SPAM Filter funktionsweise und Konfiguration

Version: V0.1
Datum: 17.01.06
Ablage: ftp://ftp.clinch.ch/doku/Spam-Filter.doc
Autor: Manuel Magnin
Änderungen: 13.09.06 MM Beschreibung Implementation HoneyPot eMail Adresse

Inhaltsverzeichnis:

1. SPAM Service SYSTEM-CLINCH

Spam ist Zeitverschwendung, blockiert Mail-Server und ist schwer wieder loszuwerden. Die meisten Mailboxen werden täglich mit Spam-Mails (unerwünschter Werbung) überflutet. Tatsächlich sind heute mehr als 80% aller Emails weltweit Spam-Mails!
Bei vielen Lösungen sind Installation und Betrieb aufwendig und setzen tiefgehendes technisches Verständnis voraus. Unser Mail-Filter Service wurde von Grund auf so konzipiert, dass die Konfiguration und Benutzung so einfach wie möglich ist.

Wie funktioniert das? Ganz einfach, die Mails der zu filternden Domäne werden nicht direkt zum Mail Server geleitet sondern zuerst zu einem SPAM-PROXY. Dort werden:
- die Mails auf Viren geprüft und Mail mit Vieren gelöscht.
- die Mail auf SPAM Wahrscheinlichkeit geprüft und gegebenenfalls im Betreff markiert

2. Anti SPAM funktionsweise

Der SPAM Filter macht diverse Tests, einige davon kurz erklärt:

1. Als erstes wird der Text Inhalt der Mail auf **Schlüsselwörter** geprüft. Wörter wie Sex, Viagra usw... haben jeweils einen SPAM Index z.B. 150% oder so... . Andere Worte wie Zürich ... haben nur 20%. Also 100% ist somit neutral und alles unter 100% reduziert die SPAM Wahrscheinlichkeit.
2. Weiter wird das **Verhältnis von Mail Text zu Farben, Schriften, Anhängen** errechnet und mit einem Prozentsatz versehen.
3. Weiter wird die Mail mit **Signaturen** in SPAM Listen auf dem Internet abgeglichen wie z.B. www.spamcop.com
4. HoneyPot eMail Adressen zur SPAM erkennung
5. Weiter wird die Email auf **Viren geprüft** und bei Virus Befund gelöscht
6. Weiter werden gewisse **Anhänge auf Sicherheitsgründen blockiert**. Folgende Endungen von angehängten Dateien werden blockiert:

{*} bat chm cmd com cpl crt dll hlp hta inf ins isp js jse lnk mdb msi msp nws ops ocx pcd pif prf reg rm rt scf scr sct shb shm shs shtm shtml url vb vbe vbs vbx vxd wsc wsf wsh

7. Weiter werden bestimmte **IP Adressen** von SPAMern gesperrt
8. Weiter werden bestimmte Mail-Server von SPAMern gesperrt auf Grund der **Hello / Ehllo Meldung des Mail-Servers**
9. Berechnung der Anzahl Mail-Server die zur Weiterleitung verwendet werden. Z.b. mehr als 4 **Mailserver Relais** deuten auf eine Verschleierungstaktik
10. IP-Test: Lässt sich die IP-Adresse des Server zu einem **Namen auflösen**
11. und noch einige Test mehr ...

Am Schluss werden alle SPAM Prozente ihrer **Gewichtigkeit nach verrechnet** und in einen **SCORE** umgerechnet. Der Score reicht von 0 bis ca. 33. Alle Mail mit einem Score grösser als 6.0 werden im **Betreff Markiert.**
D.h. es werden also **keine Mails vom SPAM-PROXY** gelöscht!! Diese werden nur markiert! Allerdings können Teile oder alle SPAM Mail im Mail-Server umgeleitet oder gelöscht werden dies wird im weiteren noch beschrieben.
Folgende Markierungen werden im Betreff vorgestellt:

[SPAM?]	**Absende Mail-Server SCORE ist zu hoch**
[SPAM!]	**Absende Mail-Server mehrfach falsch konfiguriert!!**
[SPAM: 12.4]	**Mail wurde als SPAM deklariert. In diesem Falle mit dem Score von 12.4 (6.1 bis ca. 33.0 ist möglich)**

3. Email Einstellungen am PC (Regeln...)

So könnten die empfangenen Emails aussehen:

[Spam: 10.0]	SPAM aufgrund des Innhaltes
[Spam!]	SPAM aufgrund des Absenders

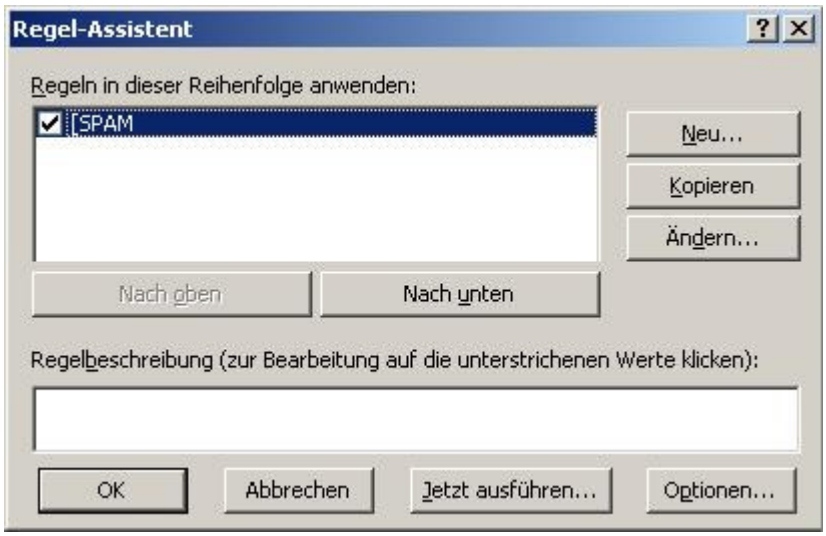
Jetzt können wir Regeln einrichten, sodass die SPAM Mails automatisch in den Ordner SPAM verschoben werden (also nicht mehr im Ordner Posteingang erscheint)

Als erstes müssen wir einen Ordner SPAM erstellen:

Um einen Ordner SPAM zu erstellen klicken wir mit der rechten Maustaste auf Outlook Heute / Persönlicher Ordner und wählen dann neuer Ordner erstellen.
Name: SPAM
Typ: Email
und Bestätigen

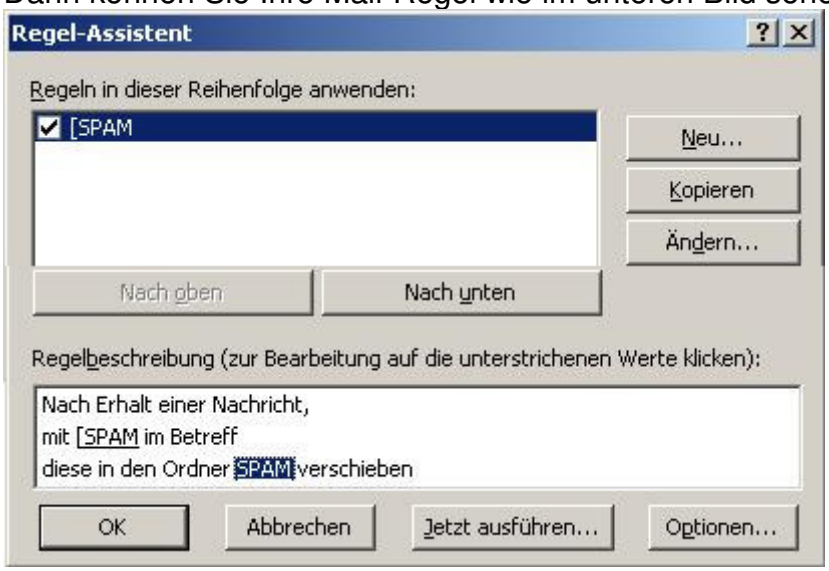
Jetzt möchten wir eine Regel erstellen um alle SPAM Mail direkt in den neu erstellten Ordner zu verschieben:

Im OUTLOOK:
unter **EXTRAS**
dann **REGEL-ASSISTENT**



Wählen Sie: **Nach Erhalt der Nachricht**
Weiter: **mit dem Betreff**
Filtern nach: **[SPAM:**
Weiter: **in den Ordener verschieben**
>> Odener **SPAM** auswählen
Und: **Fertigstellen**

Dann können Sie Ihre Mail-Regel wie im unteren Bild sehen:



Natürlich können auch mehrere Filterregeln erstellt werden:

Filter Zeichen	**Was wird gefiltert**
[SPAM	filtert alles ev. auch gewollte Mails z.B. [SPAM?]
[SPAM?	Filtert Mails die ev. SPAM sind ?? aber nicht sicher
[SPAM!	**filtert absende Mail-Server falsch konfiguriert**
[SPAM: 1	**filtert SPAM-Mails mit einem Score grösser = 10 und <20**
[SPAM: 2	**filtert SPAM-Mails mit einem Score grösser = 20 und <30**
[SPAM: 3	**filtert SPAM-Mails mit einem Score grösser = 30 und <40**

Die Erste Position ist zu wählen wenn jemand alle SPAM Filtern möchte und gegebenen Falles auch im Ordner SPAM mal nachsehen will.
Die **fetten** Zeilen sind für alle die auf Nummer sicher gehen wollen und Teils SPAM Mails auch im Posteingang haben können.

4. Email Einstellungen Domänen SPAM Filterung

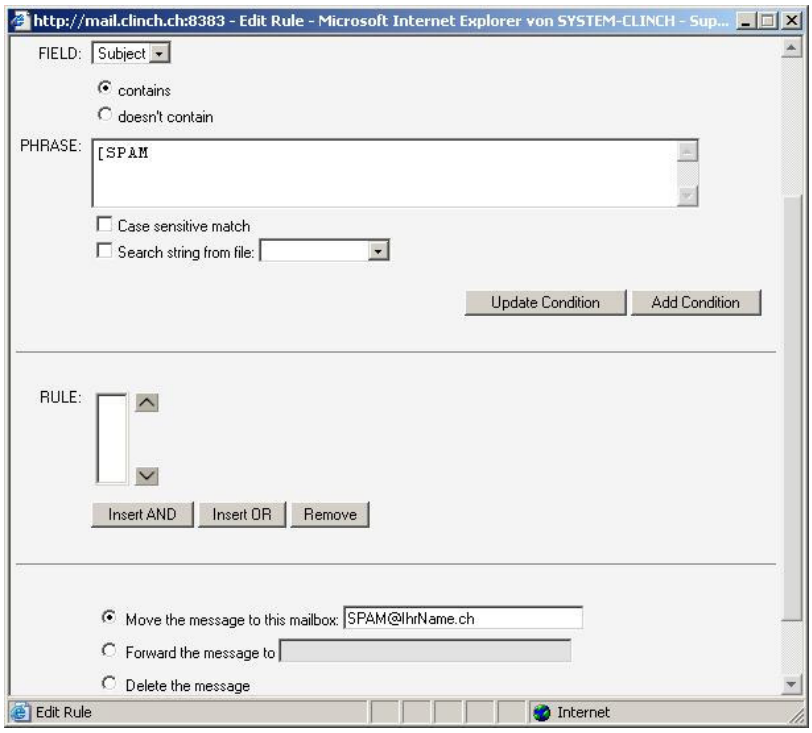
Wenn die Mails nach der SPAM Prüfung auf einem Mailserver von uns landen können auch User-Konten oder Domänen Regeln eingerichtet werden.
Dies kann via Webmail gemacht werden via WebBrowse z.B. **http://mail.clinch.ch .**

Jeder Benutzer kann so seine eigenen Filter für sein Konto einrichten und wenn gewollt die SPAM Mail auch gleich unwiederrufflich löschen.

Wenn Sie Domänen Administrator Rechte haben, können Sie auch Regeln für die ganze Domäne erstellen.

Es könnten alle SPAM Mails der gesamten Domäne an ein spezielles Konto SPAM@IhrName.ch weitergeleitet werden. Dieses wird dann vom Administrator abgeholt und bei Ihn in den Ordner SPAM verschoben. Mit diesem verfahren können Mitarbeiter die glauben Mails nicht erhalten zu haben dies beim Administrator klären.

Im SYSTEM-CLINCH Webmail unter OPTIONS >> RULES eine Regel erstellen



5. DNS und fremd Domain Filter

DNS eintrage für SPAM Filterung, dies wird im Normalfall durch uns erledigt. Die folgenden Angaben sind nur zur Information des Ablaufes.
Um ganze Domänen von SPAM zu befreien können müssen die MX Records auf unseren SMPT-PROXY geleitet werden.

MX	60	smtp-proxy.clinch.ch
MX	80	mail.ihrname.ch
A	mail	217.xx.yy.zz

Der secondary Mail Server mit der Priorität 80 wird verwendet wenn der SMPT Filter Service gekündigt wurde ohne die DNS Einträge anzupassen. Ev. sollten der secondary Eintrag entfernt werden, da es bereits SPAMer gibt die bemerkt haben, dass der secondary Mail Server schlechter gesichert ist!

User SMTP-PROXY leitet dann alle Ihre Mails an unseren Mail-Server oder den von Ihnen gewünschten Exchange oder Mail-Server weiter.

Mit diesem Verfahren sind wir in der Lage beliebige Domänen und Mailserver vor zu Filtern egal wo sich diese befinden.

6.0 HoneyPot eMail Adressen

Spammer benutzen bots zum automatischen sammeln von eMail Adressen von Web-Seiten. Die grund Idee hinter der Spam Suche mittels HoneyPot ist, dass ein Spamer alle gefunden eMail Adressen einer Page bespamen wird. Also auch eine nicht sichtbare eMail Adresse!

Wenn also eMail auf diese Adresse gesendet werden (eine Adresse die gar nicht sichtbar ist), so muss die von einem Bot gesammelt worden sein und ist auch sicher SPAM. So kann der Spam Filter diese eMail in einem Topf ablegen, dem Honig Topf und diese eMails als SPAM Vorgabe zum lernen benutzen.

Ein unverschlüsselter HTML MailTo Tag sieht folgender massen aus:

```
<a HREF="MailTo:Info@Clinch.ch">Info@Clinch.ch</a>
```

Ein weiterer Eintrag für de automatisch auch bespamt so z.B.:

```
<a HREF="MailTo:Honig.Topf@Clinch.ch"></a>
```

Natürlich ohne Text, dass niemand den Link optisch sieht

Wenn eMail's auf die Adresse " Honig.Topf@Clinch.ch" gesendet werden, so wird der Spam Filter diese Adressen Filtern und in einer SPAM Datenbank ablegen (ohne Zustellung)
Wenn nun gleiche oder ähnliche eMail's auf irgend eine der wirklichen Adressen gesendet werden, so werden diese als Spam erkannt!

Ein einfacher wie auch genialer Trick

Jeder der eine eigene Domäne durch uns auf Spam Filtern lässt, kann auch HoneyPot eMail Adressen erstellen und diese uns zukommen lassen.

6.1 eMail Adressen verstecken!!

Bei neuen WebSides müssen Sie sich vor Spam schützen, in dem Sie Ihre eMail Adresse nicht im Klartext auf Ihrer Webseite darstellen, sondern codiert.
Spamer suchen nach eMail Adressen und nicht nach Codes oder Programmen!

Ein Beispiel:
Klartext: **`<a HREF="MailTo:info@clinch.ch"></a>`**
kann auch folgender massen dargestellt werden Codiert:

```
<a href="mailto:&#105;&#110;&#102;&#111;&#64;&#99;&#108;&#105;&#110;&#99;&#104;
&#46;&#99;&#104;">
&#105;&#110;&#102;&#111;&#64;&#99;&#108;&#105;&#110;&#99;&#104;&#46;&#99;&#104;</a>
```

Oder besser mit JavaScript: (So braucht es keine ASC Umrechung ...)

```
<script language="JavaScript">
  //eMail für SPAM Robots verstecken
  var name1 = "info";
  var domain1 = "clinch.ch";
  document.write('<a href="mailto:' + name1 + '@' + domain1 + '">');
  document.write(name1 + '@' + domain1 + '</a>');
</script>
```

Dies aber nur wenn Sie nicht bereits in diversen Spam Listen geführt werden