

Spam Mails Filtern

Wie Sie die Spamflut mit einem Filter in den Griff bekommen können

Über dieses Dokument

Dieser Workshop soll eine Hilfe für Nutzer sein, die ihren Posteingang wider übersichtlich halten wollen. Alles hier dargestellte basiert auf persönlichen Erfahrungen, keinesfalls kann und soll eine Garantie für Richtigkeit übernommen werden.

Dieses Dokument wurde verfasst von Jens Ferner,
(<http://www.datenschutzbeauftragter-online.de>). **Anregungen und Fragen per Email:** jens@familie-ferner.de. **Copyright © Jens Ferner, Weitergabe erlaubt & erwünscht, Nachdruck nur nach vorheriger Genehmigung.**

Aktuelles rund um den Datenschutz unter
<http://www.datenschutzbeauftragter-online.de>

Kapitel I. Einleitendes

Spam Emails sind leider ein tägliches Übel. Wer eine halbwegs bekannte Internetseite hat, kann über mehrere dutzend Emails am Tag klagen.

In Zeiten von DSL & Flatrates geht es weniger um die Internetanbindung, als vielmehr über die Übersichtlichkeit des Posteingangs, wenn man sich über Spam Mails beschwert. Wer einmal über sein Firmenpostfach täglich 40 oder 50 Spammails erhält, hat große Probleme die richtige Post vom Müll zu trennen. Das führt dazu, dass tatsächlich jede Email einzeln betrachtet werden und gefiltert werden muss. Das kostet wertvolle Arbeitszeit.

Dieses Tutorial wendet sich an die bereits Geschädigten. Wessen Email Adresse bereits erfasst wurde kann nur noch gut Filtern. In einem zweiten Teil möchte ich diverse Techniken vorstellen um das Erfassen von Email Adressen zu verhindern. Um das ganze verständlich zu halten, trenne ich die beiden Themen aber.

Eines dennoch vorab: Viele Spammer setzen so genannte Email Crawler ein. Von der Programmstruktur ähnlich eines Suchmaschinen Crawlers, durchsuchen diese Programme vollautomatisch das Internet. Gesucht (und gespeichert) werden allerdings nur Email Adressen die dann in einer Datenbank zum späteren zu-Müllen gespeichert werden. Insofern kann der Kampf gegen die Spammails also in 2 Teile gesplittet werden:

1. Verhindern dass Emails überhaupt erfasst werden
2. Wenn doch Spam kommt, diesen aussortieren

Teil 1 wendet sich eher an Webmaster. Es gilt Webseiten so zu konzipieren, dass Email Crawler keine Chance mehr haben. Wie

bereist gesagt: Darum geht es im 2. Teil des Tutorials. Hier befassen wir uns nur mit dem Thema des Filterns.

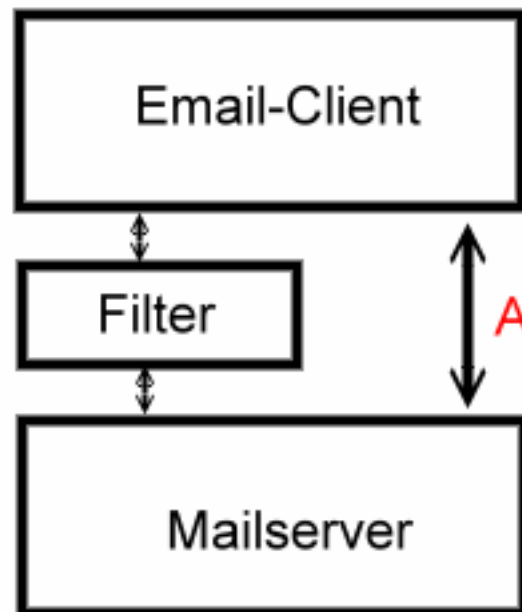
Im Allgemeinen können 2 Techniken unterschieden werden. Zum einen können Sie mit **Versender-Datenbanken** arbeiten. In solchen Datenbanken werden die Versender von Spammails gespeichert. Dabei wird von jedem Spammail – Versender die IP abgelegt. Wenn Sie nun eine Email erhalten, können Sie die IP des Absenders mit einer solchen Datenbank abgleichen und feststellen ob es sich um einen bekannten Spammer handelt.

Die andere Möglichkeit ist das Einsetzen eines **Algorithmus**. Aufgrund eines bestimmten Verfahrens wird bei jeder einzelnen Email geprüft, ob es sich um eine Spammail handeln könnte. Dabei wird nicht auf offizielle Listen, sondern einen Algorithmus zurückgegriffen, der aufgrund allgemeiner Merkmale eine Erkennung vornimmt.

Für beide Techniken gibt es diverse Softwarelösungen. Ich möchte hier im näheren 2 kostenlose und gut funktionierende Programme vorstellen. Außerdem gebe ich am Ende noch Links zu weiterer (auch kommerzieller) Software sowie ein kleines Fazit.

Ich habe mich hier nur auf Client-Seitige Lösungen festgelegt. Das bedeutet, ich stelle Software vor, die auf Ihrem Rechner zum Einsatz kommt wenn Sie die Post von Ihrem Mailserver abholen. Ich denke, dies ist der häufigste Fall. Daneben gibt es noch Server-Seitige Produkte (etwa SpamAssassin), die man auf seinem Webserver direkt installiert. Auf diese Lösungen gehe ich hier nicht ein!

Normalerweise haben Sie einen Emailclient, etwa Outlook®. Dieser greift direkt auf den Mailserver im Internet zu und holt Ihre Emails ab (A):



Wenn Sie nun eine Filtersoftware einsetzen, schaltet diese sich üblicherweise zwischen Email Client und Mailserver. Das bedeutet, Ihr Client greift ab sofort auf die Filtersoftware zu. Diese holt dann wiederum die Emails vom Mailserver, checkt diese und gibt sie weiter an den Email Client. Das bedeutet vor allem eins: Neu konfigurieren. Denn damit Ihr Email Client die Filtersoftware auch findet, muss diese richtig konfiguriert werden. Aber dabei hilft ja auch dieses Tutorial.

Ich setze dabei auf den TAG-Modus. Das bedeutet, mein Filterprogramm holt alle Emails ab und markiert nur die Spam Mails. Keinesfalls werden Spam Mails sofort gelöscht. Sicherlich hat das sofortige löschen einen Vorteil: Sie benötigen weniger Übertragungszeit da Spammails nicht mehr vom Webserver bis zu

Ihnen transportiert werden. Andererseits haben alle Programme eine gewisse Fehlerquote und ich möchte immer die Sicherheit haben, selber nachprüfen zu können, was als Spam gelöscht wird und was nicht.

Kapitel II. Filtern mit Methode 1 : Der Absender Check

Diese Methode bevorzuge ich. Das hier vorgestellte Programm setze ich seit ca. 4 Monaten ein und es arbeitet ausgezeichnet: Spampal. Sie können das Programm unter <http://www.spampal.de> kopieren. Es ist kostenlos und ohne Werbung. Dieses Programm prüft bei jeder einzelnen erhaltenen Email, von welcher IP diese gesendet wurde und markiert dabei bekannte Spam Versender mit einer frei definierbaren Zeichenkette. Wenn Ihnen jemand eine Spammal sendet, wird zum Beispiel die Zeichenkette **[**SPAM**]** in den Betreff der entsprechenden Email gesetzt. Sonst passiert nichts. Allerdings können Sie nun mit Ihrem Emailclient alle Mails bei denen diese Zeichenkette im Betreff vorkommt aussortieren und nach Wunsch direkt löschen oder in einen speziellen Ordner verschieben um dann später einmal drüber zu sehen. Weiter unten gebe ich einige kleine Tipps zum Umgang mit diesen Mails.

Ich möchte hier keine Erläuterungen zur Installation verschwenden. Kopieren Sie sich die Datei und führen Sie diese aus. Es gibt hierbei nichts zu beachten. Nach der Installation finden Sie in Ihrer Taskleiste einen kleinen Regenschirm – dieser signalisiert, dass Spampal installiert ist und läuft. Nun müssen Sie Ihren Email Client konfigurieren. Notieren Sie Ihre bisherigen Mailserver Einstellungen. Ich nutze hier beispielhafte Angaben um das Vorgehen zu verdeutlichen:

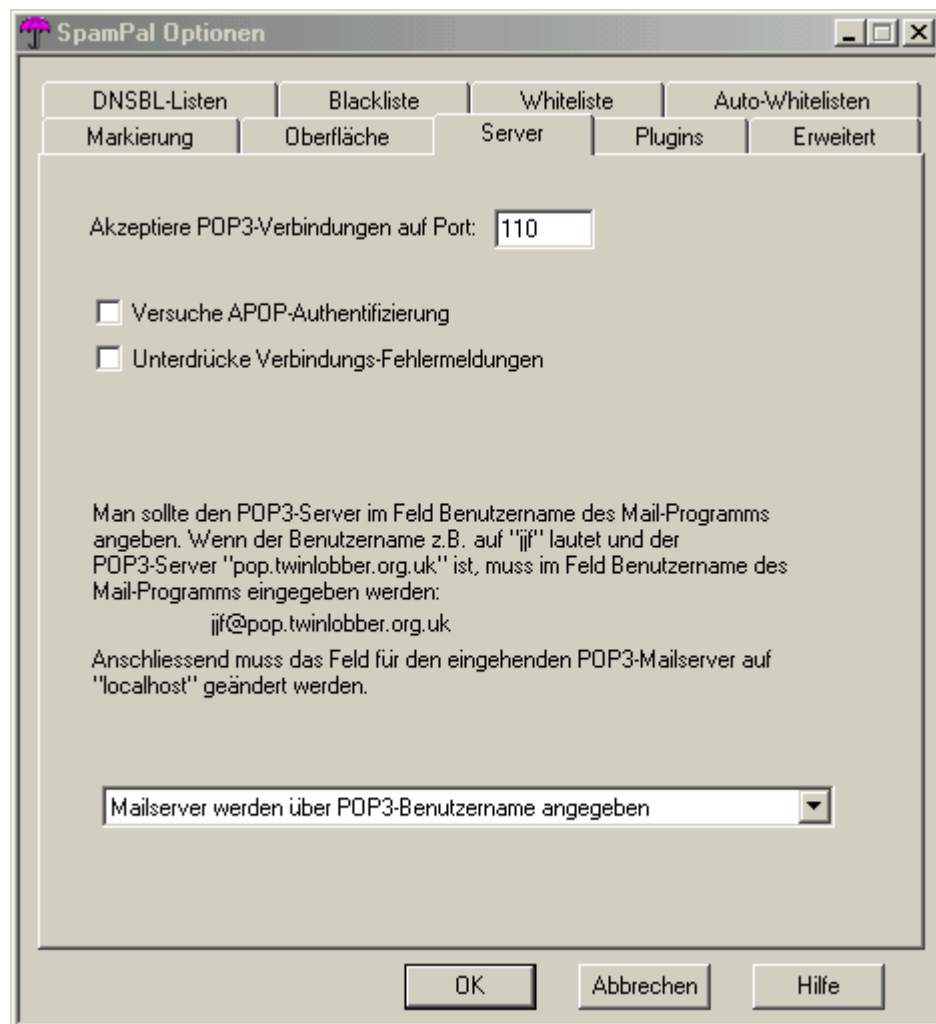
POP Server: pop.server.de

Benutzername: postfach

Passwort: passwort

Port:110

Diese Daten haben Sie bisher direkt in Ihrem Mailclient angegeben. Klicken Sie nun einmal kurz mit der rechten Maustaste auf den Regenschirm in Ihrem Tray-Menü und wählen Sie Optionen, im folgenden Fenster „Server“. Folgendes Bild wird sich öffnen:



Es sollte genau so aussehen – wenn nicht, ändern Sie es. Ändern Sie hier keine Werte, mit diesen Daten werden wir nun arbeiten. In

Ihrem Mailclient müssen Sie nun die bisherigen Werte angeben, damit Ihre Filtersoftware gefunden wird. Mit unseren obigen Beispieldaten müssen Sie folgende Werte angeben:

POP Server : localhost

Benutzername : postfach@pop.server.de

Passwort: passwort

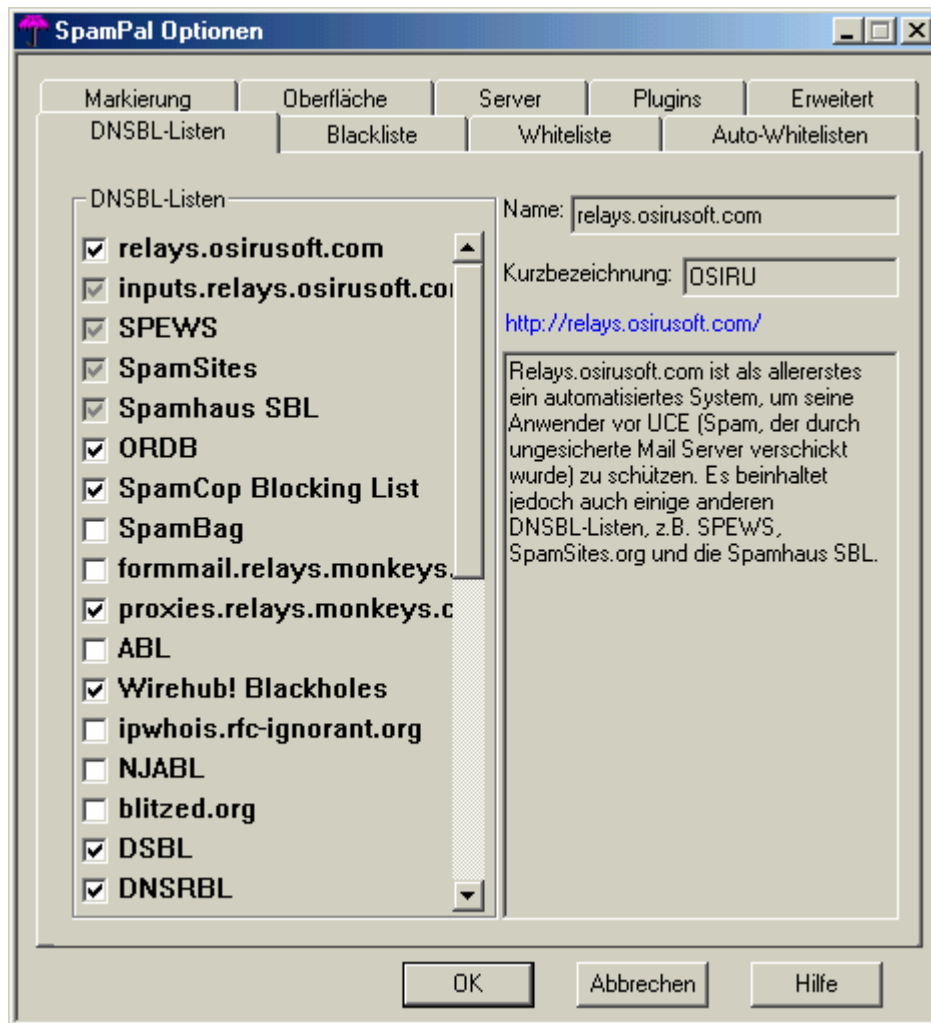
Port:110

Das ganze hat folgenden Sinn: „localhost“ ist Ihr eigener Rechner, hier wird nun das Filterprogramm angesprochen. Damit dieses auch weiß, wo sich ihr wirklicher Mailserver befindet, geben Sie den Mailserver über den Benutzernamen in Ihrem Mailclient an. Dazu müssen Sie als Benutzernamen immer

Benutzername@Mailserver

Verwenden und schon weiß SpamPal wo es die Mails erhält. Ansonsten bleibt alles beim alten. Sie können nun bereits Emails abholen. Wenn Sie dies tun, werden Sie bemerken, dass der Regenschirm sich bewegt. Damit wird angezeigt, dass Ihr Mailclient auf Spampal zugreift.

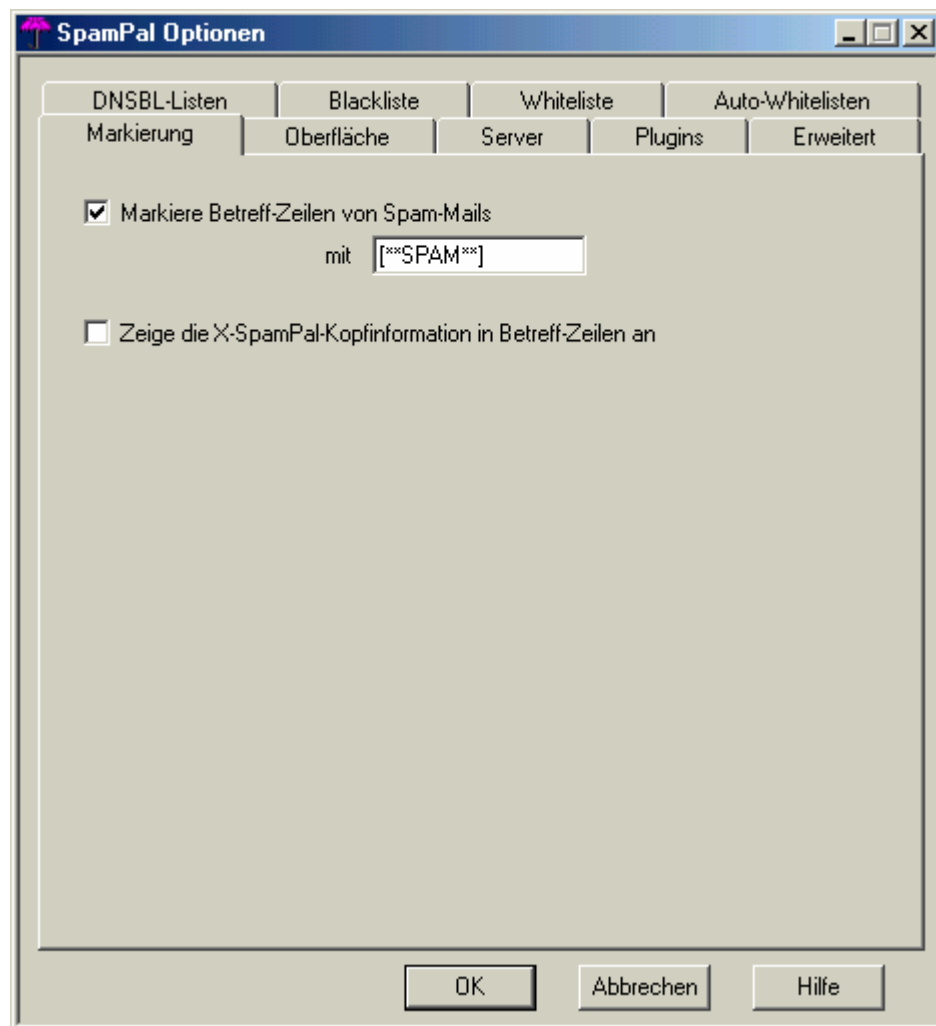
Nun kurz einige Erläuterungen zu den wichtigsten Optionen von Spampal. Wie bereits gezeigt. Müssen Sie mit der rechten Maustaste auf den Regenschirm klicken und „Optionen“ auswählen. Interessant ist hierbei das erste Fenster:



Hier wählen Sie aus, welche Datenbank-Anbieter Sie abfragen möchten. Zu jeder Datenbank erhalten Sie rechts einige Angaben mit Informationen, etwa zur Zuverlässigkeit des Anbieters. Beachten Sie auch, dass die Bearbeitungsdauer mit der Zahl der Datenbanken steigt, da jede Datenbank bei jeder Email einzeln angefragt wird.

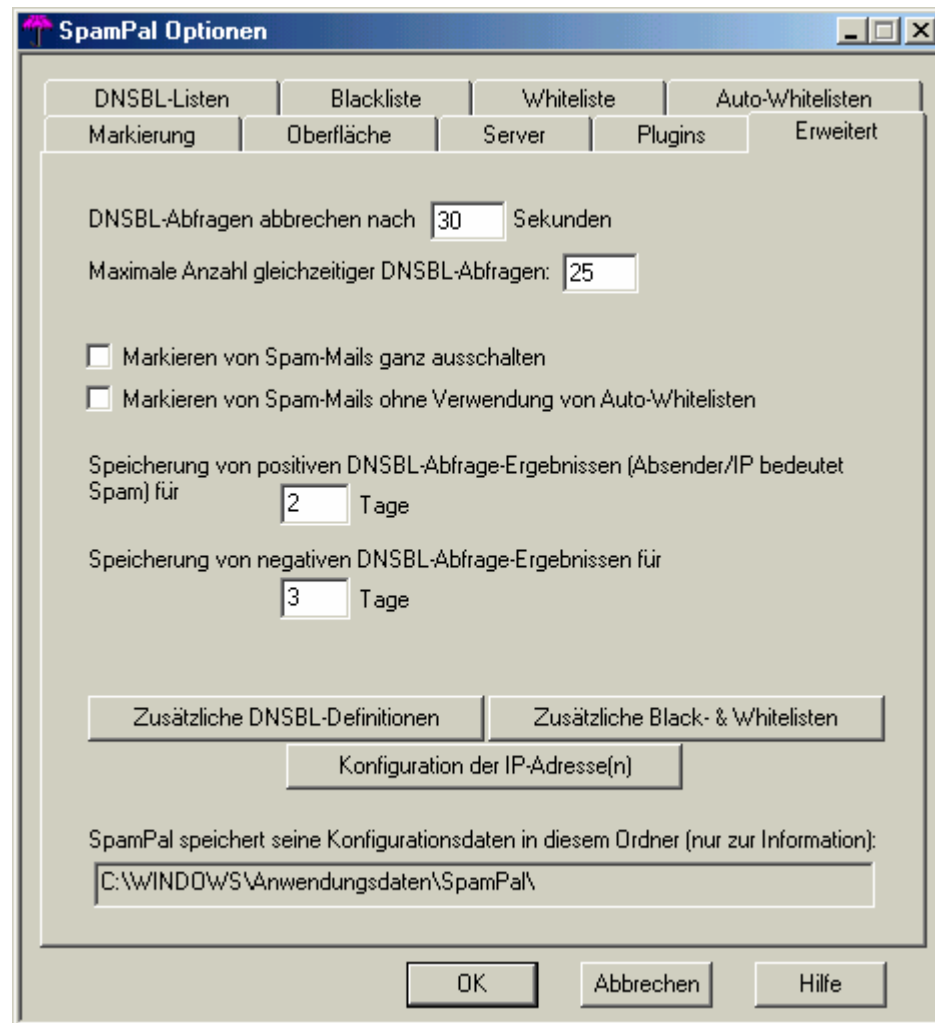
Unter „Whitelist“ und „Blacklist“ können Sie erwünschte oder unerwünschte Email Adressen eintragen. Etwa um Freunde nicht als Spam zu markieren oder von vornherein bestimmte Emailabsender zu sperren.

Im Bereich „Markierung“ geben Sie eine Zeichenkette an, die in den Betreff einer jeden Spammail eingebaut werden soll. Der Standard ist eigentlich ausreichend, aber vielleicht möchten Sie etwas noch eindeutigeres hinterlegen



Das darunter stehende Feld macht nur Sinn wenn Sie auch hier einen Filter definieren können. Ignorieren Sie es üblicherweise. Sie können in Ihrem Email Client einen Filter definieren. Geben Sie hier einfach an, dass die angegebene Zeichenkette „***SPAM***“ im Betreff enthalten sein muss und dass jede Email hiermit sofort in einen bestimmten Ordner verschoben wird.

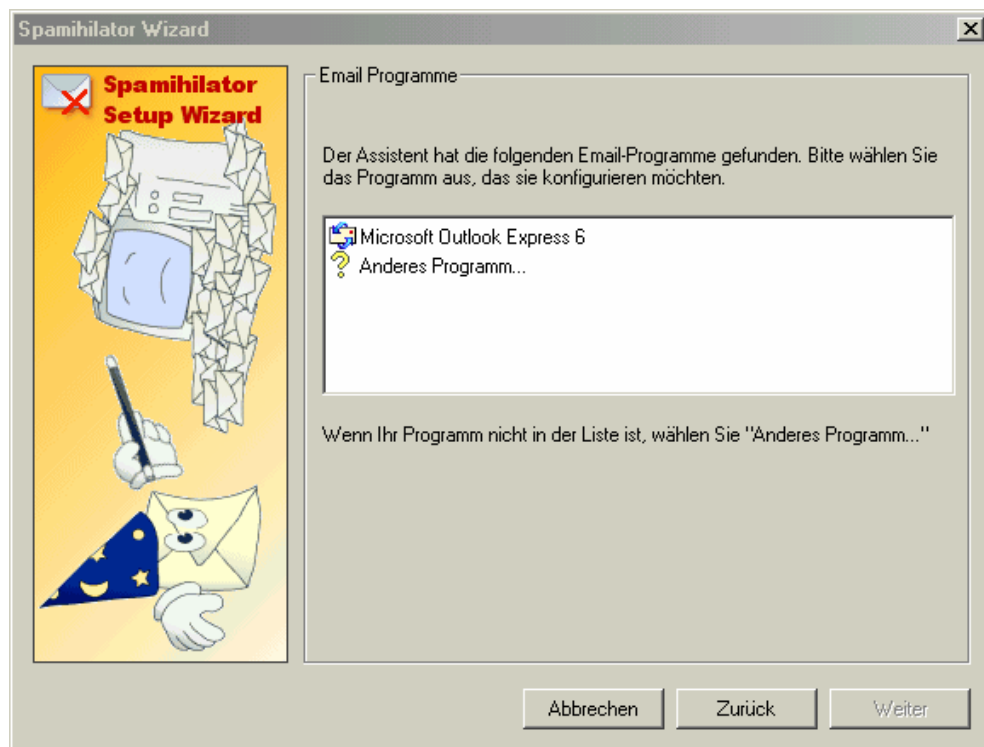
Die Erweiterten Optionen helfen Fehler zu verhindern



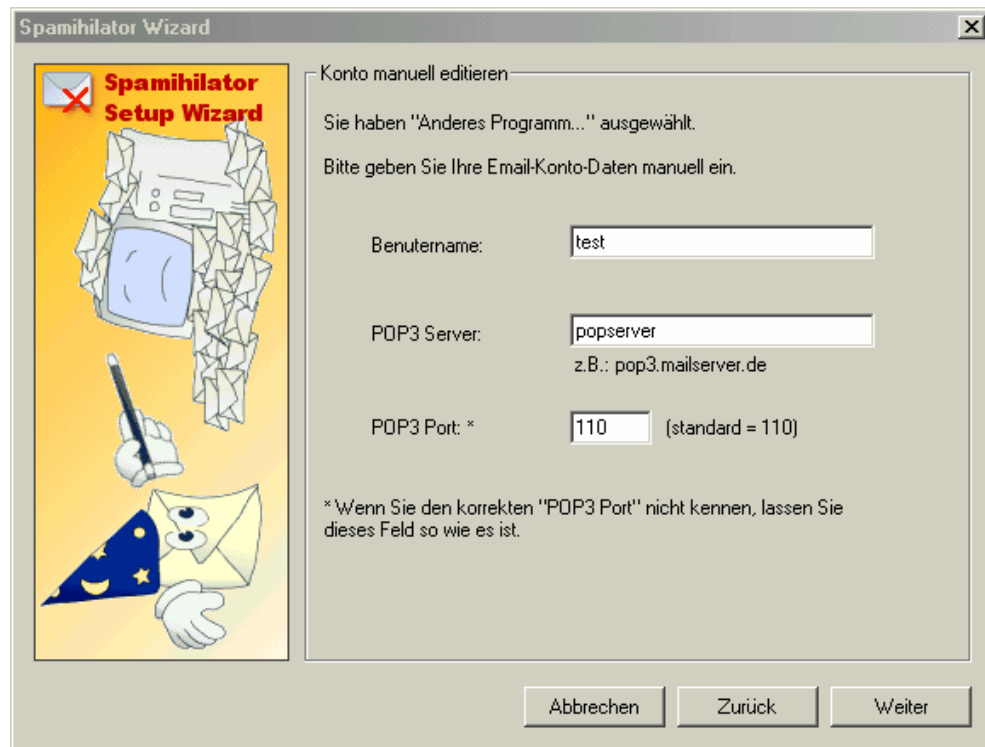
Für Anfänger sind nur die oberen beiden Optionen von Interesse. Ab wann sollen die Abfragen der Server abgebrochen werden und wie viele Server werden gleichzeitig Adressiert. Den ersten Wert sollten Sie irgendwo um die 30 Sekunden halten um einen Timeout Ihres Email Clients zu verhindern. Lassen Sie die anderen Optionen einfach wie sie sind.

Kapitel III. Ohne Listen mit Spamihilator

Der Spamihilator funktioniert ähnlich. Kopieren Sie sich die Datei unter <http://www.spamihilator.com>. Die Installation geht schnell und einfach – keine Besonderheiten. Der Spamihilator kommt mit einem Assistenten, der die Konfiguration für die einzelnen Emailclients vornimmt



Jedenfalls hinsichtlich Outlook Express® ist das ganze funktionstüchtig und läuft hervorragend. Bei anderen Emailclients ist allerdings eine Handkonfiguration nötig. Aber auch hier hilft der Assistent. Wählen Sie „Anderes Programm“ und Sie geben die Daten zu Ihrem Mailserver an:



The screenshot shows the 'Spamihilator Wizard' window with the title 'Konto manuell editieren'. On the left is a vertical panel with the wizard's logo and a cartoon character. The main area contains the following text and fields:

Konto manuell editieren

Sie haben "Anderes Programm..." ausgewählt.
Bitte geben Sie Ihre Email-Konto-Daten manuell ein.

Benutzername:

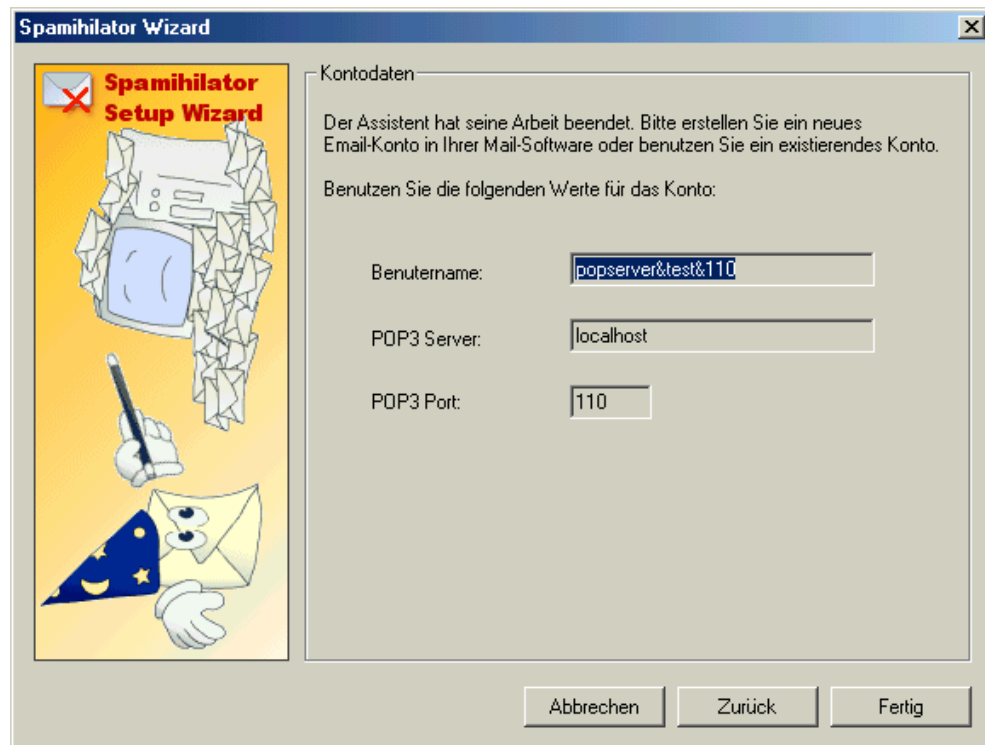
POP3 Server:
z.B.: pop3.mailserver.de

POP3 Port: * (standard = 110)

* Wenn Sie den korrekten "POP3 Port" nicht kennen, lassen Sie dieses Feld so wie es ist.

Buttons: Abbrechen, Zurück, Weiter

Nach einem Klick auf „Weiter“ erhalten Sie die Daten, die Sie stattdessen in Ihren Client eintragen sollen:



The screenshot shows the 'Spamihilator Wizard' window with the title 'Kontodaten'. On the left is the same vertical panel as in the previous screenshot. The main area contains the following text and fields:

Kontodaten

Der Assistent hat seine Arbeit beendet. Bitte erstellen Sie ein neues Email-Konto in Ihrer Mail-Software oder benutzen Sie ein existierendes Konto.
Benutzen Sie die folgenden Werte für das Konto:

Benutzername:

POP3 Server:

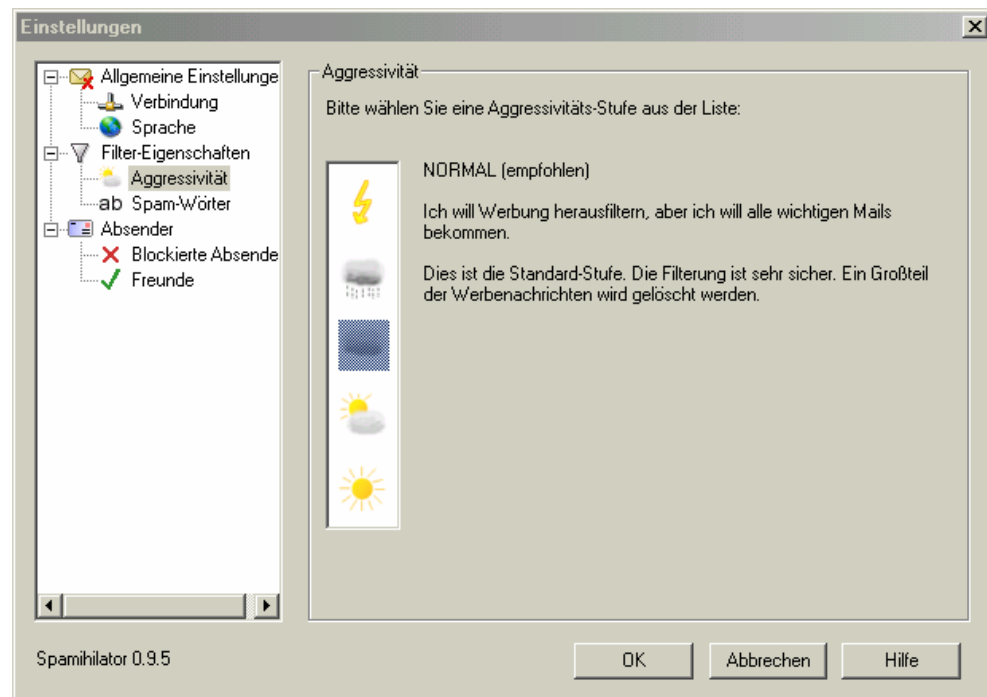
POP3 Port:

Buttons: Abbrechen, Zurück, Fertig

Das war's dann auch schon. Wenn Sie nun Ihre Emails abholen, werden diese durch Spamihilator gefiltert. Das erkennen Sie an dem sich bewegenden Briefsymbol in der Task-Leiste.

Die Einstellungen nehmen Sie –wie bei SpamPal- durch einen Klick mit der rechten Maustaste auf das Brief-Symbol und die Auswahl „Einstellungen“ vor. Unter „Verbindung“ und „Sprache“ nehmen Sie allgemeine Einstellungen vor – hier kann alles bleiben wie es ist.

Unter „Aggressivität“ stellen Sie ein, mit welcher Sensibilität Spammails markiert werden. Dabei gilt: Je höher der Wert umso höher auch die Fehlerquote

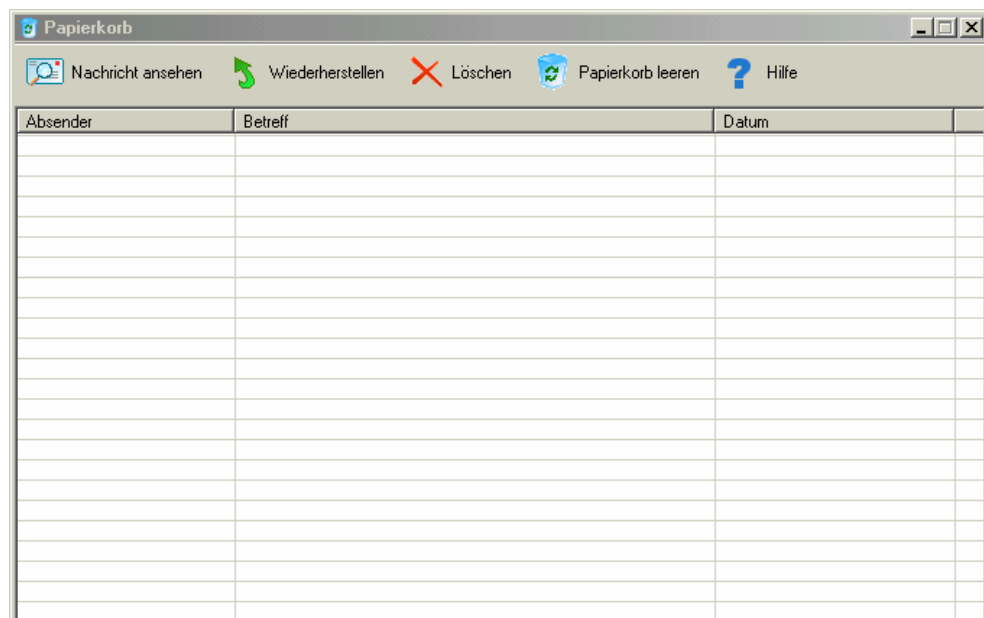


Unter „Spam Wörter“ können Sie eigene Wörter angeben, die Spammails indizieren. Einige kurze Erläuterungen zum Algorithmus: Sie können verschiedene Wörter definieren, die auf Spam Mails hindeuten. Jedem Wort geben Sie eine Gewichtung, das bedeutet

eine bestimmte Zahl. Wenn nun eine Reihe dieser indizierten Wörter auftaucht, addiert Spamihilator einfach die Gewichtungen der Wörter und ermittelt so einen bestimmten Wert. Wenn dieser Wert eine bestimmte Schwelle erreicht hat wird die Email als Spam markiert. Wie Hoch die Schwelle zur Indizierung ist legen Sie unter „Aggressivität“ fest.

Weitere Optionen sind „Blockierte Absender“ und „Freunde“. Hier können Sie Emails direkt abschmettern oder immer zulassen.

Spamihilator arbeitet anders als SpamPal: SpamPal markiert die Emails lediglich. Spamihilator dagegen hat einen internen Papierkorb. Sobald eine Email als Spam erkannt wird, landet sie im internen Papierkorb von Spamihilator – wird also nicht an das Email Programm weiter gereicht. Den Papierkorb können Sie jederzeit einsehen, indem Sie mit der rechten Maustaste auf das Brief-Icon klicken und „Papierkorb“ auswählen:



Hier können Sie die Emails dann endgültig löschen oder an ihr Email Programm weiterreichen

Kapitel IV. Fazit

Ich bevorzuge SpamPal – allerdings habe ich auch DSL. Wer viele Emails täglich erhält und zum Beispiel nur eine 56k Anbindung an das Internet hat wird sich vielleicht nicht freuen, wenn bei jeder Email erst der Absender mit verschiedenen Datenbanken abgeglichen wird. Wem es also zu langsam ist, der sollte vielleicht lieber auf Spamihilator setzen

Ich hatte beide Programme im Einsatz, dabei fand ich, dass SpamPal erheblich effektiver arbeitet. Bei weitem nicht alles wurde bei Spamihilator richtig erkannt – und wenn mal was falsch erkannt wurde, musste ich erst über den Papierkorb die Mail wiederherstellen. Das war mit zu viel Mühe.

Die Datenbanken haben allerdings einen Nachteil: Sie leben häufig an der Realität vorbei. Gerade bei großen Providern ist es üblich – solange man keinen eigenen Server hat – dass man sich eine IP mit anderen teilt. Meine Netz-ID.de IP ist zum Beispiel die gleiche wie die eines bekannten Spammers. Aus diesem Grund werden Emails meines Servers häufig als Spam markiert - dabei versende ich keine Spammails. Insofern sollten Sie immer den Tag Modus nutzen und nicht blind alles löschen oder ablehnen