Leidtragende

Christoph Puppe

Derzeit ist so viel Spam unterwegs, dass manch ein E-Mail-Anwender oder Postmaster am liebsten seinen Account abschalten oder die Internet-Domain aufgeben möchte. Doch es gibt Alternativen dazu.

Als Inhaber mehrerer Domains und Betreiber eines eigenen Mailservers steht man vor der Frage, wie man den eingehenden Datenmüll einfach aussortiert und dabei nicht die vereinzelt eintreffenden Mails verliert, die man wirklich haben will. In der Regel kommt Filtersoft- oder Hardware zum Einsatz, die ein Unternehmen in eigener Regie betreibt. Alternativ lässt sich der Mail-Verkehr komplett externen Dienstleistern überlassen. Wer denen nicht gleich den Betrieb seines Mailservers übertragen möchte, kann dort einen Weiterleitungs-Zugang für Testzwecke einrichten.

Ob diese Methode zu brauchbaren Ergebnissen führt, mussten zwei solcher Dienstleister zeigen: Eleven mit seinem Produkt eXpurgate und Antispameurope von Solidsystems. Während Eleven seinen Zugang für nichtkommerzielle Zwecke ohne Begrenzung anbietet, ist der Testzugang bei Antispameurope auf 30 Tage begrenzt. Das Hauptgeschäft beider Anbieter besteht darin, komplette Mailsysteme im Kundenauftrag zu übernehmen, doch nur duplizierte und gleichzeitig weitergeleitete E-Mails erlauben einen direkten Vergleich der Filterwirksamkeit.

Die Testgrundlage bildeten rund 6000 E-Mails, die beim Autor innerhalb von vier Tagen ein- und umgehend unter realen Bedingungen an die Filter-Accounts weitergingen – also keine alten Spam-Sammlungen, wie sie gelegentlich als wenig brauchbare Grundlage für Filtertests dienen. Spammer ändern ihren Ausstoß mittlerweile so schnell, dass die Filteranbieter zum Teil mehrmals täglich nachziehen müssen.

Beide Anbieter ermöglichen es, die ankommenden E-Mails dorthin weiterzuleiten und gefiltert zurückzuerhalten. Das Setup für den Test war denkbar einfach. Alle für die Domain eintreffenden Mails wurden per Regel in der Konfiguration von Postfix an jeweils einen Account bei den Anbietern weitergegeben. Black-, Grey- oder Whitelisting kamen nicht zum Einsatz, ebenso wenig eine Vorfilterung. Alle Mails wurden anschließend in einer Datenbank erfasst und anhand ihrer Message-ID identifiziert. Die Datenbank speicherte, welcher Anbieter welche E-Mail als Spam klassifizierte und ob die manuelle Verifikation zum gleichen Ergebnis kam. Zum Vergleich lief außer Konkurrenz Brightmail 6.0.4 als lokale Filterlösung mit.

Eleven: Vielseitige Weiterleitung

Ein eXpurgate-Konto beim Berliner Anbieter Eleven hat der Filteranwender schnell eingerichtet. Zum Account gehört eine E-Mail-Adresse als Ziel für Weiterleitungen. Die Mails gehen nach dem Filtern an eine oder mehrere E-Mail-Adressen des Kunden. Es handelt sich um einen reinen Weiterleitungsdienst. Ein Speichern der E-Mails erfolgt nicht, und damit stehen sie auch nicht per IMAP, POP oder Web zur Verfügung. In der Konfiguration kann man fein differenzieren, wohin welche Mail gehen soll.

Es gibt volle 16 Kategorien, in die eXpurgate die Mails einsortiert, und jede erlaubt eine gesonderte Behandlung. So kann die E-Mail-Adresse zur Weiterleitung der Mails dieser Kategorie genauso eingestellt werden wie sich Betreff- oder andere Header-Zeilen entfernen, hinzufügen oder umschreiben lassen. Üblicherweise wird man alle als „sauber“ Identifizierten an eine bestimmte Adresse, alle anderen an eine andere weiterleiten. Die Sortierung kann aber auch beim Ziel der Weiterleitung anhand von Betreff- oder anderer Header-Zeilen erfolgen. Der wahlweise integrierte – bei den kostenpflichtigen Lösungen für Unternehmenskunden optionale – Virenscanner und die hilfreichen Statistiken runden das kostenlose Angebot ab.

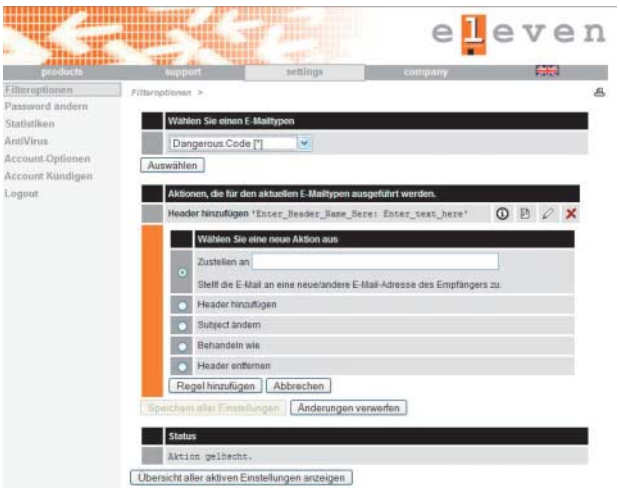
Antispameurope: Webmail inklusive

Auch Antispameurope-Kunden eröffnen ein Konto mit eigener E-Mail-Adresse, an das die E-Mails gesendet werden können. Nach dem Filtern stehen die E-Mails in einer Weboberfläche klassischer Bauart zur Verfügung. Diese Oberfläche wies bis zum Test im Rahmen des vorliegenden Artikels einige

Sicherheitslücken auf, die der Anbieter jedoch innerhalb weniger Stunden beheben konnte.

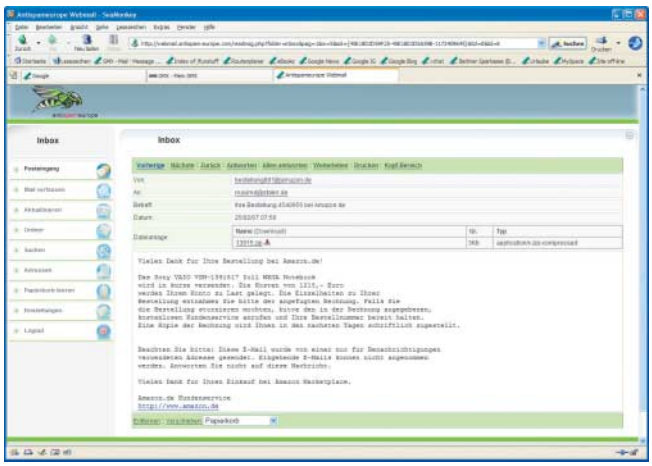
Weniger Spam heißt mehr Fehlalarme

Alternativ können Kunden die E-Mails per POP3 oder IMAP4 abholen. Dabei fällt auf, dass zwar eine verschlüsselte Verbindung zum Einsatz kommt, das vom Anbieter eingesetzte Zertifikat allerdings ein selbst unterschriebenes aus der Distribution des eingesetzten Mailservers ist. Die entsprechenden Warnmeldungen muss der Nutzer akzeptieren. Die Weboberfläche ist übersichtlich und funktional. Einstellungen für die Filterung und den Umgang mit den gefilterten Mails sucht man vergeblich. Es gibt die Möglichkeit, Ordner zu erstellen, allerdings können E-Mails nicht nach selbst zu bestimmenden Kriterien dort hineinsortiert werden. Spam und Viren stellt Antispameurope nicht zu, sondern stattdessen einmal täglich eine Liste der zurückgehaltenen E-Mails. Mit deren Hilfe lassen sich per Klick die Mails aus der Quarantäne entfernen. Das Angebot von Antispameurope wird nach einem Monat kostenpflichtig (ab 4,99 € pro Monat).



eXpurgate-Anwendern stehen diverse Filter-Optionen zur Verfügung (Abb. 1).

Nach einem überzeugenden ersten Eindruck schnitt eXpurgate auch bei der Filterwirksamkeit sehr gut ab und erkannte über 98 Prozent der Spam-Mails (112 False Negatives). Noch weniger Spam-Mails (27) ließ Antispameurope während des Testzeitraums durch. Während der Zählung der Trefferquoten kam leider kein Virus an, aber in einem vorherigen Test der Konfiguration fielen bereits aussagekräftige Daten an. Hier hatte eXpurgate klar die Nase vorn und erkannte sogar Viren, die bis dahin noch kein Virenscanner auf dem Radar hatte. Die Technik von Eleven kann Malware-Ausbrüche schon im Frühstadium erkennen, indem sie die zahlreichen Mails



Elevens eXpurgate untersucht den Mail-Datenstrom an Millionen von Accounts laufend auf Malware-typische Muster und kann auf diese Weise umgehend vor Würmern und Trojanern warnen. Sowohl Antispameurope als auch GMX waren in diesem Fall langsamer (Abb. 2 und 3).

an die Kunden-Accounts auf entsprechende Muster hin auswertet. Antispameurope erkannte neue Viren erst mit der von AV-Scannern bekannten Verzögerung, dann aber ebenso zuverlässig. Die Früherkennung hat der Anbieter inzwischen nach eigenen Angaben verbessert.

Spam-Mails im Posteingang (False Negatives) sind ärgerlich, schwerer wiegen allerdings die als Spam eingestuften E-Mails, die der Empfänger eigentlich hätte bekommen müssen (False Positives). Hier ist Antispameurope im Nachteil: Sechs E-Mails hielt der Filter zurück (jeweils Newsletter), die eigentlich erwünscht gewesen wären. Nur eine einzige erwünschte E-Mail schaffte den Weg zu Eleven erst gar nicht, weil sie wegen eines vorübergehenden Konfigurationsfehlers abgewiesen wurde. Das hätte ein potenzieller Absender per Unzustellbarkeitsbenachrichtigung (NDR) erfahren. Alle anderen kamen durch.

Nicht selten sind Zustellbenachrichtigungen von Postmaster, MAILER-DAEMON et cetera (Bounces) selbst Objekte der Weiterleitung. Sie sind nur dann als Spam einzustufen, wenn sie selbst als Antwort auf Spam entstehen, der vorgeblich von der eigenen Mail-Adresse ausging. Im Test wurden alle Bounces und ähnliche System-Mails gesondert betrachtet. Bei Antispameurope war das Bounce-Management aktiviert: Fast alle (163 von 166) Mails dieser Art filterte das System aus, weil es zuvor keine passenden abgehenden Mails registriert hatte. Eleven sah 57 Bounces als Spam an.

Beim Bearbeiten der Mails lieferten beide Kandidaten gelegentlich Fehlermeldungen. eXpurgate gab 52-mal aus, dass der Mailserver die maximale Anzahl von Prozessen erreicht habe. Antispameurope meldete 8479-mal, dass der Mailserver keine neuen Verbindungen annimmt. Hier griff laut Anbieter eine nur für Weiterleitungs-Accounts eingerichtete Limitierung.

Der zum Vergleich mitlaufende Filter von Brightmail war von den Werten und Möglichkeiten her fast völlig identisch mit dem System von Eleven. Anzumerken bleibt, dass ein Filter umso wirksamer arbeiten kann, je näher er in der SMTP-Zustellkette am Spammer angesiedelt ist. Wer also seinen MX von Eleven oder Solidsystems betreiben lässt, darf mit noch besseren Filterergebnissen rechnen als bei der in diesem Test eingesetzten einfachen Weiterleitung – und damit auch als bei lokalen, nur im eigenen Unternehmen eingesetzten Filtersystemen.

Fazit

Da beide Anbieter unterschiedlich pro Disziplin abgeschnitten haben, gibt es keinen klaren Sieger. Wer sehr viel Spam bezieht, durchschnittliche Virus- mit hervorragender Spam-Erkennung benötigt und dafür ein gewisses False-Positive-Risiko bei Newslettern in Kauf zu nehmen bereit ist, findet bei Antispameurope für 4,99 € im Monat eine Alternative zum Aufgeben der E-Mail-Adresse. Wer keine False Positives akzeptiert, eine exzellente Virus-Erkennung und sofortige Zustellung bevorzugt, wird eher einen kostenlosen Account bei Eleven eröffnen. (un)

CHRISTOPH PUPPE

ist Security Consultant bei der HiSolutions AG in Berlin, CISSP und seit mehreren Jahren als Berater tätig.

Daten und Preise

Antispameurope

Hersteller: Solidsystems, Hannover, www.antispameurope.de

Preise: Weiterleitungs-Account ab 4,99 €/Monat (30-Tage-Test kostenlos), 100er-Lizenz 2952 €/Jahr

⊕ besonders wirksame Spamfilterung

⊖ einige Fehlalarme bei Newslettern

eXpurgate 2.0

Hersteller: Eleven, Berlin, www.eleven.de

Preise: Weiterleitungs-Account für private Zwecke kostenlos, 100er-Lizenz 1598 €/Jahr

⊕ sehr geringes False-Positive-Risiko

⊕ Malware-Früherkennung

Filterergebnisse vom 24. bis 28. Mai 2007

	eXpurgate 2.0	Antispameurope	Brightmail	manuell
fehlende Ham[1]	1	–[2]	1	0
fehlende Spam[1]	2	–[2]	8	0
fehlende Bounces[1]	0	–[2]	3	0
Erkennung				
Spam als Spam	5546	5633	5548	5660
Ham als Spam	0	6	0	0
Ham als Ham	147	142	147	148
Spam als Ham	112	27	104	0
Bounces als Spam	57	163	55	0
Bounces nicht als Spam	109	3	108	166

[1]Einige Mails ließen sich nicht weiterleiten, siehe Text. [2]Antispameurope hat nur erwünschte Mails (Ham) zugestellt.