Technische Details

Funktionsweise des Spamfilter: Greylisting

Im Webmail haben Sie die Möglichkeit mehrere vordefinierte Spamfilter zu aktivieren. Einer der beiden neuen Spamfilter ist "Greylisting". Auf Wikipedia.org ist die Funktionsweise sehr ausführlich erklärt:

Der Begriff **Graue Liste** bzw. **Greylisting** (brit.)/**Graylisting** (USA) bezeichnet eine Form der Spam-Bekämpfung bei E-Mails, bei dem E-Mail von unbekannten Absendern temporär abgewiesen und erst nach einem zweiten Zustellversuch angenommen wird.

Wird ein SMTP-Server kontaktiert, damit dieser eine E-Mail in Empfang nimmt, so sind diesem Mailserver folgende drei Daten bekannt, bevor der Mail-Server die E-Mail annehmen muss:

1. IP-Adresse des absendenden Mailservers
2. E-Mail-Adresse des E-Mail-Senders
3. E-Mail-Adresse des E-Mail-Empfängers

Wurde eine E-Mail mit dieser Kombination von Adressen noch nie empfangen, dann wird der Zustellversuch durch den SMTP-Server abgeblockt mit einer Meldung, dass ein temporärer Fehler aufgetreten sei, der SMTP-Client die Zustellung also später noch einmal versuchen soll. Wird ein nächstes Mal eine E-Mail mit der selben Kombination von Daten versucht zuzustellen (was ein regulärer und RFC-konform konfigurierter SMTP-Server auf jeden Fall tun sollte), so wird diese E-Mail (nach einem konfigurierbaren Zeitintervall) akzeptiert. Ob und wann ein erneuter Zustellversuch unternommen wird, hängt einzig und allein vom Versender ab. Es gibt auch Greylisting-Implementierungen, die die Regeln ein wenig lockern, indem z.B. die beteiligten Domains statt der E-Mail-Adressen eingetragen und überprüft werden.

Vorteile

Typische Software für den Massen-Versand von E-Mails (insbesondere Würmer oder Trojaner) versucht oft nicht, eine (Spam-)E-Mail ein zweites Mal an den selben SMTP-Server zuzustellen. Solche E-Mails werden durch „Greylisting“ erfolgreich gefiltert. Zur Zeit (Stand Oktober 2006) ist damit eine sehr effektive Spambekämpfung möglich, die den Spam auf bis zu ein Zehntel reduziert.

Anders als bei heuristischen Spam-Bekämpfungs-Verfahren geht durch „Greylisting“ im Idealfall keine E-Mail verloren.

Nachteile

Die negative Wirkung von Greylisting beschränkt sich lediglich auf eine Verzögerung der E-Mails von typischerweise 15 Minuten (je nachdem, wann es der zustellende Mail-Server erneut versucht, 5m bis 1h sind üblich). Diese negative

Technische Details

Wirkung ist in vielen Fällen eingeschränkt auf die erste E-Mail einer Kombination von Sender und Empfänger. Des Weiteren sei darauf hingewiesen, dass E-Mails keine Garantie auf umgehende Zustellung bieten können.

Leider gibt es auch einige (evtl. fehlerhafte) Mailserver-Programme, die bei temporären Fehlern keinen späteren Zustellversuch unternehmen, sondern die E-Mails trotz nicht erfolgter Zustellung verwerfen. Eine gewünschte Nachricht geht somit verloren. Für diesen Fall sollte auf jeden Fall der zuständige Mailadministrator angehalten werden, diese Schwachstelle seines Systems zu beheben. Des Weiteren bieten viele Greylisting-Implementationen eine Whitelist, die allerdings eher für legitime als für fehlerhafte Absender genutzt werden sollte, beispielsweise zum Whitelisting großer Provider wie AOL oder GMX. Der durch den hohen Anteil gefälschter Absender-Adressen wieder erhöhte Spam-Anteil kann durch Verwendung von SPF negiert werden.

Einige Mailserver-Programme generieren bereits beim ersten Versuch einer durch Greylisting abgewiesenen E-Mail einen Zustellbericht an den Absender. Dieser Bericht wird oft nicht genau gelesen bzw. nicht verstanden und somit oft als Bericht über eine endgültig fehlgeschlagene Zustellung behandelt.

Wie alle Methoden der Spambekämpfung kann Greylisting durch Weiterentwicklung der Spam-Software an Effizienz verlieren. Zur Zeit ist davon noch nicht viel zu bemerken, doch könnte z. B. ein zweiter Zustell-Versuch implementiert werden, um Greylisting zu umgehen. Dadurch benötigen Spam-Versender jedoch mehr Ressourcen und können weniger Spam pro Zeiteinheit ausliefern. Die zeitliche Verzögerung kann zudem dazu benutzt werden, Spam-Versender zu erkennen. Trotzdem ist es sinnvoll, auch andere Verfahren wie beispielsweise SPF einzusetzen.

Weiterhin ist zu beachten, dass nach Möglichkeit alle für eine Domain zuständigen Mailserver Greylisting aktiviert haben, da Spamversender bereits heute häufig direkt den – oft schlechter geschützten – MX mit der geringsten Priorität zur Einlieferung benutzen.

Bei Implementierungen auf Cluster-Servern ist zu beachten, dass die Greylist-Datenbank auf alle Serverknoten repliziert wird, da sonst der Mail-Empfang stark verzögert werden kann.

Weblinks

- http://www.greylisting.org
- Greylisting an der RWTH Aachen: http://www.rz.rwth-aachen.de/infodienste/email/greylisting.php
- Postgrey, Greylisting - Implementierung für Postfix als Policy - Server: http://isg.ee.ethz.ch/tools/postgrey/
- Greylisting mit Sendmail: http://hcpnet.free.fr/milter-greylist/
- Adding Greylisting support to qmail on Plesk 8 (deutsch): http://clausvb.de/doku_greylisting.htm

Technische Details

Danke an die Quelle dieser Erläuterung: http://de.wikipedia.org/wiki/Greylisting
Version: 20:09, 20. Jun. 2007 (5.176 Bytes) (http://clausvb.de/doku_greylisting.htm)

Eindeutige ID: #1021
Verfasser: Suleitec Support Team
Letzte Änderung: 2009-06-23 20:15