window.respimage && window.respimage({ elements: [document.images[document.images.length - 1]] });

SPAM

Glücklich der sie nicht oder nicht mehr kennt, die Flut von Angeboten für gewisse Pillen oder dubiose Geschäfte, Gewinnbenachrichtigungen und ähnlichem, die tagtäglich die Mailboxen überquellen lässt. Die eine oder der andere hat vielleicht schon resigniert und sich damit abgefunden, diese lästigen, als SPAM oder auch UBE bezeichneten Mails, täglich per Hand auszusortieren und dafür eine Menge anderweitig nutzbarer Zeit aufzuwenden.

Um welche Fragen geht es in diesem Artikel?

- Wie vermeide ich SPAM?
- Wie unterscheiden sich SPAM Abwehr im Mailprogramm und auf dem Mailserver?
- Was kann ich als Anwender oder Betreiber des Mailservers einer Firma aus eigener Kraft, ohne den Provider (kostenpflichtig) zu bemühen, zur SPAM Vermeidung tun?

Um das Verständnis der verschiedenen Varianten zu ermöglichen oder zu erleichtern, sollen einige Worte zum Gesamtbild die Einordnung und Bewertung der einzelnen Maßnahmen ermöglichen. Der Artikel richtig sich an technisch Interessierte, die nach verständlichen Informationen in deutscher Sprache suchen.

So, und nun mal Butter bei die Fische:

Welche Maßnahmen haben sich denn nun bei den Kunden der edv2g als unabdingbar bzw. nützlich erwiesen, wenn es um das Trennen von erwünschter und unerwünschter Mail geht? Wir reden hier selbstverständlich über automatisierte maschinelle Verfahren der Separierung von gut und schlecht, nicht über Techniken zum überblicksmäßigen schellen Lesen und Erfassen von Texten oder Betreff-Zeilen und anschließende händische Sortierung.

Zunächst einmal ist grundsätzlich zu unterscheiden zwischen dem "Wegfiltern" bereits zugestellten Mülls und der Verweigerung der Annahme desselben. Naheliegend ist vielleicht das erstgenannte, schließlich hat dieses Problem ja der Mailnutzer direkt vor sich.

SPAM Filter im Mailprogramm

Dieses können manuell trainierte Filter in den Mailprogrammen (Stichwort **Bayes Klassifikator**) nahezu perfekt.
WENN sie sowohl mit guten als auch mit schlechten Beispielen hinreichend angelernt wurden. Nahezu alle aktuellen Mailprogramme (wie Outlook®, Outlook Express®, Thunderbird™, oder wie sie auch heißen) bieten diese Funktion von Hause aus oder lassen sich mit einer Erweiterung nachrüsten.

Neben der steigenden Übersichtlichkeit der Mailbox sinkt so ganz nebenbei auch das Infektionsrisiko für den PC. Denn nicht selten enthalten diese Mails Bestandteile, die beim Anklicken/Öffnen der Anhänge oder auch schon beim bloßen Anzeigen der Mail den PC infizieren können. Oder über das Anzeigen der präparierten Webseiten hinter den Links aus der Mail. (Und dagegen hilft eben keine Personal Firewall auf dem PC!)

Eine Standardtechnik ist es beispielsweise, Bestandteile wie Links oder aus dem Internet nachzuladende Bilder in die Mails einzubetten, die eine Auswertung des Zustellerfolges erlauben. Also ob eine benutzte Mailadresse auch zu einem Postfach führt, das gelesen wird. Um es noch einmal ganz deutlich zu sagen: Mails können Konstruktionen enthalten, wie zum Beispiel per individuellem Link aus dem Internet geholte Bilder, die es dem Absender erlauben festzustellen, welche seiner Millionen verschickten Mails angezeigt wurden. Nebeneffekt dieser Techniken: der Wert einer Adresse steigt, wenn nachgewiesen ist, das Mails an diese auch angezeigt, wahrscheinlich also gelesen werden. Es wird also tendenziell noch mehr Post nachkommen, wenn jede Mail in einer Vorschau angezeigt wird, und das am besten gleich mit allen aus dem Internet nachgeholten Inhalten. Das ist nur noch durch das Klicken auf die Links in diesem Mails zu übertreffen.

Gegen diese Techniken bieten die aktuellen Mailprogramme Einstellmöglichkeiten. Diese darzustellen sprengt aber den Rahmen dieses Artikels. Wenn Sie spezielle Fragen dazu haben, zögern Sie nicht, sich mit uns in **Verbindung zu setzen**.

So nützlich diese Verfahren des Filterns im Mailprogramm auch sind: schon das erfolgreiche Versenden der Mail ist ein Erfolg für die Spammer und bringt ihnen Geld. Deshalb sind auch

SPAM Filter und Klassifikatoren auf dem internen Mailserver

nicht viel besser als das Filtern und Sortieren im Mailprogramm. Die Technik, mittels bestimmter Schlüsselworte oder anderer typischer Merkmale die SPAM Mails erkennen zu wollen, erreicht recht schnell ihre Grenzen, die sich in doch recht vielen fälschlich als SPAM bewerteten und in den SPAM Ordner des Nutzers verschobenen guten Mails oder andersherum in durchgelassenem Müll äußern.

Daher ist es erheblich besser, Mails schon bei der Annahme am ersten Mailserver bzw. auf der Firewall zu prüfen. Und offensichtlich von einem nicht richtig konfigurierten Server (Stichwort HELO und DNS Tests) stammende Mails oder solche mit ungültigen Absenderadressen gar nicht erst anzunehmen. Gleichzeitig sinkt bei diesem Verfahren der Anteil von "konnte nicht zugestellt werden" Nachrichten, da solche Nachrichten erst versandt werden, wenn ein Mailserver die Mail zur Weiterbeförderung angenommen hat. Wenn der Erstversender die Mail gar nicht erst verschicken kann, gibt es auch keine Fehlermails.

SPAM Filter vor dem Mailserver, auf der Firewall

Eine typische Anordnung: Eine Firma nutzt ein Mailgateway, eine Firewall mit Mailschleuse, die eingehende Mails unter anderem auf Viren prüft, und einen Mailserver im Hausnetz. Wenn diese Schleuse nicht bei jeder Mail sofort prüfen kann, ob der Nutzer auch existiert, muss sie alle Mails für die Firma erst einmal annehmen. Erst bei der Weiterleitung an den eigentlichen Mailserver stellt sich heraus, dass der Empfänger nicht existiert. Beispielsweise wegen eines Tippfehlers in der Mailadresse. Natürlich sollte jetzt eine Fehlermeldung erzeugt und an den Absender geschickt werden: die Mail konnte nicht zugestellt werden, da der Empfänger nicht existiert.

Nur dummerweise entstehen diese Nachrichten sowohl beim Tippfehler, wo sie nützlich und wertvoll sind, als auch bei den durch Rateversuche gebildeten Empfängeradressen unserer unerwünschten "Freunde".

Wesentlich besser ist es daher, auf dem ersten System, welches Mail für eine Domain annimmt, ***zu prüfen, ob der Empfänger überhaupt*** *existiert*. Schlägt dieser Test fehl, wird die Mail überhaupt nicht angenommen, der Spam gar nicht erst verschickt.

Weiterhin ist die Abfrage einer Realtime Black List (RBL) obligatorisch. Über die IP Adresse des sendenden Systems wird so geprüft, ob dieses als SPAM Versender bekannt ist. In diesen Listen tauchen auch meist die kompletten Adressblöcke der Provider auf, die diese Kunden ohne feste IP Adresse zuweisen (Einwahladressen, typisch für private Internetnutzer). Was wiederum erklärt, warum es sinnlos ist, von solchen Systemen direkt Mail versenden zu wollen, nicht über den Mailserver eines Providers: nur schlampig konfigurierte Systeme werden eine E-Mail, die von einer Einwahl-IP kommt, überhaupt annehmen.

Durchaus effizient ist auch **Greylisting**. Die Details zu diesem Verfahren können bei Interesse im Wikipedia Eintrag nachgelesen werden. Kurzfassung: wer es ernst meint mit dem Wunsch, eine Mail zuzustellen, der unternimmt auch einen zweiten Versuch. Viele **Zombie-PCs** tun das nicht.

Wenn sich die Probleme der Art, dass es einem Partner nicht gelingt, eine Mail an Sie als Mailserverbetreiber oder Ihre Nutzer zu schicken, nicht durch Korrektur der Konfiguration an der Quelle beseitigen lassen, helfen dann meist Whitelist-Einträge auf Ihrem Server weiter.

Zusammenfassung

Bei den Kunden der edv2g ist der unerwünschte Werbemüll (SPAM) kein Thema mehr. Im Durchschnitt schaffen es gerade mal noch zwei oder drei der Plagegeister, sich im Laufe der Woche in ein Postfach zu schmuggeln. Dieser Erfolg lässt sich einfach und kostengünstig durch den Einsatz einer Firewall mit integriertem Spamschutz, hier also der astaro Firewall, erreichen.

p.s.
Hat Ihnen dieser Artikel weitergeholfen? Dann sagen Sie es weiter. Verlinkungen sind mit Bedacht zu setzen, da wir keine Zusagen geben können, wie lange dieser Artikel unter dieser Adresse erreichbar ist. Es sei denn wir wissen davon, dann können wir es auch berücksichtigen. Bevor Sie aber die Inhalte kopieren und wieder veröffentlichen: holen Sie sich unser Einverständnis ein. Dies ist keine Bitte.

Fanden Sie den Artikel interessant und Sie haben ein Problem mit diesem Bitmüll, die Fachbegriffe waren

aber **böhmische D**örfer für Sie? Dann sprechen Sie uns doch einfach an, ob nun per Telefon oder auch per - nun ja doch - E-Mail. Gerne beantworten wir Ihnen Ihre Fragen oder helfen Ihnen auch ganz praktisch bei Ihrem Mailsystem weiter. Die Kontaktdaten finden Sie im Fuß dieser Webseite.

Und auch für Ihre Anregungen zur Verbesserung dieses Artikels oder weitere Themen haben wir offene Ohren und Briefkästen. :-)