network Computing

IT-SICHERHEIT: SPAM-FILTER

Praxis - Mit Black-Lists Spam-E-Mails effizient eliminieren

Von: Stefan Rubner / bre

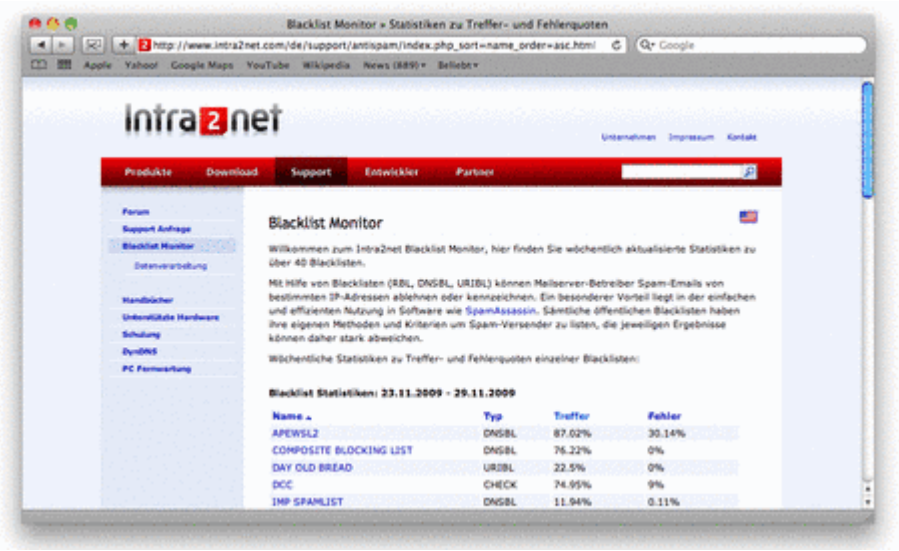
Durch den Einsatz von Black-Lists im lokalen Spamfilter lässt sich Spam mit vergleichsweise geringem Aufwand drastisch reduzieren. Doch nicht alle Black-Lists arbeiten gleichermaßen zuverlässig. Eine Lösung der deutschen Firma Intra2Net filtert dagegen mehr als 99 Prozent der unerwünschten Nachrichten aus.

Spam in seinen unterschiedlichen Ausprägungen ist nach wie vor eines der größten Probleme, mit denen sich IT-Administratoren herumschlagen müssen. Dabei verlassen sich die meisten IT-Fachleute auf lokale Spamfilter wie beispielsweise Spam Assassin, machen aber gerne einen großen Bogen um externe Black-List-Dienste.

Der Grund dafür ist, dass diesen schwarzen Listen ein zweifelhafter Ruf vorauseilt. Meist erfolgt der »Erstkontakt« mit einer Black-List, weil der eigene Mailserver auf einer solchen gelandet ist und man sich nun damit herumschlagen muss, wieder von der Liste herunter zu kommen, um Mail zu versenden. Dabei könnte gerade der sinnvolle Einsatz von Black-Lists dabei helfen, gar nicht erst auf einer zu landen.

Drei Typen von Black-Lists

Generell existieren drei unterschiedliche Arten von Black-Lists: Die bekannteste sind die **DNS-Black-Lists** (DNSBL). In diesen finden sich die IP-Adressen von Systemen, die bekanntermaßen Spam versenden. Die Abfrage erfolgt über das DNS-Protokoll. Das sorgt zum einen für eine schnelle Bearbeitung von Anfragen und ermöglicht es zudem, Systeme auch schnell wieder von der Liste zu entfernen.



Dass gute Trefferraten nicht alles sind, zeigt der Black-List-Monitor von Intra2net eindrucksvoll.

Eine zweite Variante sind **Hash-Black-Listen**. Diese dienen dem Vergleich von Mail-Inhalten. Sie eignen sich besonders dafür, um beispielsweise von einem Bot-Netz ausgelöste Spam-Wellen zu erkennen. Bei einem solchen Angriff sendet eine große Anzahl von Rechnern, die zuvor mithilfe von Malware gekapert wurden, dieselbe Spam-Nachricht an Millionen von Empfängern.

DNSBL ist nicht gut genug, um solchen Attacken abzuwehren. Der Grund: Bot-Netz-Betreiber können immer neue Computer und damit ständig wechselnde IP-Adressen zum Versand verwenden. Da sich jedoch die eigentliche Nachricht nicht wesentlich ändert, greifen Hash-Black-Lists und sorgen dafür, dass auch Spam von bislang »unbescholtenen« Systemen frühzeitig erkannt wird.

Die **dritte Kategorie der Black-Lists** bilden diejenigen, die nach im Nachrichtentext enthaltenen URLs entscheiden, ob es sich bei einer Nachricht um Spam handelt. Denn oft führen die in den Spam-Mails enthaltenen Links zu bekannten Seiten, die Werbung enthalten, im schlimmsten Fall aber der Verbreitung von Schadsoftware dienen.

Performance von Black-Lists abhängig von der Pflege

Aus diesen Unterschieden wird ersichtlich, dass eigentlich nur der kombinierte Einsatz verschiedener Black-Lists zum erwünschten Ziel führt, nämlich der Reduzierung des Spam-Aufkommens. Dabei gibt es jedoch ein kleines Problem: Zwar existieren mittlerweile viele, teils kommerzielle, teils kostenlos nutzbare Black-Lists, die sich relativ einfach in den eigenen Mailserver einbinden lassen.

Allerdings gilt bei Black-Lists Ähnliches wie bei einem Viren-Scanner: Das Produkt ist nur so gut wie die Pflege, die es erfährt. Ein drastisches Beispiel ist beispielweise eine DNSBL, die IP-Adressen nicht täglich aktualisiert.

Denn Spam-Wellen haben in der Regel eine »Lebensdauer« von nur wenigen Stunden. Wer selten aktualisierte Black-Lists verwendet, setzt sich daher zum einen der Gefahr aus, Spam von mittlerweile betroffenen Servern zu akzeptieren und im schlimmsten Fall weiter zu verbreiten. Zum anderen werden aber auch E-Mails von nicht mehr betroffenen Systemen fälschlicher Weise nicht mehr akzeptiert.

Ein weiteres Problem sind die so genannten False Positives. Eine zu aggressiv arbeitende Black-List sorgt in diesem Fall dafür, dass eigentlich unbedenkliche Nachrichten als Spam erkannt und entsorgt oder zumindest in den Spam-Ordner verschoben werden.

Das mag bei privaten Anwendern noch akzeptabel sein, die nicht allzu viele E-Mails erhalten. Im Business-Umfeld ist es das mit Sicherheit nicht. Wer will schon seinem Chef erklären, dass eine wichtige Kooperation nicht zustande kam, weil die Nachricht dazu im Spam-Ordner landete und nicht rechtzeitig gefunden wurde?

Kurz gesagt sind die Anforderungen an eine Black-List, dass sie

- möglichst viel Spam als solchen erkennt und
- keine echten E-Mails als Spam klassifiziert.

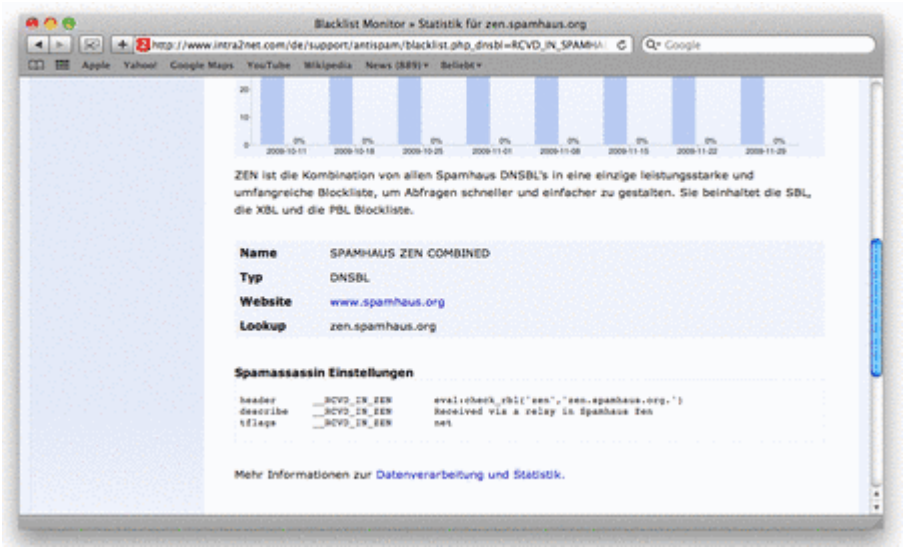
Doch wie beurteilt man als Endnutzer, ob das bei einer Black-List wirklich der Fall ist? Und wenn man das weiß, wie bindet man die Black-List in das eigene Mailsystem ein?

Black-List-Monitor checkt die Schwarzen Listen

Einen interessanten Ansatz hat das deutsche IT-Security Unternehmen Intra2net entwickelt. Als Anbieter der »Intranator«-Appliance wollte die Firma ihren Kunden einen möglichst sicheren und gleichzeitig effektiven Spamfilter anbieten.

Im Rahmen eines Forschungsprojektes mit der Hochschule Furtwangen, bei dem neue Methoden der Spam-Filterung untersucht wurden, entstand – quasi als Nebenprodukt – der »Black-List Monitor«. Dabei handelt es sich um ein ständig aktualisiertes System, das die Effizienz diverser Black-Lists anhand mehrerer »echter« Mail-Datenströme misst.

Die Ergebnisse sind hoch interessant. So bescheinigt Intra2net dem renommierten Anbieter Spamhaus sehr gute Ergebnisse, mit einer Spam-Erkennungsrate von bis zu 97 Prozent. Andere Black-List-Betreiber sehen dagegen ganz und gar nicht gut aus.



Die Einstellungen, die zum Einbinden einer Black-List in Spam Assassin notwendig sind, liefert der Black-List-Monitor in der Detailansicht.

Dass die ermittelten Werte nicht aus der Luft gegriffen sind, lässt sich mithilfe eigener Tests leicht nachvollziehen. Zwar weichen, abhängig von Menge und Art des Mail-Aufkommens, die Ergebnisse hier und dort um den einen oder

anderen Prozentpunkt ab. Insgesamt ist aber belegbar, dass die vom Black-List-Monitor ermittelten Werte ziemlich genau das Ergebnis widerspiegeln, das lokal auf dem eigenen Mail-Server erreichbar ist.

Doch damit nicht genug. Der Black-List-Monitor gibt nicht nur Aufschluss über die Wirksamkeit der einzelnen Listen. Zusätzlich bietet er auch einen attraktiven Service für Mail-Verantwortliche: Zu jeder vom Monitor überwachten Black-List liefert Intra2net auch die notwendigen Konfigurations-Einstellungen, die zum Einbinden in Spam Assassin notwendig sind. Gerade für E-Mail-Verantwortliche ist das eine unschätzbare Arbeitserleichterung.

Verhaltensbasierte Analyse

Noch einen Schritt weiter gingen die Entwickler bei Intra2net bei ihrem eigenen Produkt, dem Intranator. Aktuell ist die Appliance in der Version 5.2.1 verfügbar. Sie bietet im Vergleich zu herkömmlichen Systemen einen geradezu radikalen Ansatz zur Spam-Bekämpfung.

Während die meisten Systeme nach wie vor hauptsächlich auf bayesische Filter zur Bewertung der Mail-Inhalte setzen, ist diese Methode beim Intranator nur eines, aber nicht mehr das wichtigste Kriterium zur Ermittlung von Spam.

Anstatt, wie bei bayesischen Filtern üblich, die Häufigkeit bestimmter Schlüsselwörter und Phrasen sowie deren Relation zueinander aufwändig zu analysieren, setzt der Intranator auf ein System, das sich am besten als verhaltensbasiert beschreiben lässt.

Nachrichtentext und Empfänger als Kriterien

Das Verfahren geht davon aus, dass sich die meisten Mails anhand einfacher Kriterien recht genau als Spam klassifizieren lassen. Wie zu erwarten, sind Black-Lists dabei ein wichtiges Hilfsmittel. Zum einen liefern sie die Information, ob ein Absender einer Nachricht ein bekannter Spammer ist.

Zusätzlich erlauben sie es, mithilfe einer unscharfen Hash-Überprüfung grob festzulegen, ob der Nachrichtentext eventuell eine Spam-Nachricht ist. Und letztlich dient auch der Empfänger einer Nachricht als Kriterium.

Mit einer Spam-Filterquote von über 99 Prozent ohne False Positives sorgt die Intranator-Appliance Pro für eine zuverlässige E-Mail Kommunikation.

Bei der Spamabwehr stehen dem System zwei unterschiedliche Filterstufen zur Verfügung. Zunächst kommt der Standard-Modus zum Einsatz. Dieser erzielt schon recht hohe Trefferraten, ist aber darauf ausgelegt, im Zweifelsfall eher eine Spam-Nachricht zu viel in den Posteingang durch zu lassen, anstatt fälschlicher Weise erwünschte Mail in den Spam-Folder zu verschieben.

Während der Standard-Modus aktiv ist, analysiert der Intranator die empfangenen Mails hinsichtlich ihrer technischen Merkmale des Transportweges und entscheidet nach einer gewissen Zeit, ob in den leistungsstarken Modus gewechselt werden kann.

Dieser erhöht die Trefferrate nochmals deutlich. Bei einem Test, den wir mit der Intra2Net-Lösung durchführten, lag sie konstant über 99 Prozent, und das, ohne False Positives zu erzeugen.

Erkennungsquote von über 99 Prozent

An diese Werte wird man mit Systemen im Eigenbau nur schwerlich heran reichen, selbst wenn die Informationen aus dem Black-List-Monitor zum Einsatz kommen. Trotzdem lassen sich auch mit seiner Hilfe beachtliche Verbesserungen der eigenen Trefferrate erzielen.

Das einzige, was dem Mail-Administrator noch fehlt, ist ein Proxy-Service, der sich direkt aus dem eigenen Mail-System ansprechen lässt und die laut Black-List-Monitor jeweils optimale Black-List-Kombination zur Spamfilterung verwendet. Oder eben doch eine Intranator-Appliance.