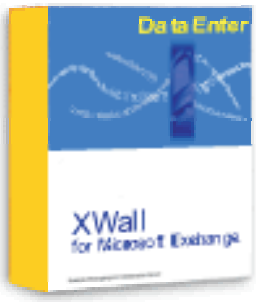
Spam Bekämpfung beim CCC[1)]

Werner Illsinger



Der CCC hat schon seit längerer Zeit (wie vermutlich alle anderen Betreiber von Mail Diensten) das Problem, dass die unerwünschte Zusendung von E-Mails an die Clubmitglieder überhand nimmt. Ich habe versucht das Problem in den Griff zu bekommen und habe dabei verschiedenste Lösungen evaluiert. Dabei bin ich auf XWALL gestoßen. XWALL ist eine Mail-Firewall, die auch zur Spam-Bekämpfung eingesetzt werden kann.

SMTP Blocking

XWALL ist eine Firewall Lösung, die für Microsoft-Exchange entwickelt wurde, aber grundsätzlich mit jedem SMTP basierten Mailserver zusammenarbeiten kann. XWALL klemmt sich dabei zwischen den Mail-Server und das Internet und kann damit jede ein- oder auch ausgehende Mail analysieren.

XWALL kann unter Windows 2000 als Applikation (Benutzer muss am System angemeldet sein) oder auch als Service (wird automatisch beim Booten im Hintergrund gestartet) betrieben werden.

Die Konfiguration von XWALL wird über eine graphische Benutzeroberfläche den sogenannten „XWALL-Admin“ durchgeführt. XWALL bietet verschiedene Ansatzpunkte zur Spam Bekämpfung:

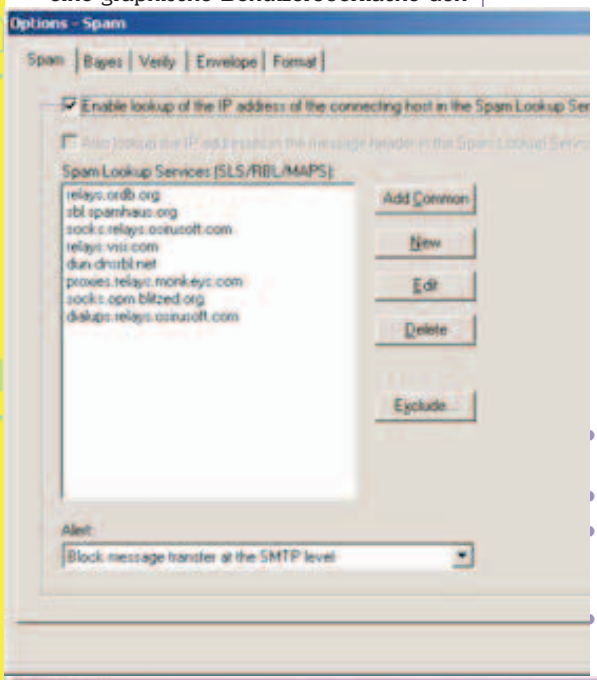
SMTP Blocking

Dabei können bestimmte IP-Adressen oder -Bereiche in eine Sperrtabelle eingetragen werden. Dabei wird keinerlei Mail mehr von diesen Adressen angenommen. Diese Methode bietet sich an, wenn eine bestimmte Site Probleme macht und man das System komplett dagegen abschotten möchte.

SPAM Lookup Service (SLS)

Unter ***Options SPAM*** im XWALL-admin findet man die Möglichkeit zur Konfiguration sogenannter *Spam Lookup Services*. Das sind im Internet betriebene Datenbanken in denen nach verschiedenen Kriterien *Spam Sites* gelistet werden. XWALL kann konfiguriert werden, welche SLS es verwenden soll.

Im nachstehenden Bild ist unsere derzeitige Konfiguration abgebildet. Wir verwenden einige Listen, die sogenannte *Open Relays* im Internet listen und auch solche, die *Proxy Server* listen, über die im Internet ohne Anmeldung Mails verschickt werden können. Wir haben davon Abstand genommen, Listen zu verwenden, die *Spam Sites* im Allgemeinen listen, weil diese sehr oft zu restriktiv sind und oft auch große Provider gelistet sind, weil einige deren Kunden Spam verschicken.



Die Erstkonfiguration dabei ist sehr einfach. Man hakt die Option *„Enable lookup of the IP addresses of the connectiong host in the SLS database“* an. Dann drückt mann den Button *“Add Common”* und schon läuft die Sache. Mann kann dann nach Belieben die entsprechenden Listen hinzufügen oder auch weglassen.

Man kann dann als Nächstes bestimmen, was passieren soll, wenn eine Mail von einer Site kommt, die im SLS gelistet ist. Die Optionen sind:

- Transfer auf SMTP-Level verhindern
- Nachricht verwerfen.
- Betreff der Nachricht markieren und Nachricht an Empfänger senden.
- Nachricht an Administrator weiterleiten.

Man übrigens leicht überprüfen ob, eine IP-Adresse eines Mail-Servers in einem der vielen SLS gelistet ist (`http://relays.osirusoft.com/cgi-bin/rbcheck.cgi`).

Die SLS funktionieren technisch mittels Domain-Name-Servern, in die die Spam-Server eingetragen werden. Die Abfrage von XWALL funktioniert damit ebenfalls mittels des DNS-Protokolls.

Bayes Filter

Als zweite Option unterstützt XWALL sogenannte *Bayes Filter*.

Bayes'sche Filter sind “lernend”. Der Algorithmus berechnet anhand der in der E-Mail enthaltenen Wörter die Wahrscheinlichkeit, dass es sich um eine *Spam-Mail* handelt. Grundlage für die Berechnung sind Worthäufigkeiten in bereits vom Benutzer klassifizierten E-Mails. Dieser bewährte Ansatz zum Textfiltern gilt derzeit als wirkungsvolle Methode, unerwünschten E-Mails den Garaus zu machen, da er es den Spammern — anders als die statischen Filter — erschwert, auf Regeln mit Anpassungen zu reagieren.

Zusätzliche Möglichkeiten

XWALL bietet die Möglichkeit auch „gewöhnliche Prüfungen“ vorzunehmen. Zum Beispiel zu verifizieren, ob die Absender-Domain gültig ist (damit scheiden Nachrichten mit nicht existierenden Absender-Domains aus (z.B. `hugo@xyzabz.at`)).

Es kann natürlich auch nach bestimmten Texten in Betreff oder Text der Nachricht gesucht werden (z.B. „Viagra“) und mit der Nachricht entsprechend verfahren werden.

Andere Features von XWALL ist es, ein und/oder ausgehende Mails mittels externen Virenscanner auf Viren überprüfen zu lassen.

Zusammenfassung

XWALL ist ein sehr gutes Mail-Firewall-Produkt von einem österreichischen Hersteller (Firma Dataenter) zu einem sehr guten Preis (ca. 340 Euro incl. MWSt.). Es gibt regelmäßig (gratis) Updates für die Software und unter den Referenzen sind namhafte Firmen wie Bank Austria, Erste Bank oder die US Army um nur einige zu nennen.

Weitere Informationen und auch online Bestellung unter
`http://www.dataenter.co.at`

1) Die Mail-Server des CCC werden von CCC- und PCC-Mitgliedern gemeinsam genutzt. (Domains ccc.at, pcc.ac, iam.at, pcnews.at und zahlreiche private Domains von Clubmitgliedern.