KASPERSKY lab

Kaspersky Security Network

Kaspersky Security Network (KSN) jest złożoną, rozległą infrastrukturą, którą tworzą miliony użytkowników z całego świata. KSN służy do przetwarzania zdepersonalizowanych strumieni danych powiązanych z bezpieczeństwem internetowym. Inteligentne narzędzie chroni każdego partnera i klienta firmy Kaspersky Lab, który posiada połączenie z internetem, zapewniając najszybszy czas reakcji na pojawiające się zagrożenia oraz gwarantując najwyższy poziom ochrony. Usługę KSN posiada większość produktów firmy Kaspersky Lab przeznaczonych dla klientów indywidualnych oraz biznesowych.

W przypadku pojawienia się nowego, nieznanego szkodliwego oprogramowania, KSN gwarantuje natychmiastową reakcję oraz bezprecedensowy poziom wykrywania zapewniający ochronę najwyższej jakości. Kaspersky Security Network został stworzony, aby wzmocnić poziom ochrony użytkowników na całym świecie. Usługa KSN nie tylko pozwala na wykrywanie i blokowanie znanych zagrożeń, lecz także pomaga w zlokalizowaniu i umieszczeniu źródeł ataku na czarnej liście, dostarczając tym samym informacje na temat reputacji stron i aplikacji. Podsumowując, Kaspersky Security Network jest jednym z najważniejszych komponentów zaawansowanej ochrony firmy Kaspersky Lab.

Szybka i skuteczna ochrona przed cyberatakami

Szkodliwe programy, takie jak wirusy, robaki i trojany, stały się głównymi zagrożeniami dla komputerów oraz przechowywanych na nich informacji. Obszar i zakres działania szkodliwego oprogramowania stale się powiększa, stanowiąc ciągle rosnące wyzwanie dla bezpieczeństwa komputerów. Według wewnętrznych danych Kaspersky Lab, codziennie pojawia się ponad 325 000 nowych próbek szkodliwego oprogramowania. Szkodniki wykorzystują nowe metody wnikania do systemów, ukrywając swoje działania i unikając wykrycia przez oprogramowanie antywirusowe. Obecnie żadne konwencjonalne metody wykrywania szkodliwych programów nie zapewniają kompletnej ochrony, jeśli są używane jako autonomiczne narzędzia.

Dzisiejszy cyberświat wymaga zastosowania nowego, zintegrowanego sposobu ochrony komputerów. Sposób ten powinien łączyć w sobie korzyści i minimalizować braki tradycyjnych metod walki ze szkodliwymi programami, a także obejmować możliwości globalnego monitorowania i automatycznego aktualizowania bazy danych nowych, rzeczywistych zagrożeń. Takie właśnie podejście zostało zastosowane w Kaspersky Security Network.

Podstawowe zasady działania Kaspersky Security Network

Kaspersky Security Network gromadzi informacje o próbach zainfekowania komputerów od użytkowników z całego świata, którzy dobrowolnie zgodzi się na udział w tworzeniu bezpieczniejszego środowiska internetowego. Wszystkie napływające informacje zostają

zdepersonalizowane. Firma Kaspersky Lab porządkuje otrzymane informacje przydzielając je do poszczególnych kategorii w zależności od rodzaju danych w taki sposób, aby nikt nie był w stanie dojść do tego, skąd one pochodzą. Kaspersky Lab zabezpiecza dane zgromadzone przez KSN zgodnie z obowiązującymi przepisami prawnymi oraz wszelkimi wymogami ustawowymi.

Na mechanizm działania Kaspersky Security Network składa się kilka kluczowych procesów takich jak ciągłe, geograficznie rozproszone, globalne monitorowanie rzeczywistych zagrożeń dla komputerów użytkowników, analiza zebranych informacji oraz szybkie dostarczenie niezbędnej wiedzy oraz skutecznych środków do punktów końcowych.

Informacje zebrane podczas próby infekcji komputera zostają poddane analizie przy użyciu silnej wewnętrznej technologii i zasobów eksperckich firmy. Zapewnia to niezwykle szybkie i dokładne wykrywanie nowych szkodliwych programów wśród legalnych aplikacji. W ocenie bezpieczeństwa programu kluczową rolę odgrywa kilka czynników: dostępność podpisu cyfrowego oraz weryfikacja źródła i integralności programu. Program, który zostanie uznany za bezpieczny, zostaje dodany do listy zaufanych aplikacji.

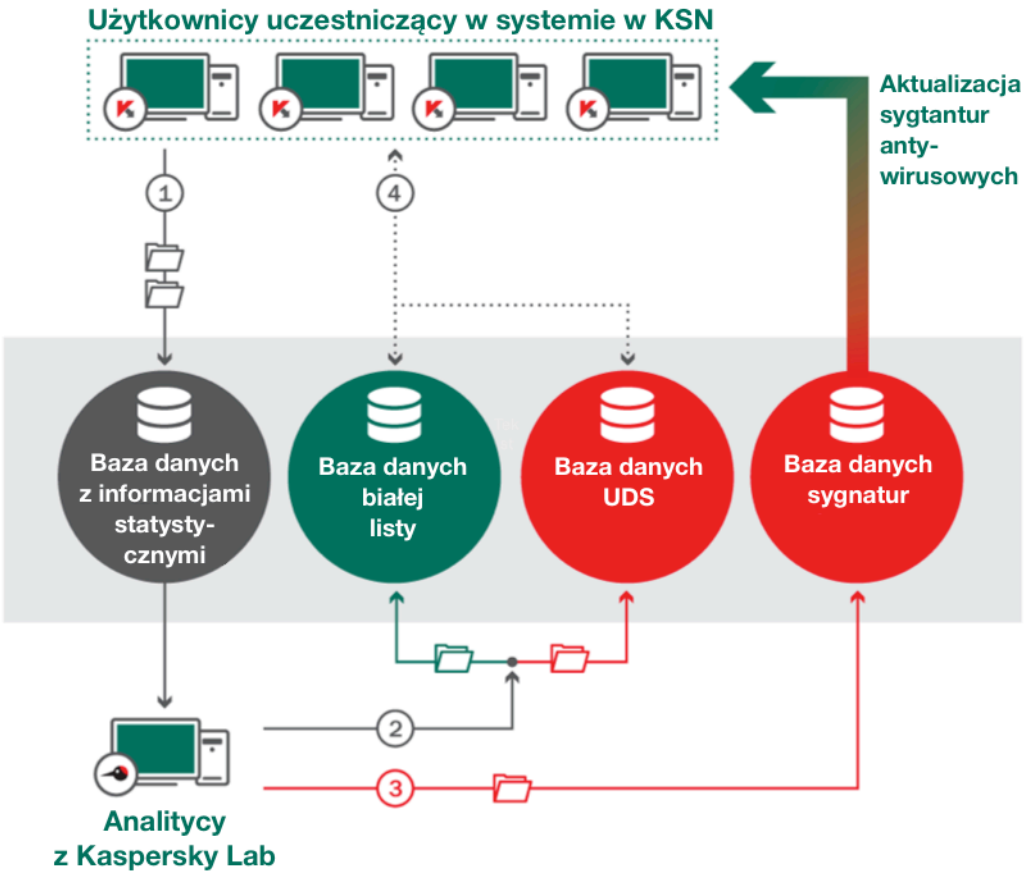
Program jest uznawany za szkodliwy po zakończeniu wykonywania wszystkich niezbędnych analiz. Jak tylko program zostanie zdefiniowany jako szkodliwy, informacja o nim natychmiast pojawia się w systemie szybkiego reagowania (Urgent Detecion System) Kaspersky Lab oraz automatycznie staje się dostępna dla użytkowników Kaspersky Security Network. Dlatego użytkownicy punktów końcowych są chronieni nawet zanim sygnatura tego szkodliwego programu zostanie utworzona i zaktualizowana na ich komputerach. W ten sposób klienci Kaspersky Lab otrzymują natychmiastową informację o nowych i nieznanych zagrożeniach w kilka minut po rozpoczęciu cyberataku, dzięki czemu szkodliwa aktywność może zostać zablokowana. W przypadku tradycyjnej aktualizacji baz danych sygnatur ten sam proces może twać nawet kilka godzin.

Każdy program uruchamiany przez użytkownika zostaje sprawdzony w oparciu o białą listę i listę mechanizmu Urgent Detection System. Na podstawie dalszych informacji program może uzyskać prawa dostępu do zasobów komputera lub zostać zablokowany. Technologia Kaspersky Security Network odgrywa ważną rolę w uzupełnianiu tych list, zapewniając skuteczną kontrolę nad uruchamianymi programami.

Istnieje jeszcze jedna technologia pozwalająca użytkownikom na podejmowanie decyzji odnośnie korzystania z danego programu, króra wykorzystuje zasoby KSN. Jest to technologia reputacji zwana „mądrością tłumu” (z ang. Wisdom of the Crowd, w skrócie WoC), która dostarcza informacje na temat popularności i reputacji danego programu wśród innych użytkowników KSN.

Kaspersky Security Network pomaga w wykrywaniu szkodliwego oprogramowania wspomagając metody oparte na sygnaturach zagrożeń, metody heurystyczne oraz korzystając z białych list i technologii kontroli aplikacji.

Jedną z wyróżniających się funkcji KSN jest wspomagana przez chmurę technologia antyspamowa. Wykorzystuje ona informacje z chmury do wykrywania i blokowania niechcianych wiadomości i nie wymaga lokalnego filtra antyspamowego.



Powyższy schemat przedstawia interakcję użytkowników produktów Kaspersky Lab z systemem KSN. Interakcja ta obejmuje 3 różne etapy:

1. Statystyki na temat wykrytych zagrożeń oraz podejrzanych działań są przetwarzane w obrębie infrastruktury chmury Kaspersky Lab przy użyciu danych pochodzących od wszystkich uczestników KSN. Jeżeli nasze bazy danych nie zawierają informacji odpowiadających danej sekwencji wskaźników (przykładowo, jeżeli wykrycie zagrożenia zostało dokonane za pomocą technologii heurystycznych), eksperci kontynuują dalszą analizę informacji.
2. Jeżeli okaże się, że sprawdzane kody lub adresy URL są szkodliwe, zostają natychmiast dodane do bazy danych mechanizmu Urgent Detection System i tym samym informacja na ich temat staje się dostępna dla wszystkich użytkowników produktów firmy Kaspersky Lab (nie tylko subskrybentów Kaspersky Security Network) w przeciągu kilku minut od momentu ich pierwszego wykrycia.
   W analogiczny sposób wszystkie legalne i nieszkodliwe pliki są dodawane do białej listy.
3. Eksperci kończą analizę podejrzanego kodu, określając stopień zagrożenia i dodając opisy do bazy danych sygnatur, która jest regularnie aktualizowana na wszystkich komputerach korzystających z produktów Kaspersky Lab.
4. Jeżeli użytkownicy produktów Kaspersky Lab napotkają znane zagrożenie, rozwiązanie bezpieczeństwa kieruje zapytanie do KSN po czym otrzymuje

natychmiastową ocenę zagrożenia - bez potrzeby przeprowadzania analizy zwiększającej obciążenie systemu.

Dostępność

Usługa Kaspersky Security Network jest dostępna w większości produktów firmy Kaspersky Lab:

Dla użytkowników domowych

- Kaspersky Internet Security
- Kaspersky Internet Security – multi-device
- Kaspersky Total Security – multi-device
- Kaspersky Anti-Virus
- Kaspersky Internet Security for Mac

Dla biznesu

- Kaspersky Endpoint Security for Business
- Kaspersky Small Office Security
- Kaspersky Security for Virtualization
- Kaspersky Security for Linux Mail servers
- Kaspersky Security for Microsoft Exchange
- Kaspersky Security for SharePoint

Zasady funkcjonowania i interakcji Kaspersky Security Network z poszczególnymi produktami firmy Kaspersky Lab są zbliżone, jednak można wyróżnić odrębne funkcje w przypadku rozwiązań dla użytkowników domowych i biznesowych.

Ochrona w chmurze dla klientów indywidualnych

Poza ogólnymi korzyściami płynącymi z korzystania z ochrony wspomaganej przez chmurę, produkty dla klientów indywidualnych oferują otrzymywanie ogólnych statystyk dotyczących Kaspersky Security Network, tj. liczby chronionych użytkowników, zablokowanych szkodliwych obiektów i przetworzonych legalnych danych.

Kolejna funkcją dostępną w produktach Kaspersky Lab dla klientów indywidualnych jest możliwość sprawdzenia reputacji dowolnego pliku wykonywalnego w oparciu o dane z Kaspersky Security Network. Takie zapytanie skutkuje otrzymaniem danych na temat oceny poziomu bezpieczeństwa danego pliku, a także wyświetla informacje o dacie pierwszego pojawienia się pliku, jego popularności według kraju i wiele innych statystyk. Funkcja ta umożliwia użytkownikom sprawdzenie podstawowych informacji o nieznanych programach przed ich uruchomieniem. Te same informacje są również wysyłane automatycznie, gdy użytkownik próbuje uruchomić dany plik.

Jeszcze skuteczniejsza ochrona w chmurze dla użytkowników biznesowych

Kaspersky Security Network posiada szereg funkcji stworzonych z myślą o produktach korporacyjnych. Przede wszystkim mowa tu o technologii ochrony wspomaganej przez chmurę, która jest używana do umieszczania aplikacji na białej liście przy wykorzystaniu danych z Kaspersky Security Network. Znane legalne pliki są automatycznie dzielone na kategorie, takie jak gry, oprogramowanie komercyjne itd. Korzystając z tych kategorii, administrator systemu może szybko zainstalować i zastosować pewne reguły dla określonych typów oprogramowania, zgodnie z profilem bezpieczeństwa. Dane dla białych list aplikacji są również dostarczane przez ponad 300 czołowych twórców oprogramowania.

Konsola administracyjna Kaspersky Security Center umożliwia firmom szczegółową kontrolę wykorzystania Kaspersky Security Network do ochrony korporacyjnych punktów końcowych. Administrator może zdecydować, czy ochrona wspierana chmurą ma być włączona w określonych modułach Kaspersky Endpoint Security for Business. Istnieje również możliwość wyłączenia funkcji wysyłania danych do Kaspersky Security Network. Aby zmniejszyć przepustowość, do pobierania danych z KSN można wykorzystać wewnętrzny serwer proxy.

Zalety Kaspersky Security Network

Obecnie technologia Kaspersky Security Network jest używana na milionach komputerów na świecie, przedstawiając globalny i szczegółowy obraz ewolucji i rozprzestrzeniania się szkodliwych programów, pochodzenia nowych zagrożeń oraz liczby prób infekcji pojawiających się w określonym czasie. Globalny monitoring aktywności szkodliwego oprogramowania z różnych miejsc na ziemi zapewnia skuteczną reakcję na nowe zagrożenia, bez względu na lokalizację źródła i celu ataku.

Kaspersky Security Network pomaga w budowaniu skutecznej, proaktywnej ochrony. Usługa KSN umożliwia identyfikację i blokowanie nowych zagrożeń zanim zdążą się one rozprzestrzenić i dokonać poważnych szkód w sieciach klientów. System ochrony proaktywnej jest niezbędny dla stabilnego i niezakłóconego działania sprzętu IT oraz przeprowadzanych przy jego użyciu procesów biznesowych.