Anti-Spam Tool Kit. Edycja polska

Autorzy: Paul Wolfe, Charlie Scott, Mike W. Erwin
Tłumaczenie: Szymon Kobalczyk (wstęp, rozdz. 1 – 9, Marcin Jędrysiak (rozdz. 10 – 16, dod. A, B)
ISBN: 83-7361-587-3
Tytuł oryginału: Anti-Spam Tool Kit
Format: B5, stron: 416

Przygotuj arsenał do walki ze spamem

- Zaplanuj walkę
- Poznaj metody filtrowania spamu
- Zainstaluj narzędzia antyspamowe

Spam męczy użytkowników internetu od dawna. Reklamy, informacje o serwisach WWW dla dorosłych, łańcuszki szczęścia i inne pseudowiadomości powodują, że znalezienie przesyłki od kontrahenta lub znajomego zajmuje coraz więcej czasu. Regulacje prawne nic nie zmieniły – polscy spamerzy przeredagowali treści swoich wiadomości tak, aby spełniały wymagania ustawy, a zagraniczni prawdopodobnie nie zdają sobie sprawy z istnienia w Polsce jakichkolwiek przepisów odnośnie spamu. Jedynym rozwiązaniem jest wypowiedzenie spamowi wojny na własną rękę. Na szczęście wielu zirytowanych spamem programistów pokusiło się o napisanie narzędzi umożliwiających zablokowanie autorom spamu dostępu do naszej poczty.

„Anti-Spam Tool Kit. Edycja polska" to książka dla wszystkich, którzy mają dość wszechobecnego spamu. Przedstawia najnowsze techniki zwalczania spamu, narzędzia filtrujące spam, metody zabezpieczania serwerów i kont pocztowych przed spamem oraz te właściwości internetu, które spamerzy wykorzystują w swoich działaniach. Dzięki zawartym w niej wiadomościom nauczysz się tworzyć systemy kontroli niechcianej poczty, wykorzystujące różnorodne narzędzia — od darmowych po komercyjne, od podstawowych filtrów działających u klienta po złożone rozwiązania realizowane na serwerach. Zaplanujesz strategię walki ze spamem.

- Opracowywanie planu walki
- Metody filtrowania spamu na podstawie treści przesyłek
- Implementacje rozwiązań antyspamowych
- Blokowanie spamu z wykorzystaniem czarnych list
- Instalacja i konfiguracja programu Spam Assassin
- Filtrowanie spamu na podstawie klasyfikatora Bayesa
- Blokowanie spamu w programach pocztowych
- Narzędzia antyspamowe dla Windows, Mac OS i Linuksa
- Zabezpieczanie danych osobowych przed spamerami

Wydawnictwo Helion
ul. Chopina 6
44-100 Gliwice
tel. (32)230-98-63
e-mail: helion@helion.pl

Spis treści

Rozdział 5.

Blokowanie spamerów przy użyciu czarnych list opartych na DNS

W rozdziale 4., „Strategie implementacji rozwiązań antyspamowych" wprowadziliśmy Cię w tematykę czarnych list opartych na DNS (ang. *DNS Blacklists*) jako jednego z kilku sposobów zwalczania spamu. W tym rozdziale przyjrzymy się poszczególnym popularnym serwisom czarnych list, wyjaśnimy, jak wdrażać je na serwerze pocztowym oraz pomożemy Ci w podjęciu decyzji, z której listy najlepiej korzystać. Mówiąc o czarnych listach opartych na DNS, często stosuje się skrót DNSBL i tak właśnie będziemy odnosić się do nich w tym rozdziale.

Zanim zaczniemy mówić o konkretnych czarnych listach i o tym, jak je wdrażać, zagłębimy się w to, czym są listy DNSBL i jak działają.

Czarne listy DNS dla każdego

Listy DNSBL są integralną częścią każdego zestawu narzędzi do zwalczania spamu. To, że aktualizuje je bardzo wielu użytkowników internetu, oznacza, że zyskujesz możliwość zablokowania spamera, zanim jeszcze pierwsza porcja spamu trafi do Ciebie. Aby zrozumieć, jak listy DNSBL mogą Ci pomóc, musisz poznać, jakie typy DNSBL są dostępne i jak działają.

Typy list DNSBL

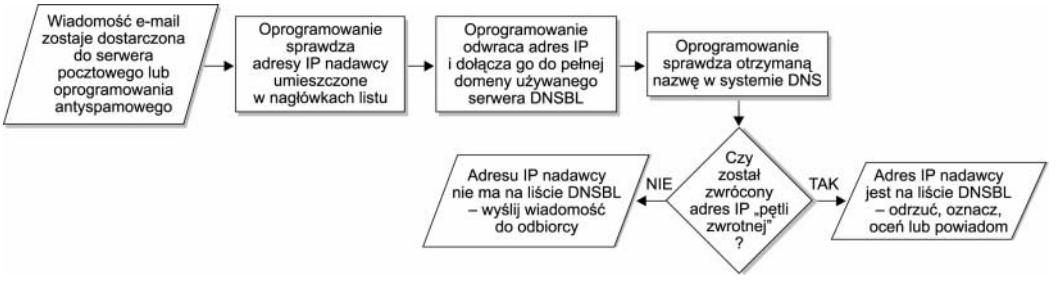
Obecnie stosuje się dwa różne typy czarnych list opartych na DNS:

- Czarne listy adresów IP
- Czarne listy domen

Większość list DNSBL jest oparta na adresach IP, czyli sprawdza adres IP (ang. *Internet Protocol*) serwera wysyłającego pocztę. Każdy komputer, w tym serwery e-mail podłączone do internetu, ma swój własny, unikatowy adres IP. Ten adres jest kontrolowany względem bazy danych, aby sprawdzić, czy wskazuje znanego spamera, znany otwarty

przekaźnik lub znane otwarte proxy, czy nie. Z reguły listy DNSBL oparte na adresach IP działają następująco:

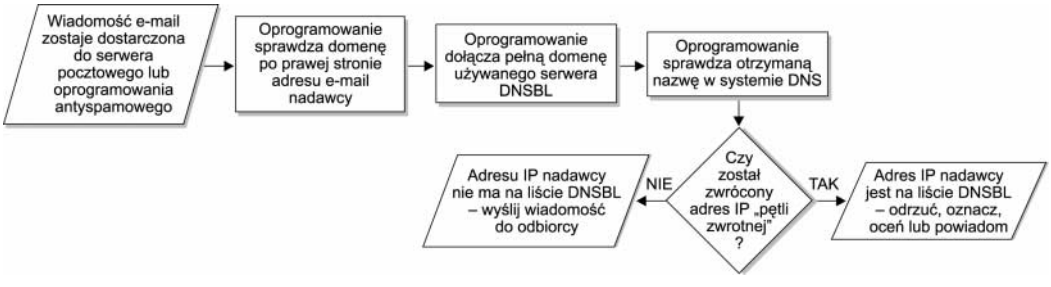
1. Następuje próba dostarczenia wiadomości e-mail do Twojego serwera pocztowego lub oprogramowania antyspamowego.
2. Twój serwer pocztowy lub oprogramowanie antyspamowe sprawdza adresy IP serwerów pocztowych, przez które przeszedł e-mail, by trafić do Ciebie.
3. Następnie Twój serwer pocztowy lub oprogramowanie antyspamowe odwraca kolejność adresów IP i dodaje pełną złożoną nazwę domeny (ang. *fully qualified domain name — FQDN*) używanego serwera DNSBL. Pełna nazwa domeny składa się z internetowej nazwy domeny, w której znajduje się serwer (takiej jak *ordb.org*) oraz nazwy komputera dla serwera (takiej jak *relays.ordb.org*). Zatem jeśli na przykład adresem IP serwera wysyłającego byłoby *192.168.42.6*, a pełną nazwą domeny byłoby *relays.greatdnsbl.tld*, połączona nazwa to *6.42.168.192.relays.greatdnsbl.tld* (w przykładzie użyliśmy fikcyjnego adresu prywatnego).
4. Następnie Twój serwer pocztowy lub oprogramowanie antyspamowe sprawdza połączoną nazwę w systemie nazw domen (ang. *Domain Name System — DNS*). Jeśli zwrócony zostanie rzeczywisty adres IP, oznacza to, że serwer znajduje się na czarnej liście. W przeciwnym razie nie ma go tam lub czarna lista jest nieczynna. Zwracany adres IP powinien zawsze należeć do specjalnej sieci „pętli zwrotnej" (127.0.0.0/8, zgodnie z RFC 3330). Zwrócony adres IP może mieć jakieś specjalne znaczenie dla danej listy DNSBL.
5. Twój serwer pocztowy lub oprogramowanie antyspamowe na podstawie odpowiedzi otrzymanej od listy DNSBL podejmuje decyzję, co zrobić z listem. Jeśli zdecyduje, że list pochodzi z systemu znajdującego się na liście DNSBL, może go odrzucić, oznakować lub ocenić, zależnie od oprogramowania i jego konfiguracji.



Domenowe listy DNSBL nazywane są również *prawostronnymi czarnymi listami* (ang. *righ-hand side balcklists — RHSBL*). Te listy sprawdzają jedynie domeny najwyższego i drugiego poziomu (na przykład *.com* oraz znajdujące się przed nim yahoo — *yahoo.com*) danego adresu e-mail lub pełniej nazwy domeny. Oto jak działają:

1. Następuje próba dostarczenia wiadomości e-mail do Twojego serwera pocztowego lub oprogramowania antyspamowego.
2. Twój serwer pocztowy lub oprogramowanie antyspamowe przygląda się domenie na prawo od znaku @. Na przykład z adresu *spam4you@spammer.tld* wyodrębnione zostanie *spammer.tld*. Bądź w przypadku serwera *spamserver.spammer.tld* uwzględni tylko fragment *spammer.tld*.

3. Następnie ta nazwa domeny jest dodawana przed pełną nazwą domeny serwera DNSBL. Na przykład jeśli wyodrębnioną domeną jest *spammer.tld*, a serwer DNSBL nosi nazwę *relays.greatdnsbl.tld*, połączona nazwa to *spammer.tld.relays.greatdnsbl.tld*.
4. Następnie Twój serwer pocztowy lub oprogramowanie antyspamowe sprawdza połączoną nazwę w systemie DNS. Jeśli zwrócony zostanie rzeczywisty adres (ponownie, z zakresu sieci pętli zwrotnej), oznacza to, że serwer znajduje się na czarnej liście. W przeciwnym razie nie ma go tam lub czarna lista jest nieczynna.
5. Ponownie Twój serwer pocztowy lub oprogramowanie na podstawie odpowiedzi otrzymanej od serwera RHSBL podejmuje decyzję, co zrobić z listem.



Czym różnią się listy DNSBL korzystające z adresów IP od używających nazw domen? Na listach adresów IP zazwyczaj znajdują się systemy, które wysyłały spam w przeszłości lub są zdolne do wysyłania spamu (tak jak otwarte przekaźniki). Czasem składają się z całych sieci zdolnych do wysyłania spamu (jak zakresy przypisane do połączeń telefonicznych). Są dokładniejsze, ponieważ zawierają jedynie adresy IP lub sieci, które rzeczywiście wykazały się zachowaniem, przez które trafiły na listę (to jest wysyłaniem spamu), a nie tylko tym, że są częścią takiej domeny.

Kryteria czarnych list opartych na DNS

Obecnie większość list DNSBL stosuje jedno lub więcej spośród podanych poniżej kryteriów do określenia, czy dany komputer należy do listy, czy nie. Czasami organizacja prowadząca listę DNSBL ma osobną listę dla każdego z kryteriów lub może mieć jedną lub dwie listy stosujące ich kombinację.

- Lista otwartych przekaźników
- Lista otwartych proxy
- Lista znanych spamerów
- Lista użytkowników łączy telefonicznych

Pokrótce omówimy każdą z nich.

Lista otwartych przekaźników

Listy otwartych przekaźników są niezmiernie popularną formą list DNSBL. Komputer jest uznawany za otwarty przekaźnik, jeśli pozwala nieautoryzowanym użytkownikom na wysyłanie e-maili do osób trzecich — to znaczy, ani osoba wysyłająca pocztę, ani osoba ją otrzymująca nie są w domenie, dla której ten system e-mail pełni rolę serwera pocztowego. Na początku istnienia internetu, kiedy spam nie stanowił tak dużego problemu, wiele systemów było konfigurowanych jako otwarte przekaźniki. Obecnie ustawianie serwerów pocztowych jako otwartych przekaźników nie jest już konieczne, więc systemy pozostawione w takim stanie są na ogół zarządzane przez administratorów, którym po prostu brakuje czasu, środków i wiedzy, by skonfigurować je w inny sposób. Otwarte przekaźniki są atrakcyjne dla spamerów, ponieważ pozwalają im na korzystanie z cudzych zasobów do wysyłania hurtowych e-maili i odsuwają ich o jeden krok od nadawcy — przez co stają się trudniejsi do wytropienia.

Lista otwartych proxy

Otwarte serwery proxy są nawet gorsze od otwartych przekaźników. Działanie proxy (pol. pośrednik) w świecie sieciowym jest zbliżone do funkcji pełnomocnika w świecie rzeczywistym — to znaczy, jest kimś lub czymś, co zastępuje lub pełni rolę substytutu dla kogoś lub czegoś innego. W tym przypadku proxy jest urządzeniem lub serwerem sieciowym wykonującym połączenie z zasobem sieciowym w imieniu użytkownika, zamiast połączenia się użytkownika bezpośrednio z tym zasobem. Na przykład jeżeli użytkownik chce odwiedzić stronę *http://www.helion.pl*, wpisuje ten adres URL w swojej przeglądarce. Jeśli jego przeglądarka jest skonfigurowana tak, by korzystać z serwera HTTP proxy, serwer proxy otrzymuje żądanie, idzie pod adres *http://www.helion.pl*, pobiera stronę WWW i wysyła ją do przeglądarki. Użytkownik nigdy nie łączy się bezpośrednio z adresem *http://www.helion.pl*.

Zastosowanie proxy pozwala na zachowanie pewnego stopnia anonimowości. Adres IP użytkownika nigdy nie pojawi się w dziennikach serwera WWW Helionu — ale już adres IP proxy zostanie zarejestrowany. Zazwyczaj proxy ograniczają, które sieci mogą się z nimi łączyć. Jednak otwarte proxy pozwalają *każdemu* użytkownikowi na łączenie się skądkolwiek i używanie ich, by dostać się gdziekolwiek. Dlatego otwarte proxy umożliwia spamerowi nawiązanie połączenia SMTP (ang. *Simple Mail Transport Protocol*) z serwerem pocztowym, ale ukrywa, skąd pochodzi poczta. Dla systemów, z którymi się łączy, wygląda to tak, jakby nadawcą było proxy — nic poza nim nie jest widziane przez serwer pocztowy. Jest to jeszcze jedno potężne narzędzie w rękach spamera.

Lista znanych spamerów

Listy znanych spamerów zawierają domeny, systemy lub sieci będące znanymi siedliskami spamerów. W przeciwieństwie do otwartych przekaźników i otwartych proxy znajdują się one na liście nie z przyczyn technicznych, ale dlatego, że faktycznie rozsyłały spam.

Lista użytkowników łączy telefonicznych

Pomysł list użytkowników łączy telefonicznych ma zapobiegać temu, co organizacja MAPS (o której opowiemy trochę dalej) nazywa „nadużyciem spamowym", gdzie spamer dzwoni do operatora interentu (najczęściej używa podrobionego konta „próbnego"),

korzystając z systemu, na którym uruchamia serwer pocztowy lub specjalne oprogramowanie do rozsyłania spamu (nazywane w języku ang. *ratware*) i masowo wysyła e-maile. W ten sposób spamer omija tradycyjne środki wykrywania spamu. Wykorzystuje zasoby sieciowe operatora, ale nie korzysta z jego serwerów. Tego rodzaju listy często zawierają również inne konta operatorów internetu o dynamicznych adresach IP, takich jak modemy kablowe i linie DSL.

Dodawanie i usuwanie wpisów z czarnych list opartych na DNS

Każda lista DNSBL udostępnia metodę dodawania lub usuwania wpisów z czarnej listy. Najczęściej robi się to, korzystając ze strony WWW danej listy, chociaż można również za pośrednictwem poczty elektronicznej. Niekiedy by móc dodawać wpisy do czarnej listy DNSBL, trzeba być klientem płacącym za usługi bądź darczyńcą.

Na ogół dowolna osoba może usunąć serwer, sieć lub domenę z listy DNSBL. Robi się to na stronie WWW danej listy. Pozycja umieszczona na liście jest ponownie sprawdzana przed usunięciem. Jeśli notowany serwer, sieć lub domena jest pod kontrolą znanego spamera lub jest często wykorzystywana, może w ogóle nie zostać usunięta.

Wybór czarnej listy opartej na DNS

Istnieje wiele list DNSBL — ponad 100 publicznych i nikt nie wie, ile prywatnych. Pod względem organizacyjnym zazwyczaj dzielą się na trzy kategorie:

- Organizacje niezarobkowe zaangażowane w zwalczanie spamu. Organizacje te na ogół zatrudniają pracowników i mają na wpół korporacyjną strukturę.
- Luźno powiązana grupa administratorów, którzy skrzyknęli się, by wspólnie walczyć ze spamem. Grupy te zazwyczaj nie mają pełnoetatowych pracowników i przypominają projekty z otwartym dostępem do kodu źródłowego. (Na przykład chociaż mogą mieć uznanego przywódcę, podczas podejmowania decyzji kierują się zasadami demokratycznymi).
- Pojedyncze osoby, które ustawiły swoją własną listę DNSBL dla swojego własnego, prywatnego użytku, ale jeśli chcą, pozwalają innym na korzystanie z niej.

Oprócz struktury organizacyjnej listy DNSBL różnią się znacznie sposobem działania. Obszary, w których mogą występować różnice, są następujące:

- Kryteria uznawania kogoś za spamera (lub potencjalnego spamera).
- Metody wykorzystywane do pozyskania kandydatów do wciągnięcia na czarną listę.
- Reguły usuwania wpisów z listy.
- Rodzaje prowadzonych list (otwartych przekaźników, znanych spamerów, łączy telefonicznych itd.).
- Czy ich usługi są płatne, czy nie.

Wszystkie te czynniki mają wpływ na skuteczność i łatwość użycia konkretnej listy DNSBL.

Ponieważ listy są z natury dynamiczne i skonstruowane w zgodzie z konkretną filozofią swoich organizatorów, żadna z nich nie może zostać uznana za najwyższą wyrocznię orzekającą, kto jest, a kto nie jest spamerem. Każda z nich może dawać fałszywe pominięcia i fałszywe trafienia.

Na ogół organizacje niezarobkowe mają bardziej surowe reguły dotyczące tego, które systemy lub domeny trafiają na ich czarne listy, niż luźno powiązane grupy czy pojedyncze osoby. Dlatego jeśli obawiasz się fałszywych trafień, najlepszym wyborem jest tego rodzaju organizacja.

Odpowiednia lista DNSBL powinna być dostosowana do Twojej osobistej lub organizacyjnej polityki dotyczącej spamu. Jak bardzo tolerancyjny jesteś w kwestii przedostania się odrobiny spamu? Jak tolerancyjny jesteś w kwestii odrzucenia legalnej korespondencji? Czy jesteś skłonny zapłacić (lub złożyć datek) za korzystanie z czarnej listy?

Obszerne zestawienie czarnych list znaleźć można na stronie Declude: *http://www.declude.com/ Articles.asp?ID=97*. Mimo to w kolejnych podrozdziałach przedstawimy pokrótce kilka najbardziej popularnych i skutecznych.

Mail Abuse Prevention System (MAPS)

System MAPS (ang. *Mail Abuse Prevention System* — system zapobiegania nadużyciom pocztowym) jest jedną z największych, najstarszych, najbardziej kontrowersyjnych i najbardziej znanych spośród istniejących list DNSBL. Został założony w 1997 roku przez małą grupkę, do której należał programista internetowy Paul Vixie (autor oprogramowania BIND działającego na większości internetowych serwerów DNS). MAPS jest niezarobkową korporacją z siedzibą w Kalifornii. Główna witryna MAPS znajduje się pod adresem *http://www.mail-abuse.org*.

Reputacja i wiedza Paula Vixiego przysporzyła systemowi MAPS wiele szacunku wśród administratorów systemów oraz sporo zainteresowania ze strony prasy. Niestety, metody systemu MAPS (które w rzeczywistości nie różnią się zbytnio od wielu innych czarnych list), jego wysoki status oraz jego wszechobecność uczyniły zeń cel ataków prawnych dla licznych nadawców masowej poczty elektronicznej, którzy uważają, że MAPS niesprawiedliwie ich prześladuje. MAPS nawet zbiera na stronie WWW pieniądze na fundusz obrony prawniczej!

Działanie MAPS

MAPS dysponuje jednym z najszerszych dostępnych asortymentów list DNSBL. Każdą z nich zajmuje się odrębna grupa w obrębie organizacji MAPS i każda posiada swoją własną dokumentację, polityki, FAQ i narzędzia. Poniżej przedstawiamy zwięzłe podsumowanie dostępnych list.

Nonconfirming Mailing List (NML)

Typ listy:	*oparta na adresach IP*
Serwer DNSBL:	*nonconfirm.mail-abuse.org*

Lista NML jest najnowszą propozycją MAPS. Zawiera zgłoszone adresy IP, które wysyłają e-maile na listy korespondencyjne, nie potwierdzając w pełni, czy odbiorca faktycznie poprosił o wysyłane informacje. Innymi słowy, nadawcy nie potwierdzają, czy e-mail został zamówiony. Inne przyczyny umieszczenia kogoś na tej liście to:

- Niepodanie pełnych warunków danej listy korespondencyjnej.
- Niewykorzystywanie list zgodnie z ich pierwotnym przeznaczeniem.
- Nieuzyskanie odrębnego potwierdzenia dla każdej listy, do której dodają subskrybenta.

Nawiasem mówiąc, klauzule wycofania w tym przypadku się nie liczą.

Dial-Up User List (DUL)

Typ listy: *oparta na adresach IP*
Serwer DNSBL: *dialups.mail-abuse.org*

Lista DUL zawiera zgłoszone zakresy adresów IP, będące częścią sieci dostępnej telefonicznie lub jakiegoś innego dynamicznie przydzielanego zakresu. Niektórzy operatorzy internetu współpracują z MAPS, by ich własne sieci telefoniczne zostały dodane do list, tak aby nie stali się mimowolnymi współsprawcami rozsyłania spamu.

Oczywiście, niektórzy hobbyści komputerowi i zwykli użytkownicy uruchamiają serwery SMTP na swoich kontach telefonicznych. MAPS zaleca im, by nie wysyłali poczty bezpośrednio ze swojego serwera SMTP, ale zamiast tego wysyłali ją przez serwer SMTP swojego operatora internetu.

Relay Spam Stopper (RSS)

Typ listy: *oparta na adresach IP*
Serwer DNSBL: *relays.mail-abuse.org*

Lista RSS zawiera zgłoszone adresy IP, które rozsyłały masowe e-maile. Większość z nich to otwarte przekaźniki. Jednak samo to, że system jest otwartym przekaźnikiem, nie oznacza, że znajdzie się na liście RSS — musi faktycznie wysyłać spam. Pod tym względem lista różni się od listy systemu ORDB, który omówimy w podrozdziale „Open Relay Database (ORDB)".

Realtime Blackhole List (RBL)

Typ listy: *oparta na adresach IP*
Serwer DNSBL: *blackholes.mail-abuse.org*

Jest to największa ze wszystkich list systemu MAPS. Zawiera sieci i komputery, które spełniają następujące kryteria:

- Ktoś zgłosił, że rozsyłają spam.
- Są otwartym przekaźnikiem.
- Są otwartym proxy.
- Oferują dodatkową obsługę techniczną dla spamerów, jak prowadzenie serwerów WWW, udostępnianie oprogramowania, skrzynek e-mail i inne.

Ponieważ obejmują aspekt obsługi technicznej, szanse, że uprawniony serwer e-mail zostanie zablokowany, są większe niż w przypadku innych, bardziej jednorodnych list.

Realtime Blackhole List+ (RBL+)

Typ listy: *oparta na adresach IP*
Serwer DNSBL: *blackholes.mail-abuse.org*

Lista RBL+ jest najbardziej rozbudowaną propozycję dla subskrybentów i łączy w sobie większość pozostałych list, w tym RBL, DUL i RSS. Zawiera również listę dostępną tylko dla subskrybentów RBL+, o nazwie Open Proxy Monitor (OPM). Lista OPM jest podobna do RSS, ale zawiera adresy IP systemów będących serwerami otwartych przekaźników oraz takie, o których wiadomo, że rozsyłają spam. RBL+ oferuje wydajną metodę prowadzenia czarnej listy, ale korzystając z niej, masz niestety większe szanse na zablokowanie pożądanych e-maili.

Subskrybowanie się do MAPS

Po wielu latach bycia dostępnym za darmo, w lipcu 2001 roku system MAPS przeszedł na usługi odpłatne. Serwis jest nadal bezpłatny dla osób prywatnych i hobbystów, ale wszyscy pozostali muszą płacić roczny abonament. Poziomy płatności zależą od rodzaju i wielkości Twojej organizacji i są następujące:

- Niezarobkowa/oświatowa
- Mała firma (mniej niż 100 użytkowników)
- Standardowa (wszyscy pozostali)

Każda lista ma swoją odrębną cenę, przy czym RBL+ jest najdroższa, a DUL jest najtańsza. Każda lista ma inne ceny dla zapytań DNS i inne dla transferu strefy DNS. Opłaty dla organizacji na poziomie standardowym są uzależnione od liczby użytkowników.

Lista RBL+ umożliwia także wykonywania trasowania zewnętrznego za pomocą protokołu BGP (ang. *Border Gateway Protocol*). BGP jest standardowym protokołem trasowania dla sieci szkieletowej internetu. Innymi słowy, dzięki niemu połączenie internetowe „wie", jak dostać się z punktu A do punktu B. Jeśli jesteś operatorem internetu, MAPS może umieścić w Twojej tabeli trasowania BGP takie trasy, które uniemożliwią spamerom dostanie się do Twojej sieci. Jest to stosunkowo skrajny krok, ponieważ blokuje *cały* ruch internetowy od spamera, a nie tylko ruch pocztowy. Wdrożenie BGP wychodzi poza zakres tej książki.

Niezależnie od tego, do którego poziomu cenowego należysz, nawet jeśli jesteś hobbystą lub osobą prywatną, musisz wysłać do MAPS podpisaną umowę dla listy, którą chcesz subskrybować. Umowy te są dostępne w witrynie MAPS i przeważnie mają po kilkanaście stron. Podpisując umowę, wyrażasz zgodę (między innymi) na to, że wszelkie informacje przekazane przez MAPS zachowasz dla siebie oraz że rozumiesz, że bycie subskrybentem nie ustrzeże Cię przed znalezieniem się samemu na czarnych listach MAPS.

W umowie podajesz również adres IP serwera pocztowego lub DNS, którego zamierzasz używać do wykonywania zapytań lub transferów strefy przez MAPS (lub adres Twojego routera, jeśli stosujesz protokół BGP). MAPS stosuje filtry uniemożliwiające dostęp do ich list osobom, które nie podpisały umowy.

Jeśli nie jesteś hobbystą lub osobą prywatną, zakres cenowy usług MAPS jest stosunkowo szeroki. Zaczynają się od 50 USD rocznie za transfery strefy do listy DUL na poziomie cen dla organizacji niezarobkowych, do 1500 USD (lub więcej) rocznie za zapytania do listy RBL+ przy standardowym poziomie cen. Cennik MAPS na bieżący rok znajdziesz w jego witrynie (*http://mail-abuse.org/feestructure.html*).

SpamCop

SpamCop jest popularną listą DNSBL istniejącą od 1998 roku. Sama organizacja SpamCop ma siedzibę w Seattle i jest prowadzona przez Juliana Haighta (który napisał kod listy) oraz wielu jego współpracowników. SpamCop posiada unikalną metodę bieżącej aktualizacji swojej listy i usuwania z niej witryn, które zaprzestały rozsyłania spamu, co czyni ją jedną z najbardziej „sprawiedliwych" spośród działających list DNSBL.

Oprócz listy DNSBL SpamCop oferuje również filtrowane konta pocztowe POP, IMAP i z dostępem przez WWW. W tym rozdziale nie będziemy szczegółowo omawiać tych usług, ale opiszemy je pokrótce, ponieważ jest to główna część ich działalności. Serwis SpamCop obecnie kosztuje 30 USD rocznie za jedno konto e-mail. Możesz albo przekierować swoje istniejące konto e-mail do tego serwisu, albo korzystać z niego jako z nowego konta w domenie *spamcop.net* (to znaczy Twój adres e-mail będzie miał postać *twoje_konto@spamcop.net*). Serwis sprawdza przychodzącą pocztę na obecność wirusów, a następnie wykorzystuje listę DNSBL prowadzoną przez SpamCop, by zdecydować, czy wiadomość jest spamem, czy nie. Jeśli zdecyduje, że jest to spam, umieszcza list w folderze *Hold*, abyś mógł go później sprawdzić (lub nie). Pocztę możesz odbierać korzystając ze swojego obecnego klienta pocztowego za pośrednictwem protokołu POP lub IMAP albo możesz skorzystać z dostępu przez WWW na stronach SpamCop.

Działanie SpamCop

Typ listy:	*oparta na adresach IP*
Serwer DNSBL:	*bl.spamcop.net*

W odróżnieniu od MAPS SpamCop jest pojedynczą listą. Dla SpamCop nie ma znaczenia, czy prowadzisz otwarty przekaźnik, otwarte proxy lub wysyłasz pocztę z adresu IP dla łączy telefonicznych — w żaden sposób nie sprawdza konfiguracji witryny. Jedynym sposobem, w jaki witryna może znaleźć się na liście, jest zgłoszenie przez kogoś do serwisu SpamCop, że jest nadawcą spamu. Każdy może zapisać się do bezpłatnego serwisu raportującego SpamCop (chociaż wymagany jest potwierdzony adres e-mail).

SpamCop stosuje system punktujący oparty na współczynnikach do rozstrzygania, jak długo trzymać witrynę na czarnej liście. Punktacja zależy od kilku czynników, w tym od tego, jak świeży jest spam, jak długo znajduje się na czarnej liście oraz w jaki sposób SpamCop został powiadomiony o spamie. W przedstawionej poniżej liście opisujemy dokładnie poszczególne punktacje.

Poniżej przedstawiamy analizę procesu zgłaszania spamu oraz to, w jaki sposób serwery pocztowe są automatycznie dodawane i usuwane z czarnej listy:

1. Zarejestrowany użytkownik SpamCop przesyła podejrzany spam (razem z pełnymi nagłówkami!) jako załącznik do serwisu SpamCop. Witryna SpamCop podaje dobrą listę kryteriów tego, co jest uznawane za spam, a więc powinno być przesłane (na przykład nie liczą się wirusy, plotki internetowe i listy łańcuszkowe).
2. Jeśli jest to pierwszy spam z tego serwera, jaki dotarł do bazy danych SpamCop, serwer nie zostanie natychmiast umieszczony na liście. Jeśli jest to drugie zgłoszenie, serwer zostanie wciągnięty na listę na 24 godziny, o ile w międzyczasie nie dotrze więcej podejrzanych wiadomości.
3. Witryny podejrzane o spam są oceniane pod względem aktualności zgłoszeń. Im mniej czasu upłynęło od otrzymania spamu, tym wyższą punktację otrzymuje witryna, która go wysłała. Świeży spam daje danej witrynie niezmodyfikowaną ocenę 4:1, która zmniejsza się, by osiągnąć wynik 1:1 po 48 godzinach. Zgłoszenia starsze niż tydzień są ignorowane przy obliczaniu wagi.
4. SpamCap dysponuje pewną liczbą adresów nazywanych „spamołapkami", które są adresami e-mail stworzonymi wyłącznie w celu zbierania spamu. Ponieważ te pułapki nie są używane przez rzeczywistych ludzi, nigdy nie zostały subskrybowane do żadnych legalnych list i nie otrzymują legalnej korespondencji. Dla zgłoszeń nadchodzących z tych pułapek wynik jest mnożony przez 5. Na przykład jeśli witryna zostanie zgłoszona dwukrotnie przez pułapki, otrzymuje ogólną ocenę 2×5, czyli 10:1.
5. Aby uniknąć blokowania legalnej poczty z dużych witryn, które mogą wypuścić od czasu do czasu jakiś spam (takich jak AOL), zgłoszenia spamu są równoważone przez ogólną liczbę wysłanych legalnych wiadomości. Jest to wykonywane przez monitorowanie wybranych niezależnych witryn. Za każdym razem, kiedy któraś z tych niezależnych witryn sprawdza na czarnej liście SpamCop jakiś adres IP i adres ten nie zostanie odnaleziony, ten komputer otrzymuje punkt niespamu. Po uzyskaniu 1000 punktów każdy kolejny punkt otrzymywany przez komputer liczy się tylko jako połowa jego pełnej wartości. Na przykład jeśli komputer otrzyma 3000 zgłoszeń niezwiązanych ze spamem, otrzyma w sumie tylko 2000 punktów.
6. Jeśli w ciągu 48 godzin dla witryny umieszczonej na liście nie nadeszły żadne nowe zgłoszenia spamu, zostaje ona usunięta z listy.

Warto zauważyć, że SpamCop nie blokuje witryn, które wspierają spamerów, takich jak witryny WWW lub skrzynki nadawcze e-mail. Blokowane są tylko witryny, które faktycznie wysyłają spam.

Subskrybowanie się do SpamCop

W przeciwieństwie do usługi poczty POP, IMAP i dostępu WWW, korzystanie z systemu SpamCop jako listy DNSBL jest bezpłatne. Firma prosi jednak o datek, by pomóc jej w utrzymaniu serwisu. Jeśli Twój ośrodek ma od 1 do 10 użytkowników, prosi o ofiarowanie 50 USD na rok; za 11 do 100 użytkowników 150 USD na rok; dla ośrodków mających więcej niż 100 użytkowników prosi o 1 USD za użytkownika na rok. Sugerowany minimalny datek dla ośrodków większych niż 100 użytkowników wynosi 150 USD; dla ośrodków mających 10 000 użytkowników minimum wynosi 1000 USD na rok.

SpamCop nie umożliwia transferów strefy DNS, ponieważ prowadzona lista jest zbyt dynamiczna, by transfery strefy mogły być skuteczne. Zamiast tego pozwala na duplikowanie listy na Twoim własnym serwerze DNS przy użyciu narzędzi rsync i SSH. Ta usługa kosztuje jednak 1000 USD na rok.

Możesz ofiarować datek (lub zapłacić za zduplikowanie listy), korzystając z serwisu PayPal w witrynie WWW SpyCop lub możesz wysłać czek na fizyczny adres firmy.

Open Relay Database (ORDB)

Baza ORDB (ang. *Open Relay Database* — baza danych otwartych przekaźników) odnotowuje otwarte przekaźniki w internecie i robi to od 2001 roku. Operatorzy internetu oraz małe i duże organizacje korzystają z ORDB. Jest to niezarobkowa organizacja z siedzibą w Danii, ale ma współpracowników i użytkowników na całym świecie.

ORDB jest po prostu wykazem zgłoszonych i potwierdzonych otwartych przekaźników. Różni się od listy RSS w systemie MAPS pod tym względem, że dla ORDB nie jest istotne, czy witryna faktycznie była kiedykolwiek wykorzystywana do wysyłania spamu, czy nie, a jedynie czy pod względem *technicznym* jest otwartym przekaźnikiem. Dlatego jeśli z niej korzystasz, istnieje szansa zablokowania legalnych serwerów pocztowych, nawet jeśli te serwery nie są obecnie wykorzystywane przez spamerów. Pomysł zakłada, że znalezienie przez spamera otwartego przekaźnika i użycie go jest tylko kwestią czasu, więc lepiej go uprzedzić i zablokować witrynę. Zachęca to również administratorów systemów do zamykania swoich otwartych przekaźników, skoro wiedzą, że ich serwer może zostać zablokowany. Witryna firmy znajduje się pod adresem *http://www.ordb.org*.

Działanie ORDB

Typ listy:	*oparta na adresach IP*
Serwer DNSBL:	*relays.ordb.org*

Chcąc przetestować serwery pod kątem otwartych przekaźników, wystarczy podać ich adresy IP w witrynie ORDB. Osoba żądająca przetestowania musi podać poprawny adres e-mail, ponieważ przed rozpoczęciem testowania wymagane jest potwierdzenie. To wprowadza choć trochę odpowiedzialności i zmniejsza nadużywanie systemu. Testowanie może zająć do 72 godzin, w zależności od długości kolejki. Jeśli witryna nie przejdzie testu i okaże się być otwartym przekaźnikiem, zostanie wciągnięta na czarną listę ORDB.

Usunięcie witryny następuje w ten sam sposób. Adresy IP zostają podane w formularzu WWW i zostaje wysłany e-mail, na który osoba zgłaszająca musi odpowiedzieć, po czym następuje ponowne sprawdzenie witryny. Jeśli przejdzie pomyślnie test i okaże się nie być otwartym przekaźnikiem, witryna jest usuwana z listy w ciągu 72 godzin. Jeśli test nadal wykrywa otwarty przekaźnik, witryna pozostaje na liście.

Subskrybowanie się do ORDB

Lista ORDB nie wymaga opłat ani podpisywania umowy. Każdy może z niej swobodnie korzystać i jej organizatorzy wierzą, że jej używanie jest najlepszym sposobem popierania ORDB. Aczkolwiek możliwe jest przekazanie datku dowolnej wielkości za pośrednictwem serwisu PayPal lub wysyłając czek lub przekaz pocztowy na adres podany w witrynie.

Distributed Server Boycott List (DSBL)

Lista DSBL (ang. *Distributed Server Boycott List* — rozproszona lista bojkotowanych serwerów) jest grupą administratorów i użytkowników, którzy zjednoczyli się, by zwalczać spam. Zajmują się głównie źródłami spamu, które są otwartymi przekaźnikami lub otwartymi proxy. Witryna DSBL dostępna jest pod adresem *http://www.dsbl.org*.

Działanie DSBL

Organizacja DSBL sama nie sprawdza witryn. Dowolna osoba może zgłosić witrynę do listy DSBL, ale tak naprawdę robią to dwa rodzaje użytkowników: *zaufani* i *niezaufani*. Użytkownikiem niezaufanym jest każda osoba zgłaszająca spam do DSBL. Użytkownikiem zaufanym jest ktoś, kto poprosił o konto w DSBL i podał uzasadnienie, dlaczego powinien zostać zaufanym użytkownikiem. Wówczas DSBL nadaje temu użytkownikowi tymczasowe konto, które może zostać unieważnione, jeśli użytkownik naruszy standardy zgłoszeń wyznaczone przez DSBL.

List

Typ listy:	*oparta na adresach IP*
Serwer DNSBL:	*list.dsbl.org*

Ta lista zawiera tylko źródła spamu potwierdzone przez użytkowników darzonych zaufaniem przez personel DSBL. Dlatego ma mniejszączęstotliwość występowania fałszywych trafień niż inne listy DSBL.

Multihop

Typ listy:	*oparta na adresach IP*
Serwer DNSBL:	*multihop.dsbl.org*

Ta lista zawiera tylko źródła spamu przekazywanego wieloetapowo[1] (ang. *multihop relaying*), które zostały potwierdzone przez użytkowników darzonych zaufaniem przez personel DSBL. Chociaż są to zaufani użytkownicy, lista nadal może powodować fałszywe trafienia, ponieważ wyłapuje wszystkie punkty pośrednie na ścieżce spamu.

[1] Oznacza to, że e-mail jest przyjmowany przez jeden adres IP, a wysyłany przez inne — *przyp. tłum.*

Unconfirmed

Typ listy:	*oparta na adresach IP*
Serwer DNSBL:	*unconfirmed.dsbl.org*

Uzupełnienia tej listy mogą być dokonywane przez niezaufanych użytkowników, więc istnieje duże prawdopodobieństwo fałszywych trafień. Najlepiej jest korzystać z tej listy w niewielkim stopniu lub w połączeniu z innym programem, takim jak SpamAssassin, który tylko punktuje lub znakuje potencjalny spam, zamiast go z miejsca odrzucać.

Subskrybowanie się do DSBL

Nie jest wymagana żadna subskrypcja ani formularze dla żadnej z list DSBL. Wystarczy po prostu zacząć z nich korzystać.

Oprócz normalnych zapytań DNS możesz również pobrać cały plik strefy przy użyciu programu narzędziowego rsync bądź przez HTTP z witryny DSBL.

Spamhaus

Operatorzy firmy Spamhaus wierzą, że 90 procent całego spamu w Europie i Ameryce Północnej jest wysyłane przez mniej niż 200 znanych spamerów, których poczynania śledzą w swoim Rejestrze Znanych Operatorów Spamu (ang. *Registry of Known Spam Operators — ROKSO*). Dzięki rozpoznaniu swoich przeciwników i śledzeniu ich ruchów od jednego operatora internetu do kolejnego, czarna lista Spamhaus (SBL) stała się popularną i skuteczną listą DNSBL. Jej witryna WWW dostępna jest pod adresem *http://www.spamhaus.org*.

Działanie Spamhaus

Typ listy:	*oparta na adresach IP*
Serwer DNSBL:	*sbl.spamhaus.org*

Czarna lista Spamhaus (SBL) jest aktualizowana przez całą dobę przez międzynarodowy zespół administratorów, którzy obserwują znanych spamerów i trwające rozsyłanie spamu. Aktualizacje list SBL są dokonywane co godzinę.

Lista SBL odnotowuje znanych spamerów. Nie zawiera otwartych proxy lub otwartych przekaźników, więc Spamhaus zaleca wykorzystywanie swojej listy w połączeniu z dobrą listą otwartych proxy i przekaźników. Stosuje następujące kryteria, by podjąć decyzję, czy dany adres IP zostanie umieszczony na liście SBL.

- **Źródła spamu.** Spamerzy wysyłający masowo pocztę e-mail z adresu IP znajdującego się bezpośrednio pod kontrolą spamera.
- **Gangi spamowe.** Bloki sieci znanych spamerów notowanych w rejestrze ROKSO.
- **Usługi spamowe.** Serwery WWW, serwery pocztowe, serwery DNS oraz inne usługi wykorzystywane przez spamerów.

- **Serwisy popierające spam.** Adresy IP, które świadomie oferują prowadzenie serwisów WWW, oprogramowanie do rozsyłania spamu oraz inne usługi dla spamerów.

Adresy IP, które trafią na listę SBL, pozostają tam do chwili, kiedy źródło spamu zostanie usunięte i Spamhaus zostanie o tym powiadomiony. Sam Spamhaus nie wykonuje dalszych kontroli adresów IP. Jednak aby zapobiec starzeniu się wpisów, Spamhaus usuwa z listy SBL rekordy, które straciły ważność. Termin ważności wynosi dwa, siedem lub czternaście dni dla niezidentyfikowanych źródeł spamu, sześć miesięcy dla uporczywych spamerów bądź rok lub więcej dla powszechnie znanych spamerów takich jak ci w rejestrze ROKSO.

Subskrybowanie się do Spamhaus

Używanie listy Spamhaus nic nie kosztuje i nie musisz wypełniać żadnych formularzy, by móc z niej korzystać. Po prostu konfigurujesz ją tak samo, jak każdą inną listę DNSBL. Pozwala nawet na transfery strefy DNS za darmo, o ile pracujesz w dostatecznie dużej organizacji (takiej jak operator internetu, uniwersytet lub duża firma). W sprawie tej usługi musisz skontaktować się bezpośrednio z firmą Spamhaus.

Not Just Another Bogus List (NJABL)

Lista NJABL (ang. *Not Just Another Bogus List* — byle nie jeszcze jedna fałszywa lista) jest prowadzona przez grupę administratorów e-mail, którzy są poirytowani prowadzoną polityką i zawodnością istniejących list DNSBL. Postanowili wziąć sprawy w swoje ręce i stworzyli czarną listę, która jest niemal w całości obsługiwana przez administratorów e-mail, którzy z niej korzystają.

Działanie NJABL

Typ listy:	*oparta na adresach IP*
Serwer DNSBL:	*dnsbl.njabl.org*

NJABL ma tylko jedną listę. NJABL umieszcza na swojej liście wszystkie adresy IP spełniające następujące kryteria:

- System jest otwartym przekaźnikiem, otwartym proxy lub prowadzi otwartą bramę pocztową z dostępem przez WWW.
- Adres IP należy do zakresu połączeń telefonicznych lub dynamicznych. Te informacje są uzyskiwane z wpisów rejestru ARIN (ang. *American Registry for Internet Numbers*) lub od operatorów internetu zgłaszających te zakresy bezpośrednio do NJABL.
- System był wykorzystywany bezpośrednio do wysyłania spamu.

NJABL testuje otwarte przekaźniki, skanując poszczególne serwery. Następnie wykonuje test otwartego przekaźnika, skanując port SMTP. Usunięcie systemu z listy trwa około czterech tygodni.

Subskrybowanie się do NJABL

Lista NJABL jest w zasadzie prowadzona przez administratorów, którzy z niej korzystają. Nie musisz nic płacić, żeby móc ją subskrybować, ani nie musisz się nigdzie zapisywać. Możesz po prostu zacząć z niej korzystać w dowolny sposób. Operatorzy proszą jedynie o zapisanie się na listę dystrybucyjną *list@njabl.org*, byś mógł otrzymywać najświeższe zawiadomienia.

Możesz również przyczynić się do rozwoju NJABL, przekazując adresy IP, które łączą się z Twoim serwerem pocztowym. W tym celu zmieniasz swoją metodę łączenia się w taki sposób, że każdy, kto łączy się z Twoim serwerem, zgadza się na przeskanowanie pod kątem otwartości przekaźnika. Później NJABL testuje każdy z tych serwerów pod kątem otwartych przekaźników.

Lista NJABL jest zazwyczaj używana w trybie zapytań, ale możesz otrzymać transfer strefy przez rsync, wysyłając stosowny list na adres *help@njabl.org*.

RFC Ignorant (RFCI)

Lista RFC wyróżnia się na tle innych list DNSBL, ponieważ nie interesuje się tym, czy witryna jest bądź może być spamerem. Tak naprawdę zamiast martwić się spamem, RFCI jest bardziej zainteresowana tym, czy administrator domeny lub sieciowego bloku IP jest dobrym „netizenem”[2] (tj. obywatelem internetu), czy nim nie jest. Domeny i bloki sieci odnotowane na liście RFCI zostały tam umieszczone, ponieważ ich właściciele zostali uznani za ignorantów RFC.

Mogłeś już wcześniej słyszeć termin *RFC* i możesz go mgliście kojarzyć ze standardami internetowymi (liczne firmy zachwalają swoje produkty jako „zgodne z RFC”). RFC jest skrótem od *Request for Comments* (z ang. prośba o komentarze), co jest wspólną nazwą dla reguł i najlepszych praktyk zatwierdzonych i opublikowanych przez zespół IETF (ang. *Internet Engineering Task Force*). Wiele dokumentów RFC jest projektami technicznymi, ale niektóre z nich są protokołami dla ludzi — najlepszymi praktykami konfigurowania i prowadzenia sieci oraz serwisów w internecie. Domeny figurują na liście RFCI dlatego, że ich właściciele odrzucają bądź ignorują te zasady i procedury.

Jaki ma to związek z rozsyłaniem spamu? Spamerzy starają się zataić o sobie tyle informacji, ile tylko możliwe. Większość praktyk RFC sprawdzanych przez RFCI jest związana z faktyczną możliwością nawiązania kontaktu z człowiekiem. Jeśli spamer zarejestrował domenę, prawdopodobnie podał fałszywe informacje kontaktowe, przez co nie będziesz mógł go wyśledzić i złożyć skargę (lub być może zaskarżyć). Zatem spora część osób notowanych przez RFCI jest potencjalnymi spamerami.

Listę RFCI można znaleźć pod adresem *http://www.rfc-ignorant.org*. Dokumenty RFC są dostępne na stronach *http://www.ietf.org* pod łączem zatytułowanym „RFC Pages”.

---

[2] Termin powstał jako połączenie dwóch angielskich słów: net (sieć) oraz citizen (obywatel), oznaczający kogoś korzystającego na co dzień z zasobów internetu oraz uczestniczącego aktywnie w jego rozwoju — *przyp. tłum.*

Co czyni kogoś ignorantem RFC?

Dokumenty RFC nie są obowiązującym prawem, więc za ich łamanie nie grożą konsekwencje karne. Jednak od początków internetu administratorzy wolą stronić od zatwardziałych profanów (niektóre programy robią to automatycznie). Aby zostać wpisaną na listę RFCI, witryna musi okazać, że jej właściciele nie zrealizowali jednej lub więcej z wytycznych RFC wymienianych w kolejnych podpunktach.

Związane z DSN (zawiadamianiem o statusie doręczenia wiadomości)

Typ listy:	*Domenowa*
Serwer DNSBL:	*dsn.rfc-ignorant.org*
Istotne RFC:	*821*, *2821*, *2505*, *1123*

Umieszczenie na tej liście następuje, jeśli wpis przekaźnika poczty (MX) domeny nadawcy nie akceptuje korespondencji o adresach źródłowych podanych jako <> (pusty). Na przykład jeśli wyślemy list do serwera MX *przykladowadomena.tld*, korzystając z następujących poleceń SMTP:

```
MAIL FROM <>
RCTP TO <postmaster@przykladowadomena.tld>
```

i serwer nie przyjmie tej wiadomości, *przykladowadomena.tld* zostaje dodana do listy. Dla każdej domeny sprawdzane są wszystkie wpisy MX i posiadanie choć jednej, która nie akceptuje listów z pustym adresem nadawcy, jest podstawą do umieszczenia na liście. Domeny z wpisami MX zawierającymi prywatne lub zarezerwowane adresy IP (na przykład adres pętli zwrotnej lub sieci wymienianych w RFC 1981, takich jak 10.0.0.0/8) również trafiają na listę.

Związane z poczmistrzem

Typ listy:	*domenowa*
Serwer DNSBL:	*postmaster.rfc-ignorant.org*
Istotne RFC:	*2821*

Adres poczmistrza (ang. *postmaster*) ma służyć do zgłaszania problemów związanych z serwerami pocztowymi. Umieszczenie na tej liście następuje, jeśli domena nadawcy (posiadająca wpis MX) nie ma poprawnego adresu e-mail poczmistrza. Przykładem jest *postmaster@przykladowadomena.tlb*. Co więcej, e-maile wysłane do poczmistrza muszą ostatecznie trafić do adresata, nawet jeśli najpierw wysyłana jest odpowiedź automatyczna.

Związane z nadużyciami

Typ listy:	*domenowa*
Serwer DNSBL:	*abuse.rfc-ignorant.org*
Istotne RFC:	*2142*

Adres nadużyć (ang. *abuse*) służy do zgłaszania spamu, oszustw oraz innych incydentów związanych z pocztą, popełnionych przez użytkowników danej domeny. Umieszczenie na

tej liście następuje, jeśli domena nadawcy (posiadająca wpis MX) nie ma poprawnego adresu e-maill do zgłaszania nadużyć — na przykład *abuse@ przykladowadomena.tld*. Podobnie jak w przypadku poczmistrza, adres nadużyć musi ostatecznie prowadzić do człowieka.

Związane z bazą WHOIS

Typ listy: *domenowa*
Serwer DNSBL: *whois.rfc-ignorant.org*
Istotne RFC: *954*

Baza danych WHOIS zawiera informacje kontaktowe właścicieli domeny, w tym ich adresy e-mail. Obowiązuje to zarówno dla podstawowych domen wysokiego poziomu (gTLD, takich jak *.com*, *.org* lub *.net*), jak również narodowych domen wysokiego poziomu (ccTLD, takich jak *.us*, *.uk* lub *.pl*). Rejestratorzy tych domen prowadzą swoje własne serwery WHOIS służące do dostarczania tych informacji.

Jednak wielu rejestratorów domen nie sprawdza informacji podawanych przez ich klientów, więc możliwe jest umieszczanie fałszywych punktów kontaktowych, pozostawienie niektórych informacji pustych lub pozwolenie na zestarzenie się tych informacji.

Domena jest umieszczana na tej liście, jeśli spełnia następujące kryteria:

- Informacje są w oczywisty sposób fałszywe lub nieprawidłowe (na przykład w Stanach Zjednoczonych numer telefonu 555-1212 lub adres 1600 Pennsylvania Ave., Washington, D.C.dla kogokolwiek innego niż Biały Dom).
- Informacje po sprawdzeniu okazują się nieprawidłowe, tak jak niedziałające linie telefoniczne, adresy e-mail odbijające wiadomość do nadawcy lub zwroty listów wysyłanych konwencjonalną pocztą.
- Domena wysokiego poziomu dla danej domeny nie prowadzi serwera WHOIS, wskazywanego przez główny serwer WHOIS pod adresem *whois.iana.org*.
- Domeny w kontaktowych adresach e-mail nie mają poprawnych wpisów MX lub wpisy są w oczywisty sposób fałszywe (takie jak adres pętli zwrotnej bądź adresy zarezerwowane przez RFC 1918, takie jak 10.10.10.10).

Wpis domeny nie musi mieć poprawnego numeru faksu, ponieważ nie wszyscy mają faksy. Jednak siedziba domeny powinna mieć poprawne głosowe numery telefoniczne, konta e-mail oraz adres pocztowy, który ktoś faktycznie sprawdza i odpowiada z niego.

Związane z bazą IPWHOIS

Typ listy: *adresy IP*
Serwer DNSBL: *ipwhois.rfc-ignorant.org*
Istotne RFC: *954*

Baza IPWHOIS jest w dużej mierze podobna do WHOIS, tylko że dotyczy rejestru informacji kontaktowych dla bloków sieciowych adresów IP, a nie domen. Zasady umieszczania na tej liście są praktycznie takie same jak w przypadku bazy WHOIS. Jeśli dla danego

bloku sieciowego jakiekolwiek fałszywe informacje znajdują się we wpisie IPWHOIS w regionalnym rejestrze internetowym (ang. *Regional Internet Registry — RIR*), ten blok sieci znajdzie się na liście. Jeśli na liście umieszczony zostanie duży blok sieci, taki jak 192.168.0.0/16, włączane są wszystkie podsieci znajdujące się pod tą siecią (na przykład, 192.168.5.0/24). Zatem problem z siecią nadrzędną powoduje problemy z siecią potomną. Innymi słowy, jeśli Twój operator internetu nie przestrzega RFC, Twoja sieć również nie jest zgodna.

Ważne jest, by zauważyć, że lista IPWHOIS jest jedyną usługą RFCI opartą na adresach IP (to znaczy kryteria są oparte na adresach IP nadawców poczty, a nie domenach).

Subskrybowanie się do RFCI

Korzystanie z RFCI jest zupełnie bezpłatne i nie musisz podpisywać żadnej umowy, by korzystać z ich usług. Wystarczy, jeśli wprowadzisz adresy serwerów prowadzących listy w swoim serwerze lub kliencie pocztowym potrafiącym obsługiwać listy DNSBL. RFCI udostępnia interfejs WWW umożliwiający zgłaszanie ignorowania RFC oraz adresy e-mail pozwalające usunąć z listy domenę lub blok sieci IP. Możesz się również zapisać do listy korespondencyjnej, na której znajdziesz pomoc ze strony innych członków społeczności.

Teraz, kiedy już przedstawiliśmy Ci niektóre czarne listy, pokażemy, jak z nich korzystać. Skupimy się na trzech serwerach pocztowych: Sendmail i Postfix dla systemów Linux i Unix oraz Exchange dla Microsoft Windows.

Implementacja list DNSBL w Sendmailu

Sendmail jest najbardziej sędziwym agentem przesyłania poczty w internecie i działa w Uniksie i większości uniksopodobnych systemów operacyjnych. (W rzeczywistości niemal każda większa dystrybucja Linuksa zawiera Sendmaila). Bezpośrednia obsługa list DNSBL została dodana w wersji 8.9, w wersji 8.10 zaś zmieniono nieznacznie składnię. Obsługa list była również możliwa w wersji 8.8, ale żeby to osiągnąć, trzeba było przerabiać plik konfiguracyjny *sendmail.cf*. Jednak z powodu luk w zabezpieczeniach we wcześniejszych wersjach Sendmaila, wliczając poważne błędy przepełnienia bufora wykryte na wiosnę i jesienią 2003 roku (patrz raporty CERT CA-2003-12 i CA-2003-25), gorąco zalecamy, żebyś korzystał z najnowszej stabilnej wersji. Możesz znaleźć Sendmaila na stronie *http://www.sendmail.org*.

Konfiguracja Sendmaila dla list DNSBL opartych na IP

Według standardów Sendmaila konfiguracja Sendmaila po wersji 8.10 w taki sposób, aby używał list DNSBL opartych na IP, jest stosunkowo prosta. Wystarczy zmienić plik *sendmail.mc* lub równoważy plik *.mc*, z którego korzystasz. Jeśli nie wiesz, czym są pliki *.mc*, to wyjaśniamy, że są one definicjami makr kompilowanych za pomocą aplikacji *m4*, by stworzyć pliki konfiguracyjne *sendmail.cf*. Więcej informacji znajdziesz w dokumentacji Sendmaila lub na jego stronie WWW. Obsługa list DNSBL jest konfigurowana jako właściwość *m4*.

Najprostszą w użyciu listą DNSBL jest MAPS RBL, ponieważ jej obsługa jest wstępnie skonfigurowana. Wszystko, co musisz zrobić, to zmienić swój plik *sendmail.mc*, dodając następujący wiersz *przed* sekcją MAILER:

```
FEATURE(`dnsbl')
```

Zauważ, że pierwszy apostrof jest tak naprawdę lewym apostrofem (zazwyczaj umieszczonym po lewej stronie klawiatury).

Następnie zrób kopię zapasową swojego bieżącego pliku *sendmail.cf* i skompiluj plik *.mc*, aby otrzymać nowy plik *.cf*:

```
# m4 sendmail.mc > sendmail.cf
```

Jeśli kompilacja się powiedzie, nie dostaniesz żadnych komunikatów. Wtedy uruchom ponownie Sendmaila, używając nowego pliku *.cf*.

Aby użyć innych list DNSBL, w poleceniu `FEATURE` musisz podać serwer listy. Oto podstawowa składnia:

```
FEATURE(`dnsbl',<serwer strefy>, <wiadomość o odrzuceniu dla serwera zdalnego
i dzienników>)
```

Tutaj jako przykład mamy polecenie dla czarnej listy ORDB:

```
FEATURE(`dnsbl',`relays.ordb.org',`"550 Email rejected due to sending server
misconfiguration - see http://www.ordb.org/faq/\#why_rejected"')dnl
```

Przy wielu wpisach dodaj wiersz `FEATURE` dla każdego przekaźnika, z którego chcesz korzystać.

Konfiguracja Sendmaila dla list RHSBL opartych na domenie

Użycie list RHSBL w Sendmailu wymaga dodania innego polecenia `FEATURE` do pliku *sendmail.mc*. Ta właściwość nie jest częścią standardowej dystrybucji Sendmaila. Pod adresem *http://www.megacity.org/software_downloads/rhsbl.m4* możesz pobrać plik *rhsbl.m4* autorstwa Dereka J. Ballinga. Umieść ten plik w katalogu *./cf/feature* w drzewie źródłowym Sendmaila lub tam, gdzie przechowujesz swoje pliki konfiguracyjne *.cf*. Następnie dodaj listę RHSBL do Twojego pliku *.mc*, używając składni:

```
FEATURE (rhsbl, <serwer strefy>, <wiadomość o odrzuceniu dla serwera zdalnego
i dzienników>)
```

Tutaj mamy przykład, jak używać czarnej listy opartej na domenie RFCI DSN:

```
FEATURE (rhsbl , `dsn.rfc-ignorant.org',`"550 Mail from domain " $`'&{RHS} " refused.
MX of domain do not accept bounces. This violates RFC 821/2505/2821 - see
http://www.rfc-ignorant.org/"')
```

Tak jak w przypadku list DNSBL, dodaj instrukcję `FEATURE` dla każdej listy RHSBL, z której chcesz korzystać.

Implementacja list DNSBL w Postfiksie

Postfix jest kolejnym popularnym zastępcą Sendmaila dla Uniksa i uniksopodobnych systemów operacyjnych, zaprojektowanym przez Wietse Venema w czasie, gdy pracował dla IBM. IBM wypuściło publiczną wersję w 1998 i Postfix jest rozpowszechniany zgodnie ze strategią otwartego dostępu do kodu źródłowego lansowanego przez tę firmę. Postfix był projektowany z myślą o bezpieczeństwie i szybkości. Omówimy tutaj tylko Postfix w wersji 2.*x*. Program można pobrać ze strony *http://www.postfix.org*.

Konfiguracja Postfiksa dla list DNSBL opartych na IP

Postfix jest prawdopodobnie jednym z najprostszych serwerów pocztowych, jeśli chodzi o konfigurację list DNSBL. Wszystko, co musisz zrobić, to przeredagować plik *main.cf* (zwykle znajdujący się w */etc/postfix*) i zmienić (lub dodać) wiersz `smtpd_client_restrictions`. Ten wiersz steruje wieloma funkcjami powiązanymi ze spamem, w tym zabezpieczeniami przed przekazywaniem (ang. *anti-relaying*).

Żeby skonfigurować Postfix 2.x w taki sposób, żeby odrzucał korespondencję umieszczoną na liście DNSBL, wprowadź następujące zmiany:

```
smtpd_client_restrictions =
      reject_rbl_client <serwer strefy>
```

gdzie `<serwer strefy>` jest listą DNSBL, z której chcesz korzystać. Na przykład:

```
smtpd_clients_restrictions =
      reject_rbl_client sbl.spamhaus.org
```

Aby dodać kilka list, oddziel przecinkiem każdy wiersz `reject_rbl_client`:

```
smtpd_client restrictions =
      reject_rbl_client sbl.spamhaus.org,
      reject_rbl_client relays.ordb.org,
      reject_rbl_client lists.dsbl.org
```

Żeby wprowadzić w życie te zmiany, uruchom ponownie Postfiksa. Odrzucona korespondencja będzie rejestrowana w pliku dziennika.

Konfiguracja Postfiksa dla list RHSBL opartych na domenie

Postfix 2.*x* ma wbudowaną obsługę list RHSBL. Konfiguruje się je w bardzo podobny sposób, jak to robiliśmy dla list DNSBL, z wyjątkiem tego, że używa się polecenia `reject_rhsbl_sender`. Robi się to następująco:

```
smtpd_client_restrictions =
      reject_rhsbl_client <serwer strefy>
```

Oto przykład dla listy RFC Ignorant:

```
srntpd_client_restrictions =
       reject_rhsbl_sender dsn.rfc-ignorant.org
```

Aby dodać kilka list RHSBL (lub połączyć je z listami DNSBL), wystarczy oddzielić je przecinkami:

```
smtpd_client_restrictions =
      reject_rbl_client sbl.spamhaus.org,
      reject_rbl_client relays.ordb.org,
      reject_rbl_client list.dsbl.org,
      reject_rhsbl_sender dsn.rfc-ignorant.org,
      reject_rhsbl_sender postmaster.rfc-ignorant.org,
      reject_rhsbl_sender whois.rfc-ignorant.org
```

Po wprowadzeniu zmian ponownie uruchom Postfix. Odrzucona korespondencja będzie rejestrowana w pliku dziennika.

Implementacja list DNSBL w Microsoft Exchange

Podczas gdy Sendmail i Postfix są nadal ulubieńcami wielu operatorów internetu, centrów danych oraz zakładów stworzonych w oparciu o Uniksa, serwer Microsoft Exchange jest najpopularniejszym korporacyjnym systemem poczty elektronicznej. Chociaż bez wątpienia wiele firm ustawia przed swoim serwerem Exchange drugi serwer, na którym uruchomiona jest jedna z dwóch wspomnianych wcześniej implementacji, to również nie ulega wątpliwości, że wiele serwerów Exchange przetwarza pocztę samodzielnie.

Exchange 2000 (zakładamy, że większość z Was dokonała już aktualizacji z Exchange 5 i 5.5) posiadał niewiele właściwości z zakresu zwalczania spamu. Exchange 2000 wymagał modułów rozszerzających niezależnych producentów lub dodatkowych serwerów, aby móc uporać się ze spamem. Exchange 2003 naprawił sytuację, wprowadzając własne rozwiązania do walki ze spamem. Omówimy ten postęp w odniesieniu do list DNSBL.

Exchange 2000

Exchange 2000 wymaga korzystania z aplikacji innych producentów, by móc korzystać z list DNSBL. Niemal wszystkie pakiety antyspamowe dla Exchange obsługują listy DNSBL, w tym te przedstawione w rozdziale 11., „Serwery antyspamowe dla Windows". W połączeniu z Exchange 2000 możesz również używać dwóch darmowych programów (ale nie z otwartym dostępem do kodu źródłowego).

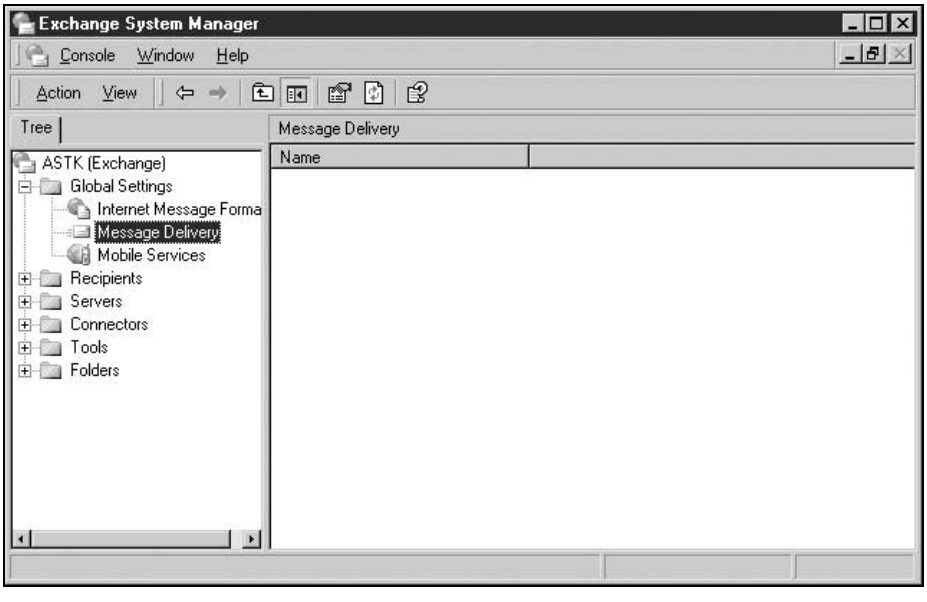
Pierwszym z nich jest darmowa wersja pakietu GFI Mail Essentials, którą można znaleźć pod adresem *http://www.gfi.com*. W wersji darmowej brakuje kilku właściwości antyspamowych z wersji pełnej, ale w kwestii list DNSBL spisuje się ona całkiem dobrze. Jeśli zostanie ustalone, że e-mail pochodzi od spamera, GFI pozwala Ci go oznakować i opcjonalnie przerzucić do folderu publicznego. Zauważ, że GFI wymaga również uruchamiania usługi SMTP w serwerze IIS 5 (ang. *Internet Information Services*).

Kolejnym darmowym programem obsługującym listy DNSBL dla Exchange jest ORFilter, dostępny na stronie *http://www.martijnjongen.com/eng/orfilter/*. Możesz skonfigurować ORFilter, żeby blokował spam lub tylko go znakował. ORFilter współpracuje z Exchange 2000 lub usługą Microsoft SMTP.

Exchange 2003

Microsoft Exchange 2003 ma wbudowaną możliwość korzystania z list DNSBL opartych na IP. Obsługa RHSBL być może pojawi się w przyszłości, ale obecnie nie jest dostępna. Jak można się spodziewać po środowisku Windows, dostępny jest przyjemny graficzny interfejs użytkownika, umożliwiający zarządzanie listami DNSBL oraz czarnymi i białymi listami.

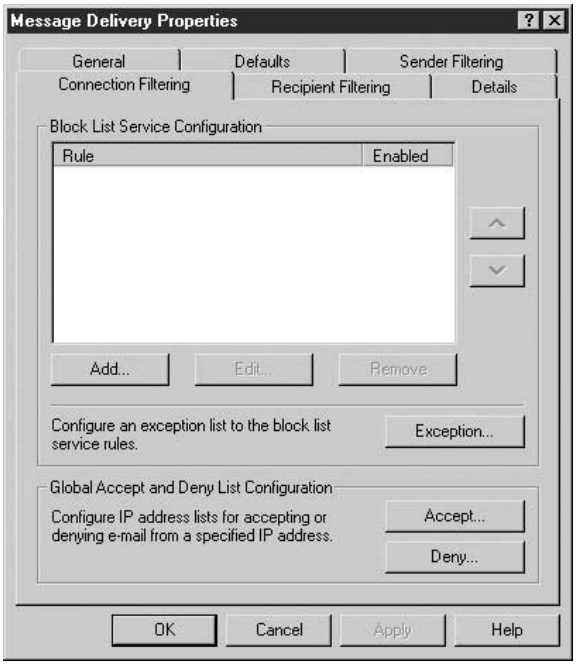
Żeby dodać listy DNSBL do Exchange 2003, otwórz *Exchange System Manager*, wybierając *Start/Programy/Microsoft Exchange* (jeśli zainstalowałeś go gdzie indziej, idź do odpowiedniej pozycji w menu). Powinien pojawić się *Exchange System Manager*. W drzewie po lewej stronie okna otwórz folder *Global Settings*, tak jak pokazano na rysunku 5.1.



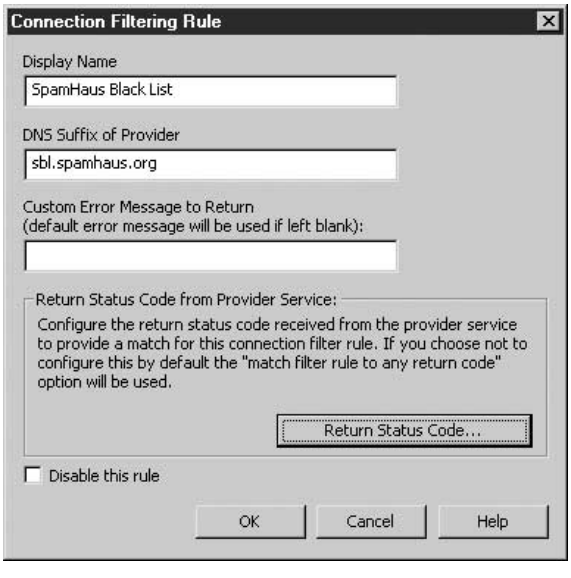
Rysunek 5.1. *Exchange System Manager dla Exchange 2003*

Kliknij prawym przyciskiem myszy pozycję *Message Delivery* poniżej folderu *Global Settings* i wybierz opcję *Properties*. Zobaczysz okno *Message Deliver Properties* pokazane na rysunku 5.2. Kliknij zakładkę *Connection Filtering* umieszczoną na górze. Lista *Block List Service Configuration* zawiera dwie kolumny: *Rule* i *Enabled*. Jeśli nigdy wcześniej nie konfigurowałeś listy DNSBL na swoim serwerze, te pola będą puste.

Żeby dodać listę DNSBL, kliknij na przycisku *Add*. Pojawi się okno dialogowe *Connection Filtering Rule*. To tu podasz informacje o DNSBL. Pierwszym polem jest *Display Name*, gdzie możesz wpisać dowolny opis, jaki chcesz nadać tej konkretnej regule. Naszą pierwszą listą DNSBL będzie Spamhaus SBL, dlatego nazwiemy naszą pierwszą regułę *Czarna lista(Black List) SpamHaus*. Drugie pole, *DNS Suffix Of Provider*, jest tym samym, co wcześniej określaliśmy jako serwer DNSBL. Serwerem strefy Spamhaus jest *sbl.spamhans.org*, więc podamy tę informację. To jest naprawdę wszystko, czego potrzebujesz, żeby rozpocząć filtrowanie i wygląda to tak jak na rysunku 5.3.



Rysunek 5.2. *Okno Message Delivery Properties, w którym zarządzasz listami DNSBL w Exchange 2003*

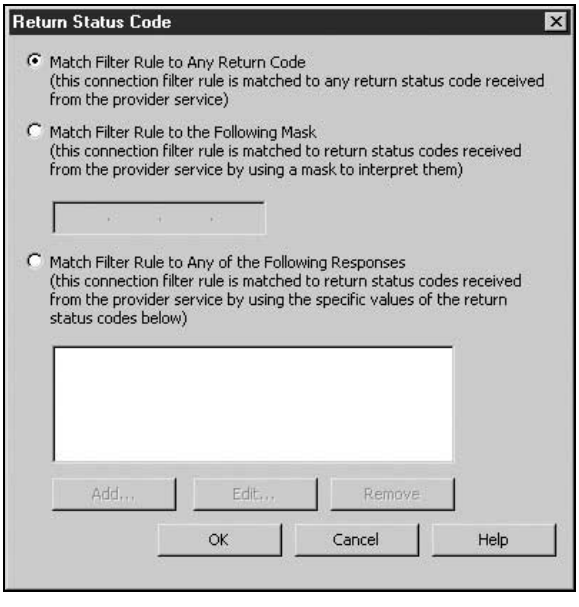


Rysunek 5.3. *Okno dialogowe Connection Filtering Rule do dodawania list DNSBL w Exchange 2003*

W tym momencie możesz się cofnąć i dodać inne listy DNSBL oparte na IP, oprócz Spamhaus.

Inną opcją w tym oknie jest dodawanie własnych komunikatów o błędach przez wpisanie ich w polu *Custom Error Message To Return*. Jest to pole opcjonalne i nie jest wymagane do poprawnego funkcjonowania DNSBL. Jest to jednak użyteczne, jeśli chcesz, żeby poczta była odrzucana z jakimś konkretnym komunikatem o błędzie (tylko bez drwin, proszę!).

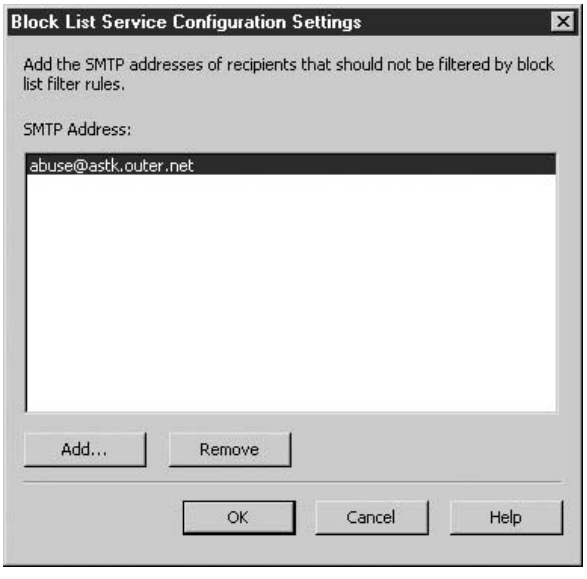
Na koniec możesz także zmienić kod statusu zwracany przez DNSBL, wykorzystywany przez serwer Exchange, klikając przycisk *Return Status Code From Provider Service*. Wyświetlone zostanie okno dialogowe *Return Status Code*, pokazane na rysunku 5.4. Pamiętaj, że większość list DNSBL odpowiada „kodem" (w rzeczywistości adresami IP) w obrębie zakresu pętli zwrotnej 127.0.0.0/8. Domyślną opcją (i pierwszym przyciskiem opcji) jest użycie każdej odpowiedzi z DNSBL jako odpowiedzi pozytywnej. Drugi przycisk opcji pozwala Ci wykorzystać konkretną maskę dla adresów. Trzecia opcja pozwala Ci wybrać konkretną wartość odpowiedzi. Ostatnie dwie opcje są użyteczne dla list DNSBL, które mają jeden serwer strefy, ale w jego obrębie działają różne „listy". Na przykład lista otwartych przekaźników DNSBL mogłaby zwracać odpowiedź 127.0.0.5, lista otwartych proxy 127.0.0.6, a lista łączy z dostępem telefonicznym 127.0.0.7. Dzięki tym opcjom możesz tworzyć oddzielne reguły dla każdej z tych list.



Rysunek 5.4. *Okno dialogowe Return Status Code pozwala zmieniać spodziewane odpowiedzi z list DNSBL w Exchange 2003*

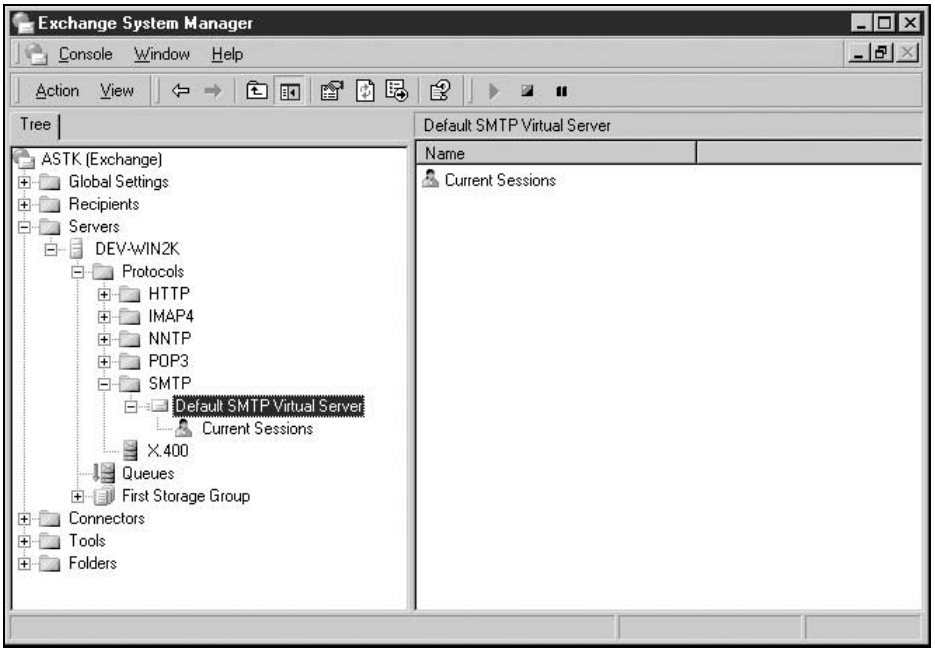
Wracając do okna *Message Delivery Properties* (rysunek 5.2), zobaczysz przycisk oznaczony *Exception*. Kliknięcie go spowoduje wyświetlenie okna *Block List Service Configuration Settings* pokazanego na rysunku 5.5. Możesz w nim podać lokalne adresy e-mail, dla których nie chcesz stosować czarnych list. Jest to szczególnie przydatne dla adresów, które muszą akceptować każdą dostarczaną pocztę, takich jak adresy poczmistrza (ang. *postmaster*) lub adres do zgłaszania nadużyć (ang. *abuse*) oraz dla adresów, w przypadku których obawiasz się utraty korespondencji — na przykład adresów sprzedawców.

Inne opcje w oknie *Message Delivery Properties* umożliwiają zezwolenie i zakazanie pewnym określonym adresom IP lub podsieciom IP wysyłania do Ciebie poczty. Jest to odpowiednik lokalnych białych i czarnych list i są one konfigurowane w oknach dialogowych, które są otwierane przez kliknięcie odpowiednio przycisków: *Accept* i *Deny*. Zauważ, że te ustawienia przesłaniają ustawienia DNSBL,a adresy lub sieci umieszczone na liście *Accept* przesłaniają te na liście *Deny*.



Rysunek 5.5. *Okno dialogowe Block List Service Configuration Settings pozwala wykluczyć lokalnych użytkowników, których poczta ma nie być sprawdzana względem czarnych list w Exchange 2003*

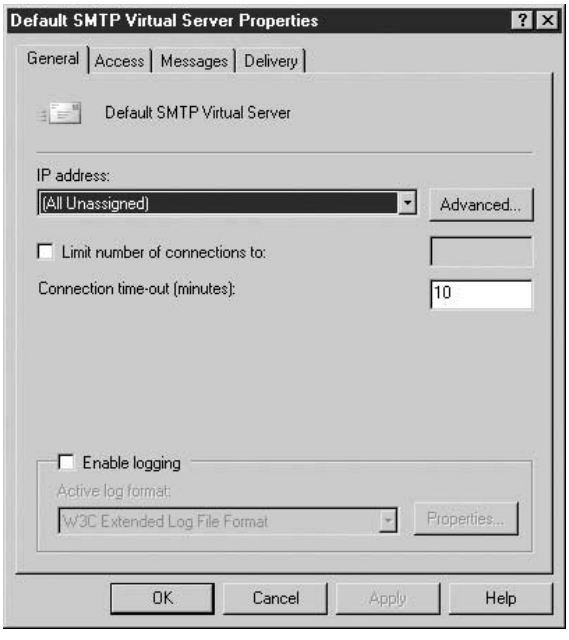
Kiedy już skonfigurujesz swoje reguły i klikniesz *OK*, to jeszcze nie wszystko, co musisz zrobić. Musisz też zastosować filtry na swoich wirtualnych serwerach SMTP. Będąc z powrotem w *Exchange System Manager*, otwórz na drzewie folder *Servers* i idź do *Servers/<Nazwa Twojego systemu>/SMTP/Default SMTP Virtual Server*, tak jak jest to pokazane na rysunku 5.6.



Rysunek 5.6. *Położenie opcji Default SMTP Virtual Server w drzewie Exchange System Manager dla Exchange 2003*

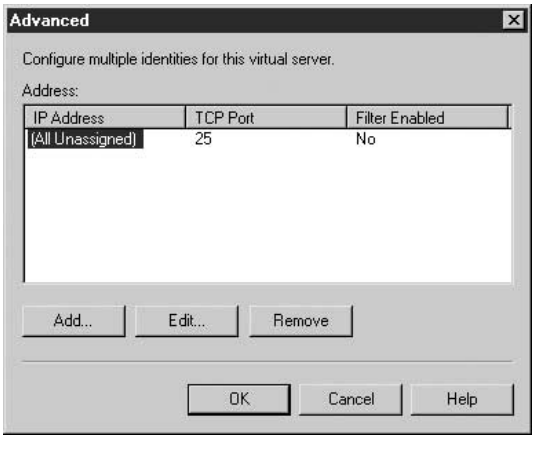
Kliknij prawym przyciskiem myszy opcję *Default SMTP Virtual Server* i wybierz opcję *Properties*. Wyświetlone zostanie okno *Default SMTP Virtual Server Properties* pokazane na rysunku 5.7. Kliknij na przycisku *Advanced*.

Rysunek 5.7. *Okno Default SMTP Virtual Server Properties w Exchange 2003*

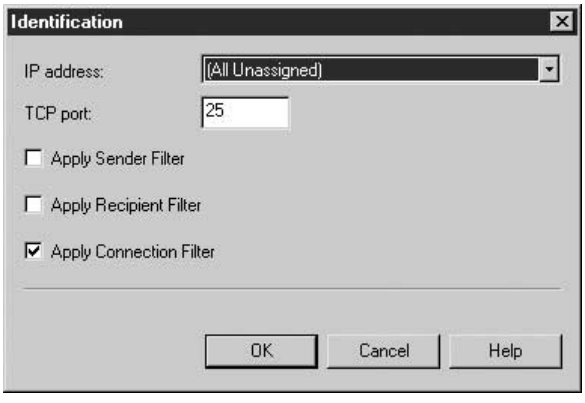


Przycisk *Advanced* zaprowadzi Cię do okna *Advanced*, które zawiera listę tożsamości IP wirtualnych serwerów i informuje, czy każda jest filtrowana, czy nie. Pokazuje to rysunek 5.8. Wybierz tożsamość serwera, do którego chcesz zastosować filtr, i kliknij przycisk *Edit*.

Rysunek 5.8. *Okno Advanced informuje o statusie filtrowania tożsamości wirtualnego serwera w Exchange 2003*



Po kliknięciu przycisku *Edit* pojawi się okno dialogowe *Identification*. Jedyną pozycją w tym oknie dialogowym, która jest związana z filtrami, jest umieszczone na samym dole pole wyboru *Apply Connection Filters*, tak jak to zostało pokazane na rysunku 5.9.



Rysunek 5.9. *Okno dialogowe Identification, gdzie włączasz filtry DNSBL dla wirtualnych serwerów w Exchange 2003*

Zaznacz to pole, a następnie kliknij przycisk *OK*, żeby zastosować te ustawienia. Sprawdź w oknie *Advanced*, czy filtrowanie zostało włączone. Musisz wykonać te same kroki dla każdego wirtualnego serwera, do którego chcesz zastosować filtry DNSBL.

Podsumowanie

Czarne listy DNS pomagają ograniczyć ilość spamu, dając możliwość odrzucenia, oznakowania lub ocenienia wiadomości e-mail pochodzących od znanych lub potencjalnych źródeł spamu. Dzięki nim możesz korzystać z doświadczenia i środków innych osób. Podstawowym problemem dotyczącym DNSBL jest stosunkowo duża szansa otrzymania fałszywych trafień — większa niż w przypadku większości innych rozwiązań antyspamowych. Potencjalnie całe sieci poczty elektronicznej mogą zostać zgubione, w razie gdyby jakiś większy serwer lub serwis pocztowy trafił na listę DNSBL. Co więcej, w dużym stopniu pokładasz zaufanie w ludziach, którzy prowadzą i współpracują z listami DNSBL.

Przez zrozumienie technologii i filozofii stojących za poszczególnymi czarnymi listami jesteś w stanie wybrać te, które najlepiej pasują do Twoich potrzeb. Większość serwerów e-mail i oprogramowania antyspamowego obsługuje listy DNSBL albo bezpośrednio, albo przez rozszerzenia innych producentów, więc nie ma żadnych powodów, żeby listy DNSBL nie miały być częścią Twojej strategii antyspamowej. Aczkolwiek nie licz na nie jako na Twój podstawowy środek do blokowania spamu.