spam-sperre.de:

Können Sie sich ein Leben ohne Spam vorstellen?

Ich war verzweifelt. Seit wenigen Wochen, erst seit wenigen Wochen, wurde ich von einer neuen Welle von Spam-Mails überrollt. "Neu" deshalb, weil diese Mails in großer Zahl durch meine dreifache Abwehrmauer hindurch marschierten, als gäbe es kein Morgen.

Ernst Weinzettl

Ein Anruf bei meinem Provider stelle klar, dass sowohl die provider-eigene Abwehr in Betrieb war und eben dabei war, etwas "nachzuschärfen" als auch mein bis dahin recht zuverlässiger SpamAssassin am Laufen und auf aktuellem Stand war.

Ich wartete also ein paar Tage, bis bei der Provider-Abwehr die schärferen Einstellungen gegriffen hatten und war dann doch schwer erschüttert: Es war kaum eine Reduzierung der Spam-Mails zu bemerken. Und eine nicht geringe Zahl davon schlugen auch den Outlook-Regeln ein Schnippchen.

Spam mag manchmal sehr schmackhaft sein - aber nicht so, wie er in unsere Mailbox geliefert wird.

Das Dumme an der Sache war, dass alle Mails, die den Weg bis in mein Postfach finden, auch in einem Junk-Ordner sehr lästig sind. Auch die bereits vorsortierten Mails müssen nämlich auf False Positivs (irrtümlich als Spam erkannte Mails) kontrolliert werden. Die eine falsch zugeordnete Mail unter den siebzig bis hundert eingelangten Spams-Mails pro Tag zu finden, benötigt Zeit, ein gutes Auge und Konzentration, die mir dann bei der Arbeit fehlen.

In Summe eine halbe Stunde pro Tag (für mich alleine, meine liebe Chefin braucht auch nochmal so viel), das geht nicht nur an die Nerven, sondern auch ans Geldbörserl. Und außerdem fressen auch Spam-Mails Bandbreite - spätestens meine, wenn sie an mein Postfach zugestellt werden.

So konnte das also nicht weiter gehen!

Welch ein Zufall: Beim Durchforsten meiner Mails stieß ich auf eine Anfrage eines Herstellers, ob wir nicht seine unvergleichlich treffsichere Spam-Abwehr unseren Lesern näher bringen wollten. Man würde uns auch temporär einen Account für einen Test zur Verfügung stellen.

Also sah ich mich zuerst mal auf der Webseite (http://spam-sperre.de) um. Was kann die Software, was kostet sie? Ist sie interessant nicht nur für mich, sondern auch für unsere Leser?

"Schnell und einfach durch jedermann einzurichten.
Wartungsfrei. Zuverlässig.
Für große und für kleine Unternehmen geeignet."

Aha! Und wie geht das?

"° Spam-Mails bleiben beim Absender. Die Erkennung erfolgt ähnlich dem Türsteher in der Disko.
° Die Mail, die als echt erkannt wird, wird freigegeben, alle anderen bleiben draussen.
° Wenn die Annahme verweigert wird, erhält der Absender eine Fehlermeldung. Das gewährleistet Zustellsicherheit, auch wenn der Absender - z.B. durch einen Trojaner - selbst zum Spammer wurde.
° Echte eMails kommen ohne Zeitverzögerung an. Der Spam bleibt weg. Die Qualität ist nachprüfbar, das System protokolliert jeden Übertragungsversuch."

Ja, da bleiben aber noch jede Menge an Fragen offen! Denn so wirklich begriffen habe ich noch nicht, wie das funktionieren soll. Ich kenne z.B. Produkte zur Spam-Abwehr, die von jedem Absender beim ersten Mal eine Registrierung verlangen, die dann erst sicherstellt, dass seine Mails auch durchgelassen werden. Das entspricht zwar dem bereits zitierten Türsteher in der Disko, verärgert und verscheucht (wegen des zusätzlichen Aufwands) aber viele Kunden und Lieferanten, die dann ausbleiben. Das muss also noch abgeklärt werden.

Und dann noch:

"Juristisch einwandfrei. Im öffentlichen Dienst und in der Privatwirtschaft eingesetzt."

???

Ich bin verwirrt. Was soll denn "juristisch einwandfrei" in diesem Zusammenhang bedeuten? Öffentlicher Dienst klingt mal nicht schlecht. Wer, wo?

Preise fand ich auch keine, zumindest nicht ohne Hilfe. Der Klick auf den "Preise"-Button ist fürs erste unergiebig: "Zu unterschiedlich sind die Anforderungen, als dass wir den Preis pauschal darstellen können." Na, da bin ich aber begeistert!

"Von 1 bis ca. 40.000 eMail-Konten auf einer Domain sind unser Kundenklientel. Wenn Sie bis zu 10 eMail-Adressen bereinigen möchten, verwenden Sie einfach dieses Bestellformular: LINK [hinter diesem "LINK" verbirgt sich nur leider kein Link, Anm. d. Red.] Andernfalls füllen Sie einfach diese Anfrage aus und wir erstellen Ihnen umgehend Ihr persönliches Angebot."

Darunter befindet sich ein Anfrage-Formular, das ausschließlich für Unternehmen ausgelegt ist. Die Angabe einer "Firma" ist zwingend notwendig. Gut, ich könnte immerhin fürs erste unseren Verlag angeben - aber was machen Sie als Privatperson in diesem Fall?

Dann steht dort aber auch: "Für noch schnellere Antworten stehen wir Ihnen natürlich auch gerne telefonisch zur Verfügung. Spam-Sperre.de Hotline: +49 9396 9701-50".

Eine Telefonnummer gab es auch bereits in der Mailanfrage. Ein Telefon ist immer in meiner Nähe. Nun also denn!

Die Dame, deren Name unter der Rezensions-Anfrage steht, ist nicht erreichbar. Ist ja auch der Freitag vor dem langen Pfingst-Wochenende. Ich habe auf diese Weise aber das Glück, direkt mit einem der beiden Geschäftsführer und Firmeninhaber sprechen zu können.

Sehr schnell wird klar, warum die Homepage so strikt an Unternehmen gerichtet ist: spam-sperre.de funktioniert auf Domain-Ebene. Und ohne Beschränkung trudeln dann ganz sicher tausende Anfragen für den Spam-Behandlung von mustermaennchen@t-online.de, max@aon.at, liesl@chello.at etc. ein.

Das ist ein Argument, dem ich mich nicht verschließen kann: Solche Anfragen binden zuviele Resourcen. Natürlich aber können auch Privatanwender spam-sperre.de nutzen - wenn sie eine eigene Domain haben und ihre Mails darüber abwickeln.

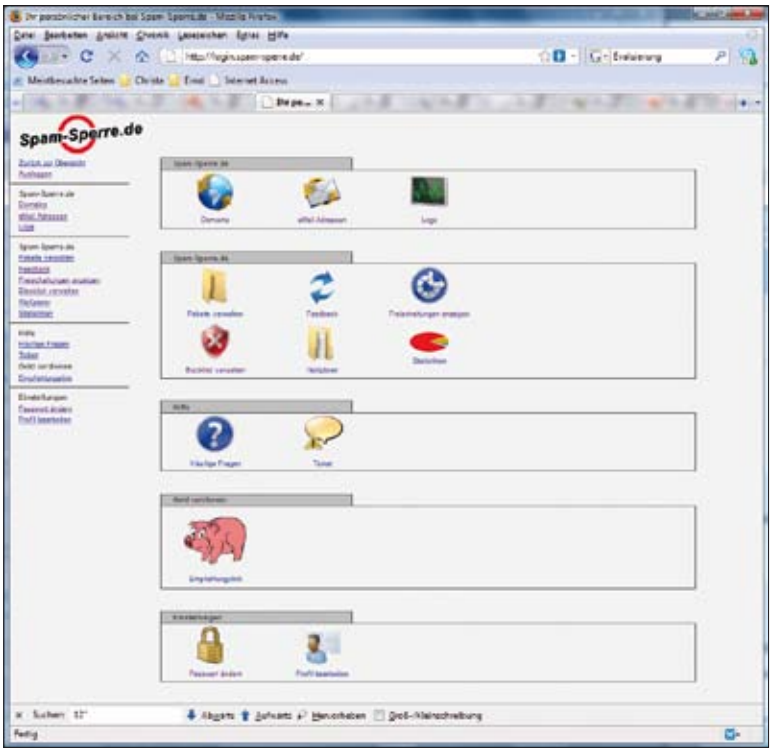
Mir geht es schon wieder besser. Schließlich suche ich letztlich nach einer Lösung für mich und meine Chefin ganz privat. Im Zuge dieses Tests läuft sozusagen gleich meine eigene Evaluierung. ;)

Wir vereinbaren einen Testaccount bis 15. Juni, und ich beginne mit der Anmeldung. Das geht zwar flott, stößt aber unvermittelt auf die erste Hürde: Um das Service von spam-sperre.de nutzen zu können, ist es notwendig, den MX-Eintrag der zu schützenden Domain auf den Post-Server des Spamschutz-Anbieters zu ändern.

Der MX Resource Record oder Mail Exchange Resource Record (MX-RR) einer Domain ist ein Eintrag (Resource Record) im Domain Name System, der sich auf den Dienst E-Mail (SMTP) bezieht. Ein MX-Record sagt aus, unter welchem FQDN (Fully Qualified Domain Name) der Mail-Server einer Domäne oder Subdomäne erreichbar ist. Ist also nicht gerade trivial, solche Änderungen für einen temporären Test vorzunehmen.

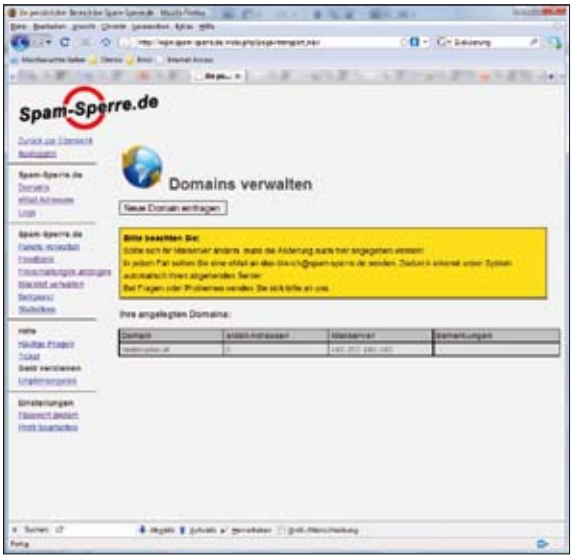
Es ist zwar üblich, für eine Domäne mehrere MX-Records mit unterschiedlichen Prioritäten zu definieren, sodass bei Ausfall eines Mail-Servers ein anderer die E-Mails entgegennehmen kann. Dies erhöht die Wahrscheinlichkeit, dass eine Mail trotzdem an die Empfängerdomain zugestellt werden kann.

Der Admin-Bereich von spam-sperre.de im Überblick



Das allerdings ist wiederum genau das, was Sie in diesem Fall nicht tun sollten. Denn dann wird Spam eben an den zweiten MX Record-Eintrag zugestellt. Also keine Backup-Domain.

Auch recht, mein Provider weilt derzeit auf Urlaub, und ob ich die temporäre Änderung des MX-Records mit seiner Urlaubsvertretung so ohne Weiteres (sprich "ohne weitere Beschädigung des Nervenkostüms und ohne weitere Kosten") über die Runden bringe(n werde)? Gut, das werde ich am Dienstag nach Pfingsten feststellen.



Zwischenzeitlich ist mein Account freigeschalten, die Spam-Sperre kann aber natürlich erst arbeiten, wenn der MX-Record umgestellt ist. Jetzt aber kann ich bereits mit der Administration meines Accounts beginnen.

Das Passwort vom zugewiesenen auf ein eigenes umzustellen, ist schnell erledigt (linkes Menü, vorletzter Menüpunkt), danach beginne ich mit der Eingabe der Domain-Adresse. Einfach, ganz easy. Es können auch mehrere

Domains zur Überwachung angegeben oder "nachnominiert" werden - alles eine Frage des Preises. Hatten wir die Preisfrage nicht schon irgendwo? ;)

Preise

Ich kann mittlerweile auch schon Preise für Kleinunternehmer und Private (nur mit eigener Domain) angeben, der Link befindet sich am unteren Ende der Homepage:

Nachdem die Homepage sich ausschließlich an Unter-

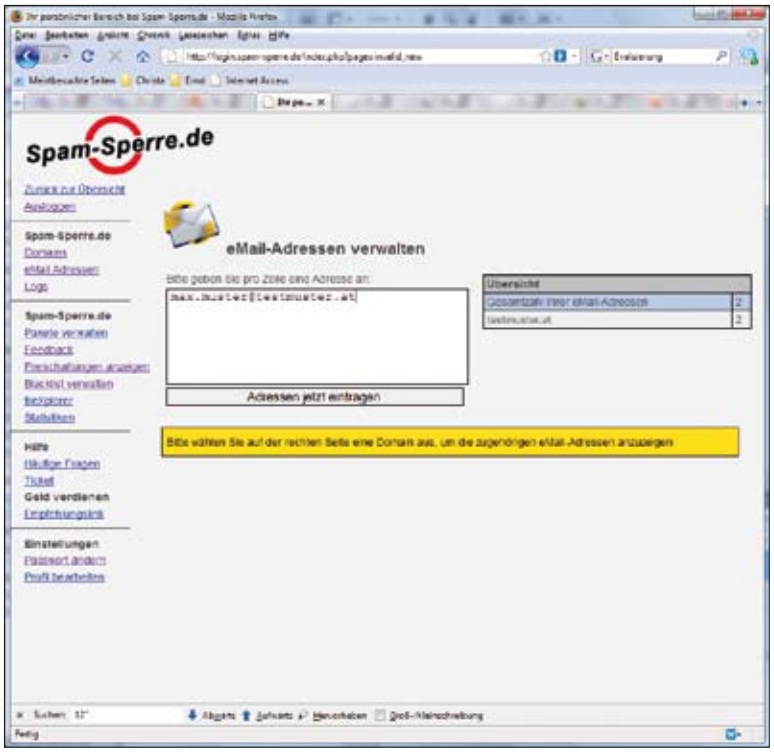
	Paket	Beschreibung	Monatlich	Einrichtung
!	Sparfuchs	1 Domain, 1 eMail-Adresse	4,95 €	29,90 €
	Basis	1 Domain, 4 eMail-Adressen	9,95 €	~~29,90 €~~
	Profi	1 Domain, 10 eMail-Adressen	19,95 €	~~29,90 €~~

nehmen wendet, sind die Preise netto USt. angegeben. Als nicht vorsteuerabzugsberechtigter Privater müssen Sie derzeit die deutsche USt. mit 19% noch hinzurechnen. Die Preise sind aus meiner Sicht fair, wenn ich den monatlichen Arbeitsaufwand bedenke, den ich mir mit dieser Spam-Abwehr ersparen will. 15 Stunden mehr Freizeit pro Woche? Geschenkt!

Eine kleine Erfreulichkeit, die zwar nicht viel ausmacht, aber dennoch spart: Ich brauche die Abwehr für 2 Adressen, muss aber nicht zum Basispaket greifen: zum Sparfuchs werden einfach pro weiterer Mailadresse € 2 addiert.

Weiter mit der Administration

Nachdem ich meine Domain eingetragen hatte, reagierte die Spam-Sperre umgehend: Eine Mail verkündete mir, dass meine Domain (bzw. deren IP) noch nicht verifiziert sei. Ich möge doch bitte eine leere Mail zurücksenden. Kein Problem, mache ich doch glatt. Dann wende ich mich der



Eingabe der zu schützenden Mailadressen zu.

Auch dieser Vorgang ist "deppensicher" gestaltet, was ich eindeutig als Vorteil mitzähle. Der überwiegende Anteil der Anwender besteht nicht aus IT-Freaks und möchte trotzdem seine Werkzeuge funktionierend wissen, ohne deshalb einen Informatik-Kurs machen zu müssen. Es interessiert den Benutzer - zurecht - nicht, wie toll denn ein notwendiges Tool programmiert ist oder welche gigantischen Einstellmöglichkeiten er "mit dem Finger durchs rechte Auge" hätte. Es zählt nur, dass das Teil funktioniert. Und deshalb halte ich einfach zu bedienende Interfaces für so wichtig. Erfreulich ist auch, dass er sich weiters nicht - oder zumindest kaum mehr, und das in sehr vertretbarem Rahmen - mit dem hier beschriebenen Dienstprogramm auseinandersetzen muss, da es zentral gewartet wird.

Zwei Tage nach den ersten Eintragungen hat es mich dann doch gejuckt. Klar, funktionieren konnte das Tool noch nicht, da musste ich bis nach Pfingsten warten. Aber trotzdem wäre doch ein Blick in den Log .... man weiß ja nie...

Na, schau mal einer an! Nachdem ich das gewünschte Datum sowie die Domain eingestellt und "finden" gedrückt hatte, zeigte sich, dass zumindest die an mich gerichtete Mail zwecks Verifizierung meiner Domain als eingelangt und durchgeleitet mitgelogt war.

Jetzt hieß es vorerst warten. *seufz*

Dachte ich.

Ein paar Tage nach Umstellung des MX-Eintrages fragte ich mal nach. Mein Log zeigte nämlich noch keinerlei Aktivität an. Ein freundlicher Techniker erklärte mir, woran es lag. Der MX-Eintrag zeigte leider in ein Subverzeichnis der gewünschten Adresse. Ja, das ist dumm. Einerseits. Andererseits nützt Warten alleine eben doch nicht immer.

Nach Korrektur lief die Spam-Abwehr an. Und zwar ziemlich ruckartig. Plötzlich hatte ich frühmorgens nur mehr zwei Spammails im Junk-Ordner. Und keinen einzigen im Posteingang. Im Posteingang hatte ich bis vor drei Monaten auch keine Spams, die wurden nahezu alle gleich mit Markierungen für die Spam-Wahrscheinlichkeit in die "Quarantäne" (Junk-Ordner) verfrachtet. Der absolut sichere Spam landete noch am Mailserver im Rundordner. Seit einigen Wochen aber kam die Welle der in amüsantem bis grimmigem Deutsch gehaltenen "Werbungen". Und davon kamen einige bis in den Posteingang durch.

Spam-Sperre bzw. einer der Geschäftsführer hatte von einer 99,999%igen Erkennungsrate gesprochen. Wie sah das nun in der Praxis aus?

Das Logfile ist einfach gehalten und zeigt alles Wichtige an: Welche Mails von welchen Adressen sind wann

a) durchgeleitet

b) abgelehnt

c) zu einer weiteren Prüfung beim Absender belassen (zurückgestellt)

d) nach einer eingehenderen Prüfung später (es geht hier um Bruchteile von Sekunden) zugestellt

worden. Diese Daten zeigt das Logfile zeilenweise an. Darüber hinaus wird bei jedem Mail angegeben, warum es abgelehnt wurde - nebst einiger zusätzlicher, für mich nicht so wichtigen Einträge. Es sind also im Logfile alle Daten sichtbar, die ich benötige, um im Fall der Fälle auch selbst einschreiten zu können.

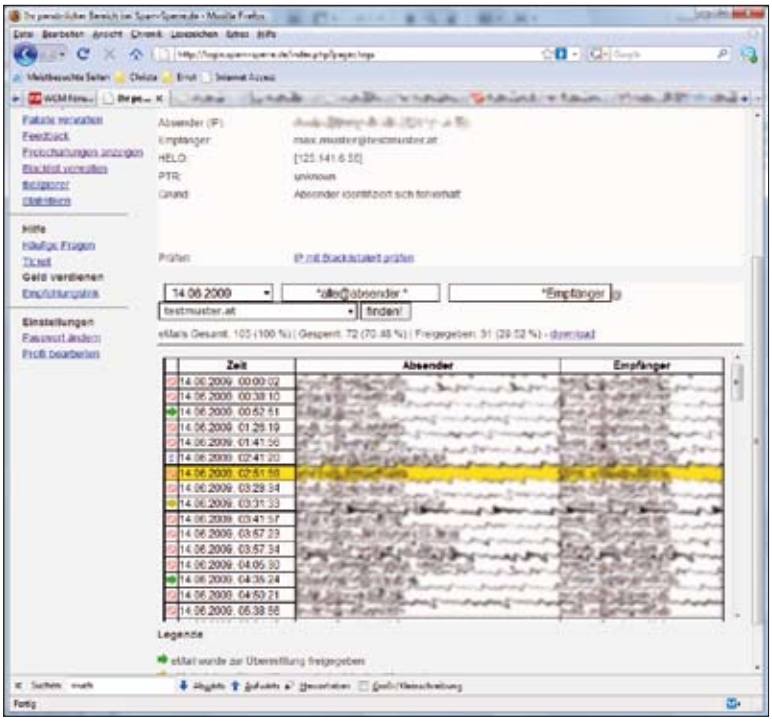
Wann müsste ich überhaupt selbst eingreifen?

Bei "False Positives" z.B., das wären "echte" Mails, die irrtümlich vom Spam-Filter als Spam eingestuft würden. "Würden", den es gab keine. Es gab wohl einige "leicht verdächtige" Mails, die nach einer genaueren Prüfung aber als okay befunden und zugestellt wurden. Es gab aber keine Ablehnungen solcher Mails. Keine einzige während der ersten zehn Tage bis zur Druckabgabe.

Hätte es False Positives gegeben, so hätten neben meiner Einmischung aber auch andere Mechanismen von spam-sperre.de gegriffen. Dazu noch später. Ich jedenfalls hätte in einem solchen Fall die Freischaltung der betreffenden Mail-Adresse oder der gesamten Mail-Domain eintragen können. In solchen Fällen würde die Post von solchen (realen) Adressen gar nicht geprüft, sondern unmittelbar weitergeleitet. Was ich für ganz wenige Adressen auch so eingetragen habe. Es ist ziemlich unsinnig, Adressen abzuprüfen, die 100%ig sauber, täglich mehrere Mails an mich senden müssen.

Oha! Was ist denn, wenn eine Absende-Mailadresse gefaked wird, wie das heute schon üblich ist? Oft doch sogar mit der Empfängeradresse ident zu sein scheint? Dann rutscht doch auch mal ein Trojaner rein wie nichts, oder?

Oder. Denn spam-sperre.de meldet dann z.B. "Absender identifiziert sich fehlerhaft" oder "Trojaner am Werk" und sperrt. Das ist eine der schätzenswertesten Eigenschaften, die ich kennengelernt habe. Diese Spamabwehr prüft immer Mailadresse und Absendeserver (und noch ein paar weitere "Kleinigkeiten") auf Plausibilität und Seriosität.



Der Log versorgt seinen Admin mit klaren Aussagen.

Wann müsste ich eventuell noch eingreifen?

Wenn Mails durchkommen, deren Absender zwar echt sind, deren Reverse Lookup funktioniert, deren Absendeserver sauber sind - und die doch höchst unerwünschte (und im Regelfall auch unverlangte) Werbung verbreiten. Sie kennen das sicherlich: Absender "dickabsahnen.de", Text "Sie erhalten diese Mails, weil Sie sich für diesen Newsletter eingetragen haben oder eingetragen wurden. Wenn Sie keine Mails mehr wünschen, klicken Sie bitte hier." Wenn Sie dann klicken, löst das meist eine Lawine an weiteren Mails von "gewinnspiel.de", "hastduschon.com" etc. aus. Viele davon entpuppen sich beim näheren Hinsehen als Spam-Klones von gleichen Servern ("kjm2.de, kjm3.de...) oder sogar vom

In manchen Fällen leider unumgänglich - aber kurz: die eigene Blacklist.

Wie funktioniert spam-sperre.de?

Die Spamabwehr liegt - und das ist wichtig - vor den zu schützenden Mailboxen. Spam wird also nicht zugestellt und danach behandelt, sondern bereits vor der Annahme.

spam-sperre.de arbeitet nicht mit den üblichen Blacklists, die oftmals ganze Segmente großer Provider sperren, weil in diesen Segmenten einzelne, sehr schlecht geschützte User-PCs als Spambots dienen. sondern mit eigenen Listen bereits erkannter Spamschleudern (laufend aktualisiert durch die Erkennung bei der Betreuung vieler Kunden), Adressen- und Serverprüfung, Virenscannern und, wenn unklar, auch mit Inhaltsprüfung.

Das System ist wirklich überraschend treffsicher, wie ich diesem Test bemerken konnte. Keine False Positives, ganz wenige (deutsche) unerwünschte "Newsletter".

Wird ein Mail - aus welchem Grund auch immer - als Spam klassifiziert, so kommt dieses Mail nicht - wie bei vielen anderen Abwehrdiensten - in eine Art Quarantäne, sondern wird abgewiesen, also von versendenden Server gar nicht angenommen.

Zur Sicherheit schickt die Abwehr auch ein Mail an den Versender, dass sein Mail abgelehnt wurde und daher den Empfänger nicht erreicht hat. Ein "realer" Versender würde also bei einem "False Positive" verständigt und sich, so er selbständig denken kann, auf andere Weise, z.B. per Telefon, beim Empfänger melden. Bots können aber nicht selbständig denken und würden sich, selbst, wenn sie könnten, kaum zum Telefon greifen, um ihre unerwünschte Werbung an den Mann/an die Frau zu bringen.

Dem Empfänger wird per Logfile ebenfalls mitgeteilt, welche Mails angenommen bzw. welche abgelehnt wurden. Auch er kann also eventuelle Fehlreaktionen der Spam-Abwehr kontrollieren und auf Fehler reagieren.

In unserem Test sind allerdings keine Fehler passiert, die das Durchforsten der Logs überhaupt nötig gemacht hätte. Aber Sie kennen mich ja, ich suche primär nach Fehlern; ich habe daher die Logs ausgiebig durchstöbert - ich habe nur keine bemerkenswerten Schwächen gefunden. Fast schon frustrierend.

Von sicheren Servern weitergeleitete Mails aus anderen eigenen Postfächern werden allerdings, so sie nicht verseucht sind, angenommen - und müssen auch angenommen werden. Will man dieses Problem lösen, so gibt es eine einfache Möglichkeit: Spam-Sperre.de schützt so viele Domains und Mailadressen wie gewünscht - alles eine Frage des Geldes. ;)

selben Server aus. Da taucht "couponarena.srv3.de" ebenso auf wie " b2c-mail4.com" oder " mailserver27.supercomm.de" und all seine 26 Brüder.

Dieses Problem betrifft eigentlich jeden Empfänger, der seine Mail-Adresse länger als ein halbes Jahr verwendet. Geschäftlich, aber auch privat.

Gut, in dieser Angelegenheit musste ich tatsächlich ein paar Versender - insgesamt sechs Stück - manuell niederknüppeln. Aber bisher ist davon keiner wieder aufgestanden. Gott sei Dank.

Nach zehn Tagen also eine kurze Bilanz: ca. 75% unserer (meiner Chefin und meiner) Mails sind Spam, etwa ein Viertel "echte" Post, privat und geschäftlich gemischt.

Wir hatten innerhalb der letzten Tage in beiden Mailboxen insgesamt 12 (in Worten "zwölf") Spammails in der Post, die von acht Adressen kamen. Sechs davon sind nun gesperrt, da kam seit Tagen nicht eine mehr durch. Zwei sind Weiterleitungsadressen.

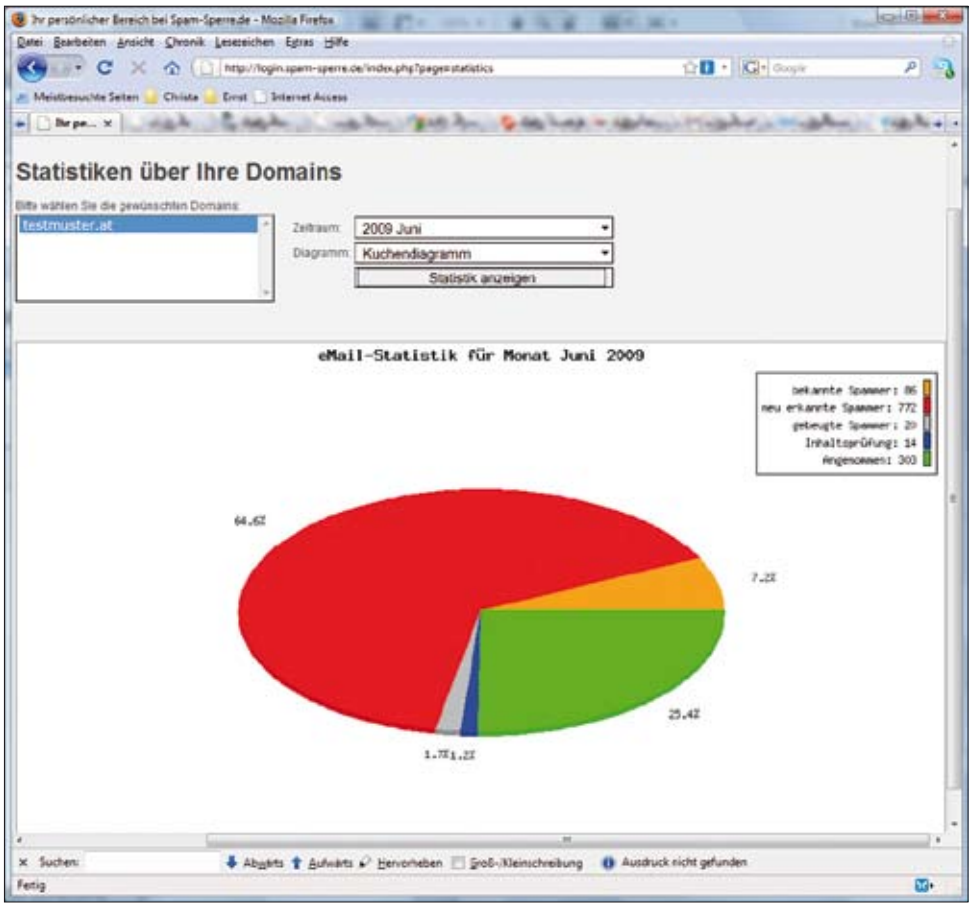
Und da sind wir beim einzigen echten Haken im System.

Wird eine Mailadresse per automatischer Weiterleitung an mich zugestellt (z.B. "ernst.w@wcm.at" an meine Privatadresse), so gibt es keine Möglichkeit der Prüfung mehr, so sich der Weiterleitungsserver als sauber und korrekt erweist. Wird ein Mail von einem solchen Server weitergeleitet, so muss die Post auch übernommen werden. Schließlich hat dieser Server keine Möglichkeit mehr, die Nachricht abzuweisen, da er sie (zwecks Weiterleitung) bereits übernommen hat. Lehnt meine Spam-Sperre die Annahme einer solchen Nachricht ab, so entsteht nicht nur ein rechtliches Problem (bei Verlust), sondern auch ein Ping-Pong-Spiel mit der Benachrichtigung der Abweisung. Ich habe die Vorgänge, etwas vereinfacht, in einem separaten Kasten dargestellt.

Da wird dann schnell ersichtlich, was ich meine.

Gut, mit den drei Mails kann ich leben. Im selben Zeitraum musste ich mich wenigstens nicht mit den anderen 878 (gezählt, nicht geschätzt) Spammails herumschlagen.

Der Beobachtungszeitraum war nur wenige Tage lang, das Statistikergebnis hat in dieser Zeit aber nur minimale Verschiebungen gezeigt.



Fazit

Ja, wir brauchen ein Fazit, klar. Ja, der Dienst ist gut, auch für Privatanwender. Ja, der Dienst kostet Geld - aber meine Zeit, in der ich mich bis jetzt mit diesem Spam-Mist rumschlagen musste, kostet viel mehr. Ja, auch meine Freizeit hat einen Wert, einen sehr hohen sogar. Der liegt jedenfalls weit über einer Jahresprämie. Und dann belastet diese Spam-Abwehr meinen Posteingang bandbreitenmäßig gar nicht, Spam wird bereits vor meiner Haustüre abgewimmelt - sehr fein.

Sehr angenehm ist, dass sich Kunden selbst kaum mit dem administrativen Teil befassen müssen.

Ich denke, es ist am besten, ich sage Ihnen, dass ich heute den Dienst, den ich bislang nur testweise hatte, für unsere private Domain kostenpflichtig für ein Jahr bestellt habe. Und wenn die Trefferquote so bleibt, wie sie derzeit ist, wird mich spam-sperre.de wahrscheinlich auch in den Folgejahren schützen. ◘