Komunikat

Ochrona antywirusowa poczty elektronicznej

Piotr Jankowski

Zwrócono uwagę na coraz groźniejszy problem wirusów przenoszonych pocztą elektroniczną, które zagrażają systemom komputerowym. Opisano ochronę utworzoną w Instytucie Łączności z użyciem programów Amavis oraz Sophos Anti-Virus, zainstalowanych na serwerze pocztowym.

poczta elektroniczna, ochrona antywirusowa, Amavis, Sendmail, Sophos Anti-Virus

Zagrożenie wirusami komputerowymi

Dziesięć lat temu poczta elektroniczna była zjawiskiem egzotycznym i mało powszechnym, a pięć lat temu umieszczanie na wizytówce adresu e-mail było swego rodzaju ekstrawagancją. Obecnie poczta elektroniczna jest jedną z najbardziej popularnych usług w Internecie, a Internet największą siecią komputerową na świecie. Liczba kont pocztowych jest szacowana na setki milionów, a adres e-mail na wizytówce podaje się tak samo, jak numer faksu czy telefonu. O popularności poczty zdecydowała jej prostota oraz ogromne możliwości. Choć pierwotnie poczta miała być przeznaczona wyłącznie do transmisji wiadomości tekstowych, to obecnie można nią przesyłać różnego rodzaju dane. Jest to bardzo wygodne, np. w tym samym liście można wysłać znajomym zdjęcia bliskich lub fragment nagrania. Biznesmeni używają poczty do wymiany dokumentów, a programiści – programów. Pocztą można przesłać dowolną liczbę danych dowolnych typów, a jedynymi ograniczeniami są możliwości transmisyjne sieci Internet oraz rozmiary skrzynek pocztowych. W tych skrzynkach mogą też się znaleźć listy z wirusem komputerowym. Najczęściej nie jest to miła i oczekiwana przesyłka. Może się także okazać, że jest ona przyczyną wielu problemów.

Warto byłoby zatem określić, czym są te wirusy i kto lub co jest nimi zagrożone. Otóż wirusami są zagrożone przede wszystkim systemy operacyjne wyprodukowane przez firmę Microsoft. Teoretycznie są też podatne na nie systemy z rodziny Unix, ale od kilku lat nikomu nie udało się opracować skutecznego wirusa przeznaczonego dla systemu Unix[①]. Wirusy i systemy operacyjne marki Microsoft współistnieją ze sobą od dawna. Zmiany polegają na tym, że jeszcze pięć lat temu główną drogą przenoszenia się wirusów były dyskietki, a obecnie wirusy rozprzestrzeniają się przez Internet, w szczególności przez pocztę elektroniczną. Dużą winę za ten stan rzeczy ponosi firma Microsoft, która wypuszczała na rynek bardzo „dziurawe" programy pocztowe.

Próbując określić, czym jest wirus komputerowy, można stwierdzić, że w zasadzie nie ma jednoznacznej jego definicji. Najlepiej jest przyjąć, że wirusy są programami, które mają zdolność samodzielnego powielania się oraz przenoszenia z komputera na komputer. Zdolność ta sama w sobie nie jest groźna, groźne są inne cechy związane już z konkretnym wirusem. Wirusy są opracowywane przez ludzi w różnych celach. Część autorów wirusów pisze je tylko z chęci zaprezentowania swoich zdolności programistycznych lub pokazania „dziur" w różnych systemach. Takie wirusy najczęściej

① *Podobno za napisanie wirusa zagrażającego systemowi Linux można otrzymać wysoką nagrodę.*

nie są zbyt groźne. Wypisują tylko komunikat na ekranie lub wygrywają melodyjkę. Niestety oprócz takich, niegroźnych wirusów komputerowych występują również wirusy bardzo groźne, których skutki działania są bardzo bolesne. Niektóre z nich niszczą zawartość dysków twardych, a inne są w stanie zablokować dużą część sieci Internet. Przykładem może być wirus Nimba, który w sierpniu i wrześniu 2001 r. spowodował duże szkody w Internecie. Skutki jego działania odczuwali też ci użytkownicy Internetu, których komputery nie zostały zarażone. Wirus generował bowiem bardzo duży ruch w sieci, co powodowało blokowanie łączy, a w konsekwencji niedostępność dużej części usług. Należy pamiętać, że jeśli wirus jest skuteczny, czyli np. wykorzystuje jakąś „dziurę" w systemie pocztowym, to często jego kod zostaje zmodyfikowany. Zjawisko to określa się mutowaniem wirusa. Kolejne mutacje wirusów mogą powstawać w kilkudniowych odstępach. Wymusza to więc na użytkownikach konieczność stałego, co najmniej codziennego, aktualizowania programów antywirusowych, co niestety zazwyczaj nie jest bezpłatne.

Rozpatrując działanie poczty od strony architektury systemu można stwierdzić, że poczta elektroniczna pracuje w architekturze klient–serwer. Rolę klienta pocztowego spełnia program pocztowy użytkownika, który w literaturze fachowej jest określany skrótem `MUA` (*Mail User Agent*). Za pomocą programu klienta pocztowego użytkownik poczty może napisać, wysłać, a także odebrać list. List jest odbierany ze skrzynki pocztowej mieszczącej się w komputerze, który pełni rolę serwera pocztowego. Odbiór listu najczęściej jest realizowany przez klienta poczty za pomocą jednego z dwóch protokołów `POP3` (*Post Office Protocol Version 3*) lub `IMAP` (*Internet Message Access Protocol*). List jest wysyłany przez klienta poczty przy użyciu protokołu `SMTP` (*Simple Mail Transport Protocol*) do najbliższego serwera pocztowego. Serwer pocztowy `MTA` (*Mail Transport Agent*) ustawia listy w kolejce i próbuje je za pomocą protokołu `SMTP` przekazać do serwera, na którym znajduje się skrzynka pocztowa adresata. List może zostać przekazany bezpośrednio na serwer, na którym adresat ma skrzynkę lub też do serwera pośredniczącego (tzw. *Relay Server*). Listy przychodzące serwer pocztowy umieszcza w skrzynkach pocztowych. Może to czynić np. przez wywołanie odpowiedniego specjalizowanego programu, takiego jak choćby `procmail`.

Ochrona poczty w komputerze

Za ochronę poczty w komputerze, w którym działa klient pocztowy, jest odpowiedzialny użytkownik, który z tego komputera korzysta. Może on bronić się przed wirusami za pomocą kilku różnych sposobów. Najpopularniejszymi metodami są: usuwanie listów od nieznajomych oraz nieotwieranie podejrzanych załączników. Ponadto użytkownik powinien mieć zainstalowane najnowsze programy pocztowe oraz oprogramowanie antywirusowe. Teoretycznie powinno to wystarczyć, ale najczęściej nie wystarcza. Przyczyn jest kilka. Część wirusów potrafi się samodzielne rozsyłać, korzystając z książek adresowych, a zatem można otrzymać wirusa nawet od kogoś znajomego. Niektóre programy pocztowe oferują różnorodne ułatwienia, np. automatycznie otwierają załączniki. Jest to bardzo wygodne, zwłaszcza dla osób mniej zaznajomionych z komputerami, ale jakże często powoduje zarażenie wirusem. Można zazwyczaj tego typu mechanizmy wyłączać, ale rzadko kto tak postępuje. Najlepiej jest więc używać programu pocztowego, który takich opcji nie ma. W komputerze powinien być również zainstalowany program antywirusowy z aktualną bazą wirusów, którą należy codziennie aktualizować. Niestety najczęściej odbywa się to raz w miesiącu – podczas wgrywania nowszej wersji programu antywirusowego. Bardzo często użytkownicy wyłączają też programy antywirusowe, gdyż mogą one spowalniać nieco pracę komputera.

Ochrona poczty na serwerze pocztowym

Pocztę elektroniczną można chronić na serwerze pocztowym, uniezależniając się wtedy od postępowania użytkownika. Wszystkie decyzje o tym, co zrobić z listem zawierającym wirusa, podejmuje wówczas administrator systemu. W zależności od możliwości konfiguracyjnych systemu antywirusowego może on np. list z wirusem skasować i powiadomić nadawcę, że wysyła wirusy, natomiast adresata o niczym nie informować. Aby jednak zainstalować system antywirusowy na serwerze pocztowym, trzeba odpowiednio dobrać serwer oraz program antywirusowy, który z tym serwerem będzie współpracował. Większość serwerów pocztowych pracuje pod kontrolą systemu operacyjnego Unix lub Windows NT/2000. Już kilka lat temu pojawiły się programy antywirusowe, które można było zintegrować z serwerami pocztowymi pracującymi pod kontrolą systemów WindowsNT/2000, bowiem wirusy są popularne właśnie w tym środowisku. Dla serwerów unixowych wirusy to egzotyka, niemniej jednak od kilku lat niektóre firmy produkujące oprogramowanie antywirusowe oferują oprogramowanie umożliwiające sprawdzenie, czy pliki nie zawierają wirusów. Oprogramowanie to jest przeznaczone do kontroli plików udostępnianych na serwerze unixowym i najczęściej nie jest możliwa jego prosta integracja z systemem serwera pocztowego pracującego pod kontrolą Unixa. Takie możliwości są oferowane dopiero od niedawna. Jeśli jednak ktoś ma program antywirusowy, który daje się uruchomić pod Unixem, można wówczas wykorzystać pakiet Amavis z `www.amavis.org`, umożliwiający integrację programu antywirusowego z serwerem poczty elektronicznej.

Amavis

Amavis jest skryptem przygotowanym w dwóch językach. Jedna z wersji jest napisana w Bourne shellu, a druga – w Perlu. Amavis nie jest programem antywirusowym, choć często jest tak określany. Bez programu antywirusowego nie potrafi on wykryć wirusa. Jego zadaniem jest połączenie serwera pocztowego z programem antywirusowym. Lista programów antywirusowych, z którymi Amavis współpracuje jest długa. Są to między innymi następujące programy:

```
* CyberSoft VFind
* Dr Solomon's AntiVirus
* F-Secure Inc. (former DataFellows) F-Secure AV
* H+BEDV AntiVir/X
* KasperskyLab AVP/Linux & AVPDaemon
* Network Associates Virus Scan for Linux
* Sophos Sweep
* Trend Micro FileScanner
* CAI InoculateIT
```

Możliwa jest też integracja z Amavisem programu antywirusowego, który nie występuje na tej liście, lecz wtedy należy dokonać modyfikacji kodu Amavisa. Nie powinno to być trudne, gdyż jest on dobrze udokumentowany. Amavis umożliwia jednoczesne użycie kilku programów antywirusowych, co może dać większą gwarancję bezpieczeństwa antywirusowego systemu pocztowego. Amavis może współpracować z różnymi serwerami pocztowymi. Na jego liście znajdują się takie serwery, jak Sendmail, Exim i Qmail. Nie ma natomiast Zmailera, ale Amavis bez problemów daje się z nim integrować. Amavis nie jest programem antywirusowym, za to przekształca kopie listu elektronicznego w strukturę katalogów i plików. W pliki zostają przekształcone załączniki. Potem następuje sprawdzenie,

czy dany załącznik nie jest archiwum plików. W tym celu Amavis wykorzystuje unixowe polecenie systemowe *file*. Jeśli plik stanowi archiwum plików, jest rozpakowywany. Następnie zostaje wywołany program antywirusowy, który sprawdza, czy w strukturze katalogów i plików utworzonych z listu jest zawarty wirus. Jeśli wirus zostanie wykryty, są podejmowane akcje, zdefiniowane w konfiguracji. W przypadku niewykrycia wirusa list jest dostarczany do adresata.

Instalacja Amavisa

Instalacja Amavisa zostanie opisana w niniejszym artykule na przykładzie instalacji wykonanej w Instytucie Łączności. Amavisa wybrano za względu na bezpłatną integrację oprogramowania antywirusowego Sophos (na które IŁ ma wykupioną licencję) z serwerem poczty Sendmail 8.9 pracującym w komputerze SUN Ultra 2 pod kontrolą systemu Solaris 2.5.1. Przed ostateczną instalacją przeprowadzono wiele testów porównujących wersję perlową i shelową Amavisa. Zdecydowano się na wybór wersji perlowej, gdyż lepiej współpracowała ona z systemem Solaris. Przed instalacją ustalono następujące założenia dotyczące jego konfiguracji:

1) nadawca ma otrzymać informację o wirusie,

2) o wirusie muszą być powiadomieni administratorzy,

3) o liście z wirusem nie jest powiadamiany adresat,

4) kopia listu jest zachowywana,

5) będą kontrolowane jedynie listy adresowane do naszej sieci.

Przed instalacją dokonano uaktualnienia Perla z wersji 5.004 do wersji 5.6.0. Aby zainstalować Amavisa, stało się konieczne zainstalowanie wielu modułów, których Amavis potrzebuje do pracy. Moduły perlowe realizują funkcje, które w wersji shellowej Amavisa realizowały zewnętrzne programy. Aby zainstalować pakiet `Amavisa` w wersji perlowej, należy pobrać pakiet z archiwum na stronie WWW `http://www.amavis.org`,[①] a następnie rozpakować i wydać następujące polecenie:

```
./configure --disable-x-header --with-mailfrom=viruskiller
```

Polecenie konfiguracyjne `./configure` parametry pracy programu `Amavis` jest uruchomione z dwoma parametrami, które zmieniają standardowe ustawienia programu:

- `disable-x-header` – wyłącza dopisywanie do nagłówków listów informacji o skanowaniu poczty,
- `with-mailfrom=viruskiller` – ustawia, w nagłówkach listów wysyłanych do nadawców z informacją o wirusie, pole *From* na użytkownika `viruskiller`.

① *W Instytucie Łączności posłużono się wersją Amavis-Perl10.*

Pozostałe parametry są ustawione następująco:

```
-----------
** Configuration summary for amavis perl-10 2000-12-07:

Install amavis as:          /usr/sbin/amavis Configured for use

with:    sendmail Relay configuration:        no Original

sendmail.cf: Use virus scanner(s):       Sophos Sweep Scanner runs

as:            root Log file directory:         /var/log/amavis

Quarantine directory:       /var/virusmails Max. recursion depth:

20 Add X-Virus-Scanned header: no Warn sender:                yes

Reports sent to:            virusalert Reports sent by:

viruskiller
-----------
```

Następnie w celu kompilacji i instalacji pakietu należy wydać następujące polecenia:

```
  make

  make install
```

W pliku konfiguracyjnym programu Sendmail `/etc/sendmail.cf` należy dokonać następujących zmian w makrze *Mlocal*, które odpowiada za dostarczanie poczty do skrzynki pocztowej:

```
 Mlocal, P=/usr/sbin/amavis, F=lsDFMAw5:/|@qSPfhn9, S=10/

30, R=20/40, T=DNS/RFC822/X-Unix, A=amavis $f $u

/usr/local/bin/procmail -Y -a $h -d $u
-----------
```

W przypadku konieczności wyłączenia systemu ochrony poczty elektronicznej i przywrócenia pierwotnego trybu dostarczania poczty należy przywrócić poprzednią wersję pliku konfiguracyjnego `/etc/sendmail.cf`. Aby tego dokonać, należy wykonać następujące operacje:

```
cat /etc/mail/sendmail.cf.amavis > /etc/mail/sendmail.cf

/etc/init.d/sendmail stop /etc/init.d/sendmail start
```

Przed ostatecznym uruchomieniem Amavisa został dodany następujący komunikat w języku polskim, informujący o wirusie:

```
From: $mailfrom To: $SENDER Subject: VIRUS IN YOUR MAIL

                O S T R Z E Ż E N I E  O  W I R U S I E

Nasz system antywirusowy wykryl wirusa w przeslanej przez Ciebie
przesylce poczty elektronicznej skierowanej do:

EOF
        my $recipient;
        foreach $recipient (@RECIPS) {
                print MAIL "-> $recipient\n";
        }
        print MAIL <<"EOF";

Dlatego tez Twoj list nie zostal dostarczony do adresata. Prosimy
abys usunal wirusy ze swojego systemu.

Inforamacje na temat naszego programu antywirusowego mozna znalezc
pod adresem:

$pkg_home_url AMaViS - A Mail Virus Scanner, licensed GPL
```

Komunikat ten jest wysyłany do nadawcy, gdy zostaje potwierdzona obecność wirusa w liście.

Zalety i wady Amavisa

Amavis jest bezpłatny i umożliwia zintegrowanie serwera pocztowego z programem lub kilkoma programami antywirusowymi. Są to niewątpliwie jego najważniejsze zalety. Ponadto wykorzystuje on wiele dobrych i sprawdzonych narzędzi, jak np. unixowy program *file*. Dzięki temu Amavis jest mniej podatny na typowe oszustwa związane ze zmianami w rozszerzeniach plików[①]. Ponieważ Amavis jest skryptem, nie zawsze może być zastosowany. Jako skrypt nie jest zbyt wydajny, co powinno być brane pod uwagę przy bardzo obciążonych serwerach pocztowych. W Instytucie Łączności serwer pocztowy, wyposażony w dwa procesory UltraSparc 170 MHz i 512 MB RAM, obsługuje ponad 300 kont pocztowych i system pracuje bez większych problemów. Dla większej liczby kont lub bardziej obciążonych serwerów należy jednak dobrać mocniejszy komputer, z większą liczbą pamięci operacyjnej.

Sophos Anti-Virus

Wykorzystywany w Instytucie Łączności program Sophos Anti-Virus ma możliwość codziennej aktualizacji bazy wirusów przez Internet. Trzeba mieć wykupioną na to licencję. W dokumentacji Amavisa znajduje się przykładowy skrypt, który umożliwia dokonanie aktualizacji. Jak często będzie uruchamiany, zależy od decyzji administratora. Na serwerze pocztowym Instytutu Łączności

① *Niektóre serwery pocztowe odrzucają listy, zawierające pliki z określonymi rozszerzeniami plików, np. zip. Aby to ominąć, użytkownicy zmieniają rozszerzenia plików.*

jest uruchamiany cztery razy dziennie za pomocą usługi `crona`. `Cron` jest standardowo dostępny we wszystkich Unixach. Powierzenie zadania aktualizacji `cronowi` pozwala na większą automatyzację obsługi programu antywirusowego, a co się z tym wiąże – mniejsze nakłady pracy. Oczywiście można wykorzystywać inne programy antywirusowe, ale przy wyborze programu możliwość codziennej aktualizacji oprogramowania przez Internet powinna stanowić podstawowe kryterium.

Podsumowanie

Amavis nie jest jedynym programem, umożliwiającym integrację oprogramowania antywirusowego z serwerem pocztowym. Dziś jest ich więcej. Ponadto producenci oprogramowania antywirusowego zauważyli, że istnieje rynek serwerów pocztowych pracujących pod kontrolą Unixów i zaczynają oferować oprogramowanie, dające się integrować z serwerami pocztowymi bez potrzeby użycia Amavisa lub podobnych narzędzi. Amavis być może nie był pierwszym programem, ale dzięki niemu uwierzono, że na serwerach unixowych można realizować ochronę antywirusową. Okazało się, że można i to bez ponoszenia wygórowanych kosztów. Nawet jeśli się nie ma oprogramowania antywirusowego, to zakup pojedynczej licencji na serwer unixowy może być niższy od zakupu licencji na wszystkie stanowiska w firmie. Taki zakup szybko się zwraca, o czym przekonują na przykład raporty z serwera pocztowego w Instytucie Łączności. Dziennie przechwytywanych jest tu kilka listów z wirusami. Niektóre z tych wirusów są na tyle groźne, że gdyby dotarły do komputerów użytkowników, mogłyby spowodować spore straty.

Piotr Jankowski

Mgr inż. Piotr Jankowski (1969) – absolwent Wydziału Elektroniki i Technik Informacyjnych Politechniki Warszawskiej (1996); pracownik Politechniki Warszawskiej (od 1996) oraz Instytutu Łączności w Warszawie (od 1997); zainteresowania naukowe: sieci komputerowe – bezpieczeństwo i administracja.
e-mail: P.Jankowski@itl.waw.pl