Uniwersytet w Białymstoku

Wydział Matematyczno-Fizyczny

Instytut Matematyki

Mariusz Kozikowski

Przegląd oprogramowania służącego do filtrowania poczty elektronicznej

Praca dyplomowa napisana
pod kierunkiem
dr. Jana Kowalskiego

Białystok 2004

Spis treści

Wprowadzenie

W swojej pracy związanej z ochroną poczty elektronicznej podejmę wyzwanie walki z jednym z poważnych zagrożeń współczesnej komunikacji internetowej, czyli z masowym przesyłaniem na nasze skrzynki pocztowe dużej ilości reklam, a także innego rodzaju niezamawianej poczty elektronicznej. Wstępnie przedstawię ogólne pojęcia związane ze spamem, ich rodzajami, sposobami w jaki adresy pocztowe są zdobywane przez spamerów, sposobami obrony i kontrataku. W ramach pracy przedstawione zostanie oprogramowanie służące do ochrony naszej prywatności przed zalewem niechcianej informacji, gdzie brana będzie pod uwagę jego funkcjonalności i skuteczność, a także możliwość dostosowania działania programu do indywidualnych potrzeb użytkownika.

Rozdział 1

Problematyka spamu

1.1 Ogólne wiadomości o spamie.

O zaletach Internetu można napisać bardzo wiele. Szczególnie uwagę zwraca się na możliwość taniej i swobodnej komunikacji, wymiany informacji, dzięki niemu mamy dostęp do baz danych informacji z całego świata. Stąd też możemy wyróżnić jego dwie funkcje: informacyjną i komunikacyjną. Stwarza to ogromne możliwości do rozwoju dla firm, czyli elektronicznego biznesu. To właśnie Internet stwarza możliwość dotarcia z reklamą do milionów użytkowników. Bardzo często podstawą sukcesu całych kampanii reklamowych jest promocja nowych towarów w sieci. przy takich kampaniach bardzo często wykorzystywany jest tzw. direct-mailing, czyli bezpośrednie przesyłanie na skrzynki pocztowe materiałów reklamowych. Właśnie z tą formą reklamy jest kojarzone pojęcie SPAM'u, czyli Stupid Person Advertisement.
Pojęcie 'spamu' możemy określić jako wysłanie tej samej wiadomości do jednej lub wielu skrzynek pocztowych. Treść i kontekst informacji nie mają tutaj większego znaczenia, liczy się tutaj głównie fakt, iż adresat nie jest zainteresowany taką wiadomością, a czasem w sposób wyraźny protestuje przed jej przyjęciem. Właśnie z powodu takich niechcianych wiadomości uniemożliwione jest bardzo często normalne korzystanie ze skrzynki pocztowej. Indywidualny użytkownik traci czas na przeglądanie i kasowanie niechcianych listów, co jest szczególnie dotkliwe, gdy korzysta się z łącza komputerowego. W firmach i instytucjach poważnym problemem z pewnością okaże się pochłanianie przez spam zasobów systemowych serwera pocztowego. Podejrzane listy zajmują miejsce w kolejce listów do wysłania lub generują dodatkowe procesy obsługującą tę kolejkę. W skrajnych przypadkach rozsyłanie spamu może zapchać połączenie z Internetem, utrudniając funkcjonowanie firmy.
Uciążliwość spamu nie musi być nikomu udowadniana. Do walki z tym procederem powoływane są coraz to nowe organizacje: Coalition Against Unsolicited Commercial Email(CAUCE) oraz stworzony w 1999 roku jej europejski oddział, natomiast obowiązujące w Polsce prawo może przeciwdziałać prak-

tykom reklamowym opartym na spamie. Należy pamiętać, iż spam osłabia potencjał reklamowy tkwiący w poczcie elektronicznej zmniejszając zaufanie konsumentów do promocji towarów w ten sposób.

1.2 Odmiany spamu.

Spam może występować pod kilkoma postaciami:
Pierwszy z nich to Excessive Multi-Posting, czyli zbyt wiele kopii tej samej wiadomości. Do wiadomości tego typu możemy zaliczyć przesyłki, które w identycznej lub w niewielkim stopniu zmodyfikowanej formie kierowane są do dużej ilości użytkowników lub grup dyskusyjnych, jednym słowem są to listy reklamujące po wielokroć tę samą usługę.
Drugą odmianą spamu jest Excessive Crossposting, czyli dużo postów do więcej niż jednej grupy newsowej lub więcej niż jednego użytkownika. Warto wspomnieć, iż istnieją specjalne algorytmy matematyczne, które administratorom serwerów pocztowych i grup dyskusyjnych potrafią pomóc określić stopień 'agresywności' takiej partii przesyłek.
Spam możemy również podzielić ze względu na rozsyłane treści:
Pierwszą grupą będą przesyłki komercyjne - reklamowe oraz zawierające oferty zawarcia umów: Unsolicited Commercial E-mail(UCE).
Do drugiej grupy należą wszelkie niekomercyjne przesyłki: Unsolicited Bulk E-mail(UBE), do których zaliczymy agitację polityczną, religijną oraz np. zaproszenia do odwiedzin stron www.

1.3 Sposoby pozyskiwania adresów pocztowych.

Bardzo ważnym elementem obrony przed spamem jest świadomość tego w jaki sposób adresy pocztowe trafiają w ręce spamerów. Najbardziej narażoną na spam grupą użytkowników Internetu są uczestnicy grup dyskusyjnych. Osoby zajmujące się rozsyłaniem spamu, stosując specjalne oprogramowanie zbierają adresy dyskutantów. Adresy pobierane są przede wszystkim z nagłówków *From:* i *Reply-To:* postów i listów. Sprawdzane są także inne ciągi znaków zawierające znak @ zarówno w nagłówku, jak i w treści.
W zdobywaniu adresów wpomagają spamerów przeglądarki. Niektóre z nich wysyłają adres pocztowy w polu *HTTP_FROM* żądania HTTP przekazywanego do serwera lub padają ofiarą dołączonego do strony programu w JavaScript, który powoduje wysłanie poczty na określony adres bez zatwierdzania przez użytkownika.
Spamerzy wykorzystują również adresy pocztowe udostępniane na stronach WWW, szczególnie w odsyłaczach *mailto:*. Użycie adresu e-mail w księdze gości ulubionej witryny może skończyć się opublikowaniem go i udostępnieniem go spamerom. Bazy danych adresów poczty elektronicznej mogą być również

zdobyte w wyniku przestępstwa, jakim jest włamanie do systemu informatycznego, lub dzięki specjalnym formularzom udostępnionym na stronach www, oferującym wszelkiego rodzaju korzyści w zamian za podanie naszego adresu skrzynki pocztowej.
Tak zdobyte zbiory adresów są bardzo często przedmiotem dalszej odsprzedarzy, co powoduje, że kolejny spamer wysyła na dany adres przesyłki elektroniczne. Warto przy tym wspomnieć, iż nie będzie rozsyłaniem spamu wysyłanie przesyłek, jeżeli adresat wyraził zgodę na otrzymywanie takich przesyłek za pośrednictwem formularza, w którym wyraźnie przewidziano rozsyłanie informacji o nowościach, reklamach, etc. Jest to po prostu cena jaką płacimy zazwyczaj na serwerach pocztowych oferujących darmowe konta pocztowe.

1.4 Jak się bronić.

Wiemy już w jaki sposób spamerzy pozyskują adresy kont pocztowych, warto więc przyjrzeć się sposobom ich ochrony. Większość czynności sprowadza się do utrudnienia pracy robotom skanującym zasoby Internetu w poszukiwaniu adresów pocztowych.
Ważne jest aby nasz adres w sieci pozostał zrozumiały dla użytkowników, a jednocześnie był błędnie interpretowany przez automaty spamerów. Jedną z metod jest wprowadzanie adresu w takiej postaci aby stał się on 'nieklikalny'. Wystarczy np. usunąć znak @ i zastąpić go elementem graficznym. Można również wykorzystać maskowanie adresu e-mail za pośrednictwem kodów używanych w HTML. Kolejnym sposobem jest zniekształcenie adresu*(adress munging)*. Polega on na modyfikacji ciągu znaków w naszym adresie np. identyfikator@domena.pl.usun.to, identyfikator[at]domena[kropka]pl, im bardziej pomysłowo to zrobimy, tym mniejsze szanse są na przechwycenie prawdziwego adresu przez robota filtrującego zawartość sieci. Również ważne jest aby nasz adres był złożony, zawierał różnorodne znaki, utrudnia to automatyczne generowanie adresów przez nadawców spamu. Bardzo istotnym w walce ze spamem jest wykorzystanie technik kryptograficznych służących do uwierzytelniania nadawcy, jest to głównie poczta oparta na tokenach oraz szyfrowaniu PGP.
Gdy powyższe metody zawodzą warto zdecydować się na zastosowanie specjalistycznego oprogramowania do filtrowania i zarządzania naszą pocztą. Rozwiązań antyspamowych jest bardzo dużo, ale wszystkie one stosują jedną lub kilka opracowanych technik. Zatem zanim zdecydujemy się na zainstalowanie odpowiedniego dla nas oprogramowania warto się przyjrzeć mechanizmom stosowanym podczas filtrowania naszej poczty elektronicznej.

Rozdział 2

Mechanizmy filtrowania poczty elektronicznej

2.1 Analiza nagłówka.

Jest to metoda najbardziej popularna, wykorzystywana w prawie każdym programie pocztowym. Opiera się ona na wyszukiwaniu określonych ciągów znaków, które będą kwalifikowały dany list jako spam. Większość aplikacji rozróżnia małe i wielkie litery, co jest bardzo ważne gdyż spamerzy zawsze starają się przyciągnąć swoją uwagę kompozycją listu, zauważalne stają się słowa pisane wielkimi literami np. WIN, FREE, SEX, etc. . Często stosowana jest analiza zaczerpnięta z tradycyjnych wyszukiwarek, która sprawdza czy dany ciąg znaków rozpoczyna lub kończy dany wyraz. Taka reguła zadziała przy słowach *seks*, *seksowna*, *seksu*, itp., czasem w metodzie tej stosowane są wyrażenia regularne. Podczas filtrowania wiadomości w taki sposób sprawdzane są: treść wiadomości, temat, nadawca, odbiorca oraz inne nagłówki. Metoda ta jest bardzo łatwa w stosowaniu dla użytkownika, który sam może wprowadzać nowe reguły, poza tym istnieje możliwość opisania tych reguł w pliku tekstowym, umożliwiającym wymianę reguł z innymi użytkownikami. Powstał do tego specjalny język zwany *Sieve (www.cyrusoft.com/sieve/).*
Skuteczność tej metody jest niestety ograniczona. Spamerzy stosują coraz bardziej przebiegłe metody oszukiwania takich filtrów. Brak automatycznego tworzenia reguł sprawia , iż bardzo często trzeba dodawać ręcznie nowe reguły, przez co obsługa tego mechanizmu zajmuje bardzo dużo czasu. Poza tym bardzo ważne jest jakie reguły stosujemy, czasem wystarczy jeden zły wyraz i list który nie jest spamem zostanie za niego uznany. Kolejną wadą jest prostota takich reguł, spamerzy coraz częściej stosują przewrotne metody omijające takiego typu filtry. Stosują fałszywe adresy nadawcy(przez co przy okazji omijają czarne listy). Omijają przeglądanie treści listu stosując kodowanie, zapisywanie pod postacią HTML'u, w treść wtapiane są niewidoczne dla użytkowników wyrażenia np. Via¡!–GH–¿ra, wyrazy są zmieniane np. m0ney, itp. Tak więc

metoda ta jest małoskuteczna na dłuższą metę, jednak wystarczająca dla niewymagających użytkowników.

2.2 Czarna i biała lista

Zasada działania czarnej listy opiera się na obserwacji ruchu poczty elektronicznej. Spamerzy wysyłają wiele e-maili oraz robią to często. Wystarczy zidentyfikować adresy nadawcy ulokowane w polu nagłowka *From*. Kolejnym krokiem jest zignorowanie kolejnych przesyłek od namierzonych wcześniej osób. Do niedawna ten sposób był jednym z bardziej skutecznych. Obecnie spamerzy często używają cudzych serwerów pocztowych, wstawiają fałszywe adresy nadawcy, powstały także wirusy, które wysyłają maile reklamowe z komputerów zwykłych użytkowników, przez co skuteczność czarnych list wyraźnie spada.
Biała lista ma odmienną rolę. Zawiera ona zaufane adresy, zwykle znajomych lub kontrahentów. Przesyłki pochodzące z tych źródeł akceptowane są zawsze.
Czarna i biała lista mają swoje odmiany. Stosowane w nich reguły potrafią przyjmować i odrzucać listy należące do wybranych domen, a podstawą do odmowy odbioru wiadomości może być adres IP, domena nadawcy lub jego serwera pocztowego. Podobnie traktowane są przesyłki nadchodzące z niezabezpieczonych serwerów proxy lub maszyn Open Relay, czyli takich, przez które e-maile może wysyłać każdy i do każdego.
Czarne listy są wykorzystywane także przez administratorów serwerów pocztowych, którzy aby zwiększyć skuteczność tej metody informacje wymieniają ze specjalnymi bazami danych. W Polsce jedną z takich baz jest PolSpam. Bazy te tworzone są przez wielu administratorów i zwykłych użytkowników.

2.3 Szara lista.

Metodę tę opracował Evan Harris. Jest ona mechanizmem opierającym się na założeniu iż spamerzy zazwyczaj wysyłają bardzo wiele kopii wiadomości naraz i nie troszczą się o ich dalszy los. Przy wykorzystaniu tej metody wszystkie listy są identyfikowane za pomocą numeru IP nadawcy, adresu nadawcy oraz odbiorcy. Jeżeli do serwera dotrze przesyłka o nieznanych danych, nastąpi odmowa przyjęcia listu wraz z komunikatem o tymczasowym błędzie. Podobnie traktowane są przesyłki, które nadejdą przez zadany czas. Zatem kolejne partie listów ze strony spamera zostaną odrzucone bez zbędnego identyfikowania. Takie odrzucone wiadomości reklamowe zazwyczaj nie są wysyłane ponownie, w odróżnieniu od zwykłych listów, które po określonym czasie przyjdą ponownie.
Metoda ta jest bardzo skuteczna i nie wymaga interwencji użytkownika. Jej jedyną 'dziurą' jest fakt iż w momencie ponownego wysłania listu przez spa-

mera, przejdzie on przez zaporę szarej listy. Poza tym działanie szarej listy w dużym stopniu opóźnia dostarczanie zwyczajnych e-maili, co w wielu sytuacjach ma bardzo duże znaczenie.

2.4 Pytanie - Odpowiedź.

Pytanie - Odpowiedź *(ang. challenge-response)*.
W tej metodzie użytkownik przyjmuje wyłącznie listy od nadawców którym ufa(podobnie jak przy białej liście). Nadawcy, którzy są nieznajomi dla adresata, otrzymują od niego wiadomość z łatwym pytaniem lub z prośbą o odpowiedź. Listy nadawców, którzy odpowiedzą na nasze pytanie są przepuszczane, zaś pozostałe są kasowane. Metoda ta jest w miarę obiecująca, ponieważ roboty i automaty wykorzystywane przez spamerów, nie są w stanie wykonać tego zadania w tak logiczny sposób, w jaki to zrobi człowiek. Jedyną wadą takiego rozwiązania jest fakt, iż nie zawsze oczekiwanym przez nas nadawcą jest człowiek. Bardzo często bowiem przesyłane są nam informacje z list dyskusyjnych, informacje związane z rejestracją, itp. Dlatego dobrym uzupełnieniem metody jest dopisanie 'pewnych' nadawców do białej listy.
Dopatrując się luki w metodzie można stwierdzić, iż bardzo często zdarza nam się wysyłać sobie kopie listów lub artykułów. Pociąga to konieczność dopisania naszego własnego adresu do białej listy. Możliwość ta, dla bardziej doświadczonych spamerów daje szansę na obejście naszej zapory. Niektórzy spamerzy wykorzystują właśnie tę lukę ustawiając jako nadawcę nasz własny adres, przez co spam zdoła przedrzeć się przez nasze zabezpieczenie w bardzo prosty sposób. Metoda pytanie - odpowiedź w niektórych rozwiązaniach została nieco zmodernizowana, za pośrednictwem ingerencji systemu *TMDS (tmda.net)*, który dodatkowo na podstawie określonych nagłówków może wiadomości przepuszczać(biała lista) lub odrzucać(czarna lista).

2.5 Statystyczny filtr antyspamowy.

Statystyczny filtr, zwany filtrem bayesa posiada ogromne możliwości filtrowania. Został on szczegółowo opisany w artykule Paula Grahama p.t. *"A Plan for Spam"* oraz w jego kontynuacji zatytułowanej *"Better Bayesian Filtering"*. Ogólna zasada działania filtru opiera się na wykorzystaniu statystyki i rachunku prawdopodobieństwa podczas analizy poczty przychodzącej. Przy wykorzystaniu podanego rozwiązania analizie zostaje poddana zarówno zwykła poczta, jak również listy traktowane jako spam. Efektem jest wygenerowanie tablicy, której każde wyrażenie z listów posiada określone prawdopodobieństwo iż wiadomość zawierająca to wyrażenie można zakwalifikować jako spam lub jako zwykły list.

Rozdział 3

Ochrona antywirusowa

3.1 Wirusy a poczta elektroniczna

Każdy, kto w swojej codziennej pracy korzysta z dostępu do globalnej sieci komputerowej bez wątpienia zetknął się z problemem wirusów i robaków internetowych przenoszących się za pomocą poczty elektronicznej. Ponad 95% wirusów rozprzestrzenia sie poprzez email. Zagrożeniem są najczęściej wirusy pokroju :

- *Klez.H*, zawierające własny serwer SMTP, podszywający się pod wybranego nadawcę.
- *Bugbear.B*, który wysyłając swoją kopię wybierał losowy list ze skrzynki użytkownika zainfekowanego komputera oraz wpisywał losowo wybranego nadawcę i odbiorcę.
- *Sobig.F*, który rozprzestrzeniał się w zastraszającym tempie. On również wstawiał losowo wybrany adres w pole *From* : nagłówka, powodując zamieszanie wśród użytkowników Internetu i utrudniając wykrycie zainfekowanych komputerów.

Oraz inne takie, jak: *Lirva*; *Deloder*; *Peido−B*; *Fizzer*; *Blaster* czy *Welchia*, które oprócz masowego rozprzestrzeniania się, swoją sławę zawdzięczają takim cechom, jak: wbudowane konie trojańskie (podsłuch klawiatury, bot IRCnet, serwer HTTP); próby unieszkodliwiania oprogramowania antywirusowego czy Personal Firewall; automatyczne uaktualnianie; udawanie wiadomości systemowej z serwera pocztowego o niedostarczeniu korespondencji (zmylenie użytkownika tak, aby otworzył załącznik zawierający złośliwy kod); przejęcie pełnej kontroli nad system (potencjalne przeprowadzenie z niego ataku).

Według firmy Sophos, w pierwszej połowie roku 2003 odnotowano 3855 nowych wirusów [1]. Wszystkie wirusy z pierwszej dziesiątki rozprzestrzeniały się przy wykorzystaniu poczty elektronicznej. CERT/CC w lipcu bieżącego roku opublikował raport [2], w którym zwraca uwagę na wzrastającą szybkość

rozprzestrzeniania się wirusów/robaków. Aby skutecznie bronić się przed tym zagrożeniem, należy zastosować kilka warstw zabezpieczeń, a także w miarę możliwości oprogramowanie różnych producentów.

3.2 Lepsza ochrona

Wielu użytkowników Internetu stosuje oprogramowanie antywirusowe myśląc iż ochroni ono ich przed ingerencją wirusów. Ciężko jest dla nich wpoić nawyki, dzięki którym nie udostępnialiby zasobów sieciowych, nie uruchamiali załączników dostarczonych pocztą elektroniczną (często od nieznanych nadawców) i programów nieznanego pochodzenia. Dobrym pomysłem wydaje się zaimplementowanie mechanizmów ochrony antywirusowej już na etapie serwera pocztowego. Jeżeli serwer pocztowy będzie w stanie odfiltrować zainfekowane wiadomości, to dzięki temu wiadomość zawierająca wirusa nie dotrze do użytkownika. Przy czym nie może to być jedyny element ochrony antywirusowej a raczej dodatkowy element mający na celu zwiększenie skuteczności działania systemu ochrony antywirusowej. Nie należy zapominać o zainstalowaniu oprogramowania antywirusowego na poszczególnych stacjach roboczych oraz o jego aktualizacji, jak również na stosowaniu się do zasad profilaktyki antywirusowej takich, jak na przykład zalecenia CERT Polska[3].

3.3 Oprogramowanie *OpenSource*

Wielu dostawców oferuje gotowe, komercyjne systemy ochrony antywirusowej działające na serwerze pocztowym. Jeżeli jednak miałby to być dodatkowy element systemu antywirusowego, to niejednokrotnie cena potrafi skutecznie zniechęcić do wprowadzenia tego typu rozwiązania. Dlatego warto zwrócić uwagę na rozwiązania typu *OpenSource*. Pomimo tego, że są one darmowe, większość z nich rozwijana jest przez szerokie grono programistów i użytkowników którzy zgłaszają twórcom informacje o nieprawidłowościach funkcjonowania lub zgłaszają zapotrzebowanie na nowe funkcjonalności. Oprogramowanie to oferuje dość duże możliwości i działa niezawodnie. Pozwala instalować się na wielu popularnych darmowych platformach systemowych takich, jak choćby systemy z rodziny *BSD, czy całe grono dystrybucji Linux'a. Nie stanowi problemu uruchomienie ich na systemach takich, jak Solaris, HP-UX czy AIX. Do najpopularniejszych rozwiązań *OpenSource* umożliwiających ochronę antywirusową i/lub anty-spam'ową zaliczyć możemy:

- *Exiscan*[4] - jest to łata (ang. patch) na Exim'a (dość popularny MTA, instalowany na przykład domyślnie wraz z dystrybucją Debian GNU/Linux), która rozszerza jego możliwości o sprawdzanie zawartości wiadomości odbieranych przez ten MTA. Można dzięki niemu badać obecność wirusów, spam'u, wskazanych wyrażeń regularnych (zarówno w treści, jak i

w nagłówkach) oraz określonych rozszerzeń załączonych do wiadomości plików.

- $MIMEDefang$[5] - jest to oprogramowanie, które służy do szeroko pojętego filtrowania poczty elektronicznej. Współdziała z Sendmail'em. Wykorzystywane zwykle jest do blokowania wirusów; blokowania spam'u; usuwania części wiadomości napisanej w formacie HTML; dodawania stopki/sygnaturki do treści każdej wiadomości; usuwania lub modyfikacji załączonych do wiadomości plików; wstawiania zamiast załączników odsyłacza do lokalizacji, z której może on być pobrany; konstruowania zasad dostępu do usługi e-mail.

- $MailScanner$[6] - oprogramowanie filtrujące pocztę elektroniczną, które potrafi z niej usunąć wirusy, spam i zapobiec próbom wykorzystania znanych luk bezpieczeństwa oprogramowania do obsługi poczty elektronicznej użytkownika końcowego. Potrafi współpracować z różnymi MTA oraz różnorodnym oprogramowaniem antywirusowym (w tym komercyjnym), które potrafi automatycznie uaktualniać.

- $Qmail - Scanner$[7] - oprogramowanie oferujące funkcjonalności zbliżone do poprzedników, ale współdziała tylko z Qmail'em. Potrafi również podejmować akcje względem wiadomości na podstawie zawartości określonych nagłówków.

- $AMaViS$[8] - jest to rodzina produktów służąca podobnym celom co poprzednicy, wśród których można wyróżnić: amavis (dla serwerów słabo obciążonych), amavisd (dla serwerów bardziej obciążonych), amavisd-new (dla serwerów bardziej obciążonych wzbogacony o funkcje anty-spam'owe), amavis-ng (modularna wersja amavis'a).

3.4 Skaner antywirusowy

Oprogramowanie takie, jak $MailScanner$, $Qmail - Scanner$, $Exiscan$ czy $MIMEDefang$ potrafi wykryć wirusy w filtrowanej poczcie elektronicznej, ale nie robi tego całkowicie samodzielnie - wykorzystuje do tego celu zewnętrzne programy, którym przydziela sprawdzenie konkretnych wiadomości na obecność wirusów. Oprogramowanie to spełnia rolę elementu łączącego oprogramowanie serwera pocztowego ze skanerem antywirusowym. W zależności od tego, czy skaner antywirusowy znajdzie w wiadomości kod wirusa, czy też nie, podejmuje ono odpowiednie, określone przez administratora działanie.

Na korzyść użytkowników został stworzony $OpenAntiVirusProject$[10] stanowiący platformę będącą miejscem wymiany informacji pomiędzy ludźmi zainteresowanymi rozwijaniem rozwiązań zwiększających bezpieczeństwo systemów w kontekście ochrony antywirusowej.

Jeżeli chodzi o skanery antywirusowe(również te do zastosowań komercyjnych), bardziej znane i jednocześnie darmowe warto wyróżnić:

- $ClamAntiVirus$[9]- jest to zestaw narzędzi przeznaczonych do pracy w systemach należących do rodziny UNIX. W jego skład wchodzą trzy elementy: daemon, skaner uruchamiany na żądanie oraz narzędzie automatyzujące aktualizację bazy sygnatur wirusów (oparta ona jest na bazie udostępnianej przez OpenAntivirus Project, zawiera jednak sporo dodatkowych sygnatur i jest ciągle aktualizowana).

Warto tutaj również wspomnieć o istnieniu innych skanerów antywirusowych takich jak: $Sophos$, $eTrust$, $Trend$, $McAfee$, $F-Prot$, $Command$, $Kaspersky$, $Inoculate$, $Inoculan$, $Nod32$, $F-Secure$, $Panda$, RAV, $Antivir$, $Vscan$, MKS_vir. Cechują się one dużą funkcjonalnością, jednak nie tak bogatą jak oferuje ClamAV.

3.5 MailScanner

Spośród wymienionych wcześniej rozwiązań MailScanner wydaje się być bardzo potężnym narzędziem . Według twórców obecnie filtruje on wiadomości na około 30 000 serwerach pocztowych. Posiada przejrzysty plik konfiguracyjny. Jego główną zaleta jest wysoka funkcjonalność.

1. Z punktu widzenia ochrony antywirusowej jego najważniejsze cechy to:
   - współpraca z szeroką gamą oprogramowania antywirusowego ($Trend$, $McAfee$, $Kaspersky$, $F-Secure$, $Panda$, RAV, $Antivir$, $ClamAV$, $Vscan$ i inne, przy czym możliwe jest jednoczesne wykorzystanie kombinacji kilku z nich)
   - automatyczna aktualizacja baz sygnatur wirusów
   - współpraca z najpopularniejszymi MTA: $Postfix$, $Sendmail$, $Exim$ lub $ZMailer$
   - rozpakowuje skompresowane załączniki w celu zbadania ich zawartości
   - odrzuca(lub nie) załączniki na podstawie dopasowania nazwy pliku do określonych wzorców
   - zastępuje zainfekowane załączniki powiadomieniami o infekcji
   - powiadamia administratora o każdej zainfekowanej wiadomości
   - przechowuje usunięte załączniki, tzw. kwarantanna
   - powiadamia nadawcę wiadomości o prawdopodobnej infekcji jego stacji roboczej
   - samodzielnie chroni się przed niektórymi atakami DoS, takimi jak Zip of Death
   - przesyła zwykłe wiadomości tekstowe nawet jeżeli skaner antywirusowy przestanie poprawnie funkcjonować
2. W swoim działaniu $MailScanner$ wykonuje stale następujące działania:
   - pobiera wiadomości z kolejki wiadomości przychodzących
   - podejmuje decyzję o ewentualnym zakwalifikowaniu ich jako spam
   - jeżli są to wiadomości czysto tekstowe, to automatycznie bez sprawdzania przenosi je do kolejki wiadomości wychodzących i uruchamia proces dostarczenia ich do adresata
   - dekomponuje strukturę MIME każdej z pozostałych wiadomości
   - sprawdza wszystkie zdekomponowane elementy na obecność wirusów (w tym celu uruchamia zewnętrzne oprogramowanie antywirusowe)

- sprawdza czy nie zachodzi dopasowanie nazw plików do określonych przez administratora wzorców
- sprawdza wiadomości pod kątem prób wykorzystania znanych luk bezpieczeństwa niektórych programów pocztowych (np. Outlook lub Eudora)
- jeżli ustawiona była odpowiednia opcja, przenosi zainfekowane pliki do kwarantanny
- zastępuje usunięte pliki powiadomieniami o zaistniałej infekcji
- dodaje na początku oryginalnej wiadomości prośbę o zapoznanie się odbiorcy z załączonymi powiadomieniami
- przenosi oryginały nie zainfekowanych wiadomości do kolejki wiadomości wychodzących
- ponownie buduje wiadomości, które były wcześniej zainfekowane ale już ze sprawdzonych elementów
- kasuje oryginalne wiadomości (zainfekowane) z kolejki wiadomości przychodzących
- wyzwala proces dostarczania do adresatów wiadomości znajdujących się w kolejce wiadomości wychodzących
- wysyła powiadomienia o infekcji do administratora i/lub nadawcy (o ile oczywiście tak właśnie jest skonfigurowany)
- jeżeli to możliwe, dezinfekuje oryginalne załączniki i wysyła je do adresata wraz z powiadomieniem, że udało się je oczyścić.

Aby zminimalizować niebezpieczeństwo dostarczenia zainfekowanej wiadomości, której nie udało się oczyścić, proces skanowania ponawiany jest po każdej próbie dezinfekcji. Tylko te wiadomości, które po ostatnim skanowaniu uznane zostały za bezpieczne są wysyłane do adresata.
Cena produktów komercyjnych chroniących pocztę elektroniczną na poziomie serwera zwykle liczona jest w tysiącach dolarów. *MailScanner* współpracując z dużo tańszym oprogramowaniem (poniżej 200$) lub nawet darmowym (*ClamAV*) spełnia te same funkcje, co jego droższe odpowiedniki.

MailScaner może być zainstalowany bezpośrednio na serwerze pocztowym (o ile serwer spełnia wymagania sprzetowe i programowe). Ponieważ wymagania sprzętowe są praktycznie minimalne, można go także zainstalować na osobnym komputerze. Wystarczy wtedy przekonfigurować istniejący serwer pocztowy tak, żeby przed wysłaniem poczty przesyłał ją do sprawdzenia na komputer z zainstalowanym MailScanner'em. Pakiet źródłowy zawiera skrypty, które w znacznym stopniu ułatwiają instalację wymaganych modułów oprogramowania, jak i samego MailScanner'a. Oryginalny plik konfiguracyjny zawiera bogato opisane ustawienia domyślne pozwalające na bezproblemowe

uruchomienie programu. Dołączona dokumentacja stanowi bardzo dobrze opisaną instrukcję pozwalającą na bezproblemową integrację z klientami typu: *Sendmail*, *Exim*, *Postfix* lub *ZMailer*.

Zatem łatwo możemy zauważyć, iż *MailScaner* jest bardzo wydajnym narzędziem, którego koszt oraz stopień skomplikowania nie jest wcale taki wysoki.

3.6 Podsumowanie

Coraz częściej oprogramowanie antywirusowe jest jednym z elementów ochrony poczty elektronicznej. Ochrona oparta na jednym tylko elemencie bywa zawodna. Wprowadzenie jednego z wymienionych wcześniej rozwiązań pozwala na zwiększenie skuteczności działania ochrony antywirusowej przy stosunkowo niskich nakładach oraz nie wiąże się z dokonywaniem skomplikowanych zmian w strukturze sieci czy konfiguracji urządzeń lub usług.

Innym aspektem jest opinia, iż produkt darmowy nie jest produktem w pełni wartościowym. Niektórzy administratorzy rezygnują z instalacji oprogramowania darmowego, twierdząc, że nie ma ono gwarancji, oraz że w każdej chwili rozwiązanie to może przestać być dalej rozwijane i nie można liczyć na pomoc techniczną w przypadku kłopotów. Pomysł na ciekawy i użyteczny software jest błyskawicznie podchwytywany przez szerokie grono Internautów, którzy zgłaszają uwagi dotyczące poprawności działania, funkcjonalności, a także przyłączają się oni do prowadzenia projektu. Oprogramowanie Open Source bywa wykorzystywane przez instytucje komercyjne, akademickie lub nawet militarne. Listę użytkowników *MailScanner'a* można znaleźć pod adresem: *http* : *//www.sng.ecs.soton.ac.uk/mailscanner/users.shtml*

Biorąc pod uwagę wybór skanera antywirusowego, warto zainteresować się *ClamAV*. Programiści zaangażowani w tworzenie *ClamAV'a* zadbali o to, żeby ich produkt działał niezawodnie oraz, żeby dysponował aktualnymi bazami sygnatur wirusów. Umożliwiają oni wysyłanie przez odpowiednią stronę internetową (oraz przez pocztę elektroniczną) zainfekowanych plików, które nie są dotychczas wykrywane. W ten sposób każdy użytkownik Internetu może pomóc w rozwoju projektu oraz przyczynić się do bieżącej aktualizacji bazy sygnatur a tym samym do skuteczniejszego wykrywania pojawiających się wirusów.

Spis literatury

Magazyn internetowy [1] Magazyn internetowy WWW.; „Spam czyli sieciowe śmiecie - Czym jest spam?”; http://www.www-mag.com.pl/porady/podlupa/l009/2.html