Ochrona hybrydowa: połączenie technologii chmury oraz wszechstronnego rozwiązania bezpieczeństwa

Eksperci z Kaspersky Lab wykrywają codziennie około 35 tysięcy nowych szkodliwych programów. W związku z tym konieczne jest dostarczanie aktualizacji sygnatur zagrożeń tak szybko i tak często, jak to możliwe, nie obciążając przy tym znacznie zasobów komputera. Z drugiej strony użytkownicy oczekują niezakłóconej pracy na swoim sprzęcie i nikt nie chce poświęcać zbyt dużej przestrzeni swojego dysku twardego na przechowywanie baz antywirusowych. Podobnie, cenione jest jak najmniejsze wykorzystywanie pamięci RAM na analizowanie aktywności programów w celu wykrycia potencjalnie niebezpiecznego zachowania.

Eksperci z Kaspersky Lab zajmują się tym problemem od jakiegoś czasu i oferują wiele możliwych rozwiązań tego problemu.

Ochrona w chmurze

Stworzenie ochrony w postaci technologii chmury stało się jednym z największych wyzwań do pokonania. Jest ona zaimplementowana w produktach firmy Kaspersky Lab w postaci systemu Kaspersky Security Network (KSN). Z milionów komputerów na całym świecie, które są chronione przez produkty firmy Kaspersky Lab, KSN gromadzi określone informacje (np. wszelkie próby zainfekowania, wykryte podejrzane zachowanie) i wysyła je do scentralizowanych serwerów Kaspersky Lab. System ten korzysta także z wielu innych źródeł, nieustannie monitorując sytuację szkodliwego oprogramowania w wirtualnym świecie. W ten sposób, gdy nowe szkodniki próbują zainfekować pojedynczy komputer, informacja o szkodliwym programie oraz jego aktywności jest natychmiast dostarczana do ekspertów Kaspersky Lab za pomocą KSN. System ciągle ulepsza odpowiednie narzędzia ochrony, np. sygnatury, szablony niepożądanego zachowania oraz listy adresów szkodliwych stron, i implementuje je w każdym produkcie Kaspersky Lab. W wyniku tego użytkownicy zawsze posiadają aktualną ochronę przed nowymi zagrożeniami otrzymywaną bezpośrednio „z chmury” oraz niezależnie od terminarza regularnych uaktualnień antywirusowych.

Zalety ochrony w chmurze są oczywiste:

- szybka reakcja na zagrożenia, nawet na poziomie kilku sekund;
- chmura posiada wirtualne nielimitowane zasoby i z tego powodu może równocześnie przetwarzać dane, pozwalając na szybką analizę nowych zagrożeń;
- dzięki ochronie przy pomocy chmury obciążenie komputerów użytkowników jest minimalne, ponieważ wymiana informacji odbywa się w tle.

Chmura wymaga klienta

- Powstaje pytanie, czy można korzystać jedynie z produktu opartego na technologii chmury. Teoretycznie byłoby to rozwiązanie idealne – użytkownik mógłby się cieszyć natychmiastową reakcją na nowe zagrożenia bez dodatkowego obciążenia zasobów komputera. Niestety, wbrew pozorom nie jest to najlepszy pomysł.
- Po pierwsze, im więcej informacji jest wysyłanych do chmury, tym bardziej efektywnie może ona chronić. W zawiązku z tym, kluczową rolę pełnią tu źródła informacji o szkodliwym oprogramowaniu i wszystkim, co się z nim łączy. Źródłami tymi są specjalne komputery-pułapki tworzone przez specjalistów z Kaspersky Lab, informacje wymieniane miedzy firmami antywirusowymi, a także dane zebrane z komputerów użytkowników za pomocą systemu Kaspersky Security Network. Oczywiście, aby otrzymywać takie informacje, muszą istnieć specjalne metody ich gromadzenia i analizowania, dlatego sam produkt antywirusowy musi być zainstalowany lokalnie na komputerach użytkowników.
- Po drugie, do działania ochrony przy pomocy chmury konieczne jest ciągłe połączenie komputera z Internetem. Wciąż istnieje jednak duże ryzyko infekcji komputera również poprzez sieć lokalną lub przenośne urządzenie USB. Według danych Kaspersky Lab, w przypadku, gdy istnieje połączenie z Siecią, technologia oparta na chmurze przechwytuje około 30% wszystkich zagrożeń. Pozostałe są przetwarzane lokalnie na komputerach użytkowników przez zainstalowany produkt antywirusowy.

Posiadanie rozwiązania antywirusowego na swoim komputerze jest bardzo istotne, ponieważ:

- Chroni ono sprzęt, gdy nie ma połączenia z Internetem. Komputery pozostające offline mogą zostać zainfekowane z takich źródeł jak sieć lokalna lub pendrive;
- Jeśli komputer został zainfekowany mimo działania ochrony z użyciem chmury, często nie można go wyleczyć za pośrednictwem Internetu. Na przykład, po uzyskaniu kontroli nad komputerem przez szkodliwy program może on blokować wszelki ruch sieciowy z wyjątkiem własnej komunikacji z cyberprzestępcą.

Hybryda – rozwiązanie problemu

Rozwiązanie bezpieczeństwa IT, które nie wykorzystuje technologii opartej na chmurze, wydaje się być przestarzałe na tle dzisiejszego krajobrazu zagrożeń. Z drugiej strony, dostawcy oprogramowania antywirusowego nie mogą przenieść do chmury wszystkich swoich technologii ochrony, ponieważ znaczna liczba zagrożeń rozprzestrzenia się niezależnie od Internetu.

Dlatego prawdziwie efektywne rozwiązanie, które będzie skuteczne w każdej sytuacji, musi być hybrydą, czyli korzystać z chmury oraz modułów zainstalowanych lokalnie na komputerze użytkownika. Chmura odbiera na bieżąco wszystkie dane o najnowszych zagrożeniach i niebezpiecznych obiektach, a następnie wysyła je do scentralizowanych serwerów w czasie rzeczywistym natychmiast po tym, jak pojawią się na

dowolnym komputerze. Na tej podstawie generowane są metody ochrony (np. szczepionki) lub dane o niebezpiecznych obiektach, które są wysyłane za pośrednictwem KSN do milionów komputerów.

Proces taki eliminuje konieczność wykonywania na każdym komputerze analizy pochłaniającej zasoby, minimalizuje liczbę fałszywych alarmów i chroni przed najnowszymi zagrożeniami jeszcze przed opublikowaniem odpowiednich sygnatur.

Gdy komputer pozostaje offline i nie ma połączenia z chmurą, jest wciąż chroniony przez w pełni funkcjonalne rozwiązanie bezpieczeństwa zawierające technologie proaktywne, takie jak kontrola aktywności niechcianych programów, analiza heurystyczna klasyfikacja zagrożeń itd., które także wykorzystują informacje zbierane w obrębie KSN.

W zrozumieniu hybrydowego podejścia do ochrony zastosowanego przez Kaspersky Lab może pomóc krótki film dostępny w oficjalnym kanale Kaspersky Lab Polska na YouTube: http://youtu.be/thhoh3OMM2o (aby włączyć polskie napisy, wystarczy kliknąć ikonę „CC” w prawym dolnym rogu okna z filmem na YouTube).