Wielosilnikowe rozwiązanie do ochrony serwerów pocztowych

Agnieszka Kacprzycka

Bezpieczeństwo serwerów pocztowych, a potrzeby rynku

Współczesne przedsiębiorstwa coraz częściej poszukują kompleksowych, zaawansowanych, wielosilnikowych rozwiązań antywirusowych i antyspamowych. Dlaczego się tak dzieje? Przyczyną jest świadomość, że przy obecnym poziomie zagrożenia rozwiązania jednosilnikowe o ograniczonej konfiguracji powinno się odłożyć do lamusa.

Nie wszystko złoto, co się świeci

Firma podejmując kluczową decyzję dotyczącą ochrony antywirusowej i antyspamowej nie powinna decydować się na wąskie gardło w postaci jednego silnika antywirusowego. Podstawowymi wadami takiego rozwiązania jest ścisła zależność od danego producenta.

Pojawia się problem szybkości dostarczenia szczepionki w momencie wykrycia nowego wirusa, co wynika np. ze stref czasowych. Dzięki poczcie elektronicznej wirusy rozprzestrzeniają się niemalże z prędkością światła. Należy pamiętać, że jeden wirus jest wystarczający do zainfekowania całej sieci firmowej. Czas pobrania aktualnej szczepionki jest w takim przypadku priorytetowy.

Każdy z programów antywirusowych dostępnych na rynku reklamuje się szybkim czasem reakcji. Rzeczywistość pokazuje, że bywa różnie. Żadna z firm nie dostarcza szczepionek jako pierwsza. W jednym przypadku jest to Kaspersky, w innym Symantec czy Norman. W Tabeli 1 przedstawiono przykład czasu reakcji na robaka W32/Sober.C odkrytego 20 grudnia 2003 roku o godzinie 03:00. Maksymalna różnica czasu reakcji wyniosła 45 godzin. Przez tak długi okres czasu komputery niemal każdej organizacji mogłyby zostać sparaliżowane.

Kolejnymi argumentami przemawiającymi za oprogramowaniem wielosilnikowym są wyniki testów przeprowadzanych przez niezależną organizację VirusBulletin (www.virusbulletin.com), które pokazują, że nie ma idealnego silnika antywirusowego, który przeszedłby wszystkie testy pozytywnie.

Każdy producent stosuje inną metodologię postępowania podczas wykrywania wirusów oraz przygotowywania szczepionek. Różne są także algorytmy wyszukujące nieznane wirusy. Technologie stosowane przez producentów chronione są ścisłą tajemnicą.

Podejmując decyzję o zakupie, przedsiębiorstwa często nie zdają sobie sprawy, że jeżeli w trakcie okresu subskrypcji dokonają zmiany systemu operacyjnego lub zmiany serwera poczty, może okazać się, że wybrane oprogramowanie nie obsługuje nowej infrastruktury, a producent wymaga zakupu innej wersji dla nowo wdrożonego systemu.

Jaka alternatywa?

Tendencje na rynku pokazują, że coraz częściej odchodzi się od dawnych systemów na rzecz innowacyjnych, zaawansowanych rozwiązań. Najlepiej postrzegane są programy kompleksowe o szerokich możliwościach konfiguracji. Oprogramowanie powinno być tak zaprojektowane, aby nie sprawić problemów instalacyjnych początkującym administratorom, ale jednocześnie pozostawić pole manewru najbardziej wymagającym użytkownikom.

Podstawowym celem jest maksymalizacja bezpieczeństwa przy minimalizacji kosztów. Często okazuje się, że za-

Rysunek 1.

kup oddzielnych, dedykowanych rozwiązań (firewalli, ochrony antyspamowej i antywirusowej) przekracza możliwości budżetowe średniej wielkości przedsiębiorstwa. Dla wielkich firm zakup kilku różnych produktów może nadszarpnąć budżet. W takich przypadkach nie powinno się wycofywać z zakupu, lecz szukać programów modularnych, umożliwiających rezygnację z niepotrzebnych elementów na rzecz niezbędnych. Złożona topologia nie powinna wymagać instalacji na każdym serwerze, ale łatwej dystrybucji z możliwością szybkiej aktualizacji. Przy takim rozwiązaniu firma może odciążyć lokalnych administratorów. Wybór powinien paść na rozwiązania niezależne od konkretnej platformy sprzętowej i operacyjnej, umożliwiające zdalną administrację przez przeglądarkę WWW.

Oczekiwania klienta

O gustach klientów nie należy dyskutować. Jeśli poszukiwany jest zaawansowany firewall, trzeba go dostarczyć. Jeśli priorytetem jest ochrona antyspamowa, powinno się dobrać rozwiązanie wykazujące największą skuteczność. Jeśli klientowi zależy na ochronie antywirusowej, należy zaproponować produkt konkurencyjny. Teoretycznie najtrudniej jest zaoferować rozwiązanie spełniające wszystkie powyższe wymagania, a jednocześnie posiadające przystępną cenę.

Inwestycja w przyszłość

Odpowiedzią na problemy poruszone wcześniej jest oprogramowanie Secure Mail Intelligence! – modularny system adekwatny do potrzeb każdego klienta. Łączy on ze sobą ponad 20 dowolnie dobieranych modułów, podzielonych na dwa etapy kontroli: przed i po nawiązaniu połączenia. Pierwszy etap pozwala już na wejściu „odcinać" permanentnych spamerów, blokować próby ataków, sprawdzać poprawność protokołu SMTP, unikać ataków dedykowanych konkretnym serwerom (poprzez zmianę tożsamości, tzw. identity spoofing). Drugi etap łączy ze sobą kontrolę IP, sprawdzanie DNS przy dowolnym zagłębieniu, potwierdzanie istnienia

Tabela 1. Przykład czasu reakcji na robaka W32/Sober.C odkrytego 20 grudnia 2003 roku o godzinie 03:00

Nazwa programu antywirusowego	Data dostarczenia szczepionki	Godzina dostarczenia szczepionki
BitDefender	20.12.2003	13:20
Kaspersky	20.12.2003	14:45
F-Prot (Frisk)	20.12.2003	15:25
F-Secure	20.12.2003	15:45
Norman	20.12.2003	18:25
eSafe (Alladin)	20.12.2003	18:35
Trend Micro	20.12.2003	19:50
AVG (Grisoft)	20.12.2003	20:15
AntiVir (H+BEDV)	20.12.2003	22:20
Symantec	21.12.2003	04:05
Avast! (Alwil)	21.12.2003	09:55
Sophos	21.12.2003	14:35
Panda AV	21.12.2003	17:05
McAfee/NAI	22.12.2003	04:10
Ikarus	22.12.2003	10:35

nadawcy poprzez próbę połączenia, analizowanie treści i załączników pod kątem spamu i wirusów, składowanie poczty, działanie jako serwer kolejkowania i routingu. W trakcie analizy listu współpracują ze sobą moduły odpowiedzialne za poprawne działanie każdego etapu, a w przypadku problemów restartujące dany moduł bez konieczności restartu całego systemu.

Ochrona antywirusowa oparta została o 8 pracujących jednocześnie silników różnych producentów: Kaspersky, Norman, VirusBuster, Authentium, QuickHeal, Symantec, Sophos i ClamAV. Jednokrotna inicjalizacja silników powoduje osiągnięcie najwyższej wydajności. Wirusy wyszukiwane są nie tylko w załącznikach listu, ale także w treści i zagnieżdżonych elementach MIME oraz w obrazkach. W momencie wykrycia wirusa w załączniku, załącznik może zostać skasowany, można usunąć cały mail lub przenieść go do kwarantanny. Każdy z silników posiada inne sposoby wykrywania znanych i nieznanych wirusów, więc ich jednoczesne wykorzystanie minimalizuje możliwość infekcji niemalże do zera. Aktualizacje baz szczepionek odbywają się nawet 12 razy w ciągu doby, a skuteczność nowej bazy jest testowana na nieszkodliwym wirusie.

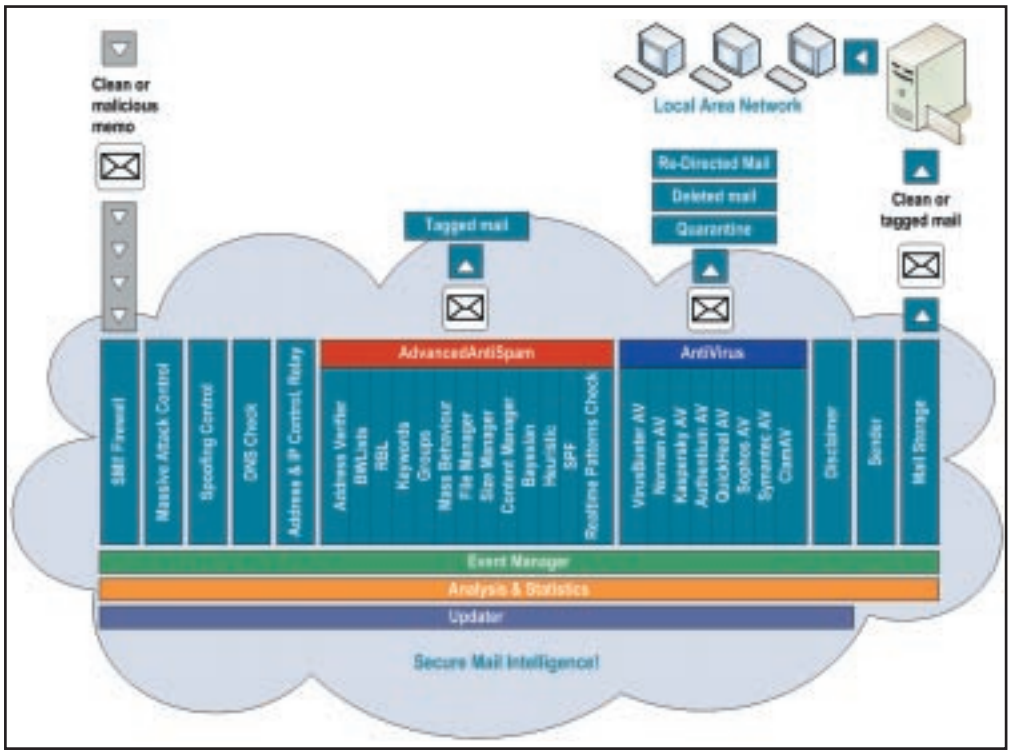
Wykrywanie spamu odbywa się za pomocą 15 warstw zgrupowanych w trzech niezależnych modułach. Moduł Verifier odpowiada za sprawdzenie, czy konto pocztowe, z którego wysłano wiadomość istnieje fizycznie na serwerze nadawcy. Realizuje to podczas próby wysłania do nadawcy testowego listu. SMI! for Gateway pobiera dane z serwerów RBL oraz z czarnych i białych list. SMI! Może także zablokować list na podstawie zdefiniowanych słów kluczowych, automatycznie przeciwdziałać masowym zachowaniom takim jak np. bombardowanie mailami. Osoba próbująca w ten sposób obciążyć serwer, zostaje odcięta na określony czas, a przy kolejnych próbach może zostać trwale zbanowana SMI! for Gateway wykorzystuje samouczący się algorytm Bayes'a oraz analizę heurystyczną.

Administrator ma możliwość sprecyzowania ustawień, które nadaje poszczególnym użytkownikom. Ustawienia te dotyczą typów odbieranych plików oraz ich wielkości. Dzięki temu np. dział marketingu może wysyłać załączniki w postaci dużych grafik, a dyrektor firmy odbierać maile o nieograniczonej wielkości. Istnieje możliwość binarnej analizy obrazów na okoliczność pojawienia się niechcianej zawartości, takiej jak zeskanowane dokumenty firmowe, kreskówki, czy pornografia.

Oprogramowanie wyposażono w moduł dodawania zastrzeżeń prawnych. Dzięki niemu pracownicy firmy wysyłają pocztę opatrzoną odpowiednim komunikatem.

Za analizę działania systemu odpowiedzialny jest zaawansowany moduł statystyczno-analityczny, który przesyła raporty dotyczące wybranych zdarzeń i informuje administratora o stopniu wykrywalności wirusów i spamu. Analizy w postaci liczb i wykresów reprezentują dane ze wskazanego przez użytkownika przedziału czasowego (Rysunek 1).

Wszystkie zdarzenia realizowane przez SMI! for Gateway zapisywane są w rejestrach tekstowych (log) i w relacyjnej bazie danych, dzięki którym można szybko przeanalizować problem (np. dlaczego poprawna wiadomość została uznana jako spam) i dostroić konfigurację systemu. Dokonać tego można przy użyciu wygodnej, spójnej dla wszystkich systemów operacyjnych konsoli administracyjnej, dostępnej przez HTTP. Istnieje możliwość dopisywania nieograniczonych reguł przy użyciu prostego języka skryptowego SMI! Script lub edycji plików tekstowych (Rysunek 2).



Rysunek 2.

SMI! a dedykowane serwery pocztowe

SMI! for Gateway został tak zaprojektowany, aby był uniezależniony od konkretnych producentów serwerów pocztowych. Cały ruch SMTP przejmowany jest przez SMI! for Gateway, poddawany szybkiej i wydajnej analizie i dopiero po sprawdzeniu szeregu warunków i kontroli, czy ruch nie nosi znamion ataku – przepuszczany dalej do docelowego serwera pocztowego. SMI! for Gateway instalowany jest bezpośrednio przed serwerem pocztowym lub na tej samej maszynie, co serwer.

Obok wersji for Gateway istnieją dwie wersje dedykowane. SMI! for Domino (dla IBM Lotus Domino w wersji R5 i wyższej) oferuje kompleksową ochronę serwerów poczty i pracy grupowej Lotus Domino. Pozwala chronić pocztę i aplikacje Lotus Notes oraz wykorzystać specyficzne funkcje Domino. SMI! for Exchange (dla Microsoft Exchange w wersjach 2000/2003) oferuje kompleksową ochronę serwerów poczty Microsoft Exchange. Pozwala chronić pocztę, skanować skrzynki i foldery publiczne oraz korzystać ze specyficznych funkcji Microsoft Exchange. Istnieje możliwość instalacji wszystkich produktów w obrębie jednej sieci klienta.

Polityka licencyjna i cenowa

Cena oprogramowania zależy od ilości chronionych kont mailowych oraz wybranych modułów. Klient sam decyduje o poziomie bezpieczeństwa poprzez dobór liczby i typów silników AV. Licencja SMI! pozwala zainstalować dowolną liczbę serwerów i dowolnych programów z rodziny SMI!

Dla kogo przeznaczony jest SMI!?

SMI! jest przeznaczony zarówno dla korporacji posiadających rozproszoną strukturę opartą na wielu lokalizacjach, jak i dla mniejszych przedsiębiorstw z dostępem do Internetu i własnym serwerem poczty elektronicznej.

Secure Mail Intelligence! może pracować w systemach Microsoft Windows NT 4.0/2000/XP/2003 w wersjach Professional i Server, Linux i Solaris 9 (x86 i SPARC). Wymaga minimum 140 MB wolnego miejsca na dysku i około 500 MB na przetwarzane listy. Maszyna z zainstalowanym SMI! powinna dysponować procesorem co najmniej Pentium III 800 MHz lub jego odpowiednikiem oraz posiadać co najmniej 128 MB pamięci RAM dla każdej instancji SMI!. ■

Agnieszka Kacprzycka pracuje na stanowisku Product Managera w firmie M2 NET S.A. Odpowiada za sprzedaż produktów i usług z zakresu Bezpieczeństwa IT. Kontakt: agnieszka.kacprzycka@m2net.pl.