiter. Der Spammer versteckt sich irgendwo hinter 120.210.149.87, was wahrscheinlich nur eine dynamische dialup IP Adresse ist.

In anderen Worten, die Polizei könnte diese Person finden, wenn sie zum Eigentümer von kustanai.co.kr gehen würde und nach Serverlogs und einem Ausdruck von Verbindungen der örtlichen Telefongesellschaft fragen würde. Du selbst hast kaum eine Chance herauszufinden, wer es war.

Es könnte auch sein, daß der erste Teil gefälscht ist und der Spammer tatsächlich hinter dsl−200−67−219−28.prodigy.net.mx steckt. Dies ist sehr wahrscheinlich, da es keinen guten Grund gibt, warum symail.kustanai.co.kr die Mail zu msn.com über die dsl dialup Verbindung (dsl−200−67−219−28.prodigy.net.mx) schicken sollte. Der mailserver.of.your.isp (symbolischer Name) ist der Server deines ISPs und nur der Teil von dieser "Received:" Zeile ist verläßlich.

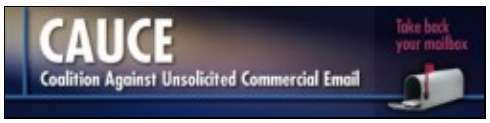
Es ist möglich, den Spammer zu finden, aber du brauchst internationale Intelligenz und Polizei, um zu prodigy.net.mx zu gehen.

Schlußbemerkung

Wenn Spam weiter mit der jetzigen Rate steigt, dann wird das Internet bald sehr viel mehr Spam als wirkliche Email transportieren. Spam wird auf Kosten der Empfänger transportiert. Mehr Bandbreite ist nötig und oft müssen Mailsysteme upgegradet werden, um die Spam zu handhaben.
Die Gesetze in vielen Ländern tun wenig, um die Bürger vor kriminellen Spammern zu schützen. Tatsächlich gibt es in vielen Ländern Gesetze, die nur ehrliche Leute einschränken (digital rights management etc. ...) und den Kriminellen helfen (z.B. um schöne Statistiken über die Spam zu bekommen).

Schließ dich der Koalition gegen UCE an!

http://www.euro.cauce.org/en/



http://www.cauce.org/

Internet Service Provider sollten ihre Mailsysteme überprüfen. Kein unautorisierter Zugriff zu Mailservern sollte gestattet werden und die Menge an Mails, die ein einzelner Benutzer pro Sekunde senden kann, sollte limitiert werden.

Referenzen

- http://spamassassin.org/: spamassassin Homepage
- http://www.procmail.org/: procmail Homepage
- http://www.spambouncer.org/: spambouncer: ein auf procmail basierender Spamfilter
- http://www.postfix.org/: Homepage des postfix MTA
- http://www.exim.org/: Homepage des exim MTA
- http://messagewall.org/: Homepage des messagewall smtp proxy
- http://www.unicom.com/sw/blq/: das blq perl Skript, um nach DNS basierten Blocklisten zu durchsuchen

- http://www.ordb.org/: DNS basierende offene relay Blockliste
- http://www.spamhaus.org: DNS basierte Blockliste
- http://www.samspade.org/: Where does the spam come from?
- http://www.dnsstuff.com/: verschiedene Blocklisten und auf DNS basierende Werkzeuge
- http://www.geektools.com/cgi−bin/proxy.cgi: geektools Whois proxy
- http://www.tuxedo.org/~esr/bogofilter/: bogofilter mail filter
- http://razor.sf.net/: razor
- http://pyzor.sourceforge.net: razor implementiert in python
- http://lwn.net/Articles/9460/: Linux weekly news Artikel, der bogofilter und spamassassin miteinander vergleicht.

Translation information:
en −−> −− : Katja and Guido Socher <katja/at/linuxfocus.org guido/at/linuxfocus.org>
en −−> de: Katja Socher <katja(at)linuxfocus.org>

2005−01−11, generated by lfparser_pdf version 2.51