

Praktyczne metody ochrony poczty elektronicznej

Opracował: Mariusz Stawowski

Poczta elektroniczna jest w większości instytucji powszechnie wykorzystywaną usługą Internetu, szczególnie w zakresie wymiany informacji z klientami i partnerami handlowymi. Usługa ta stwarza jednak wiele problemów w zakresie bezpieczeństwa, m.in.:

- serwer poczty może zostać zaatakowany przez hakera, a następnie posłużyć do włamania do sieci prywatnej,
- serwer poczty może zostać zablokowany za pomocą ataku Denial of Service (DoS), bądź ulec awarii,
- wiele groźnych aplikacji (np. wirusy, robaki, konie trojańskie) może przedostać się do sieci prywatnej poprzez wiadomości pocztowe,
- serwer poczty może odebrać wiele niepożądanych przesyłek pocztowych tzw. spamów,
- serwer poczty może zostać wykorzystany przez hakerów (nazywanych także lamerami) do wysyłania spamów do innych serwerów w Internecie,
- poufne informacje przesyłane za pomocą poczty mogą zostać odczytane przez osoby nieupoważnione, bądź zmodyfikowane w niepożądany sposób,
- serwer DNS udostępniający informacje nt. serwera poczty może zostać zablokowany lub ulec awarii.

Problemy te zostaną przeanalizowane i dla każdego z nich przedstawione możliwe rozwiązanie. Rozwiązania praktyczne oparto o technologie zabezpieczeń Check Point VPN-1/FireWall-1 i Trend Micro InterScan VirusWall. VPN-1/FireWall-1 nie wymaga dodatkowego przedstawienia, ponieważ jest to renomowany produkt, od wielu lat na świecie najczęściej stosowany w systemach zabezpieczeń klasy Firewall i VPN (rozwiązanie to w Polsce jest dobrze znane, posiada rozbudowaną sieć dystrybucyjną, pomocy technicznej i szkoleń). Należałoby jednak bliżej przedstawić pakiet sieciowych zabezpieczeń antywirusowych InterScan VirusWall. Produkty firmy Trend Micro mogą być bowiem bardziej znane w konwencjonalnych zastosowaniach (np. skanery dla komputerów PC).

InterScan VirusWall składa się z trzech podstawowych komponentów: E-mail VirusWall, Web VirusWall i FTP VirusWall. Komponenty te mogą funkcjonować na tej samej maszynie lub oddzielnie. Typowe miejsce ich instalacji to stacje Internet Gateway i serwery sieciowe. Zakres funkcjonalny VirusWall można rozszerzać poprzez dodatkowe moduły, realizujące specyficzne zadania (np. zarządzanie przepływu poczty elektronicznej, ochrona przed spamami). Do istotnych własności VirusWall można zaliczyć:

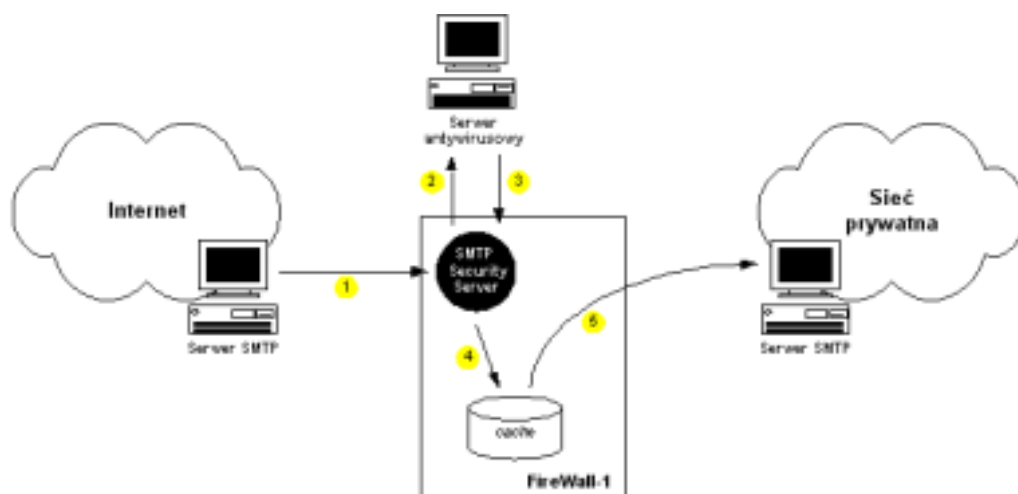
- ochrona sieci prywatnej przed atakiem wirusów, robaków, koni trojańskich i innych groźnych aplikacji, przenikających z Internetu poprzez protokoły SMTP, FTP i HTTP (m.in. ActiveX i Java),
- obsługa poczty napływającej do sieci prywatnej oraz wysyłanej do Internetu, łącznie z jej dystrybucją na podstawie wpisów DNS (priorytety MX),
- uzupełnienie konwencjonalnych zabezpieczeń klasy Firewall i Intrusion Detection System (IDS),
- współdziałanie z systemami zaporowymi Firewall poprzez protokół Content Vectoring Protocol (CVP),

- wysyłanie komunikatów i ostrzeżeń do użytkowników (E-mail VirusWall dodaje tekst do treści przesyłki pocztowej, Web VirusWall przesyła kod HTML do przeglądarki, FTP VirusWall wyświetla tekst klientowi FTP),
- samodzielna (automatyczna) aktualizacja bazy wirusów, także w trybie przyrostowym,
- zarządzanie lokalne za pomocą GUI oraz zdalne poprzez interfejs Web, bądź też zastosowanie centralnej konsoli zarządzania Trend Micro Virus Control System (VCS).

InterScan VirusWall może być instalowany w różnych konfiguracjach w zależności od potrzeb i specyfiki ochranianego systemu. E-mail VirusWall najczęściej funkcjonuje na dedykowanej stacji pomiędzy Firewall i serwerem poczty, obok Firewall (jako serwer CVP), na stacji Internet Gateway, bądź też na samym serwerze poczty. Web VirusWall zwykle instalowany jest na serwerze HTTP Proxy i konfigurowany w taki sposób, aby przeglądarki Web korzystające z Proxy najpierw łączyły się z VirusWall, a także na stacji obok Firewall jako serwer CVP. Typowe miejsce instalacji FTP VirusWall to Internet Gateway, stacja obok Firewall (jako serwer CVP) lub FTP Proxy.

Ochrona serwerów poczty przed włamaniami

Serwer poczty, podobnie jak inne serwery sieciowe może potencjalnie stać się ofiarą włamania. W przypadku serwerów poczty szczególnie groźne są próby włamań z obszaru Internetu. W razie udanego włamania na serwer poczty internetowej może stać się on dogodnym miejscem do prowadzenia dalszych penetracji sieci prywatnej. W przeszłości zarejestrowano bardzo wiele udanych tego typu włamań (np. z wykorzystaniem błędów programu sendmail). Zastosowanie Check Point FireWall-1 zapewnia nam w tym zakresie praktycznie całkowite zabezpieczenie serwerów poczty zlokalizowanych w sieci prywatnej instytucji. Wymagane jest tylko odpowiednie skonfigurowanie znajdujących się w FireWall-1 mechanizmów zabezpieczeń SMTP Security Server (patrz rysunek 1). Wszystkie połączenia SMTP z Internetu są wtedy odbierane przez SMTP Security Server (MX jest ustawiony na adres FireWall-1), zawartość przesyłek jest poddawana kontroli, a następnie są one zapisywane na dysku maszyny Firewall. Inny proces FireWall-1 odpowiada za odczytanie przesyłek z dysku i przesłanie ich do odpowiedniego serwera w sieci prywatnej. Serwery poczty instytucji nie powinny być w ogóle osiągalne z Internetu (tzn. nie powinno być technicznych możliwości nawiązania z nimi bezpośredniego połączenia nawet w razie wyłączenia zabezpieczeń Firewall).



Rys 1) Koncepcja ochrony serwerów poczty przez Check Point FireWall-1

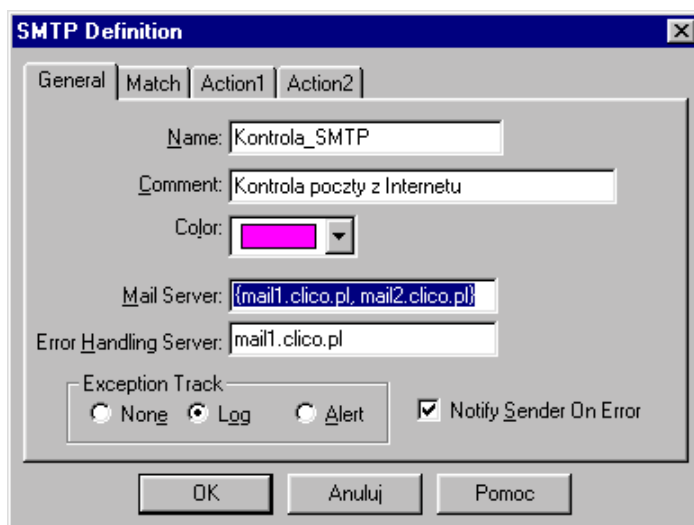
Ochrona serwerów poczty przed atakami destrukcyjnymi i awariami

W przypadku zastosowania zabezpieczeń Check Point FireWall-1 i odpowiedniej ich konfiguracji problem ataków destrukcyjnych na serwery poczty praktycznie nie istnieje. Nie ma bowiem bezpośredniego dostępu do serwerów poczty z Internetu. Zablokowanie FireWall-1 jest znacznie trudniejsze od zablokowania serwera poczty, ponieważ jako system zabezpieczeń Firewall poddaje kontroli pakiety już do 3 warstwy modelu OSI (m.in. datagramy IP poddane fragmentacji są scalane i analizowane, sprawdzana jest poprawność poleceń SMTP oraz format danych aplikacyjnych).

Ochrona przed awariami FireWall-1 realizowana jest poprzez tworzenie tzw. konfiguracji High Availability (HA). FireWall-1 może funkcjonować w trzech konfiguracjach HA:

- *hot stand-by* – konfiguracja składa się z dwóch lub więcej maszyn FireWall-1, wśród których tylko jedna jest aktywna, a pozostałe to maszyny zapasowe uruchamiane w razie awarii aktywnego Firewall (system zaporowy widoczny jest pod jednym adresem IP),
- *load sharing* – konfiguracja składa się z dwóch lub więcej maszyn FireWall-1, spiętych w klaster, współdzielących ze sobą ruch sieci rozdzielany pomiędzy poszczególne Firewall przez urządzenia zewnętrzne np. rutery (w sieci widoczne są adresy IP poszczególnych maszyn FireWall-1),
- *load balancing* – konfiguracja składa się z dwóch lub więcej maszyn FireWall-1, spiętych w klaster, dynamicznie równoważących pomiędzy sobą obciążenie sieci (system zaporowy widoczny jest pod jednym adresem IP, wymaga zastosowania modułu StoneBeat FullCluster).

Konfigurację HA samych serwerów antywirusowych VirusWall można zbudować za pomocą StoneBeat SecurityCluster. Zabezpieczenie serwerów poczty przed awariami najczęściej odbywa się poprzez tworzenie wielu serwerów SMTP, obsługujących tą samą domenę poczty. Priorytet serwerów ustala się w DNS w definicjach rekordów MX poszczególnych serwerów. W razie niedostępności serwera o najwyższym priorytecie poczta przesyłana jest do serwera o niższym priorytecie. W przypadku stosowania zabezpieczeń FireWall-1 realizowane jest to w inny sposób (FireWall-1 nie odczytuje priorytetów MX). W konfiguracji SMTP Security Server należy podać adresy IP lub nazwy DNS serwerów poczty (patrz rysunek 2). W razie niedostępności jednego serwera, FireWall-1 przesyła pocztę do następnego z listy. Jeżeli okaże się, że wszystkie serwery są niedostępne FireWall-1 przechowuje pocztę do czasu ich naprawy.

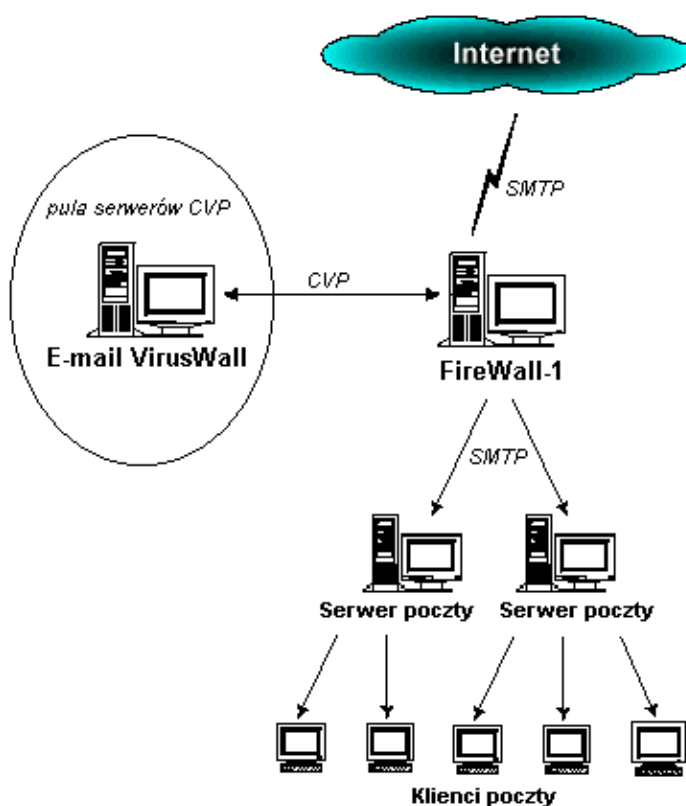


Rys 2) Konfiguracja zabezpieczeń poczty w Check Point FireWall-1

Innym zagrożeniem dla prawidłowego funkcjonowania poczty internetowej jest niedostępność (np. zablokowanie, awaria) serwera DNS, który udziela informacji nt. serwera poczty. Zagrożenie wynika z tego, iż w razie gdy adres IP serwera poczty określonej domeny nie zostanie znaleziony przesyłki pocztowe wysyłane do tej domeny są odrzucane. Jest to bardziej groźne od awarii samego serwera poczty, ponieważ gdy serwer ten jest niedostępny poczta do niego kierowana jest przechowywana przez długi czas na serwerze wysyłającym. W typowej konfiguracji podstawowy serwer DNS (primary server), posiadający lokalną bazę danych dla swojej strefy DNS, instalowany jest w sieci chronionej przez Firewall. Dodatkowy serwer DNS (secondary server), nie posiadający stałej bazy danych, instalowany jest w sieci operatora Internet. Serwer ten dla klientów DNS (tzw. resolves) jest pełnowartościowym źródłem informacji. Dodatkowe serwery DNS odczytują dane nt. swoich stref z innych serwerów DNS (najczęściej serwerów podstawowych) za pomocą operacji DNS Zone Transfer. Serwer udostępniający dane określany jest wtedy jako DNS Master Server.

Ochrona przed wirusami i innymi groźnymi aplikacjami

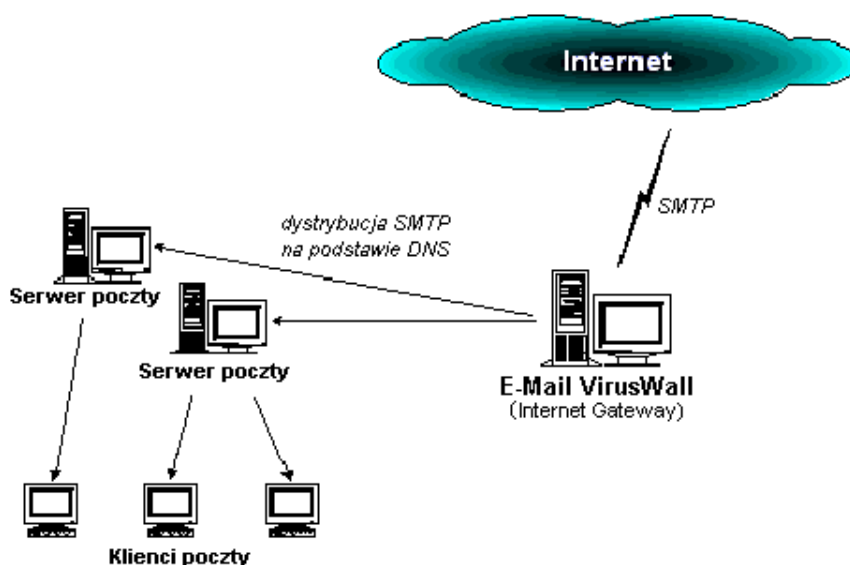
Wirusy od wielu lat zajmują najwyższe miejsce na liście zagrożeń systemów komputerowych. W środowisku Internet popularne stały się także inne groźne aplikacje: robaki (programy posiadające zdolności samodzielnego przenoszenia) i konie trojańskie (programy udające inne, legalne aplikacje). Skuteczny system ochrony przed tego typu zagrożeniami powinien opierać się na wielu warstwach zabezpieczeń. Najczęściej stosowana konfiguracja systemu ochrony przeciw wirusowej składa się z dwóch lub trzech warstw, zlokalizowanych na Firewall, serwerach i stacjach użytkowników. Poszczególne warstwy ochrony powinny opierać się na technologiach różnych producentów.



Rys 3) Architektura sieciowych zabezpieczeń antywirusowych FireWall-1 i VirusWall

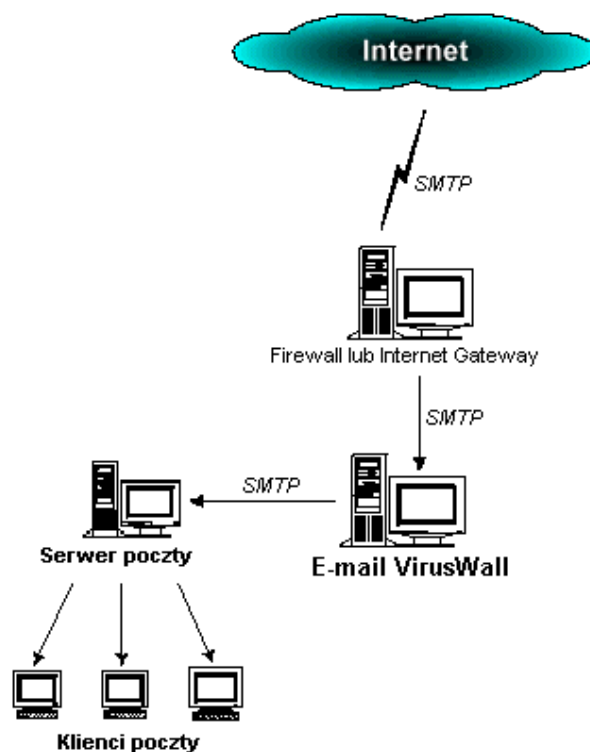
Najbardziej typowym wdrożeniem sieciowych zabezpieczeń antywirusowych Trend Micro i Check Point jest instalacja serwera E-mail VirusWall w dedykowanej strefie systemu zaporowego FireWall-1. Systemy FireWall-1 i VirusWall komunikują się za pomocą protokołu CVP (patrz rysunek 3). System DNS jest tak skonfigurowany, aby MX wskazywał na FireWall-1 lub wewnętrzny serwer poczty. Poczta nadchodząca z Internetu jest obsługiwana przez SMTP Security Server i przesyłana do kontroli do VirusWall. Po wykonaniu kontroli VirusWall przesyła z powrotem przesyłki do FireWall-1, który z kolei kieruje je do odpowiedniego serwera poczty w sieci prywatnej. Do celów podwyższenia wydajności i niezawodności kontroli możliwe jest zainstalowanie wielu serwerów VirusWall. FireWall-1 posiada mechanizmy realizujące dynamiczne równoważenie obciążenia serwerów CVP.

Możliwe są także inne konfiguracje sieciowych zabezpieczeń antywirusowych Trend Micro. Dla przykładu, E-mail VirusWall zainstalowany na Internet Gateway odbiera wszystkie przesyłki SMTP nadchodzące z Internetu i poddaje je kontroli przed ich dostarczeniem do właściwego serwera poczty (patrz rysunek 4). VirusWall jest wtedy uruchomiony na porcie typowym dla serwera SMTP (tcp/25). Dalsza dystrybucja przesyłek SMTP do odpowiednich serwerów w sieci prywatnej odbywa się na podstawie odczytu DNS (VirusWall odczytuje także priorytety MX). Dużą zaletą tej konfiguracji dla instytucji jest możliwość posiadania wielu serwerów poczty. Konfiguracja ta z reguły nie wymaga rekonfiguracji DNS. Ze względów bezpieczeństwa, a szczególnie wydajności nie jest zalecane instalowanie VirusWall na maszynie systemu zaporowego Firewall.



Rys 4) Zabezpieczenia E-mail VirusWall na styku Internetu i sieci prywatnej

E-mail VirusWall może również zostać zainstalowany bezpośrednio na maszynie serwera poczty w sieci prywatnej. Wymagana jest wtedy rekonfiguracja serwera poczty, tak aby VirusWall mógł zostać uruchomiony na porcie tcp/25 i nasłuchiwać na napływające przesyłki SMTP. Po wykonaniu kontroli, VirusWall przesyła wiadomości do rzeczywistego serwera (na wybrany w konfiguracji port), skąd trafiają do „skrzynek” (tzw. mail store), a następnie są udostępniane klientom poczty poprzez POP3 lub IMAP4.



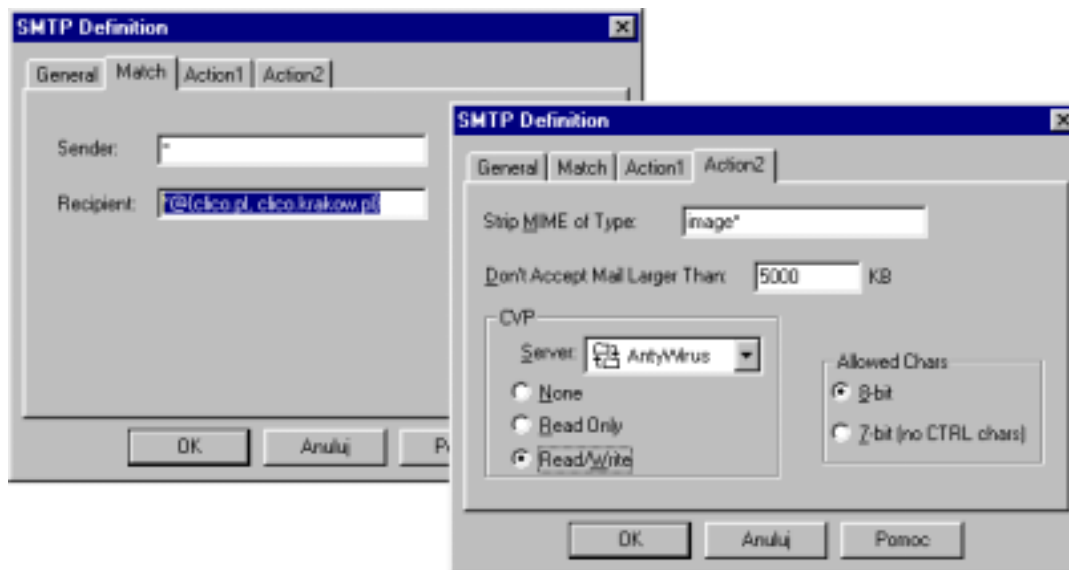
Rys 5) E-mail VirusWall na dedykowanym serwerze antywirusowym

Dopuszczalne jest także, aby E-Mail VirusWall został zainstalowany na dedykowanym komputerze w sieci prywatnej (patrz rysunek 5). Istotne jest jednak, aby był zlokalizowany na drodze poczty nadchodzącej z Internetu przed docelowym serwerem SMTP. W takiej architekturze zabezpieczeń antywirusowych wymagana jest zmiana adresu IP serwera SMTP i rekonfiguracja klientów poczty lub modyfikacja DNS, tak aby MX wskazywał na adres IP maszyny VirusWall (przesyłki z Internetu muszą najpierw trafić do VirusWall).

Ochrona przed spamami pocztowymi

Serwery poczty w Internecie z uwagi na globalny charakter tego środowiska mogą odbierać wiele niepożądanych przesyłek pocztowych. Przesyłki te określane są popularnie jako spamy. Moduł eManager dostępny jako opcja w pakiecie InterScan VirusWall oferuje w tym zakresie znaczące zabezpieczenia. Ich zadaniem jest wykrywanie spamów na podstawie analizy nagłówek wiadomości pocztowych i ich blokowanie jeszcze przed dostarczeniem do serwera poczty.

Dużo większym zagrożeniem od odbioru spamów jest wykorzystanie serwera poczty instytucji do wysyłania spamów do innych adresatów. Serwer SMTP z włączoną opcją Mail Relaying może z łatwością zostać wykorzystany przez hakerów do wysyłania spamów. Przede wszystkim może ucierpieć na tym prestiż instytucji i dostępność usługi. Serwer SMTP, z którego wysłano spamy trafia na „czarną listę” i inne serwery w Internecie nie akceptują od niego wysyłanej poczty. Skutecznym zabezpieczeniem w tym zakresie jest zablokowanie Mail Relaying. W przypadku stosowania zabezpieczeń FireWall-1 można to zrobić w systemie zaporowym, poprzez ustalenie dozwolonych odbiorców poczty dla przesyłek nadchodzących z Internetu (patrz rysunek 6).



Rys 6) Inspekcja zawartości poczty w Check Point FireWall-1

Całkowite zablokowanie Mail Relaying uniemożliwia jednak upoważnionym pracownikom instytucji, przebywającym poza terenem instytucji wysyłanie poczty za pomocą swojego serwera SMTP do adresatów z poza instytucji. Jest to bowiem także traktowane jako Mail Relaying. Jeżeli serwer poczty jest bezpośrednio osiągalny z Internetu możliwe jest włączenie na serwerze uwierzytelniania użytkowników dla protokołu SMTP (domyślnie uwierzytelnianie jest wymagane tylko dla POP3 i IMAP4). Nie jest to jednak zalecane ze względu na możliwości ataku na serwer (np. włamanie, DoS) oraz tego, że nie wszystkie serwery i aplikacje klientów poczty potrafią wykonać uwierzytelnianie SMTP. Najczęściej więc dla poczty nadchodzącej z Internetu wprowadza się dwie reguły polityki bezpieczeństwa systemu zaporowego (z rozróżnieniem miejsca nadania poczty), tak aby z zaufanych adresów IP nie blokować Mail Relaying.

Ochrona kryptograficzna poczty

Poufne informacje przesyłane za pomocą poczty w Internecie mogą potencjalnie zostać odczytane przez osoby nieupoważnione, bądź zmodyfikowane w niepożądany sposób. Skutecznym zabezpieczeniem w tym zakresie jest zastosowanie technik kryptograficznych (np. S/MIME, SSL, PGP, PEM, IPSec/IKE). Wprowadzenie zabezpieczeń kryptograficznych dla poczty elektronicznej w korporacjach sprowadza się do wdrożenia infrastruktury klucza publicznego Public Key Infrastructure (PKI). W mniejszych oraz słabiej z informatyzowanych instytucjach najczęściej stosowana jest tzw. nie-zarządzana infrastruktura PKI, w której użytkownicy sami generują swoje klucze i certyfikaty, instalują je na stacjach roboczych, dbają o ich ważność i bezpieczeństwo, a po wygaśnięciu ważności sami generują nowe, itd. W tych rozwiązaniach poziom ochrony informacji w znacznej mierze zależy od jakości posiadanego oprogramowania użytkowego. Dla przykładu, bezpieczeństwo WWW przy stosowaniu nie-zarządzanej PKI zależy głównie od dostępnych w przeglądarce algorytmów kryptograficznych. Warto też wiedzieć, że przeglądarki WWW w ogóle nie sprawdzają list unieważnionych certyfikatów CRL.

Problemy tych nie stwarza tzw. zarządzana infrastruktura PKI, która „sama dba” o klucze i certyfikaty użytkowników przez cały czas ich życia (m.in. odpowiada za ich aktualizację, kontrolę dostępu, Back-up). Zasady funkcjonowania zarządzanej PKI zostaną przedstawione na przykładzie Entrust/PKI. Jest to obecnie najbardziej rozpowszechnione rozwiązanie PKI w systemach finansowo-bankowych (m.in. e-commerce, home banking). Po wdrożeniu w instytucji Urzędu Certyfikacji opartego na technologii Entrust/PKI jedyne co użytkownicy powinni zrobić to zainstalować oprogramowanie Entrust Entelligence i przy pierwszym połączeniu z Urzędem Certyfikacji podać otrzymany numer referencyjny. Entrust Entelligence umożliwia użytkownikom wykorzystanie usług kryptograficznych bez konieczności rozumienia ich złożoności. Użytkownik może praktycznie zapomnieć o certyfikatach i kluczach kryptograficznych, ponieważ wszystko dzieje się w sposób dla niego przezroczysty. Za każdym razem po włączeniu komputera, bądź też po przekroczeniu ustalonego czasu nieaktywności, użytkownik jest poddawany uwierzytelnianiu tożsamości (tzn. podaje swój identyfikator i hasło) i na tej podstawie „odbezpieczony” jest jego profil kryptograficzny (m.in. klucze szyfrowania i uwierzytelniania). Zarządzana PKI jest więc wygodna dla użytkowników i równocześnie bezpieczna. Jediną jej wadą jest relatywnie wysoki koszt wdrożenia, który jednak zwraca się w trakcie eksploatacji technologii.

Zakres zastosowania PKI to nie tylko poczta elektroniczna. Profil kryptograficzny Entrust może także zostać wykorzystany do innych celów (np. zabezpieczenia plików na dysku, tworzenia kanałów VPN). Entrust Entelligence integruje się ze środowiskiem Windows 95/98/NT i dostarcza usług bezpieczeństwa dla wszystkich aplikacji zgodnych ze specyfikacją Entrust-Ready. W samym pakiecie Entrust dostępne są m.in. następujące aplikacje:

- Entrust/ICE - zabezpieczanie kryptograficzne plików we wskazanych katalogach,
- Entrust/TrueDelete - bezpieczne usuwanie plików/danych (zgodnie ze specyfikacjami Departamentu Obrony USA),
- Entrust/Unity – środki bezpieczeństwa zarządzanego PKI dodawane do przeglądarek Microsoft i Netscape,
- Entrust/Express - środki bezpieczeństwa zarządzanego PKI dodawane do klientów poczty Microsoft Exchange, Microsoft Outlook, QUALCOMM, Eudora Pro Email oraz Lotus Notes, zawierające także wsparcie dla standardu S/MIME.

Więcej informacji na temat przedstawionych rozwiązań ochrony poczty elektronicznej oraz produktów zabezpieczeń Check Point, Trend Micro, StoneBeat i Entrust można znaleźć w Internecie na stronach <http://www.clico.pl>. Rozszerzenie zagadnień bezpieczeństwa poruszonych w artykule czytelnik może znaleźć w publikacjach książkowych autora: „Ochrona informacji w sieciach komputerowych” i „Badanie zabezpieczeń sieci komputerowych”.