

WHITE PAPER

Ochrona antywirusowa w urządzeniach UTM NETASQ

KOMPLETNA OCHRONA

Rozwój nowych zagrożeń wymusił na dostawcach rozwiązań bezpieczeństwa IT rozstrzygnięcie kwestii konfliktu pomiędzy maksymalizacją bezpieczeństwa a wydajnością pracy. Urządzenie UTM firmy NETASQ jest propozycją dla tych, którzy chcą otrzymać maksymalną ochronę przy jednoczesnym minimalnym obciążeniu sieci.

Celem urządzenia wielofunkcyjnego jest zintegrowanie takich elementów jak:

- firewall,
- system wykrywania i blokowania ataków IDS/IPS,
- zapewnienie bezpiecznego połączenia VPN,
- autoryzacja użytkowników,
- skanera wnętrza sieci SEISMO,
- ochrona antywirusowej,
- ochrona antyspamowej,
- filtrowanie URL,
- monitoring sieci w czasie rzeczywistym,
- generowania raportów.

Zastosowanie oprogramowania antywirusowego pozwala na eliminację zagrożeń przychodzących z zewnątrz sieci, co bezpośrednio wpływa na bezpieczeństwo antywirusowe całej sieci wewnętrznej. Wirusy oraz szkodliwe programy są skutecznie neutralizowane bezpośrednio na urządzeniu NETASQ. Zapobiega to rozprzestrzenianiu się wirusów wewnątrz sieci. Nie zapewnia jednak ochrony w przypadku zagrożeń pochodzących np. z dysków przenośnych oraz nośników wymiennych, ponieważ skanowanie antywirusowe realizowane jest w ramach komunikacji sieciowej.

Niezależnie od tych ograniczeń rozwiązania wybrane przez dostawcę urządzeń wielofunkcyjnych muszą spełniać pewne kryteria wyszczególnione przez niezależny zespół badawczy. Niemniej wprowadzenie silnika antywirusowego w ograniczonym środowisku urządzenia sieciowego może oznaczać konieczność pewnych kompromisów, co w szczególności dotyczy zamkniętej bazy sygnatur (WildList).

ZALETY ROZWIĄZAŃ ZINTEGROWANYCH

Główną zaletą urządzeń wielofunkcyjnych jest połączenie kilku systemów bezpieczeństwa, które w znaczący sposób zwiększają poziom zabezpieczenia danej sieci.

Są również inne zalety takich rozwiązań, między innymi:

- ograniczenie ruchu sieciowego poprzez eliminację zagrożeń, co bezpośrednio wpływa na zmniejszenie kosztów utrzymania łączy oraz koszty stosowania alternatywnych

zabezpieczeń,

- rozwiązanie typu Plug & Play: nie ma konieczności instalacji dodatkowych aplikacji na stacjach roboczych,
- zwiększenie poziomu bezpieczeństwa oraz podniesienie wydajności pracy stacji roboczych.

Ochrona zintegrowana pozwala na blokowanie zagrożeń w urządzeniu NETASQ, zapobiegając w ten sposób ich rozprzestrzenianiu się na potencjalnie narażone stacje robocze. W połączeniu z dodatkowo zainstalowanym programem antywirusowym na stacjach roboczych daje to podwójne zabezpieczenie i zapewnia optymalną ochronę.

Gwarancja rezydentnego sieciowego skanowania antywirusowego jest ważna, gdyż użytkownicy zwykle wyłączają programy antywirusowe zainstalowane na swoich komputerach. Zastosowanie skanera antywirusowego w zintegrowanym urządzeniu umożliwia skanowanie całego ruchu w sieci i zapewnia pełną scentralizowaną ochronę stacji roboczych.

KRYTERIA WYBORU ROZWIĄZANIA

Przy wyborze rozwiązania do ochrony antywirusowej, czy jest to ochrona na poziomie sieci czy też aplikacji, pomocna jest analiza kluczowych cech takiego rozwiązania. Niezależne testy, badające skuteczność aplikacji antywirusowych, opierają swoją ocenę na kluczowych parametrach danego programu. Wyznacznikami skuteczności rozwiązania są:

- współczynnik wykrywalności znanych wirusów,
- współczynnik wykrywalności wirusów polimorficznych,
- czas aktualizacji bazy sygnatur (czas reakcji),
- szybkość skanowania (wydajność pracy),
- wykrywanie proaktywne,
- współczynnik fałszywych alarmów (false positive).

Współczynnik wykrywalności znanych wirusów jest jednym z najistotniejszych kryteriów przy pomiarze skuteczności programu antywirusowego, ponieważ rozwiązania służące do wykrywania tych wirusów stanowią podstawę takich programów.

Test taki porównuje liczbę wykrytych przez skaner znanych wirusów z ogólną liczbą istniejących wirusów znajdujących się w bazie. Pozwala to zarówno na sprawdzenie, czy baza wirusów jest aktualna, jak i pomiar skuteczności danego programu.

Współczynnik wykrywalności wirusów polimorficznych pokazuje zdolność programu antywirusowego do stosowania sygnatur generycznych, co zapewnia wykrycie mutacji wirusów przy jednoczesnej optymalizacji rozmiaru bazy sygnatur.

Czas aktualizacji bazy sygnatur to czas reakcji na nowego wirusa. Masowy wzrost

liczby wirusów oraz pojawiające się nowe metody rozprzestrzeniania się wirusów wymagają szybkiej reakcji. Testy badają częstotliwość aktualizacji bazy sygnatur wirusów danego programu. Częstsze i szybsze aktualizacje oznaczają lepszą ochronę.

Szybkość skanowania jest dla programu antywirusowego jedną z najważniejszych cech. Stosowane metody detekcji zagrożeń nie powinny prowadzić do zauważalnego zwolnienia działania sieci, w przeciwnym razie istnieje ryzyko, że zostaną wyłączone.

Skanowanie proaktywne oznacza reakcję programu na nowego wirusa bez konieczności aktualizacji bazy sygnatur wirusów. Nazywane jest to ochroną dnia zerowego (ang. zero-day protection). Kryterium to pokazuje skuteczność technik analizy heurystycznej danego programu antywirusowego.

Współczynnik fałszywych alarmów (false positive) to kryterium ważne przy ocenie jakości silnika antywirusowego. Błędne wskazanie wirusa w niezainfekowanym pliku może mieć poważny wpływ na funkcjonowanie firmy (brak możliwości przesyłania ważnych dokumentów).

Oprócz tego wybór programu antywirusowego uzależniony jest od jego umiejętności **wykrywania zagrożeń w plikach skompresowanych**. Przed rozpoczęciem skanowania konieczna jest dekompresja pliku. Skuteczność w tym zakresie jest mierzona liczbą poziomów kompresji, z którymi dany program współpracuje (skompresowany plik może zawierać kilka innych skompresowanych plików).

BAZA AKTUALNYCH WIRUSÓW (WILDLIST)

Bezpieczeństwo infrastruktury wymaga często znalezienia kompromisu między oferowanymi sposobami ochrony a różnymi związanymi z nimi ograniczeniami. Niektóre sieciowe rozwiązania antywirusowe korzystają z ograniczonej bazy sygnatur, co wynika z chęci optymalizacji jej rozmiarów ale również poprawy wydajności pracy aplikacji. Metoda ta opiera się na aktualizowanej raz w miesiącu bazie sygnatur wirusów aktualizowanej przez Wild List Organization (www.wildlist.org). Organizacja ta oferuje bazę sygnatur wirusów i złośliwego oprogramowania ocenionych jako „aktywne”. Aby program został uznany za „aktywny” musi pojawić się co najmniej kilka doniesień o jego istnieniu a także można ocenić go jako szeroko rozpowszechniony. Niektóre a w szczególności nowo powstałe wirusy mogą się zatem na niej nie znajdować, a inne mogą zostać z niej usunięte kiedy zmniejszy się zasięg ich wpływów.

Metoda ta ma jednak istotne wady:

- Po pierwsze, miesięczne odstępy w aktualizacji listy sprawiają, że pojawia się niebezpieczna przerwa między pojawieniem się wirusa a jego faktycznym wykryciem przez bazę sygnatur wirusów. W związku z ciągłym rozwojem zagrożeń takie rozwiązanie jest

ryzykowne. Sytuację tę można by zmienić poprzez częstsza aktualizację bazy sygnatur.

- Co więcej, jako że stale pojawiają się nowe wirusy (w roku 2008 było ich średnio 30 000 miesięcznie), rozmiar tej bazy sygnatur (ok. 25 000) nie może nadążyć za rozwojem zagrożeń w inny sposób niż przez częste aktualizacje.

Dlatego też stosowanie ograniczonej bazy sygnatur poświęca kwestię bezpieczeństwa na rzecz wydajności. Kompromis ten wymaga kontroli nad sygnaturami znajdującymi się w bazie poprzez stałe jej aktualizowanie, dzięki czemu może być porównywalna z typową bazą (ok. 500 000 sygnatur).

Podsumowując, choć producenci rozwiązań antywirusowych i niezależne organizacje testujące korzystają z zamkniętej bazy sygnatur, jej stosowanie jest kontrowersyjne. Co potwierdza również w swojej prezentacji Av-Test z Konferencji Virus Bulletin 2007 „WildList nie żyje, niech żyje WildList”.

OCHRONA NETASQ

NETASQ, producent rozwiązań do zabezpieczania sieci, nigdy nie godził się na kompromisy w kwestii bezpieczeństwa, gwarantując jednocześnie optymalną wydajność pracy. System IPS, serce jego zintegrowanego systemu bezpieczeństwa, znany jest z tego, że ma jeden z najwyższych współczynników przepustowości IPS przy najlepszej ochronie typu „zero day” na rynku.

Firma NETASQ stawia na rozwiązania zintegrowane, a swoją działalność opiera na współpracy z uznanymi na rynku partnerami. Właśnie dlatego filtry URL są oparte na silniku OPTENET, a rozwiązanie antyspamowe bazuje na silniku Vaderetro.

Chcąc zagwarantować najlepszą ochronę antywirusową, firma NETASQ zdecydowała się na współpracę z jednym z liderów w tej dziedzinie na rynku. Przed podjęciem tej decyzji firma sprawdziła wszystkie rozwiązania i przeanalizowała kwestie najistotniejsze dla programów antywirusowych:

- współczynnik wykrywalności znanych wirusów,
- współczynnik wykrywalności wirusów polimorficznych,
- czas aktualizacji bazy sygnatur (czas reakcji),
- szybkość skanowania,
- wykrywanie proaktywne,
- współczynnik fałszywych alarmów (false positive).

Analiza ta skłoniła NETASQ do współpracy z firmą Kaspersky Labs. Przez lata rozwiązania Kaspersky Labs osiągały jedno z najlepszych wyników w różnych testach porównawczych niezależnych instytucji badawczych.

Jednocześnie NETASQ we wszystkich swoich produktach oferuje wbudowaną ochronę antywirusową bazującą na skanerze Clam AV, cenionym rozwiązaniu open-source'owym.

PODSUMOWANIE

W związku z pojawieniem się nowych dróg rozprzestrzeniania się wirusów i zmianą natury ich ataków konieczne jest połączenie zaawansowanych rozwiązań do ochrony antywirusowej. W tym kontekście podejście oparte na skanowaniu sieciowym daje podwójną korzyść w postaci zmniejszenia kosztów operacyjnych i zwiększenia poziomu bezpieczeństwa dzięki gwarancji stałej, centralnie sterowanej ochrony.

W swoich zintegrowanych rozwiązaniach firma NETASQ oferuje pełen zakres ochrony sieci, firewall i filtry URL, jednocześnie nie zapomina o zapobieganiu i blokowaniu włamań oraz ochronie antywirusowej. Firma NETASQ nie ustępuje w kwestiach bezpieczeństwa i korzysta z możliwości wyboru spośród dwóch skanerów antywirusowych, opierając się na pełnych bazach sygnatur wirusów. Różne testy wykazały, że analiza oparta na liście WildList nie daje wystarczającego współczynnika wykrywalności, nawet wtedy, gdy organizacje przeprowadzające testy wybierają najnowsze wirusy. To ograniczenie w kwestii bezpieczeństwa wynika w głównej mierze z dużej liczby nowych wirusów pojawiających się co miesiąc.

O FIRMIE NETASQ

Firma NETASQ specjalizuje się w rozwiązaniach do zintegrowanego zabezpieczenia sieci. Jako główny cel firma postawiła sobie dostarczanie rozwiązań zapewniających ten sam, najwyższy poziom zabezpieczeń dla firmy niezależnie od ich wielkości.

Rozwiązania NETASQ obecne są na rynkach w blisko 50 krajach poprzez sieć autoryzowanych partnerów również w Polsce.

Urządzenia NETASQ UTM posiadają m. in. certyfikację Common Criteria EAL4+ na kluczowe funkcje urządzeń czyli firewall, system wykrywania i blokowania włamań oraz VPN.

ZAŁĄCZNIK – DEFINICJE

- **Adware:** program komputerowy oparty na wyświetlaniu reklam na komputerze użytkownika. Część adware jest względnie nieszkodliwa i wyświetla jedynie reklamy darmowych produktów. Jednakże niektóre firmy sprzedają targetowane kampanie promocyjne oparte na programach instalowanych bez wiedzy użytkownika. Istnieją również programy, które wyszukują dane wrażliwe użytkownika, w szczególności informacje o jego sposobie korzystania z Internetu.
- **Backdoor:** termin ten odnosi się do złośliwego oprogramowania, które w chwili uruchomienia na zainfekowanym komputerze otwiera kanały komunikacyjne z zewnętrznymi sieciami. Twórca złośliwego programu może połączyć się w ten sposób i zdalnie kontrolować zainfekowany host. Najczęściej backdoor instalowany jest przez wirusa, robaka lub konia trojańskiego. Tego typu programów używać można do wyszukiwania na zainfekowanym komputerze wrażliwych danych (loginy i hasła, adresy e-mail). A sam host może być częścią sieci botnet, a także zostać wykorzystany w kampaniach spamowych.
- **Bomba logiczna:** program komputerowy zaprojektowany, by w chwili określonego zdarzenia rozpocząć szkodliwą dla systemu działalność. Zdarzeniem tym może być upływanie jakiegoś terminu, zmiana konkretnych danych lub brak wiadomości od autora programu. Ten typ zagrożenia zwykle umieszczany jest w systemie przez nieuczciwych pracowników i jest aktywowany, gdy odchodzą oni z firmy.
- **Bot:** patrz – Robot
- **Greyware:** złośliwe oprogramowanie, które wymaga zainstalowania jak też odinstalowania przez samego użytkownika, dlatego stanowi niewielkie ryzyko. Termin ten obejmuje również inne rodzaje złośliwego oprogramowania, takie jak spyware'y i adware'y. Ten typ zagrożenia pogarsza wydajność pracy zainfekowanego komputera. Może ono również przeprowadzać niechciane działania jak otwieranie okien, zbieranie informacji o zwyczajach użytkownika, a nawet wystawiać komputer na potencjalny atak przez eksponowanie jego słabych punktów.
- **Malware:** patrz – złośliwe oprogramowanie
- **Makrowirusy:** wirusy zaprogramowany z wykorzystaniem języka używanego do tworzenia makr w pakiecie programów biurowych Windows. Wirus rozprzestrzenia się we wszystkich dokumentach stworzonych przy pomocy tego modelu makr. Luki związane z makrowirusami zostały usunięte w MS Office 2000.
- **Pharming:** technika phishingu wykorzystująca dane wrażliwe na serwerach nazw domen. Choć użytkownik podaje właściwą nazwę domeny w przeglądarce, w wyniku podrobienia adresu IP serwera www, trafia na fałszywą stronę.

- **Phishing:** to zjawisko polegające na wysyłaniu fałszywych wiadomości e-mail mających na celu wyłudzenie poufnych danych (login i hasło do konta bankowego lub portali społecznościowych). W e-mailu podawany jest link do strony, gdzie użytkownik powinien podać wszystkie dane osobowe. Po przechwyceniu takich danych autorzy mają do konta ofiary. Wysyłane wiadomości najczęściej podszywają się pod banki lub inne godne zaufania instytucje.
- **Riskware:** oprogramowanie, które jako takie nie jest złośliwe, ale jego zastosowanie może prowadzić do przeniknięcia na komputer złośliwego oprogramowania. Przykładem potencjalnie niebezpiecznego programu może być klient komunikatora internetowego.
- **Robot:** program komputerowy, automatycznie wykonujący określone zadania, używany w sieciach zombie zwanych botnetami. Bot, instalowany zwykle przez robaka lub konia trojańskiego, uruchamia tzw. backdoor, przez który administrator takiej sieci, może zdalnie kontrolować hosta.
- **Rootkit:** metoda pozwalająca na ukrycie przed użytkownikiem działających programów lub procesów. Złośliwe oprogramowanie, które ma na celu przejęcie kontroli nad systemem, często korzysta z tej metody, by ukryć swoją obecność i działanie. Ten typ zagrożenia może funkcjonować na różnych poziomach zainfekowanego systemu. Od warstwy aplikacji (modyfikacja konfiguracji programu, by zapobiec wyświetlaniu informacji), przez jądro systemu operacyjnego (przejęcie funkcji, dodanie sterowników), rootkity mogą sięgać najniższych warstw i uruchamiać się przed systemem operacyjnym, czyniąc ich wykrycie jeszcze trudniejszym.
- **Złośliwe oprogramowanie:** termin używany dawniej w odniesieniu do koni trojańskich i wirusów. Obecnie termin „malware” stosowany jest do określania każdego oprogramowania działającego bez wiedzy użytkownika.