walczymy ze spamem - postfix i greylisting

24 September, 2006 (11:00) | bezpieczeństwo, debian(ized), poczta | By: vermin

W poprzednim artykule tyczącym się walki ze spamem na stacji klienckiej wspomniałem o konieczności przerzucenia ciężaru filtrowania na serwer. Ten sposób filtrowania ma niestety, jak każdy dobry kij, conajmniej dwa końce. Po pierwsze - musimy zapewnić użytkownikowi możliwość dotarcia do przesyłki, która jednak może spamem nie być (false positives), po drugie wszystkie wiadomości i tak są wrzucane na serwer - czyli mamy zajęte pasmo oraz przestrzeń dyskową.

Metodą, która pozwala obejść te minusy jest graylisting. Działa on w sposób bardzo prosty, wykorzystując sposób działania serwerów SMTP oraz typowe zasady działania spamerów. Serwery SMTP próbują przesłać wiadomość 'do skutku', to znaczy jeśli sesja SMTP nie powiedzie się przy pierwszej próbie, po chwili (równej zazwyczaj długości kolejki i interwałowi jej opróżniania - wiadomość na serwerze wysyłającym przesuwana jest na koniec kolejki przy niemożności dostarczenia), próbują ponownie. Spamerzy zazwyczaj nie wysyłają wiadomości ponownie i ignorują kody błędów. Oznacza to, że jeśli przy pierwszej próbie wysłania nowej wiadomości serwer specjalnie odpowie kodem błędu, to "za chwilę" ta wiadomość jednak do niego dotrze. Jak każda metoda, także ta ma pewne minusy - pierwszym i podstawowym jest zgoda zarządu na jej wprowadzenie - niektóre firmy nie chcą/nie mogą pozwolić sobie na opóźnienia w przyjmowaniu poczty. Ponadto ze względów organizacyjnych wprowadza się często adres publiczny, na który może przychodzić niezamówiona oferta handlowa. Drugim powodem, techcznicznym, jest dodanie kolejnego punktu, gdzie może pojawić się problem w sposobie działania serwera pocztowego. Trzecim, także technicznym problemem są sytuacje, gdy serwer po uzyskaniu kodu 450 zaprzestaje prób i raportuje problem z wysłaniem wiadomości - niestety takie rzeczy także się zdarzają.

Sposobem na zminiminalizowanie opóźnień w kontaktach z partnerami biznesowymi jest stworzenie listy ich domen pocztowych i dodanie ich do białej listy domen, które nie będą poddawane graylistingowi. Oczywiście, jeśli nie jest wprowadzony SPF pozwalający na jako-taką weryfikację adresu nadawcy, to każdy kto wstawi sobie adres domeny z białej listy będzie mógł przesłać spam na nasz serwer pocztowy... Implikuje to niestety także konieczność zastosowania także innych metod walki ze spamem.

To tyle tytułem przydługiego wstępu o samej metodzie, w końcu warto jednak dać odpowiedź na temat - czyli jak dodać graylisting do naszego postfixa? Za przykład posłuży oczywiście mój ulubiony debian i jego pakiet postgrey - o którym warto poczytać na stronie autora. Paczki postgrey są dostępne także dla gentoo, fBSD oraz Fedory.
Jego instalacja jest prosta - komenda *aptitude install postgrey* spowoduje zainstalowanie dwóch pakietów *libberkeleydb-perl* oraz *postgrey*. Automatycznie po instalacji wstaje demon postgrey umiejscawiający się na porcie tcp 60000. Port oraz interfejs (domyślnie localhost) możemy zmodyfikować w */etc/default/postgrey*. Możemy tam także zmodyfikować komunikat pojawiający się wraz z błędem 450 - wystarczy do opcji dodać parametr *–greylist-text*. Najprostsza część instalacji za nami.
Teraz musimy w */etc/postfix/main.cf* dodać do *smtpd_recipient_restrictions* część *check_policy_service inet:127.0.0.1:60000*. Warto zastanowić się po jakich regułach dodamy tą wartość. U mnie występuje ona po *permit_mynetworks, permit_sasl_authenticated* co pozwala ominąć greylisting dla wysyłających z moich sieci oraz dla użytkowników zautentykowanych.

Po restarcie postfixa mamy już działający greylisting - jak teraz jednak dopuścić pracę bez graylistingu dla konkretnych domen oraz adresów? Odpowiednie pliki znajdują się w */etc/postgrey* - są to odpowiednio whitelist_clients (częściowo zapełniony) oraz whitelist_recipients.

Na koniec ciekawostka - ze względu na te pliki właśnie, postgrey znajduje się także w repozytorium volatile...

« walczymy ze spamem na stacji klienckiej

walczymy ze spamem - postfix, spamassasin, clamav i amavisd-new »

Write a comment

OpenID

Sign in with your OpenID ?

Anonymous

Name:

E-mail:

Website:

Comment:

Submit

Drogi czytelniku!

Zapraszam Cię do lektury mojego bloga. Jeśli to co tu znajdziesz spodoba Ci się lub nie, masz jakieś pytania odnośnie treści lub też chciałbyś uzupełnić moje wpisy - gorąco zapraszam do komentowania.

Recent Posts

- organizacyjne
- Excel 2007 i Ctrl-C Ctrl-V
- Premiera Windows 2008, SQL Server 2008 oraz VS2008
- Dobrymi chęciami... traci się klientów
- Smycz

Tags

Archives

- March 2008
- January 2008
- December 2007
- November 2007
- May 2007
- April 2007
- March 2007
- February 2007
- January 2007
- December 2006
- November 2006
- October 2006
- September 2006
- August 2006
- July 2006
- June 2006
- May 2006
- April 2006
- March 2006
- February 2006
- January 2006
- November 2005
- October 2005
- September 2005
- August 2005

Recent Comments

- fraco on outlook nie wysyła wiadomości ze skrzynki nadawczej
- Mariusz Kędziora on Premiera Windows 2008, SQL Server 2008 oraz VS2008
- vermin on Premiera Windows 2008, SQL Server 2008 oraz VS2008
- Mariusz Kędziora on Premiera Windows 2008, SQL Server 2008 oraz VS2008
- vermin on Premiera Windows 2008, SQL Server 2008 oraz VS2008

Most Rated

- Wordpress update - 0 votes
- Happy New Year 2008! - 0 votes
- Windows Server 2008 QUIZ - 0 votes
- Smycz - 0 votes
- Dobrymi chęciami… traci się klientów - 0 votes
- Premiera Windows 2008, SQL Server 2008 oraz VS2008 - 0 votes
- Excel 2007 i Ctrl-C Ctrl-V - 0 votes
- organizacyjne - 0 votes

Highest Rated

- Wordpress update
- Happy New Year 2008!
- Windows Server 2008 QUIZ
- Smycz
- Dobrymi chęciami… traci się klientów
- Premiera Windows 2008, SQL Server 2008 oraz VS2008
- Excel 2007 i Ctrl-C Ctrl-V
- organizacyjne

blogi

- BigoBlog
- fascik homesite

Ktos o IT
Leniuch
RobD
smyru's squated bits

debian
Debian Administration
Ubuntu Blog

programowanie
Faboulous Adventures in Coding

rozrywka
Daily Dilbert
Nerd Quiz
Nerd Quiz PL
UF daily

windows
2k3 r2
EvolutiOn
IT Blog
Jesper Johanson
W-files
You had me at EHLO