

Spam, Viren und andere Schädlinge

Letzte Aktualisierung Saturday, 2. January 2010

In diesem Artikel geht es um die serverseitige Filterung von Spam (und Phishing) und Computer-Schädlingen (Viren, Trojaner, Schadcode etc.).

Ziel der Filterung ist es, daß Spam und Viren nicht erst auf den PC's im Firmennetzwerk landen soweit diese per Mail verschickt werden. Selbstverständlich läßt sich die Virenfilterung auch auf Netzlaufwerke erweitern.

Mails mit Viren bzw. Schadcode werden heutzutage sehr oft per Mail verschickt (z. B. vor einiger Zeit ILoveyou). Die Anzahl der Spam-Mails nimmt ständig zu und die Tricks mit den die Spam-Versender arbeiten werden immer raffinierter und unverschämter.

Eine sehr gute Lösung mit Open Source bietet die Kombination "Amavisd-new, SpamAssassin und ClamAV". Voraussetzung ist ein sauber konfigurierter Mailserver (Postfix), wobei mittels Mailserver-Konfiguration bereits ein beachtlicher Teil Spams herausgefiltert werden kann.

SpamAssassin filtert die Mails mittels Spam-Filter und einem speziellem Lernverfahren. ClamAV ist ein leistungsstarker Open Source Virenschanner. Amavisd-new (AMaViS) filtert ebenfalls Mails, ist aber hauptsächlich ein Tool, daß SpamAssassin und Virenfilter über eine Schnittstelle administrierbar macht, die Einbindung vereinfacht und für effektives und performantes zusammenarbeiten der einzelnen Tools sorgt.

Es ist auch die Abweisung von Anlagen in EMail möglich. Zum Beispiel werden dann.exe, .vbs und .cmd Dateien von der EMail gekappt.

Externe Erkennungswerkzeuge (Razor, RBL) können und sollten ebenfalls per AMaViS und SpamAssassin eingebunden werden. Damit wird die Spamerkennungsrate nochmals erhöht. Die Filterregeln für SpamAssassin sollten ebenfalls erweitert werden.

Bei richtiger Konfiguration, dauerhaften Filtertraining und Filteraktualisierung kann man das Spamaufkommen auf einem Mailserver um mindestens 90% senken.

Eine 100% Erkennungsrate ist fast nicht möglich, da manche Mails sehr grenzwertig sind und die Spam-Versender immer wieder neue Tricks finden.

Die Kosten, die für eine solche Lösung entstehen ist gering. Lizenzgebühren entstehen für die genannte Software nicht.

Möchte man statt eines Open Source Virenschanners lieber einen Virenschanner der von einer Firma hergestellt und supported wird, fallen Lizenzgebühren an. Die Höhe der Gebühren hängen von verschiedenen Faktoren und dem Hersteller ab.

Es gibt auch Komplett-Lösungen von namhaften Herstellern, die Mails- und Viren filtern. Die Lösungen sind zum Teil sehr gut - der Kostenfaktor ist allerdings auch um ein vielfaches höher als eine Open Source oder Teil Open Source Lösung.

