**Tylko 21% firm na świecie wybiera najskuteczniejszą ochronę**

**Technologie chmury stanowią istotny element współczesnych rozwiązań bezpieczeństwa, ale nie są w stanie zapewnić ochrony komputerom bez wsparcia lokalnych narzędzi bezpieczeństwa.**

Dlatego najlepszym wyjściem jest stosowanie rozwiązań hybrydowych, które zawierają lokalne technologie antywirusowe, a jednocześnie współpracują z usługą opartą na chmurze. Jednak tego rodzaju rozwiązania są wybierane przez zaledwie 21% firm – tak wynika z badania przeprowadzonego przez Kaspersky Lab we współpracy z B2B International pod koniec 2012 roku.

Obecnie ilość szkodliwego oprogramowania rośnie lawinowo: co minutę pojawia się około 140 nowych zagrożeń. Stosowanie wyłącznie tradycyjnej metody opartej na sygnaturach do walki z nimi już nie wystarczy – nowe zagrożenia pojawiają się zbyt szybko. Z tego powodu producenci rozwiązań bezpieczeństwa pracują nad połączeniem technologii proaktywnych z technologiami chmury. Te pierwsze pomagają wykrywać nieznane zagrożenia, te drugie zapewniają możliwie najszybszą ochronę przed nowymi szkodnikami. Istnieją wprawdzie rozwiązania bezpieczeństwa oparte jedynie na technologiach chmury, nie są one jednak w stanie zapewnić niezawodnej ochrony przed złożonymi zagrożeniami. Ponadto, takie rozwiązania nie mogą działać wydajnie bez stabilnego połączenia internetowego.

Przyszłością są rozwiązania hybrydowe, które łączą technologie lokalne, proaktywne i reaktywne z usługami opartymi na chmurze. Takie rozwiązania są najpopularniejsze w dużych przedsiębiorstwach - 29% ankietowanych przedsiębiorstw tej wielkości wykorzystuje ochronę hybrydową. Niestety, rozwiązania te nie są popularne wśród pozostałych firm. Według badania B2B International przeprowadzonego w listopadzie 2012 roku, wykorzystuje je tylko 21% badanych firm. Większość respondentów (51%) preferuje rozwiązania lokalne bez wsparcia chmury, a kolejne 20% wybiera narzędzia bezpieczeństwa oparte wyłącznie na chmurze.

**Rozwiązanie hybrydowe firmy Kaspersky Lab**

Eksperci z Kaspersky Lab są przekonani, że tylko rozwiązania hybrydowe mogą zapewnić skuteczną ochronę przed nowoczesnymi cyberzagrożeniami. Z tego powodu Kaspersky Lab jako jeden z pierwszych w branży wyposażył swoje produkty dla użytkowników indywidualnych i korporacyjnych w technologię opartą na chmurze - Kaspersky Security Network. Za zgodą użytkownika technologia ta zbiera anonimowe dane dotyczące prób infekcji z komputerów, na których działają rozwiązania bezpieczeństwa Kaspersky Lab, i wysyła te informacje specjalistom w celu przeprowadzenia szczegółowej analizy incydentów. Po zastosowaniu odpowiednich środków zapewnienia użytkownikom ochrony, takich jak dodanie szkodliwej strony internetowej do czarnej listy, stworzenie sygnatury itd., aktualizacje dla narzędzi bezpieczeństwa oraz antywirusowych baz danych są wysyłane do wszystkich produktów firmy Kaspersky Lab za pośrednictwem chmury Kaspersky Security Network.

Z chmurą Kaspersky Security Network współpracuje także nowa platforma dla użytkowników korporacyjnych - Kaspersky Endpoint Security for Business. Komponenty tej platformy zbierają dane o nowym szkodliwym oprogramowaniu, niebezpiecznych stronach internetowych i epidemiach spamu, tworzą białe i czarne listy aplikacji, dodają luki do baz itd. Wszystkie niezbędne aktualizacje są pobierane na komputery użytkowników kilka sekund po sprawdzeniu ich przez ekspertów z Kaspersky Lab. Efektem tych działań jest rozwiązanie bezpieczeństwa korporacyjnego, które zapewnia skuteczną i – co istotne – natychmiastową ochronę przed współczesnymi cyberzagrożeniami.

Informację można wykorzystać dowolnie z zastrzeżeniem podania firmy Kaspersky Lab jako źródła.