

## **Spammer werden immer dreister und der Kampf immer schwerer!**

Ein Artikel von M.Rogge ©September 2003

Es ist ein belastendes Problem für das gesamte Internet, für jeden einzelnen Internetuser und für die Internetprovider: SPAM.

Die Massen an E-Mails mit Werbung für dubiose Geschäftsideen, Viagra und zweifelhafte Haarwuchsmittel nehmen permanent zu.

Bisherige Anti-Spam Betreiber gehen langsam aber sicher in die Knie und geben den Kampf gegen Spam auf.

Man kann derzeit nur schwer abschätzen welcher Schaden unmittelbar durch SPAM entsteht, wenn täglich Hunderte, Tausende ja sogar Millionen E-Mails in Form von Spam mit unerwünschter Werbung ins Haus kommen.

Leider ist es oft nicht ausreichend genug, dass man seinen lokalen E-Mail Client absichert und/oder durch ein E-Mail Filtering den Postverkehr an der Firewall abfängt, denn der Traffic ist weiterhin sehr hoch und lässt sich kaum beziffern.

Durch die neuartige Spamwelle ist es nun möglich, öffentlich bekannte Domainnamen als Absender einzutragen und somit für eine Beschwerdewelle zu sorgen die bei den angeblichen Versendern eintritt. Geschieht dies über einen realen Internetprovider, so kommen natürlich auch die E-Mail Meldungen zurück, ob eine E-Mail nicht zustellbar war und/oder bei eingeschalteter Benachrichtigungsoption auch noch die Empfangsbestätigung.

Die verzeichneten Absender sind aber nicht die Urheber der Spammails, sondern sind ebenso einem Betrug aufgelaufen wie der Empfänger, der diese Werbemail in Form von Spam nicht haben möchte.

Bei einem Internetprovider aus der Region Oberfranken laufen täglich mindesten 40-50 E-Mails als Spam je E-Mail Account auf.

Nach Angaben des Providers bestehen derzeit aktuell 800 E-Mail Accounts, die dann ein Gesamt-Spam-Aufkommen von ca. 32.000 E-Mails aufweisen!

Brain-Pro Security untersuchte in einer Umfrage bei Unternehmen, wie hoch das Aufkommen an täglichen Spam E-Mails ist um einmal mehr als deutlich aufzuzeigen wie enorm die Verbreitung ist.

In dieser Umfragen wurden ca. 60 Unternehmen und Behörden angeschrieben und konkret um Auskunft über die Anzahl der eintreffenden Spam E-Mails zu geben.

Die Zahlen waren schon verblüffend, denn in allen Unternehmen wurden täglich je E-Mail Account ca. 40-50 Spam E-Mails gezählt.

Einige Unternehmen nannten hierzu entsprechende Account-Anzahlen, die eine ungefähre Berechnung zulassen:

So laufen in einem Unternehmen mit ca. 8 E-Mail Accounts nach eigenen Angaben ca. 240 Spam E-Mails auf, die mit satten 4-50 kb jeweils auf dem Server geschrieben werden.

Bei einigen Unternehmen wurden täglich auf einem Account ca. 100 Spam E-Mails gezählt die meistens noch per Hand aus dem Posteingang entfernt werden.

Dies bedeutet hier zunächst einen Mehraufwand an Arbeit und nicht zu vernachlässigen der Mehraufwand an Traffic durch den E-Mail Server, über den die E-Mails abgerufen werden.

Rechnet man also bei ca. 60 Unternehmen einmal die Belastung hoch, dann kann man von einem schadhaften Aufkommen von ca. 19.000 E-Mails durch Spam sprechen das jedoch nur auf der Basis von ca. 10 E-Mail Accounts besteht.

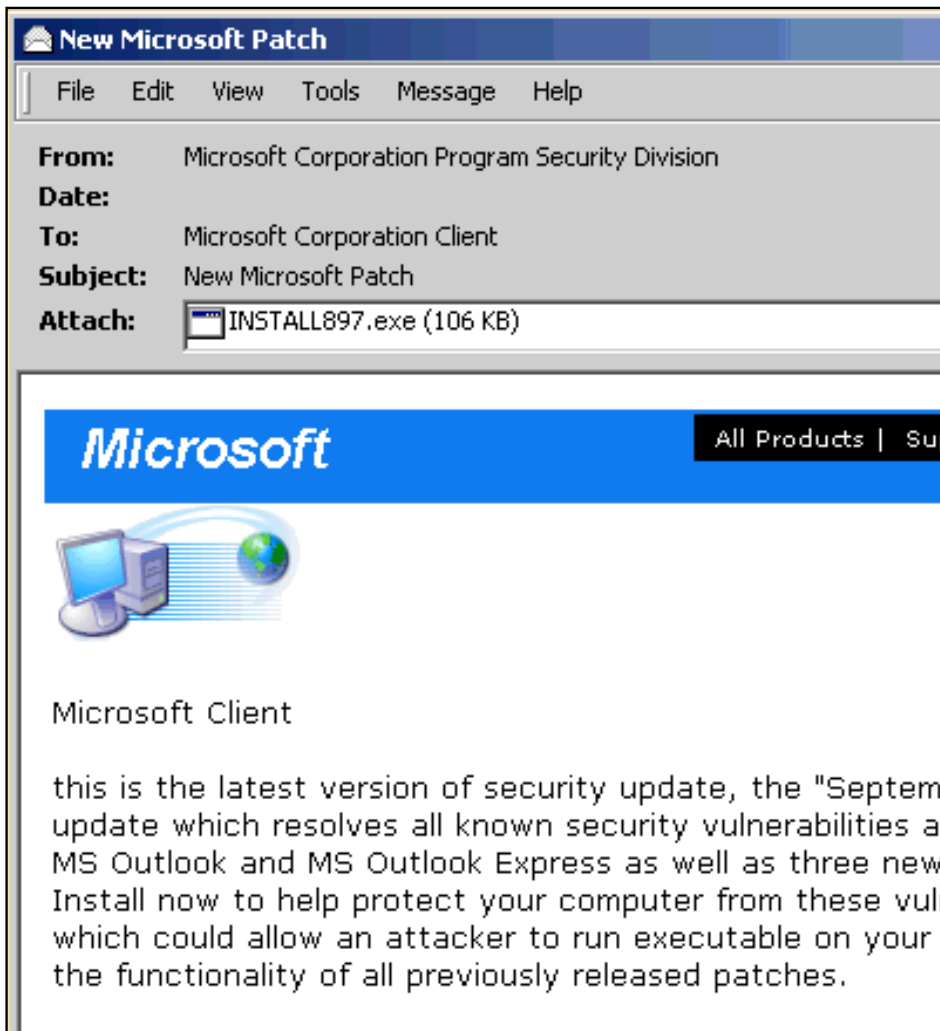
Rechnen Sie selbst hoch, wie sich das E-Mail Aufkommen nach oben korrigieren lässt.

Bei einem Unternehmen mit ca. 50 E-Mail Accounts kann man von ca. 2000 Spam E-Mails je Tag sprechen und einem erhöhtem Traffic von ca. 50 MB.

In vielen der betroffenen Fälle von Spam kommen weitere Probleme hinzu, die ernst genommen werden müssen: Computerwürmer verbreiten sich auf diese Weise!

Der recht aktuelle Computerwurm W32.Swen verbreitet sich per E-Mail und versendet als Anhang einen angeblichen Patch für Microsoft mit ca. 106kb.

Dieser Wurm gibt vor ein Update von Microsoft zu sein und installiert nach der Ausführung ein scheinbar sichtbares Update.



Einige der befragten Unternehmen gaben zusätzlich an, neben den "üblichen" Spam E-Mails auch sehr viele E-Mails mit dem angeblichen Microsoft-Updates zu erhalten.

Somit wird hier der Traffic eines jeden Internet Providers zusätzlich in die Höhe getrieben und weitere Kosten entstehen.

Mehr Informationen zu dem Wurm W32.Swen erhalten Sie auf deutsch hier:

<http://securityresponse1.symantec.com/sarc/sarc-intl.nsf/html/de-w32.swen.a@mm.html>.

Bei einem der größten Internet Provider AOL spricht man derzeit von täglich ca. 2,3 Milliarden abgeblockten Spam E-Mails und die Zahlen sind weiter steigend.

Der weltweite Schaden geht derzeit geschätzt weit in die Millionen und ein Ende dieser Internetplage ist nicht abzusehen.

Spam den Kampf ansagen!

In einem Bericht vor einigen Wochen habe ich bereits das Thema Spam aufgegriffen und auch aufgezeigt, welche Möglichkeiten es derzeit gibt, sich wirkungsvoll dagegen zur Wehr zu setzen. (<http://www.brain-pro.de/antispam.htm>)

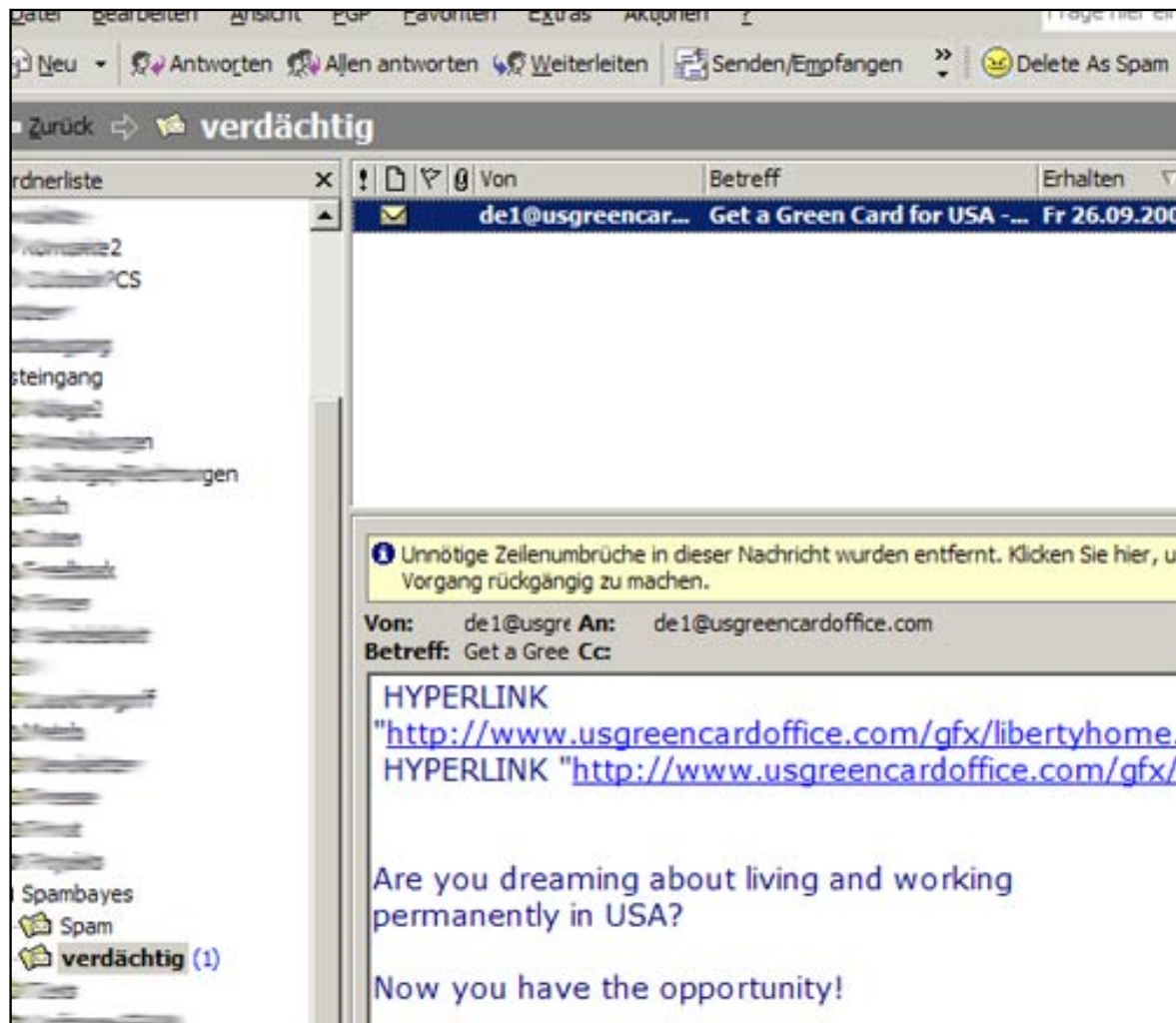
Wichtig ist hierbei auf ein System zu setzen, dass Spam auch wirkungsvoll bereits automatisch bekämpfen kann und durchaus lernfähig ist.

Eines dieser Systeme ist das kostenlose Programm Spam Bayes, dass auf ein Verfahren von Bayes beruht, wonach eine Klassifikation von Texten für eine bedingte Wahrscheinlichkeit der Bayes Formel beruht.

(<http://spambayes.sourceforge.net/>)

In kurzen Schritten habe ich hier einmal aufgeführt, wie schnell mit Spam Bayes gearbeitet werden kann und wie leicht das Programm lernt, Spam zu klassifizieren und entsprechend automatisch zu filtern.

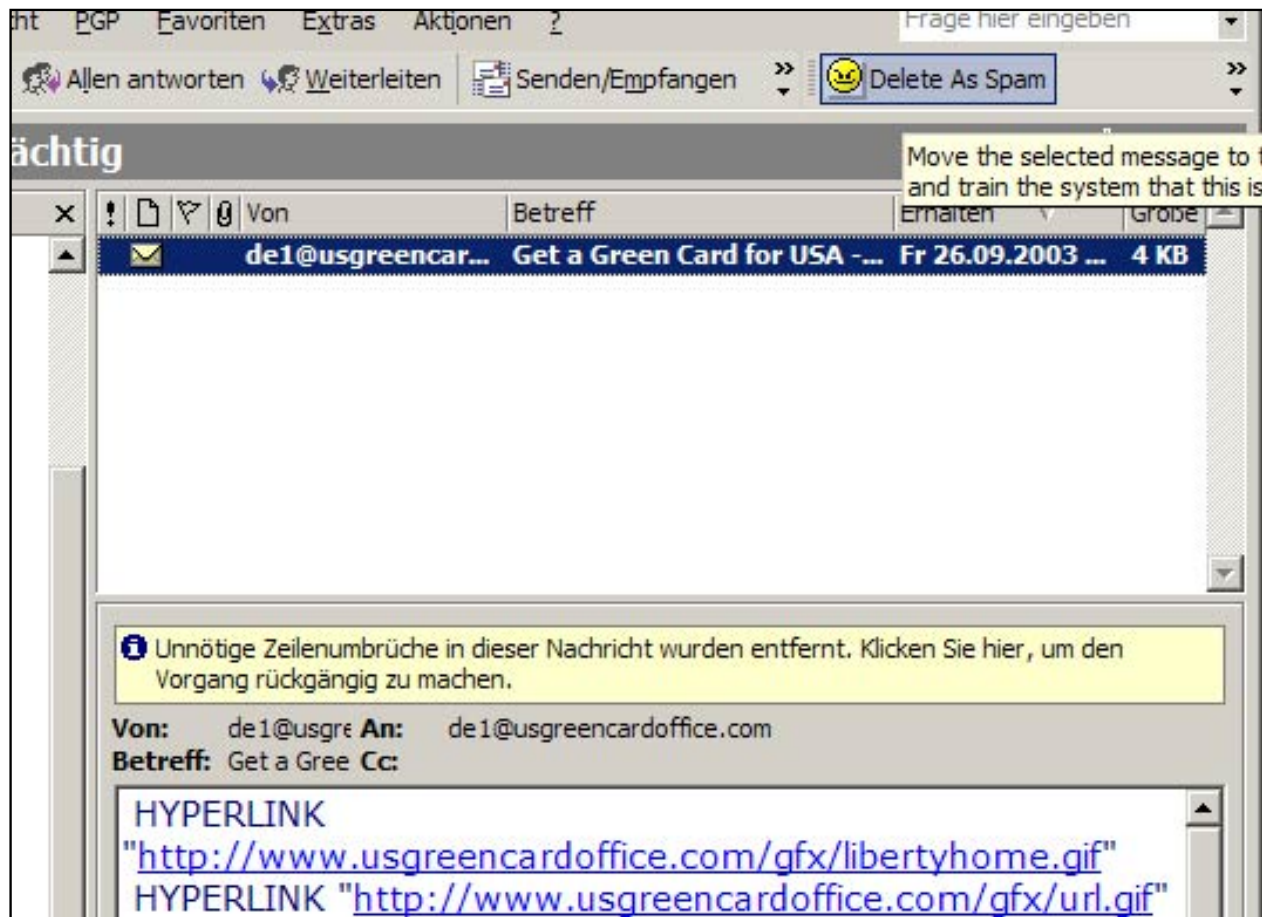
:: SPAM - ein Problem hat das Internet im Griff ::



Eine SPAM E-Mail trifft im OutlookXP ein und wird nach der Konfiguration gleich in den angelegten Ordner "verdächtig" verschoben.

Zusätzlich sehr gut zu erkennen, dass es sich hierbei normalerweise um eine HTML formatierte E-Mail handelt, die jedoch durch das zusätzliche Tool NoHTML als Text E-Mail angezeigt wird.

Sie finden am Ende des Artikels einen Hinweis auf NoHTML.



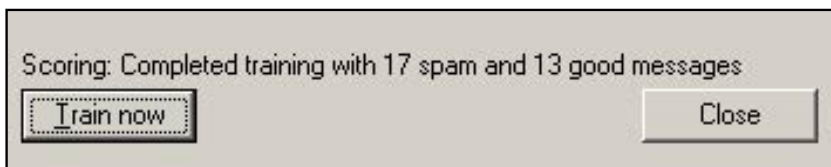
Das Programm kann in der Bedienungsleiste gleich die E-Mail als Spam löschen.



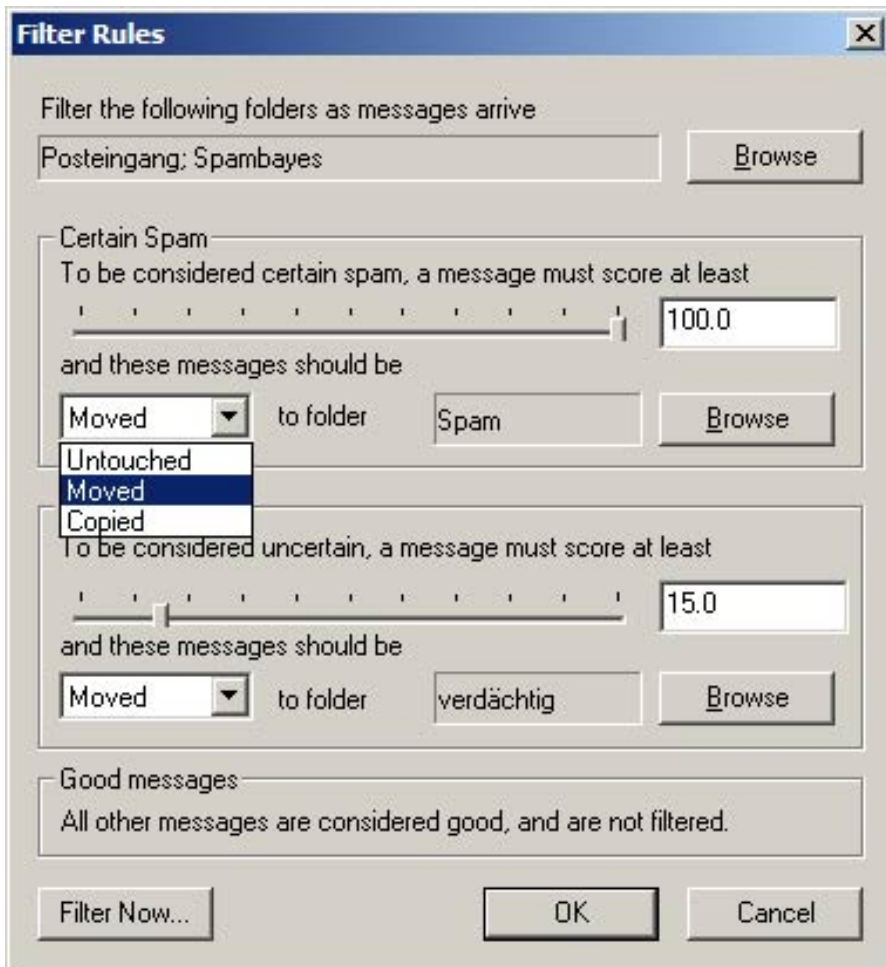
Die E-Mail verschiebt sich automatisch von "verdächtig" in den Ordner "Spam" der ebenfalls angelegt werden muss.



Sind einige Spam E-Mails einmal eingetroffen, so kann man in der Konfiguration den Trainingsmodus einstellen und Spam-Bayes erkennt alle E-Mails aus dem Posteingang und Ordner Spam und merkt sich den Stand.



Training abgeschlossen und Spam-Bayes hat die Spam E-Mails klassifiziert.



Hier sehen Sie die Einstellungsoptionen von Spam-Bayes, durch die nach einigen Trainingsläufen Spam automatisch gefiltert wird.

Oftmals ist es jedoch auch so, dass man einen Spammer direkt verfolgen kann.

Beispielsweise versendet eine deutsche Firma eine Werbemail direkt per E-Mail und wirbt um ein Kaffeeprodukt.

Der Absender ist in so einem Fall eindeutig zu ermitteln und man hat die Möglichkeit hier dagegen vorzugehen.

In einem Fall war der Spammer sogar so dreist und hat alle Empfänger in die CC Liste eingetragen und so weiterhin zur unerwünschten Verbreitung von E-Mail Adressen beigetragen.

Eine entsprechende E-Mail kann dann als Antwort an den Spammer gesendet werden, in dem auf das Datenschutzgesetz (BDSG) hingewiesen wird.

Einen entsprechenden Vordruck habe ich Ihnen in Textform hinterlegt: [antispambrief.txt](#)

Welche Maßnahmen gegen Spam helfen können habe ich bereits im ersten Artikel beschrieben, daher gehe ich hier nur kurz noch einmal darauf ein.

Beispielsweise kann man seinen Besuchern auf der Internetseite kaum verweigern, Kontakt per E-Mail aufzunehmen.

Dieser Fakt wird bekanntlich auch von Spammern ausgenutzt und das Internet wird systematisch nach E-Mail Adressen durchsucht.

Homepagebesitzer können hier schon ein wenig vorbeugen, in dem man den Quellcode im HTML etwas ändert und die E-Mail Adresse codiert hinterlässt:

```
<a href="&#109;&#97;&#105;&#108;&#116;&#111;&#58;&#109;&#114;&#64;&#98;&#114;&#97;&#105;&#110;&#45;&#112;&#114;&#111;&#46;&#100;&#101;">E-Mail an Brain-Pro - Marko Rogge senden</a>
```

Wenn Sie nun diesen Code in einen HTML Editor eingeben und als HTML ausgeben können Sie sehen, dass die E-Mail dennoch durch Anklicken aktiviert werden kann aber nicht mehr im Quellcode vorhanden ist.

Eine Testdatei in dieser Form finden Sie hier: <http://www.brain-pro.de/mailtest.htm>

Weiterhin halte ich es für erachtenswert, dass man seine E-Mail Adresse nicht in jeden Newsletter einträgt und sparsam mit Gästebucheinträgen ist.

Ratsam ist es ebenfalls, zwei E-Mail Adressen zu betreiben und bereits hier ein Filtering durchzuführen. Eine E-Mail Adresse kann für Freunde und Geschäftspartner angelegt sein und sollte nirgends weiter publiziert werden.

Die zweite E-Mail Adresse kann verwendet werden für Newsletter, Gästebucheinträge oder vergleichbare Aktivitäten im Internet.

Auf vielen Internetseiten ist es sogar Pflicht, dass man seine E-Mail Adresse angeben muss um den Umfang einer Webseite nutzen zu können.

Hierbei sollten Betreiber von solchen Internetseiten darauf achten, dass User die Möglichkeit haben sollten, die E-Mail Adresse nach außen unsichtbar zu machen und diese nicht lesbar ist.

Eine Mitgliedschaft ist hierdurch nicht gefährdet und Newslettersysteme die seriös arbeiten sind ebenfalls nicht davon betroffen.

Weiterhin existieren sehr viele kostenlose Programme (z.B. SpamBayes) die mit Spam durchaus auf einem Client fertig werden können.

Wer sich eine Homepage zulegt, der kann bei seinem Provider anfragen, ob ein Serverseitiger Schutz vor Spam möglich ist und hierbei als Beispiel Spam Assassin zum Einsatz kommt.

Die Stuttgarter Agentur Fab.45 bietet derzeit aktuell recht günstig spamDetacher an, dass ebenso auf dem Grundprinzip von Bayes arbeitet, nach dem die Analyse benannt wurde.

Aus einer Pressemeldung: "Das selbstlernende Programm schleust alle eingehenden Daten durch ein ausgeklügeltes Filtersystem, welches unerwünschte Nachrichten mit hoher Wahrscheinlichkeit erkennt und automatisch aussortiert.

Das individuelle Verhalten der Systembenutzer, die ja beim Filtern ihrer Mails meist ganz persönliche Maßstäbe anlegen, fließt dabei in die Wertung mit ein."

#### **Weitere E-Mail Spam Programme und Tools:**

NoHTML: <http://ntbugtraq.ntadvice.com/download/Nohtml.zip> (NoHTML PlugIn um E-Mails in Klartext darzustellen)

SAProxy: <http://saproxy.bloomba.com/>

SPAMNet: <http://www.cloudmark.com/>

SPAMPal: <http://www.spampal.org/>

MailShield Desktop: <http://www.lyris.com/store/mailshield/desktop/download.html>

SPAM Assassin: <http://spamassassin.org/index.html>

K9-Spam Filter: <http://www.8ung.at/thebatinfo/spam/k9.htm>

Antispamware: <http://www.antispamware.de/>

SpamDetacher: <http://www.fab45.net>

Danke schön für das Lektorat, Kontrolle, Kritik und Anregungen an: Simon Moser, Mixer, Tibor Bauer und Ines Schwanke.

Beste Grüße, Marko Rogge // IT-Sicherheits Berater

Brain-Pro Security : [www.brain-pro.de](http://www.brain-pro.de)

02.10.2003

Dieser Artikel: <http://www.brain-pro.de/spam.htm> PDF: <http://www.brain-pro.de/pdf/spam.pdf>

Dieser Bericht ist in guter Absicht und mühsamer Arbeit erstellt worden, daher möchte ich Sie bitten keine Anleitung und/oder andere Texte frei zu kopieren.

Unter Angabe des Autors und der URL sowie eine Benachrichtigung per E-Mail ist eine weitere Veröffentlichung jederzeit möglich. Vielen Dank für Ihr Interesse, Ihr Marko Rogge