**TECHNOLOGIA ANTYWIRUSOWA**

**WPROWADZANIE**

Od ponad trzech dekad złośliwe oprogramowanie jest uporczywym, denerwującym i kosztownym zagrożeniem i nie widać końca problemu. Istnieje wielu dostawców oferujących lekarstwo na wirusy i złośliwe oprogramowanie, ale samo istnienie tych szkodników oprogramowania jest zrozumiałe irytujące dla osób odpowiedzialnych za bezpieczeństwo systemu. Początkowo większość wirusów nie została zaprojektowana w celu wyrządzenia szkód, ale została stworzona, aby zyskać rozgłos dla twórcy lub jako żart. Ponieważ te wczesne wirusy zostały zaprojektowane w celu udaremniania legalnych operacji programów w wielu systemach, częściej powodowały nieoczekiwane problemy, ponieważ twórcy wirusów nie przeprowadzili wyczerpujących testów. Wirusy te, a później niektóre trojany, często uszkadzały dane i powodowały przestoje systemu. Oczyszczanie wymagane do wyleczenia nawet drobnej infekcji wirusowej było kosztowne pod względem utraconej produktywności i nieprzewidzianych w budżecie kosztów pracy. Wirusy i zachowania trojanów połączyły się i teraz oba są uważane za część większej rodziny określanej jako złośliwe oprogramowanie. Złośliwe oprogramowanie nie jest już napisane tylko dla 15 minut sławy twórcy wirusów; dziś złośliwe oprogramowanie jest tworzone głównie w celu uzyskania korzyści finansowych. Złośliwe oprogramowanie nadal może powodować szkody, ale obecnie jest bardziej prawdopodobne, że zostało stworzone w celu kradzieży cennych informacji lub zasobów zainfekowanego komputera. Złośliwe oprogramowanie może kraść cenne dane w celu sprzedaży na podziemnych rynkach, wysyłać spam z zaatakowanej maszyny lub instalować oprogramowanie zaprojektowane do podsłuchiwania działań użytkownika, którego to dotyczy, żeby wymienić tylko kilka przykładów. Niektóre złośliwe programy mogą zapewnić pełny dostęp hakerowi w celu kontrolowania zainfekowanych maszyn, a złośliwe oprogramowanie kontynuuje trend kontrolowania zainfekowanych maszyn w „botnecie”. Te kolekcje przejętych komputerów są wykorzystywane do różnych działań, takich jak przeprowadzanie ataków lub wysyłanie spamu. Botnet wykorzystuje zwiększoną moc komputerów w sieci, jednocześnie utrudniając wyśledzenie podejrzanego atakującego. Z powodu tego przejścia na motywację finansową do pisania złośliwego oprogramowania, pojawiło się coś w rodzaju społeczności open-source, aby opracować nowe złośliwe oprogramowanie. Były dwa główne obszary, w których rozwój był najbardziej godny uwagi: unikanie tradycyjnych zabezpieczeń antywirusowych i rozpowszechnianie poprzez wykorzystywanie luk w powszechnym oprogramowaniu. Próbując uniknąć tradycyjnych zabezpieczeń antywirusowych, przestępcy często nieznacznie modyfikują i kompresują złośliwe oprogramowanie za pomocą programów pakujących, które często wykorzystują wyrafinowane techniki zaciemniania lub przeciwdziałania inżynierii wstecznej. Głównym celem współczesnych twórców szkodliwego oprogramowania jest unikanie wartych opublikowania epidemii z przeszłości, pozostawanie poza zasięgiem radaru w celu przeprowadzania ataków ukierunkowanych (phishing i spear phishing). Niektóre z najpopularniejszych rodzin złośliwego oprogramowania mają obecnie nawet dziesiątki tysięcy wariantów, z których każdego dnia publikowane są setki wariantów. Po wejściu do systemu często stosują techniki ukrywania, takie jak rootkity w trybie jądra, aby ukryć się przed systemem operacyjnym i wieloma produktami antywirusowymi (AV). Każdego dnia opracowywane są nowe złośliwe programy, ponieważ luki w programach są tak liczne, a od wykrycia luki w zabezpieczeniach do wydania przez producenta poprawki bezpieczeństwa często mijają tygodnie. Jeszcze częściej łatki są ogłaszane przez producentów, ale nie wdrażane przez użytkowników. Twórcy szkodliwego oprogramowania wykorzystują te luki w zabezpieczeniach i opóźnienia, więc badanie luk w zabezpieczeniach jest konieczne, aby stworzyć skuteczną ochronę za pomocą programów antywirusowych. Warstwowa ochrona przed infekcją złośliwym oprogramowaniem jest niezbędna i powinna obejmować nowoczesny skaner antywirusowy, a także zaporę ogniową i szyfrowanie danych. Chociaż zagrożenie ze strony nowego złośliwego oprogramowania utrzymuje się, a jego wzrost stał się

wykładniczy, technologia wdrożona w celu ochrony komputerów przed wirusami i złośliwym oprogramowaniem jest jednym z najmniej poznanych aspektów architektury bezpieczeństwa. W rezultacie zabezpieczenia antywirusowe są często nieprawidłowo konfigurowane. W tym rozdziale opisano dostępne technologie antywirusowe i sposób ich działania, a także przedstawiono metody ich efektywnego zastosowania w ramach kompleksowego programu ochrony komputera.

**Terminologia antywirusowa**

Akronim AV jest powszechnie używany do opisania branży, produktów (również czasami w skrócie AVP) oraz programów opracowanych w celu zwalczania wirusów komputerowych. Wczesne programy antywirusowe wykorzystywały proste skanowanie dysków twardych i dyskietek w celu wyszukania określonego ciągu tekstowego ukrytego w określonym pliku lub sektorze rozruchowym. To jest pochodzenie terminu skaner AV, który jest obecnie powszechnie używany jako termin ogólny dla wszystkich programów AV. W ten sposób termin ten jest używany w tym rozdziale, chociaż należy podkreślić, że wiele współczesnych skanerów antywirusowych robi znacznie więcej niż tylko skanowanie w poszukiwaniu znanego złośliwego oprogramowania, a wykrywanie może teraz obejmować niechciane programy, a także podejrzaną aktywność na plikach. Przeglądając literaturę dotyczącą produktów antywirusowych, często można zobaczyć stwierdzenia dotyczące liczby istniejących wirusów i trojanów. Nie jest niczym niezwykłym szacowanie łącznej liczby wariantów złośliwego oprogramowania w setkach milionów oraz sześciocyfrowe szacunkowe liczby dodawanych każdego dnia nowego złośliwego oprogramowania. Metody liczenia stosowane przez dostawców AV różnią się w zależności od tego, a liczby te niewiele nam mówią o ich zdolności wykrywania. O wiele bardziej pouczające jest poleganie na raportach renomowanych laboratoriów testujących AV aby uzyskać jasny obraz skuteczności produktu, niż polegać na tych liczbach.

**Problemy z antywirusem**

We wczesnych dniach wirusów, poza możliwością rozprzestrzeniania się na inne komputery, utrzymywanie wirusa na komputerze przez dłuższy czas nie przynosiło żadnych korzyści. Na początku wirusy były stosunkowo łatwe do znalezienia, ponieważ wirus zwykle powodował zauważalne szkody, które uświadamiały użytkownikom, że ich systemy są zainfekowane. Innym razem na ekranie pojawiał się nieomylny komunikat lub obraz, ostrzegający użytkowników o infekcji. Ponieważ twórcy wirusów odkryli korzyści finansowe wynikające z pozostawania w systemie tak długo, jak to możliwe, liczba zaatakowanych maszyn ogromnie wzrosła. Wirusy i złośliwe oprogramowanie stały się złożone, potrafią się dobrze ukrywać i nie są tak łatwe do znalezienia i wyeliminowania. Aby przeciwdziałać temu problemowi, skanery AV stały się wyrafinowanymi maszynami logicznymi. Ten nowy poziom złożoności, zarówno problemu, jak i rozwiązania, sprawił, że jest jeszcze bardziej zagmatwany dla użytkowników. Zbyt wiele osób nie rozumie, jak ważne jest posiadanie aktualnych produktów AV. Użytkownicy nie wiedzą, czego szukać i nie rozumieją, że wirusy i złośliwe oprogramowanie nie ogłaszają swojej obecności. Nowoczesne oprogramowanie AV ma możliwość automatycznej aktualizacji, dzięki czemu aktualizacja jest mniej pracochłonna. Aktualizacje są kluczem do ochrony systemów przed złośliwym oprogramowaniem, ponieważ aktualizacje zapewniają programowi antywirusowemu informacje niezbędne do znalezienia najnowszych wirusów i złośliwego oprogramowania. Niestety, ponieważ złośliwe oprogramowanie jest publikowane w tak niesamowitym tempie, nawet codzienne aktualizacje tradycyjnego skanera opartego na ciągach mogą nie wystarczyć, aby system był całkowicie wolny od zagrożeń. Wiele produktów AV obsługuje obecnie zasadniczo stały kontakt z serwerami programistów i weryfikuje sumy kontrolne na serwerach, aby zidentyfikować zmiany wymagające pobrania. Metody te umożliwiają aktualizacje w ciągu kilku minut od jakiejkolwiek zmiany bez niedogodności dla użytkowników. Większość skanerów antywirusowych sprawdza, co wydarzyło się wcześniej (tj. znane zachowanie znanego złośliwego oprogramowania), aby wykryć

infekcje. Chociaż produkty AV próbują teraz przewidywać nowe zagrożenia, nie jest to ich mocna strona. Ponadto wielu konsumentów, którzy kupują nowy komputer, otrzymuje wraz z zakupem działający produkt AV, ale nie decyduje się na zakup subskrypcji aktualizacji AV po wygaśnięciu bezpłatnego okresu użytkowania. Nie rozumieją, dlaczego muszą płacić za coś, co wydaje się działać, i usypia ich fałszywe poczucie bezpieczeństwa, myśląc, że ich produkt AV wykonuje swoją pracę. Konsumenci, którzy przenoszą pracę z niezabezpieczonych komputerów domowych do biura, mogą szybko zainfekować całą sieć. Produkty zabezpieczające w przeszłości cierpiały z powodu braku wsparcia ze strony wyższego kierownictwa, ponieważ często są postrzegane jako produkty o wysokich kosztach/niskich zwrotach i mają niski priorytet w budżecie zabezpieczeń. Zespół ds. technologii informatycznych (IT) w organizacji potrzebuje zasobów do takich rzeczy, jak identyfikowanie i łatanie podatnych systemów, monitorowanie i zarządzanie komputerami wchodzącymi do ich sieci, monitorowanie podejrzanego zachowania identyfikowanego przez zapory ogniowe, produkty AV i skanery bezpieczeństwa. Biorąc pod uwagę szeroką gamę produktów AV do wyboru oraz dużą liczbę poprawek wprowadzanych każdego dnia, wielu administratorów systemów rozpacza. Zainstalują i załatują dokładnie to, na co mają czas, i uznają to za wystarczająco dobre.

**PODSTAWY ANTYWIRUSÓW**

Skanery AV są trochę jak policjanci chodzący w rytm. Próbują obserwować wszystko, co dzieje się wokół nich, zwracać uwagę na podejrzane zachowania i próbować wstawiać się, gdy myślą, że dzieje się coś złego lub ma się wydarzyć. Zarówno policja, jak i skanery AV szukają pewnych wzorców i zachowań i wkraczają do akcji, gdy podejrzany przekroczy z góry określony próg akceptowalności. Podobnie jak policja, skanery AV czasami wyciągają błędne wnioski. Błędy te są zwykle spowodowane niewystarczającymi danymi lub nowymi i nieoczekiwanymi wzorcami zachowań. Wykrywanie złośliwego oprogramowania jest nauką niedokładną i niemożliwe jest stworzenie skanera antywirusowego o 100-procentowym wskaźniku powodzenia. Po prostu nie jest możliwe poznanie intencji każdego kawałka kodu, który trafia do komputera, i nie jest możliwe przetestowanie każdego kawałka kodu przed jego wykonaniem. Wymagałoby to, aby skaner AV wymagał tak dużej mocy obliczeniowej procesora, że prawidłowe programy nie byłyby w stanie wykonać. Zachowania złośliwego oprogramowania są bardzo zróżnicowane, a wiele z nich wykorzystuje techniki ukrywania się lub maskowania, aby ukryć się przed systemem operacyjnym, a nawet przed samym skanerem AV. Nie ma już twardych i szybkich reguł, które użytkownik może zastosować w celu ustalenia, czy system zawiera złośliwe oprogramowanie.

**Wczesne dni skanerów AV**

Kiedy pod koniec lat 80. wirusy zaczęły pojawiać się regularnie, ich wykrywanie i eliminacja były stosunkowo proste, ale niekoniecznie łatwe. Wirusy były dość proste i zwykle nie rozprzestrzeniały się bardzo szybko. Społeczność AV szybko je zbadała, ustaliła, co sprawiło, że działają, i w krótkim czasie opublikowała skuteczne poprawki. Te poprawki były zwykle pisane dla konkretnego wirusa i nie mogły wyleczyć innych wirusów, nawet jeśli były podobnego typu. Większość pracy spadła na użytkowników w celu zidentyfikowania, którego wirusa (lub typu wirusa), o którym myśleli, że mają, a następnie wyszukania programu, który go naprawi. Ponieważ łączność internetowa nie była tak powszechna jak obecnie, użytkownicy często spędzali dużo czasu dzwoniąc do znajomych i współpracowników w nadziei, że uda im się przesłać kopię dysku niezbędnego programu antywirusowego. Dodatkowo nie było konwencji nazewnictwa wirusów i trudno było stwierdzić z jakimkolwiek przekonaniem, że uzyskana poprawka faktycznie zadziała. Wirusy z tego okresu zazwyczaj umieszczały swój kod w przewidywalnych sekcjach programu. Wczesne skanery wyszukiwały określony ciąg znaków. Gdyby go znaleźli, usunęliby kod wirusa i spróbowali przywrócić program nosicielski do jego oryginalnej, niezainfekowanej postaci. W przeciwnym razie skaner zwykle informuje użytkownika, że leczenie nie

zostało zakończone i że powinien usunąć zainfekowaną aplikację i zainstalować ją ponownie. Gdy liczba wirusów zaczęła rosnąć, firmy programistyczne, które zapuściły się na rynek AV, zaczęły zdawać sobie sprawę, że tworzenie i rozpowszechnianie indywidualnych poprawek nie jest już możliwe. Zamiast tego zaczęli opracowywać bardziej wszechstronne skanery, które mogły wyszukiwać więcej wirusów, zarówno starych, jak i nowych. Nowe generacje skanerów składały się z dwóch komponentów: silnika skanującego i plików sygnatur. Każdy składnik był całkowicie zależny od działania drugiego. Silnik składał się z interfejsu użytkownika i aplikacji skanującej system w poszukiwaniu wirusów. Pliki sygnatur były bazą danych zawierającą odciski palców (unikalne segmenty kodu) znanych wirusów. Chociaż niektóre z tych wczesnych skanerów wykonały dobrą robotę, wiele nie. Żaden z wczesnych skanerów antywirusowych nie był w stanie wykryć wszystkich znanych wirusów.

**Ważność skanerów**

Producenci skanerów programowych pod koniec lat 80. i na początku lat 90. napotkali szereg przeszkód. Wyglądało na to, że co miesiąc pojawia się nowy dostawca AV, a rynek stał się bardzo konkurencyjny w miarę wzrostu świadomości użytkowników na temat problemu z wirusami. Biorąc pod uwagę ten konkurencyjny stan, wśród społeczności AV pojawiła się ogromna różnica zdań co do tego, jak należy przechowywać i testować wirusy do badań. Wielu producentów AV utrzymywało bibliotekę wirusów na własny użytek i fakt ten został wykorzystany w ich marketingu. Twierdzenia, że jeden program działał lepiej niż inny, ponieważ sprawdzał więcej wirusów, były mylące, ponieważ nikt nie wiedział, ile istnieje wirusów. Po prostu nie było metody komercyjnych lub niezależnych testów sprawdzających słuszność twierdzeń producentów produktów AV. Dodatkowo wystąpił problem z nazwaniem wirusów. Każdy sprzedawca tworzył własne nazwy wirusów i często zdarzało się, że jeden wirus był znany pod kilkoma nazwami. Sprzedawcy AV nie byli również zgodni co do zasady działania skanerów AV. Niektórzy dostawcy uważali, że skanery antywirusowe powinny szukać tylko nowych wirusów, a inni uważali, że dobry produkt powinien wyszukiwać zarówno stare, jak i nowe wirusy. Podczas gdy ten argument szalał, wyglądało na to, że wirusy w końcu zyskają przewagę, zwłaszcza, że twórcy wirusów zaczęli używać podziemnych tablic ogłoszeniowych, a później Internetu, do udostępniania i rozpowszechniania kodu wirusa. Bez żadnych standardów dla produktów AV, opinia publiczna miała niewiele do wyboru poza tekstem marketingowym dostawców i poradami innych użytkowników. Jeśli jednak znajomy zarekomendował program antywirusowy marki X, ponieważ w systemie znajomego nie znaleziono żadnych wirusów, możliwe było, że w systemie znajomego nie zostały wprowadzone żadne wirusy, a marka X nie mogła znaleźć starych wirusów, nowe wirusy lub w ogóle jakiekolwiek wirusy. Wydarzyły się dwie rzeczy, które zrewolucjonizowały rynek skanerów AV. W 1993 roku JoeWells, redaktor naukowy magazynu biznesowego, zaczął zbierać wirusy i raporty o wirusach od ekspertów z całego świata oraz tworzyć bibliotekę tych wirusów. Nazwał tę bibliotekę wirusów WildList i udostępnił ją legalnym badaczom AV. Jego lista podzieliła wirusy na te, o których wiadomo, że zainfekowały systemy (na wolności) i te, które zostały napisane, ale nie infekowały aktywnie (w zoo). Zaczęła również pojawiać się konwencja nazewnictwa wirusów w celu utrzymania wydajnej i przeszukiwalnej bazy danych. Innym ważnym wydarzeniem było opracowanie komercyjnych testów i certyfikacji AV przez firmę znaną jako National Computer Security Association (NCSA), która obecnie znana jest jako ICSA Labs. NCSA powołało konsorcjum producentów AV, którzy za opłatą przedstawili swoje produkty do testów. NCSA i Joe Wells rozpoczęli współpracę w celu wykorzystania jego WildList, a dr Richard Ford, znany ekspert ds. wirusów, stworzył laboratorium testowania wirusów dla NCSA. Dr Ford stworzył środowisko, w którym skanery antywirusowe zostały poddane próbie, aby sprawdzić, czy mogą wykryć wszystkie wirusy z WildList. Sprzedawcy AV zgłaszali swoje produkty za każdym razem, gdy miała zostać wydana nowa wersja ich produktu. Chociaż oryginalne wyniki testów były ponure (wiele skanerów nie potrafiło wykryć więcej niż 80 procent wirusów z listy), stworzono środowisko, w którym można było osiągnąć wymierną poprawę skuteczności technologii AV.

Oczywiście opinia publiczna i prasa zaczęły szukać produktów AV, które zostały certyfikowane przez NCSA. Ostatecznie inne komercyjne i niezależne laboratoria badawcze niezależnie opracowały własne programy certyfikacji i testowania, aby pomóc użytkownikom znaleźć niezawodne produkty AV. Wkrótce inne organizacje testujące dołączyły do walki, a produkty AV stały się bardziej złożone. Było jasne, że istnieje potrzeba opracowania standardów testowania, aby pomóc użytkownikom odróżnić skuteczne, bezstronne testy od tych, które nie demonstrowały wyraźnie możliwości produktów AV. Grupa badaczy AV, naukowców, testerów i innych zainteresowanych stron utworzyła organizację, która ma opracować takie standardy, zwaną Anti-Malware Testing Standards Organization (AMTSO). Grupa ta opublikowała szereg artykułów, w których przedstawiono rozważania na temat tego, jak stworzyć lub odróżnić dobry test od nieadekwatnego. Artykuły te mają pomóc zarówno testerom, jak i osobom czytającym testy.

**Wnętrze skanera**

Jak wspomniano wcześniej, skaner AV nie może po prostu umieścić każdego programu w pamięci RAM komputera i przetestować go pod kątem złośliwego oprogramowania, zanim program zostanie uruchomiony. Aby to zrobić, wymagałoby to prawie wszystkich zasobów procesora, a użytkownicy mieliby system, który działałby w ślimaczym tempie. Aby skanery AV działały wydajnie, musiały dołożyć wszelkich starań, aby poprawić swoją szybkość w celu wykrycia ogromnej liczby istniejącego złośliwego oprogramowania bez zatrzymywania całego systemu. Stosowanie wyrafinowanych metod eliminacji w celu wykluczenia podpisów, których cechy nie odpowiadają cechom skanowanego pliku, pomaga utrzymać rozsądne prędkości. W nowoczesnym produkcie AV istnieje pięć podstawowych typów wykrywania. Większość ludzi zna wykrywanie oparte na sygnaturach, które jest również znane jako wykrywanie specyficzne, ale nie jest to już jedyna stosowana technika. Produkty AV mogą wykorzystywać niektóre lub wszystkie z tych pięciu podstawowych metod działania:

1. Specyficzne wykrywanie. Szukasz znanego złośliwego oprogramowania

2. Wykrywanie ogólne. Wyszukiwanie infekcji przez warianty znanego złośliwego oprogramowania

3. Heurystyki. Skanowanie w poszukiwaniu nieznanych wcześniej wirusów poprzez wykrywanie podejrzanych zachowań lub struktur plików, jak opisano bardziej szczegółowo w sekcji 41.3.3

4. Zapobieganie włamaniom. Monitorowanie znanych podejrzanych zmian i zachowań systemu w celu zapobiegania podejrzeniu złośliwego oprogramowania

5. Reputacja. Wykrywanie złośliwego oprogramowania na podstawie reputacji pliku lub witryny na podstawie wielu czynników, w tym liczby pobrań pliku lub witryny, raportów klientów lub wieku witryny

**Silniki antywirusowe i antywirusowe bazy danych**

Silnik AV i jego baza danych sygnatur współpracują ze sobą, aby zapobiegać i wykrywać złośliwe oprogramowanie próbujące dostać się do systemu. Silnik ogólnie zapewnia bibliotekę powszechnie używanych funkcji. Składa się z kilkudziesięciu skomplikowanych algorytmów wyszukiwania, emulatorów procesora oraz różnych form logiki programistycznej. Silnik określa, które pliki należy przeskanować, jakie funkcje uruchomić i jak zareagować w przypadku wykrycia podejrzanego złośliwego oprogramowania. Jednak silnik nie wie absolutnie nic o samym złośliwym oprogramowaniu i jest prawie bezużyteczny bez bazy sygnatur. Baza sygnatur zawiera odciski palców (fragmenty charakterystycznego kodu) setek milionów wariantów złośliwego oprogramowania. Ponieważ nowe złośliwe oprogramowanie i jego warianty pojawiają się w coraz szybszym tempie, konieczne jest częste aktualizowanie bazy sygnatur. W 1995 roku eksperci zalecili aktualizowanie plików bazy danych

przynajmniej raz w miesiącu, ale przy tak dużej liczbie wirusów pojawiających się każdego dnia, użytkownikom zaleca się aktualizowanie co najmniej raz dziennie, a najlepiej, aby umożliwić ciągłe aktualizacje kontrolowane przez ich produkt AV. Producenci AV oferują teraz produkty, które automatycznie sprawdzają dostępność aktualizacji i pobierają zmiany za każdym razem, gdy użytkownik jest podłączony do Internetu. Niektórzy dostawcy udostępniają również bazy danych sygnatur oparte na chmurze, dzięki czemu komputery połączone z Internetem mogą sprawdzać, czy są one częściej aktualizowane w zestawie sygnatur, które są hostowane na własnych zdalnych systemach dostawców. Baza sygnatur zawiera również zestawy reguł używane w skanowaniu heurystycznym. Tego typu skanowanie może być wolniejsze i bardziej inwazyjne niż proste skanowanie podpisów, a ich konstrukcja i implementacja różnią się znacznie w zależności od produktu. Większość produktów daje teraz użytkownikom konfigurowalne opcje zmniejszania lub zwiększania heurystyki zgodnie z potrzebami. Chociaż skanowanie sygnatur można uznać za samo w sobie heurystyczne, termin ten jest częściej używany do identyfikowania bardziej złożonych funkcji antywirusowych, które próbują zlokalizować wirusy poprzez identyfikację podejrzanego zachowania i/lub struktury plików. Ponieważ dla wielu administratorów systemu rozróżnienie między aparatem skanowania a bazą danych sygnatur nie jest oczywiste, wielu z nabożeństwem aktualizuje bazę danych, ale nie zdaje sobie sprawy, że silnik również może wymagać aktualizacji. Jest to kiepska strategia, która może spowodować niewykrycie wielu wirusów przez skaner.

**METODOLOGIE SKANOWANIA**

Produkty AV mogą być konfigurowane przez użytkownika lub administratora systemu w celu skanowania przy starcie, w trybie ciągłym lub na żądanie. Aby być najbardziej efektywnym, skaner powinien być ustawiony na skanowanie ciągłe lub „podczas dostępu", z okresowym, zaplanowanym skanowaniem, które ma być wykonywane, gdy system jest włączony, ale nie jest używany. Użytkownicy korzystający z mniej zoptymalizowanych programów antywirusowych mogą stwierdzić, że obniża to wydajność systemu. Niektóre skanery muszą wykorzystywać dużą część pamięci systemu podczas ciągłego skanowania, aby móc testować sekcje kodu, co może znacznie spowolnić działanie aplikacji przy pierwszym uruchomieniu. Dlatego trzeba znaleźć szczęśliwy środek - skaner AV musi być w stanie chronić system, a użytkownik musi mieć możliwość pełnego korzystania z systemu. Nie ma jednej metody skanowania, która jest lepsza od innych. Wszystkie metody skanowania mają swoje zalety i wady, ale żadna nie jest w stanie wykryć złośliwego oprogramowania z niezawodną dokładnością. Ascan szuka kodu i zachowań, które zostały zauważone w innym złośliwym oprogramowaniu, a jeśli nowe złośliwe oprogramowanie wykazuje nowe, nieznane wcześniej zachowania, może przejść niezauważony. Dlatego większość skanerów antywirusowych nie opiera się tylko na jednej metodzie skanowania w celu wykrycia złośliwego oprogramowania, ale ma kilka wbudowanych w swój projekt.

**Specyficzne wykrywanie**

Każde złośliwe oprogramowanie wykorzystuje inny kod do wykonywania swoich funkcji. Sekwencja kodu charakterystyczna dla każdego złośliwego oprogramowania jest określana jako odcisk palca lub sygnatura tego złośliwego oprogramowania. Aby wykryć obecność złośliwego oprogramowania, skaner szuka sygnatury, usuwa jego kod z pliku lub systemu hosta i próbuje przywrócić zainfekowany program lub system do stanu niezainfekowanego. We wczesnych wirusach odkryto, że sygnatury znajdowały się zwykle w określonych obszarach programu, specyficznych dla każdego wirusa. Skanery postanowiły sprawdzać tylko te obszary pliku, a nie skanować cały program od góry do dołu. Zaoszczędziło to ogromne ilości czasu i mocy obliczeniowej. Ponieważ złośliwe oprogramowanie jest często statyczne, a nie pasożytnicze, badacze AV muszą teraz być bardziej kreatywni, aby szybko identyfikować znane złe pliki. Ponieważ jednak autorzy złośliwego oprogramowania uzbroili swoje pliki, aby utrudnić badaczom ich analizę, może to również sprawić, że złośliwy plik będzie wyglądał zupełnie inaczej niż

prawidłowy dokument lub aplikacja. W związku z tym badacze mogą określić te różnice i szybko wykluczyć łagodne pliki. Każdy produkt AV każdego dostawcy ma inną implementację skanera i bazy danych, chociaż najczęściej stosowana jest technika skanowania sygnatur. Skanowanie sygnatur może określić, czy program zawiera jedną z wielu sygnatur zawartych w bazie danych, ale nie może stwierdzić z całą pewnością, czy na system faktycznie wpłynęło złośliwe oprogramowanie (np. złośliwe oprogramowanie może być obecne, ale jeszcze niewykonane). Użytkownicy mogą ufać tylko domysłom skanera AV, ponieważ szanse są na korzyść skanera. Możliwe jest jednak, że program podejrzany o zainfekowanie faktycznie zawiera losowe dane, które tylko przypadkowo wyglądają jak wirus sygnaturowy. Prawidłowy program może zawierać instrukcje, które przez przypadek pasują do ciągu wyszukiwania w bazie danych wirusów. Jeśli jednak istnieje możliwość, że kod faktycznie pochodzi z wirusa, skaner zgłasza to jako pozytywne trafienie. Fałszywie pozytywne raporty są możliwym problemem skanerów podpisów. Jeśli użytkownicy zauważą, że ich skaner zbyt często fałszywie zgłasza obecność wirusów, postrzegają to jako irytację i prawdopodobnie będą próbować wyłączyć oprogramowanie lub znaleźć sposoby na obejście skanowania.

**Wykrywanie ogólne**

Jak wspomniano wcześniej, złośliwe oprogramowanie jest obecnie często tworzone w celach finansowych, a uzyskanie jak największej ilości szkodliwego oprogramowania ma dla jego autorów sens podatkowy wykorzystać w miarę możliwości z udanych kreacji. Często tworzą kod o otwartym kodzie źródłowym, który jest powszechnie udostępniany w społeczności twórców szkodliwego oprogramowania, dzięki czemu jest często aktualizowany o nowe funkcje, takie jak możliwość kradzieży kodów exploitów lub haseł, w celu ukierunkowania na nowe gry, aplikacje lub witryny bankowości internetowej. Podobnie, sensowne jest, aby skanery antywirusowe szukały wspólnych właściwości popularnych rodzin złośliwego oprogramowania lub znanych złośliwych zachowań w celu proaktywnego wykrywania wariantów na podstawie tych baz kodu. Te ogólne detekcje mogą mieć różny charakter, od bardziej heurystycznego charakteru do dość szczegółowego. Na przykład może obejmować ochronę tak szeroką, jak wykrywanie przepełnienia bufora, aby zapobiec niektórym typom exploitów, do określonych domowych programów pakujących używanych tylko przez jedną rodzinę złośliwego oprogramowania. Wykrywanie generyczne wywołało wiele kontrowersji we wczesnych dniach produktów AV. Kiedy większość wirusów rozprzestrzenia się poprzez pasożytnicze infekowanie czystych plików, pojawiła się obawa, że ogólne wykrycie będzie wymagało ogólnego czyszczenia, co może spowodować, że pliki hosta będą zniekształcone i niemożliwe do naprawienia lub użyteczności. Ponieważ zdecydowana większość złośliwego oprogramowania infekuje teraz systemy, a nie pliki hostów, proste usuwanie złośliwych plików i czyszczenie wpisów w rejestrze może usunąć złośliwe oprogramowanie. Ale ponieważ złośliwe oprogramowanie jest również często oparte na komponentach, usunięcie jednym zagrożeniem może być tylko wierzchołek góry lodowej. Mogą istnieć inne komponenty, które nie zostały jeszcze wykryte, dlatego najlepiej jest dokładnie zbadać każdy system, w którym wykryto złośliwe oprogramowanie. W związku z tym coraz więcej administratorów systemów przyjęło zasadę po prostu ponownego tworzenia obrazów systemów, których dotyczy problem, zamiast polegać na procedurach usuwania produktów AV.

**Heurystyki**

Dodając heurystykę do swoich skanerów AV, dostawcy starali się zwiększyć efektywność swoich produktów. Skanery mogą teraz wyszukiwać złośliwe oprogramowanie, które jest nowe i nieznane i nie znajduje się w bazie danych sygnatur. Słowo heurystyka pochodzi od greckiego słowa oznaczającego „odkrywać”. Termin ten jest obecnie używany w informatyce do opisywania algorytmów, które są skuteczne w szybkim rozwiązywaniu złożonych pytań. Algorytm heurystyczny przyjmuje pewne założenia dotyczące problemu, który próbuje rozwiązać. W przypadku skanera

antywirusowego analizuje on strukturę programu, jego atrybuty i zachowanie, aby sprawdzić, czy spełniają one reguły ustanowione w celu identyfikacji złośliwego oprogramowania, nawet bez znanej jego sygnatury. Zasadniczo algorytm heurystyczny działa przy założeniu, że jeśli „wygląda jak kaczka, chodzi jak kaczka i brzmi jak kaczka, to musi to być kaczka".

Wadą skanowania heurystycznego jest to, że robi inteligentne założenia, ale mimo to popełnia błędy. Innym problemem związanym ze skanowaniem heurystycznym jest to, że w wolniejszych systemach jego uruchomienie może trwać dłużej i może wymagać interakcji użytkownika. Niektórzy użytkownicy uważają to za uciążliwe i mogą wyłączyć tę funkcję. Łącząc w swoich produktach zarówno skanowanie sygnatur, jak i skanowanie heurystyczne, dostawcy AV zwiększyli swoją skuteczność i szybkość. Skanery heurystyczne wykorzystują system oparty na regułach do weryfikacji istnienia złośliwego oprogramowania. Stosuje wszystkie zasady do danego programu i daje programowi ogólną ocenę. Jeśli wynik jest wysoki, istnieje duże prawdopodobieństwo, że jest złośliwy. Ogólnie rzecz biorąc, skaner najpierw wyszukuje cechy pliku, które są bardziej typowe dla złośliwych plików. Dobrze zaprojektowany skaner heurystyczny ograniczy badane regiony programu w celu przeskanowania jak największej liczby podejrzanych w możliwie najkrótszym czasie. Skaner następnie analizuje logikę podejrzanego programu, aby określić, czy może on próbować wykonać znane, prawdopodobnie złośliwe działania. Ten typ skanowania jest uważany za skanowanie statyczne. Metoda statyczna stosuje reguły i nadaje programowi ocenę zaliczoną/niezaliczoną - niezależnie od tego, czy program faktycznie wykonał się, czy nie. Drugi rodzaj skanowania heurystycznego to metoda dynamiczna. Ta metoda zasadniczo stosuje te same zasady, co metoda statyczna, a jeśli wynik jest wysoki, próbuje emulować program. Zamiast badać logikę podejrzanego kodu, dynamiczny skaner uruchamia symulację wirusa w środowisku wirtualnym. Ta technika jest znana jako emulacja piaskownicy i jest skuteczna w przypadku próby zidentyfikowania nowego złośliwego oprogramowania, które nie pojawia się w bazie danych sygnatur. Żadna z tych heurystycznych metod skanowania nie jest koniecznie lepsza od drugiej, ale razem dają całkiem dobre wyniki. Chociaż statyczne skanowanie heurystyczne może przeoczyć niektóre złośliwe oprogramowanie, ponieważ nie zostały one jeszcze uruchomione, dynamiczne skanowanie heurystyczne może wyłapać nieznane wcześniej złośliwe oprogramowanie, zanim zostanie ono uruchomione w systemie. Między wykrywaniem heurystycznym a generycznym coraz częściej co najmniej jeden dostawca AV identyfikuje każde nowe złośliwe oprogramowanie zaraz po jego wydaniu.

**Wykrywanie i zapobieganie włamaniom**

Ponieważ coraz bardziej złożone złośliwe oprogramowanie pojawia się w coraz bardziej zadziwiającym tempie, programy skanujące wyłącznie w poszukiwaniu sygnatur stają się mniej skuteczne w wykrywaniu wirusów. Autorzy wirusów stosują techniki szyfrowania lub zaciemniania lub udostępniają dużą liczbę pojedynczych wariantów w nadziei, że skaner antywirusowy nie znajdzie ich. Dzisiejsze systemy operacyjne i legalne programy rozrosły się do milionów linijek kodu, więc znalezienie sygnatury wirusa może być zasobem intensywnym. Ponieważ złośliwe oprogramowanie może kraść cenne dane lub uszkadzać systemy, nie jest dobrą strategią pozwalanie im na uruchomienie, a następnie podejmowanie prób posprzątania bałaganu. Lepszą strategią jest próba znalezienia złośliwego oprogramowania, zanim zdąży ono wpłynąć na system i zapobiec wyrządzeniu mu szkód. Stosowanie cyklicznej kontroli nadmiarowej (CRC) lub sum kontrolnych zostało pierwotnie dodane do niektórych produktów zabezpieczających, w tym pakietów AV, aby pomóc w wykrywaniu i zapobieganiu infekcjom wirusowym. Ta metoda śledzi nieautoryzowane zmiany w plikach i systemie, na przykład w przypadku wniknięcia złośliwego oprogramowania lub hakera do systemu i jego zmiany. Aby śledzić te zmiany, odcisk palca każdego programu wykonywalnego i pliku danych jest obliczany i przechowywany w bazie danych podczas pierwszej instalacji produktu AV. Te odciski palców są dość

małe, zwykle składają się z mniej niż 100 bajtów informacji - jest to „suma” lub suma kontrolna. Ponieważ złośliwe oprogramowanie musi dodawać lub zmieniać pliki w systemie, aby na niego wpływać, sumy kontrolne odcisków palców są porównywane z każdą nowszą wersją. Jeśli sumy kontrolne są różne, skaner AV uruchamia inne procedury w celu dalszego zbadania. W przypadku systemów zapobiegania włamaniom skanowanie oparte na zachowaniu jest wykonywane na każdy nowy plik po uruchomieniu. W przypadku zaobserwowania pewnych podejrzanych zachowań, użytkownik może zostać zapytany, czy należy zezwolić na kontynuację tego zachowania. Jeśli zostanie zaobserwowana sekwencja zachowań, która jest wystarczająco złośliwa, program może zostać całkowicie zatrzymany. Stwierdzono, że technika ta jest niezwykle skuteczna w zapobieganiu uruchamianiu nowego, nieznanego złośliwego oprogramowania, chociaż ma te same trudności, co przy skanowaniu heurystycznym. Ponownie, jako część pełnego arsenału bezpieczeństwa, może być cennym narzędziem.

**FILTROWANIE ZAWARTOŚCI**

We wczesnych dniach infekcji wirusowych eksperci ds. bezpieczeństwa komputerowego często łagodzili obawy użytkowników komputerów, mówiąc im, że nigdy nie złapią wirusa komputerowego z wiadomości e-mail. Zapewnienie to opierało się na fakcie, że e-mail składał się prawie wyłącznie z dokumentów tekstowych ASCII, bez możliwości wykonania kodu programu. Jednocześnie sceptycy mówili „nigdy nie mów nigdy”. Sceptycy wygrali. Po pierwsze, było kilka fal makrowirusów – zainfekowanych dokumentów wysyłanych jako załączniki do wiadomości e-mail. Doprowadziło to do zmodyfikowanego zapewnienia ekspertów ds. bezpieczeństwa, że nikt nigdy nie złapie wirusa komputerowego z załącznika wiadomości e-mail, jeśli załącznik nie zostanie otwarty. Następnie twórcy wirusów zaczęli osadzać polecenia korzystające z języka HTML i możliwości skryptów programów pocztowych. Doprowadziło to do dalszego zmodyfikowanego zapewnienia ekspertów, że wirus komputerowy nie może zostać przechwycony z nieotwartej wiadomości e-mail. To zapewnienie okazało się z kolei nieuzasadnione, ponieważ możliwości podglądu wiadomości e-mail zostały wykorzystane do uruchomienia złośliwego kodu nawet bez interwencji użytkownika. W pewnym momencie samo podświetlenie tematu wiadomości w MS Outlooku wystarczyło do wykonania załącznika, chociaż to domyślne ustawienie zostało później zmienione. Twórcy wirusów zaczęli również wykorzystywać funkcję poczty e-mail użytkownika, przesyłając kopie wirusa do wpisów w książce adresowej użytkownika. Wirus Melissa był pierwszym wirusem, który naprawdę wykorzystywał pocztę e-mail do szybkiego rozprzestrzeniania się. Od czasu pojawienia się wirusa Melissa użytkownikom doradza się, aby podejrzewali każdą niechcianą wiadomość e-mail. Twórcy szkodliwego oprogramowania zawsze szukają nowych metod dostarczania i zostali sowicie nagrodzeni, gdy programy pocztowe zaczęły zezwalać na kod wykonywalny w wiadomości e-mail. Chociaż użytkownicy korzystają z wygody tej funkcji typu „wskaż i kliknij”, umożliwiła ona rozprzestrzenianie się nowych wirusów w niespotykanym wcześniej tempie. W sieci nastąpiła również eksplozja dystrybucji szkodliwego kodu, szczególnie od czasu pojawienia się „Web 2.0” – serwisów społecznościowych i witryn współpracy. Dzięki obiektom Adobe Flash, Java i JavaScript, które wykorzystują luki w zabezpieczeniach przeglądarek internetowych lub oprogramowania przeglądarki multimediów, złośliwe oprogramowanie może być automatycznie pobierane i instalowane na komputerze użytkownika bez jego wiedzy. Jest to powszechnie określane jako drive-by download. Filtrowanie treści to jeden z popularnych sposobów kontrolowania zagrożeń internetowych i e-mailowych. Składa się z aplikacji serwerowej, która odpytuje cały ruch przychodzący i wychodzący, zgodnie z jego konfiguracją i zestawami reguł. Wczesne wersje były kłopotliwe w konfiguracji ze względu na interfejs tekstowy, który wymagał tworzenia wszystkich reguł w pracochłonnym edytorze tekstu. Błędy w konfiguracji były powszechne, ponieważ administratorzy często nie byli pewni, który z plików tekstowych powoduje awarię. Nowa generacja filtrów treści zwiększyła przyjazność dla użytkownika, używając

interaktywnych graficznych interfejsów użytkownika do ustawiania i dostosowywania zasad. Administratorzy mogą dostosowywać zasady tak, aby spełniały określone potrzeby ich organizacji. Na przykład wszystkie wiadomości e-mail zawierające wykonywalne załączniki mogą zostać zablokowane, poddane kwarantannie lub po prostu usunięte. Można to ustalić z reguły dla niektórych użytkowników lub wszystkich użytkowników. Filtry treści były szczególnie skuteczne w zapobieganiu infekcjom wirusami przenoszonymi przez pocztę e-mail, nawet przed opublikowaniem określonej sygnatury wirusa. Na przykład, gdy oficer bezpieczeństwa jednego z urzędów państwowych usłyszał w porannych wiadomościach o wirusie Love Bug, ta osoba ustawiła filtry treści tak, aby blokowały wszystkie załączniki do wiadomości e-mail zawierające rozszerzenie „.vbs", zapobiegając w ten sposób infekcji dużej sieci. Nie była wymagana żadna interakcja użytkownika, a większość użytkowników nie była świadoma, że blok został umieszczony. Uniknięto kosztów i przestojów ataku wirusa. Większość zagrożeń pochodzi teraz z zainfekowanych legalnych witryn, a nie z ciemnego, obskurnego podbrzusza Internetu, co zmienia sposób, w jaki produkty wyświetlają niechcianą zawartość. W związku z tym wiele z tej technologii filtrowania treści przesunęło się z nacisku na blokowanie potencjalnie złośliwych treści na blokowanie stron internetowych, które są uważane za nieodpowiednie do przeglądania w pracy lub przez dzieci. Wiele filtrów treści zawiera obszerne, często aktualizowane listy blokujące dla pornografii, „mowy nienawiści" i innych drażliwych politycznie tematów.

**Jak działają filtry treści**

Aplikacje te działają w ten sam sposób, co skanery AV. Skanują wszystkie dane przychodzące na określonych portach na serwerze i porównują ruch z regułami i ciągami w bazie danych. Ponieważ filtry treści mogą blokować więcej niż jeden typ pliku lub programu, mają możliwość skanowania plików tekstowych, grafik, plików skompresowanych, samorozpakowujących się i różnych plików wykonywalnych. Wiele filtrów treści zawiera komponenty skanowania antywirusowego, więc jeśli ruch zawiera znany złośliwy kod, może zostać przechwycony i wyleczony przed wysłaniem do odbiorcy. Standardy formatowania wiadomości e-mail do transmisji przy użyciu standardowych protokołów są od dawna stosowane i szczegółowo określają rodzaj informacji w każdej sekcji. Programowi łatwo jest wyszukać określone informacje w tych sekcjach, aby na przykład określić, co jest zawarte w załącznikach do wiadomości. Filtry treści najpierw rozpoczynają od demontażu wiadomości, aby przejrzeć jej różne części, a następnie przeskanować wiadomość w poszukiwaniu elementów, które mają zostać dopuszczone lub odrzucone w systemie. Przed wysłaniem wiadomości dalej jest składana i sprawdzana pod kątem warunków określonych w konfiguracjach. Na przykład warunek może oznaczać, że wszelkie załączniki zostaną usunięte i usunięte, treść wiadomości zostanie wysłana do odbiorcy oraz że do nadawcy zostanie wysłana zewnętrzna wiadomość e-mail z informacją, że załączniki nie są dozwolone w wiadomości e-mail. Jeśli chodzi o bezpieczeństwo danych, filtr treści dodaje kilka elementów, które wykraczają poza tradycyjny skaner AV. Na przykład treść wiadomości i załączników można przeskanować w poszukiwaniu nieodpowiednich materiałów. Mogą to być zastrzeżone informacje firmy, których pracownicy nie powinni wysyłać pocztą elektroniczną, lub mogą to być obraźliwe materiały, takie jak pornografia, które nie powinny trafiać do systemu poczty e-mail firmy. Filtrowanie treści może również powstrzymać rozprzestrzenianie się powszechnych form spamu, takich jak łańcuszki i schematy szybkiego wzbogacenia się.

**Wydajność i skuteczność**

Szybkość działania jest problemem związanym z mechanizmami filtrowania treści, biorąc pod uwagę duży ruch sieciowy w większości organizacji. Jednak ponieważ wszystkie operacje są zawarte w serwerze, użytkownicy nie zauważą żadnych zmian w wydajności swoich systemów stacjonarnych; oznacza to, że przetwarzanie zostanie zakończone przed odebraniem komunikatów przez systemy klienckie. Na przykład w przypadku poczty e-mail, jeśli filtrowanie powoduje kolejkowanie poczty,

dostarczenie poczty może opóźnić się przez pewien czas. Jeśli strony internetowe są blokowane z powodu nieodpowiednich treści, ruch po prostu nie będzie dostarczany do użytkownika. Filtry treści są również narażone na te same awarie, co tradycyjne skanery AV. Nowe złośliwe oprogramowanie może zostać pominięte, jeśli danych nie ma w skanowanej bazie danych. Dodatkowo konfiguracja produktu oraz stosowanie poprawek i aktualizacji są kluczowe dla jego pomyślnego działania. Fałszywe alarmy również stanowią problem, gdy legalna wiadomość nieumyślnie zawiera treść, która powoduje blokadę. Możliwe jest poddanie podejrzanych wiadomości kwarantannie i skontaktowanie się z administratorem systemu z nadawcą. Może to prowadzić do udoskonalenia filtrów lub wykrycia poważnych wykroczeń. Przed wdrożeniem systemu filtrowania treści ważne jest wprowadzenie mechanizmów reagowania, aby można było odpowiednio zareagować na nadużycia zasad. Może to równie dobrze obejmować kilka działów oprócz bezpieczeństwa, w tym działów prawnych i ludzkich.

**WDROŻENIE ANTYWIRUSÓW**

Skanery AV można instalować na komputerach stacjonarnych lub serwerach. Każda strategia ma swoje wady i zalety. Na przykład, jeśli system jest oparty na serwerze, złośliwe oprogramowanie na dyskach USB, dyskach DVD i CD na pulpicie nie zostanie przeskanowane. Konsensusem większości ekspertów jest jednak wykorzystanie obu. Dzięki postępom w produktach AV i systemach zarządzania siecią całkowicie możliwe jest instalowanie skanerów zarówno na komputerach stacjonarnych, jak i serwerach, przy jednoczesnym zachowaniu akceptowalnego poziomu kontroli i wydajności.

**Same komputery stacjonarne**

Jeśli polityka bezpieczeństwa organizacji pozwala na nieograniczone korzystanie z pendrive'ów, dyskietek, dysków DVD i CD, konieczne jest, aby skanery AV zostały wdrożone na pulpicie. O ile te dyski nie są zablokowane lub wyłączone, nie ma innego sposobu niż skanowanie, aby zapobiec przypadkowemu wprowadzeniu złośliwego oprogramowania przez użytkowników. W preferencjach biurkowego skanera AV można ustawić automatyczne skanowanie nośników zewnętrznych. Aktualizacje stacjonarnych skanerów antywirusowych mogą być teraz dystrybuowane za pośrednictwem centralnego serwera. Jest to szczególnie skuteczne, gdy potrzebne są nowe pliki sygnatur, aby zapobiec infiltracji przez nowo wykryte złośliwe oprogramowanie. Aktualizacje mogą być przesyłane na pulpit, a użytkownicy nie muszą być obecni na stacji roboczej, chociaż system pulpitu musi być w tym czasie włączony i podłączony do sieci. Jeśli aktualizacje są zaplanowane po godzinach pracy, ważne jest, aby sprawdzić, czy systemy mają aktualizacje przekazane do nich, gdy tylko zalogują się ponownie do sieci. Niektóre produkty AV mają konsole zarządzania, które pozwalają na to automatycznie, zamiast każdorazowo sprawdzać każdy system. Aby zapobiec nieautoryzowanym zmianom konfiguracji AV, można uniemożliwić użytkownikom zmianę konfiguracji ich biurkowych skanerów AV. Ponieważ może to nie być instalacja domyślna, należy ją sprawdzić. Ponownie, przy użyciu konsoli zarządzania, możliwe jest zdalne egzekwowanie zasad oprogramowania zabezpieczającego.

**Antywirus oparty na serwerze**

Wiele firm próbowało wzmocnić zabezpieczenia na obrzeżach swojej sieci, instalując produkty AV na serwerze, na którym często przechowywane są pliki do pobrania, a ruch jest duży. Oparty na serwerze skaner antywirusowy można skonfigurować tak, aby wysyłał alerty do administratorów w przypadku wykrycia podejrzanego złośliwego oprogramowania. Podobnie jak w przypadku skanerów stacjonarnych, reakcja na wykrycie złośliwego oprogramowania może być z góry określona. Wielu administratorów systemu ustawia program tak, aby usuwał wszystkie zainfekowane pliki zamiast wysyłać je do kwarantanny. Ta strategia zmniejsza prawdopodobieństwo, że złośliwe oprogramowanie poddane kwarantannie może zostać „uwolnione” przez pomyłkę.

**Urządzenia mobilne**

Wraz ze wzrostem korzystania ze smartfonów i tabletów przez osoby fizyczne i organizacje oraz poprzez zasady „przynieś własne urządzenie", zabezpieczenie tych urządzeń przed złośliwym oprogramowaniem zyskało na znaczeniu. W celu ochrony takich urządzeń opracowano oparte na hoście narzędzia do wykrywania włamań i oparte na sygnaturach, ale istnieją problemy związane z modelem bezpieczeństwa niektórych systemów operacyjnych (np. Android) ze względu na ścisły podział obszarów pamięci kontrolowanych przez aplikacje.

**ZASADY I STRATEGIE**

W walce ze złośliwym oprogramowaniem równie ważne jak instalacja skanera antywirusowego jest publikowanie odpowiednich polityk i wdrażanie realistycznych planów działania. Zasady powinny szczegółowo określać, jakie działania są dozwolone lub zabronione, a także powinny szczegółowo określać obowiązki użytkowników. Zasady i obowiązki powinny być regularnie aktualizowane, aby odzwierciedlały realia zmieniającego się krajobrazu złośliwego oprogramowania, zwłaszcza w ekosystemie firmy. Szkolenie uświadamiające użytkownikom końcowym AV powinno być wysoko na liście priorytetów w każdej organizacji. Użytkownicy są bardziej skłonni do współpracy w zapobieganiu infekcjom i poddawaniu ich kwarantannie, jeśli są świadomi typów złośliwego oprogramowania, które mogą wpływać na ich system i szkód, jakie mogą spowodować. Prosta tablica informacyjna o incydentach związanych z bezpieczeństwem w centralnej lokalizacji to łatwy i skuteczny sposób komunikowania się z użytkownikami. Poczta e-mail prawdopodobnie nie jest skuteczną metodą rozpowszechniania informacji o złośliwym oprogramowaniu, ponieważ użytkownicy są zdezorientowani między działaniami edukacyjnymi, rzeczywistymi i legalnymi alertami o złośliwym oprogramowaniu i fałszywymi alertami o złośliwym oprogramowaniu. Role i obowiązki każdej osoby w organizacji powinny być jasno określone i przekazane ogółowi społeczeństwa. Na przykład obowiązki przeciętnego użytkownika będą inne niż obowiązki administratora systemu, a obowiązki te powinny być odzwierciedlone w ich rolach. Rola pojedynczego użytkownika może opisywać działania wymagane od użytkownika w przypadku wykrycia złośliwego oprogramowania na stacji roboczej, natomiast rola administratora systemu może opisywać, jak obsłużyć zgłoszenie od użytkownika i przygotować się do usunięcia. Problemy i katastrofy zwykle pojawiają się w najmniej spodziewanych momentach, dlatego każda organizacja powinna mieć w swojej polityce plan reagowania kryzysowego. Plan awaryjny powinien szczegółowo określać listę osób, które należy wezwać w nagłych wypadkach oraz kolejność priorytetów w którym należy je nazwać. W przypadku każdego poważnego incydentu związanego ze złośliwym oprogramowaniem w organizacji należy zadbać o to, aby sesja „wyciągniętych wniosków" została przeprowadzona jak najszybciej po zdarzeniu. Bez względu na to, jak dobrze napisana może być polityka, nie można jej udowodnić, że jest skuteczna, dopóki nie zostanie wprowadzona do użytku. Rzeczywista infekcja zwróci uwagę na błędy w działaniu polityki, które należy naprawić przed następnym atakiem. Więcej informacji na temat wytycznych dotyczących polityki bezpieczeństwa znajduje się w rozdziale 4 niniejszego Podręcznika. Wsparcie kierownictwa dla takich polityk ma kluczowe znaczenie. Wsparcie jest wymagane nie tylko do zatwierdzenia budżetu AV i zasad, ale także do upewnienia się, że wszyscy przestrzegają zasad. Jest wysoce nieprawdopodobne, aby użytkownicy postępowali zgodnie z polityką, której wyższe kierownictwo rutynowo lekceważy.

**UWAGI KOŃCOWE**

Zarówno technologia AV, jak i technologia złośliwego oprogramowania rozwijały się szybko na przestrzeni czasu, a technologia AV w dużej mierze pozostaje w zgodzie z technologią złośliwego oprogramowania. Obecnie sukces szkodliwego oprogramowania wynika głównie z motywacji finansowej, ale w dużej mierze powodem, dla którego jest to tak lukratywny biznes, jest to, że ludzie

nadal lekceważą zagrożenie ze strony złośliwego oprogramowania. Niezależnie od tego, jak dobra jest technologia AV, nie spowoduje ona poważnego problemu ze złośliwym oprogramowaniem, chyba że zostanie odpowiednio wdrożona przez organizacje i właściwie zatrudniona przez użytkowników, którzy działają odpowiedzialnie. Ponieważ technologia AV wciąż się rozwija i staje się coraz lepiej rozumiana, mamy nadzieję, że będzie ona nadal wykorzystywana szerzej i mądrzej