Spam Bekämpfung und Virenschutz

Werner Illsinger

Spam ist ein leidiges Problem. Längst hat die Zahl der Spam-Mails die Anzahl der sinnvollen Mails übertroffen. **CC|Communications** versucht jedoch das Problem für die Anwender möglichst klein zu halten. Die in diesem Bericht beschriebenen Verfahren treffen für alle Mitglieder zu, die E-Mail-Adressen im Verwaltungsprogramm Helm konfigurieren (kostenloser Mitgliederwebspace oder Hosting-Paket).

Virenschutz

Am Mailserver ist F-Prot (www.f-prot.com) von Frisk im Einsatz. Ein automatischer Dienst wacht darüber, dass immer die aktuellen Versionen der Virensignaturen im Einsatz sind. Mails, die ein Virus enthalten werden am Server gelöscht.

Mailenable *Catch All*

Es ist empfehlenswert, beim Setup der Mail-Accounts in Helm darauf zu achten, dass die Mailbox nicht als „*catch all*"-Mailbox eingerichtet ist. Was bedeutet „*catch all*"? In diesem Fall wird in diese Mailbox jegliche E-Mail an nicht existierende E-Mail Adressen dieser Domäne zugestellt; d.h. falls irgendwas@domain.at nicht existiert, werden E-Mails an diese Adresse trotzdem an die „*catch all*"-Adresse zugestellt. Da Spammer ihre Botschaften oft an irgendwelche E-Mail Adressen senden, handelt es in diesen Fällen eben meist um Spam. In Helm ist diese Option unter ***Domains*** -> **<Domain>** -> ***e-Mail Accounts*** zu finden. Einfach das Hakerl entfernen, schon hat man weniger Spam.

Blockieren von Spam-Nachrichten am Server

Am Server werden bereits einige Maßnahmen durchgeführt, die Nachrichten komplett blocken. Diese Maßnahmen sind:

SPF *(Sender Policy Framework)*

Nachrichten, die von einer Domäne kommen, die SPF einsetzt – und wo der Name des Mailservers nicht mit einem per SPF erlaubten Mail-Server übereinstimmt - werden nicht angenommen (siehe www.openspf.org). Wenn Sie Spam von Ihrer eigenen E-Mail-Adresse bekommen, bzw. sich jemand bei Ihnen beschwert, dass SPAM mit Ihrer E-Mail Adresse versendet wird, können wir SPF gerne auch für Ihre Domain einrichten.

Open Relays

Nachrichten, die von bekannten *Open Relays* (Mail Server im Internet, die von jedermann E-Mails zum Versand annehmen) kommen, werden geblockt. Hier wird eine Reihe von Sperrlisten verwendet.

SURBL *(Spam URI Realtime Blocklists)*

Nachrichten, die URL's enthalten, die in der SURBL-Sperrliste enthalten sind, werden nicht angenommen (siehe www.surbl.org) .

Greylisting

Diese Methode blockt zwar keine Mails ist aber recht effektiv. Mails werden beim ersten Versuch abgelehnt und erst beim zweiten Versuch erlaubt. Da Spamserver oft nur einmal versuchen, eine Spam-Mail zu versenden, werden hier viele Mails einfach nicht zugestellt. Es kann durch Greylisting aber vorkommen, dass der Absender eine Warnung über eine Verzögerung bei der Zustellung erhält (siehe www.greylisting.org)

Wir verwenden diese Methoden relativ zurückhaltend, um so genannte *False Positives* zu vermeiden, also Mails, die als Spam geblockt werden, aber legitime E-Mails sind.

Markierung von Nachrichten

Die Mails werden beim Empfang von unserer Spamengine gescannt und nach verschiedenen Gesichtspunkten bewertet und danach markiert. Dies geschieht, damit echte Mails nicht versehentlich als Spam gelöscht oder nicht durchgelassen werden. So kann der Benutzer selbst entscheiden, ob er eine Nachricht löscht, in einen eigenen Ordner verschiebt, oder auch beibehält. Die Markierungen bedeuten:

[SPAM?] Die Nachricht scheint aufgrund der Inhalte oder Beschaffenheit der Mail eine Spamnachricht zu sein

[SPAM-B?] Nachrichten mit leerem (blank) Nachrichteninhalt (meist Nachrichten, die nur eine Grafik beziehungsweise sehr wenig Text enthalten) werden so gekennzeichnet. Es werden oft Spam-Nachrichten versendet, die nur aus einer Grafik bestehen. Der Nachrichtentext ist in der Grafik enthalten. So soll verhindert werden, dass Spam-Engines den Inhalt der Nachricht prüfen können.

[SPAM-G?] Ein GAP-Filter kalkuliert Zwischenräume zwischen Grafiken und Text.

[SPAM-L?] Absender der Mail befindet sich auf einer händisch gewarteten Blacklist.

Sollten wichtige E-Mails fälschlicherweise als Spam gekennzeichnet werden, senden Sie bitte eine E-Mail an support@ccc.at mit einer Erklärung und der Nachricht als Weiterleitung. Wir werden den Sender der Nachricht dann entsprechend in eine Whitelist eintragen – damit ist er von der Filterung automatisch ausgenommen.

Verschieben von Mails mit Spamverdacht

Um als spamverdächtig markierte E-Mails in einen eigenen Ordner verschieben zu lassen, wählen Sie im Mailenable-Webmail den Punkt ***Optionen*** aus der Menüzeile, dann den Menüpunkt ***Filter***. Um eine neue Regel hinzuzufügen, wählt man den Punkt ***Hinzufügen***.

Als Filterbeschreibung wählt man einen treffenden Begriff. In unserem Fall wurde ***„Spamverdacht"*** gewählt. Es sollen alle Nachrichten, die das Wort ***[SPAM*** im Betreff enthalten, verschoben werden. Als Vorgang wurde ***„Move Message to Folder"*** (Nachricht in Ordner verschieben) ausgewählt. Als Ordner wird ein Ordner mit dem Namen **SPAM** ausgewählt (Dieser Ordner muss angelegt worden sein). Natürlich können hier auch beliebige andere Regeln definiert werden.

Bei Problemen

Sollten E-Mails, die Sie versenden, nicht beim Empfänger ankommen oder sollte eine E-Mail, die an sie gesendet wurde, nicht ankommen, dann ist es hilfreich, möglichst viel von der Nachricht zu wissen. Am Besten eine Kopie der Originalnachricht oder – falls das nicht möglich ist - zumindest Absendeadresse, Empfängeradresse, Betreff und möglichst genau das Sendedatum und Uhrzeit in einer E-Mail an support@ccc.at senden. Wir versuchen dann zu klären, wo das Problem liegt.

Zukunft

Da sich die Spammer immer wieder neue Möglichkeiten einfallen lassen, müssen auch die Provider ständig auf die neuen Gegebenheiten reagieren. Wir werden diesen Artikel immer den Gegebenheiten anpassen und auf http://www.ccc.at/support/ zur Verfügung stellen.