

## Kontrolowanie spamu

# Ochrona i kontrola

Na pewno otrzymujecie pocztę, której ani nie oczekiwaliście, ani nie chcecie. Wszyscy spędzamy mnóstwo czasu przekopując setki zbędnych wiadomości?

Czas wezwać brygadę antyspamową.

**RICHARD IBBOTSON**

Ilość tzw. UCE (z ang. Unsolicited Commercial Email) czy też, jak większość z nas je nazywa – spamu, wzrosła w ostatnich latach do tego stopnia, że problemem zajęli się członkowie Kongresu Stanów Zjednoczonych. Microsoft wraz z koncernem AOL ogłosił oświadczenie o podjęciu działań mających ograniczyć liczbę spamu. Pomimo obietnic wielu firm międzynarodowych o pracach nad zmniejszeniem e-maili reklamowych, administratorzy systemów zauważają wciąż wzrost liczby tych wiadomości. Ktoś zatem nie mówi tutaj całej prawdy.

Zjawisko spamu wywodzi się ze Stanów Zjednoczonych i jest jednym z oficjalnie wykorzystywanych środków marketingowych. Na szczęście parlamenty wielu krajów wprowadzają przepisy mające ograniczyć spam. Przykładowo, w Wielkiej Brytanii zmiana prawa umożliwiła nakładanie grzywnien do 5000 funtów, w Polsce od 2003 roku obowiązuje ustawa o świadczeniu usług drogą elektroniczną, dająca pewne środki prawne do walki ze spamem. Podobne nowelizacje pojawiają się w kolejnych



Peter Doeberl, visipix.com

państwach Europy (we Włoszech najwyższą karą za przestępstwo tego typu jest nawet pozbawienie wolności do trzech lat). Generalnie prawo ma zezwalać na wysyłanie poczty reklamowej jedynie do osób, które wyraziły na to zgodę. Jednak przepisy jedno, a życie drugie. Spam nadchodzi z całego świata i administratorzy muszą po prostu szukać sposobów na walkę ze spamem.

Zanim zaczniemy, najpierw słówko o spamerach, czyli o osobach zajmujących się rozsyłaniem niechcianej poczty. Przeciwny spamer nie jest bynajmniej osobą, która rozsyła maile z nudów – choć i tacy się zdarzają. Spamerzy działają z kilku prostych pobudek. Mogą wykorzystywać niechcianą pocztę do dokonywania włamań do zdalnych systemów. Mogą prowadzić różnego rodzaju kampanie oszczerstw, czy choćby nękać odbiorców w sobie tylko znanym celu. Niechciana poczta może być nosicielem wirusów, które przekazują takie przestępstwa (nie bójmy się użyć tego słowa) informacje o naszym systemie.

Cokolwiek myślimy o spamie, niezaprzeczalnym faktem jest to, że we właściwych (choć raczej w niewłaściwych) rękach taka wiadomość może być groźnym narzędziem do łamania zabezpieczeń. Zatem spam to nie tylko uprzykrzenie życia, ale także potencjalne zagrożenie, które należy wyeliminować ze skrzynki pocztowej lub sieci lokalnej. Warto zatem poświęcić nieco czasu na walkę ze spamem.

Czy usunięcie spamu będzie kosztowne dla nas lub naszej firmy? Jeżeli będziemy pracować z oprogramowaniem Open Source, jedynym kosztem, jaki poniesiemy, będzie nasz własny czas. Można oczywiście zdobyć podobne narzędzia dla systemów Windows, ale prawdopodobnie nasza kieszeń mocno odczułaby zakup odpowiedniego oprogramowania. Oprogramowanie Open Source ma też taką przewagę nad programami komercyjnymi, że znajduje się w użyciu od jakiegoś czasu i działa w oparciu o zdobyte doświadczenia praktyczne.

Jakich programów należy użyć, aby zmniejszyć ilość niechcianej poczty? Obecnie można przebierać w różnych rozwiązaniach. Ze względu na łatwość użytkowania omówimy pokrótce programy: Procmail, Mail: Audit oraz SpamAssassin. Oczywiście istnieje wiele innych programów, ale te trzy wymienione powyżej są najchętniej używane, a zasada ich działania jest prosta i zrozumiała. Generalne założenie przyjęte na potrzeby artykułu jest następujące: korzystacie z systemu GNU/Linux lub BSD, a do wysyłania i odbierania poczty używacie programów Fetchmail, Procmail, Postfix lub Exim.

## Procmail

Program Procmail [1] jest stosowany od wielu lat do przetwarzania poczty przychodzącej, przy czym pozwala na wykonywanie filtrowania na wiele sposobów – przed dotarciem listu do skrzynki odbiorczej użytkow-

AUTOR

Richard jest organizatorem grupy użytkowników Sheflug – Sheffield Linux. Jego główne pasje to fotografia, wędkarstwo golf, dobre wino i piwo. Strona internetowa Sheflug znajduje się pod adresem <http://www.sheflug.org>.

nika. Konfiguracja Procmaila może jednak sprawić duże trudności dla początkującego. Na szczęście, w Sieci istnieje lista dyskusyjna na temat Procmail, więc zawsze można spróbować rozwiązać problem licząc na pomoc bardziej zaawansowanych użytkowników tego narzędzia.

Ostatnimi czasy Procmail jest stopniowo wypierany przez nowsze oprogramowanie, chociaż nadal jest udanym rozwiązaniem i można z niego spokojnie korzystać w codziennej pracy. Cała dokumentacja dotycząca programu Procmail znajduje się na jego stronach WWW. Przed rozpoczęciem pracy z programem zalecamy dokładne przejrzanie tej strony. Żeby przeczytać krótki opis programu Procmail można także użyć polecenia *man procmail* i *man procmailx*.

## Mail::Audit

Mail::Audit [2] to biblioteka umożliwiająca tworzenie prostych filtrów poczty przychodzącej, opracowana przez Simona Cousinsa, który potrzebował swego rodzaju odmiany w stosunku do narzędzia Procmail. Jak twierdzi autor: „Procmail jest nieprzyjemny w użyciu. Ma bardzo męczący format reguł wiadomości, którego nie znoszę. Potrzebowałem elastycznego narzędzia, dzięki któremu mógłbym filtrować pocztę wykorzystując testy Perla”. Mail::Audit to po prostu kolejny sposób tworzenia filtrów wiadomości, choć nie są to wyłącznie zwykłe filtry. Można tworzyć bardzo skomplikowane reguły analizujące treść, dzięki czemu jest to dużo lepsze rozwiązanie niż Procmail.

Przed rozpoczęciem instalacji należy sprawdzić, czy w systemie są zainstalowane pakiety języka Perl. Najlepiej zainstalować Mail::Audit z najbliższego serwera FTP CPAN. Aby rozpocząć instalację, musimy otworzyć okno główne i wpisać:

```
perl -MCPAN -e shell
o conf prerequisites_policy ask
install Mail::Audit
```

W tym miejscu może być konieczność zainstalowania nowej wersji modułów CPAN. Jeżeli ujrysz stosowny komunikat, najpierw zainstaluj moduły CPAN, przed wznowieniem instalacji Mail::Audit. Jeżeli po raz pierwszy uruchamiasz moduły CPAN, trzeba będzie ustawić kilka opcji konfiguracyjnych. Wystarczy postępować zgodnie z prostymi instrukcjami wyświetlanymi na ekranie.

Po zainstalowaniu Mail::Audit należy

utworzyć pliki *.forward* i *.spam* w swoim katalogu domowym. Zawartość pliku *.forward* będzie wyglądała mniej więcej tak:

```
"| IFS=' ' && exec /home/bob/➤
.spam -f- || exit 75 #bob"
```

Trzeba koniecznie pamiętać o cudzysłowie w tym pliku. Znak | oznacza potok, a */home/bob* to nasz katalog domowy. Teraz wystarczy wskazać pocztę w pliku konfiguracyjnym *.spam* i cała poczta będzie analizowana pod kątem obecności niechcianej poczty. Opis poczty niechcianej znajduje się w pliku *.spam*. W ramce umieszczono przykładową zawartość takiego pliku.

Pamiętajmy, że w naszym przykładzie wszystkie pliki poczty znajdują się w katalogu */home/bob/Mail*. W przypadku natrafienia na spam, nie jest on od razu usuwany z komputera, tylko przenoszony do katalogu */home/bob/Mail/Spam*. Dzięki temu, w przypadku fałszywego trafienia i uznania istotnej wiadomości za spam, można ją odszukać w tym katalogu. Od czasu do czasu warto sprawdzać, jak wiele miejsca zajmuje ten katalog, gdyż duża ilość niechcianej poczty może szybko zapełnić twardy dysk. Można oczywiście zamiast:

```
$mail->accept(/home/bob/➤
Mail/Spam');
```

wpisać następujący wiersz:

```
$mail->accept(/dev/null');
```

W ten sposób wszelkie niechciane wiadomości będą natychmiast usuwane bez zapisywania na dysku. Po zakończeniu instalacji należy przeprowadzić kilka testów, żeby upewnić się, czy wszystko działa jak należy. W tym celu najlepiej zalogować się na koncie root w terminalu znakowym i obserwować komunikaty pojawiające się podczas odbierania poczty. Do obserwacji bieżącej można użyć polecenie *less +F /var/log/mail.info* lub po prostu oglądać pliki zdarzeń systemu pocztowego. Test można uruchomić wpisując polecenie *fetchmail -d0*. Teraz wystarczy tylko obserwować generowany plik dziennika zdarzeń.

Być może będzie trzeba ustawić odpowiednie uprawnienia dla plików *.forward* lub *.spam*, używając polecenia *chmod*. Jeżeli wszystko zostało wykonane prawidłowo, będziesz dysponować w pełni działającą instalacją biblioteki Mail::Audit. Teoretycznie

## Przykładowy plik .spam

```
#!/usr/bin/perl

use strict;
use warnings;

use Mail::Audit qw/KillDups/;
use Mail::Audit;
use Mail::SpamAssassin;

my $mailbox = "/home/bob/Mail/inbox";

my $mail      = Mail::Audit->new( nomime
=> 1, );
my $spamtest = Mail::SpamAssassin-
>new();
my $status   = $spamtest->check( $mail
);

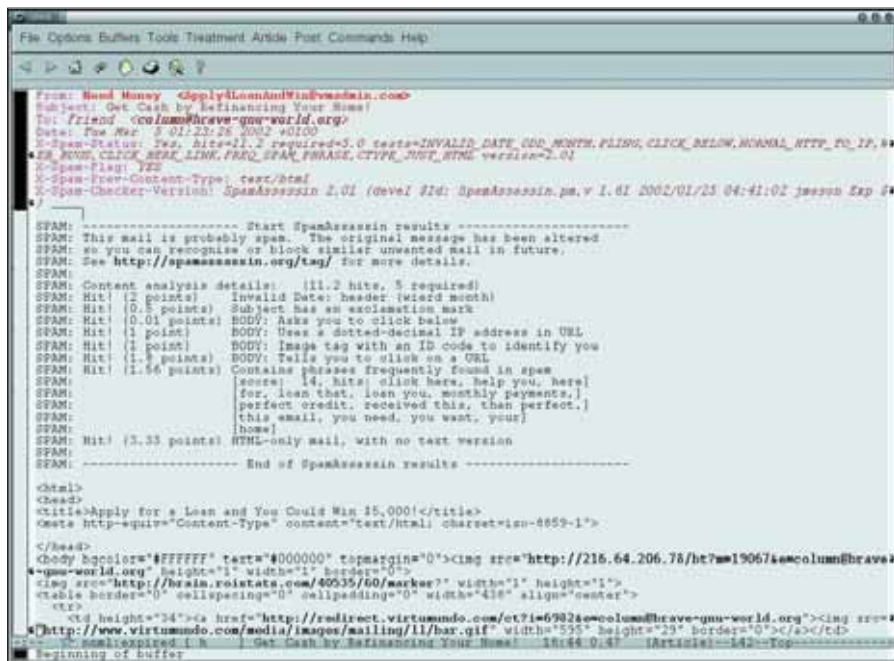
if ( $status->is_spam() ) {
    $status->rewrite_mail();
    $mail->accept(
"/home/bob/Mail/Spam" );
} else {
    $mail->accept(
"/home/bob/Mail/inbox" );
}
```

można wtedy usiąść wygodnie w fotelu i spodziewać się, że poczta będzie wolna od spamu. Niestety, nie wszystkie niechciane wiadomości będą blokowane, ale na szczęście zdecydowana ich większość wylądnie tam gdzie ich miejsce – w śmietniku.

## SpamAssassin

SpamAssassin [3] to filtr pocztowy, który oznacza przychodzące wiadomości jako spam, jeżeli spełniają one określone kryteria. Jest to obecnie najbardziej efektywne rozwiązanie tego typu. SpamAssassin działa na zasadzie scoringu – wyceny punktowej dla każdej wiadomości pocztowej, w zależności od tego, czy spełnia ona określone wcześniej kryteria. Regułom można zmieniać przyporządkowane im wartości punktowe przez dodanie linijek w pliku *~/spamassassin/user\_prefs*. Pełna lista reguł znajduje się pod adresem [4]. Identyfikacja niechcianej poczty przy pomocy SpamAssassin przeprowadzana jest w następujący sposób:

- Analiza nagłówka: osoby rozsyłające spam starają się przy pomocy różnych sztuczek ukryć swoją tożsamość, nadając jednocześnie swojej wiadomości znamiona oryginalne



Rysunek 1. Wykrywanie i ocena poczty przychodzącej przez SpamAssassin.

nalności, starając się przekonać nas, że przesiłaliśmy kiedyś w przeszłości o wysłaniu tego typu reklamy. SpamAssassin próbuje wychwycić wiadomości tego typu.

- **Analiza treści:** wiadomości reklamowe charakteryzują się specyficznym stylem językowym (mówiąc dość ogólnie).
- **Czarne listy:** SpamAssassin obsługuje wiele istniejących czarnych list, np. [mail-abuse.org](http://mail-abuse.org) [5] czy [ordb.org](http://ordb.org) [6].
- **Razor:** Vipul's Razor [7] to baza danych śledząca niechcianą pocztę, działająca na podstawie podpisu umieszczonego w wiadomości. Jako że spam działa na zasadzie rozsyłania tej samej wiadomości do wielu adresatów, Razor umożliwia wysłanie takiej wiadomości tylko do jednej osoby – potem wiadomość jest traktowana jako spam i dołączana do bazy danych. Po dodaniu do bazy danych taka wiadomość będzie od razu blokowana.

W chwili pisania tego artykułu pojawiła się właśnie wersja 2.61 programu SpamAssassin. Większość użytkowników przekonała się już do niego i chętnie korzysta z jego możliwości. Po dokonaniu „wyceny” niechcianej wiadomości, może być ona dalej przetwarzana, nawet przez własne skrypty użytkownika. Jeżeli połączymy siły SpamAssassin i Mail::Audit, otrzymamy zadziwiająco korzystne efekty. Przy poziomie ruhcou około 300-500 wiadomości dziennie, przez gąszcz kontroli i filtrów przesyłzgnie się średnio tylko jedna wiadomość na tydzień – sprawdziliśmy to w laboratorium Linux Magazine.

```
install Pod::Usage
install ExtUtils::MakeMaker
install HTML::Parser
install Net::DNS
install Mail::SpamAssassin
```

Będzie trzeba zainstalować niektóre moduły, np. Pod::Usage. Jeżeli system będzie wymagał kolejnych elementów, zostaniemy poproszeni o instalację stosownych modułów. Przed ich instalacją radzimy jednak zapoznać się z dokumentacją SpamAssassin umieszczoną na stronie WWW programu.

Po instalacji trzeba jeszcze ustalić odpowiednie reguły oraz skonfigurować plik `user_prefs`, który umożliwi uruchomienie i korzystanie ze SpamAssassin. Wszystkie reguły (np. `25_body_tests.pl.cf` i inne) prawdopodobnie będą wymagały zmian w celu dostosowania do lokalnych warunków. Przed uruchomieniem SpamAssassin należy przenieść wszystkie reguły `*.cf` do `/etc/mail/spamassassin` lub podobnego miejsca. Jest to w zasadzie najtrudniejsza część konfiguracji programu, ponieważ miejsce przechowywania reguł może się różnić w zależności od używanej dystrybucji (Debian, Slackware, Suse). Trzeba zatem wyteńczyć szare komórki, aby wszystko znalazło się na miejscu.

Przed konfiguracją pliku `user_prefs` dobrze byłoby uruchomić `spamassassin -lint`. Dzięki temu otrzymamy na ekranie zbiór komunika-

## Instalacja SpamAssassin

Obecnie istnieje wiele pakietów SpamAssassin dla Debiana, Slackware, Red Hat i innych dystrybucji GNU/Linux. Dużo łatwiejsza będzie instalacja modułów CPAN przy pomocy następujących poleceń:

```
perl -MCPAN -e shell
o conf prerequisites_policy ask
```

## Ustawienia SpamAssassin

```
require_version 2.60
report_safe 1
ok_languages en
ok_locales en
use_dcc 1
use_pyzor 1
trusted_networks
10.0.0/16
use_razor2 1
razor_timeout 10
use_bayes 1
rbl_timeout 15
check_mx_attempts 2
dns_available yes
bayes_auto_learn 1

# score SYMBOLIC_TEST_NAME n.nn
```

Jak widzimy w podanym przykładzie, SpamAssassin wymaga 5 punktów, aby oznaczyć wiadomość jako spam. Jest to bardzo niska wartość i lepiej ją od razu zwiększyć. Lepiej stosować zazwyczaj wartości 8-12. Generalnie zalecamy nieco eksperymentów i podjęcie decyzji na podstawie własnych doświadczeń. W przykładzie nie wykorzystano funkcji czarnej listy i białej listy. Poniżej, w pliku konfiguracyjnym zdefiniowano domyślny język wiadomości, włączono także kontrolę DCC, Pyzor i Razor, a także DNS.

tów dotyczących plików *\*cf* (tylko tych, które znajdują się w niewłaściwych miejscach). Jeżeli wykonanie polecenia nie powoduje wyświetlenia żadnych komunikatów, prawdopodobnie wszystko będzie działać prawidłowo.

Po zakończeniu konfiguracji przy pomocy *perldoc Mail::SpamAssassin::Conf* lub *man Mail::SpamAssassin::Conf*, możemy następnie uruchomić *spamassassin -lint* i ponownie sprawdzić pojawiające się komunikaty błędów. Jeżeli na tym etapie otrzymamy jakiegokolwiek komunikaty o błędach, będziemy zmuszeni wyłączyć problematyczne reguły z pliku *user\_prefs* (wystarczy przed daną regułą wstawić symbol #).

Następnie, po uruchomieniu *ls -a* z katalogu domowego, zauważymy katalog *spamassassin*. W nim przechowywany będzie plik *user\_prefs* razem z *bayes\_seen* i *bayes\_toks*.

Bardziej zaawansowane możliwości SpamAssassin to zadania wymagające instalacji kolejnych modułów – przede wszystkim DCC (ang. Distributed Checksum Clearinghouse) [8], a także programu Razor [7] lub Pyzor [9] (Razor w języku Python). Szczegółowe informacje można znaleźć na stronach internetowych poszczególnych programów. Po lekturze dokumentacji możemy skorzystać z tzw. czarnych i białych list. Były one bardzo użyteczne jeszcze przed erą takich narzędzi, jak Mail::Audit czy SpamAssassin. Tym niemniej warto pamiętać, że SpamAssassin „uczy” się tego, które serwery są najczęściej używane do rozsyłania spamu.

Mamy nadzieję, że niniejszy artykuł pomoże użytkownikom prywatnym i administratorom w małych środowiskach w efektywnym radzeniu sobie za spamem. ■

# Prenumerata Linux Magazine Nie przegap takiej okazji!



## INFO

- [1] Procmail: <http://www.procmail.org/>
- [2] Mail::Audit: <http://search.cpan.org/~simon/Mail-Audit-2.1/Audit.pm>
- [3] SpamAssassin: <http://www.spamassassin.org>
- [4] Reguły SpamAssassin: <http://eu.spamassassin.org/tests.html>
- [5] Organizacja Mail Abuse Prevention System (MAPS): <http://www.mail-abuse.org>
- [6] Baza danych Open Relay: <http://www.ordb.org>
- [7] Razor: <http://razor.sourceforge.net/>
- [8] DCC: <http://www.rhyolite.com/anti-spam/dcc/>
- [9] Pyzor: <http://pyzor.sourceforge.net/>

- Zamawiając prenumeratę oszczędzasz!
- Płacisz jak za 9 numerów, a otrzymujesz 12!
- Z każdym numerem DVD lub płyta CD-ROM.

**Najszybszy sposób  
zamówienia prenumeraty:**

**<http://www.linux-magazine.pl>**

**Infolinia: 0801 800 105**