**5 powodów, dla których firewall jest nadal podstawą systemów cyberbezpieczeństwa**

**Analitycy Gartnera przewidują, że wartość rynku zapór sieciowych (ang. firewall) wzrośnie z 12,5 mld USD w 2018 r. do 16,2 mld USD w 2023 r. Oznacza to, że będzie to jeden z największych rynków produktów związanych z cyberbezpieczeństwem. Specjaliści Cisco podkreślają, że zapora sieciowa jest niezbędnym elementem systemu bezpieczeństwa sieci korporacyjnych, a nowa generacja firewalli pozwala biznesowi zapewnić wyższy poziom ochrony.**

Warszawa, 21 sierpnia 2019 r. – Zapory sieciowe nowej generacji to obecnie wszechstronne rozwiązania, które pozwalają zapewnić bezpieczeństwo na wielu poziomach. Są wyposażone w zintegrowane źródła danych o najnowszych zagrożeniach, zapobiegają włamaniom, gwarantują zaawansowaną ochronę przed złośliwym oprogramowaniem, filtrowanie adresów URL i posiadają funkcje weryfikacji tożsamości użytkownika. Przykładem firewalli nowej generacji są urządzenia i oprogramowanie z serii Cisco Firepower. Dzięki bogatej telemetrii sieciowej, dają one najpełniejszy wgląd w informacje o sieci i pozwalają wykrywać nawet subtelne zagrożenia.

**Biznes nie może tracić czasu na obsługę systemów cyberbezpieczeństwa**

Jak wynika z raportu Cisco „CISO Benchmark Study 2019”, priorytetem specjalistów ds. bezpieczeństwa jest konsolidacja informacji pochodzących od rozwiązań różnych dostawców.

„Firmy nie powinny tracić czasu na obsługę systemów bezpieczeństwa. Jeżeli w danej organizacji funkcjonuje kilka niezależnych produktów, zwykle oznacza to, że musi je obsługiwać kilku specjalistów, co w realiach, gdy biznes musi zmagać się z niedoborem talentów IT stanowi duży problem. Ponadto, jeśli produkty pochodzą od różnych dostawców, nie mogą one komunikować się między sobą ani automatycznie przekazywać sobie informacji o potencjalnych zagrożeniach” – mówi Mateusz Flak, menedżer ds. sprzedaży rozwiązań cyberbezpieczeństwa w Cisco Polska. „Zapory sieciowe nowej generacji to odpowiedź na te wyzwania. Stanowią zintegrowany system bezpieczeństwa, dzięki czemu specjaliści na stanowiskach CISO (ang. Chief Information Security Officer) nie muszą żonglować wieloma różnymi narzędziami”.

**Specjaliści Cisco wskazują 5 powodów, dla których firewall jest nadal podstawą systemów cyberbezpieczeństwa:**

1. **Gotowość na realny cyberatak** – ochrona zapobiegawcza to za mało. Zapora sieciowa powinna stanowić źródło najnowszych informacji o zagrożeniach i posiadać funkcje dodatkowe, takie jak wykrywanie adresów URL czy zaawansowane wykrywanie złośliwego oprogramowania, na wypadek, gdyby pokonało ono pierwszą linię obrony.
2. **Kompleksowy wgląd w sieć** – zapora sieciowa nowej generacji prezentuje całościowy obraz wszystkich działań, niezależnie od tego, czy dotyczą one użytkowników, hostów, sieci, aktywnych aplikacji, stron internetowych czy platform do przesyłania plików.
3. **Elastyczne opcje zarządzania i wdrażania** – konfigurowalna zapora sieciowa nowej generacji może być zainstalowana w ramach infrastruktury w siedzibie organizacji lub w chmurze. Dodatkowo obsługuje szeroki zakres prędkości przepustowości, a także pozwala na scentralizowane zarządzanie wszystkimi urządzeniami lub poszczególnymi rozwiązaniami.
4. **Krótki czas wykrywania zagrożeń** – średni czas wykrywania zagrożeń wynosi obecnie od 100 do 200 dni. To zdecydowanie za długo. Zapora nowej generacji powinna wykrywać potencjalne zagrożenia w ciągu kilku sekund. Dodatkowo rozwiązanie samo nadaje priorytety wygenerowanym alertom, aby można było podjąć szybkie i precyzyjne działania.
5. **Element zintegrowanej architektury bezpieczeństwa** – nowoczesna zapora sieciowa powinna komunikować się i współdziałać z resztą architektury bezpieczeństwa, zapewniając możliwość integracji z innymi narzędziami tego samego dostawcy. Zapory sieciowe nowej generacji dają możliwość automatycznego udostępniania informacji o zagrożeniach, danych o zdarzeniach i ich kontekście.

.:|:.:|:.

**O Cisco:**

Cisco (NASDAQ: CSCO) to światowy lider technologiczny zapewniający działanie Internetu od 1984 r. Pracownicy, partnerzy i produkty Cisco pomagają społeczeństwom łączyć się w bezpieczny sposób i już dziś korzystać z cyfrowych możliwości jutra. Dowiedz się więcej na www.newsroom.cisco.com. Cisco i logo Cisco to zastrzeżone znaki towarowe należące do Cisco i/lub jego podmiotów zależnych w U.S. i innych krajach. Pełna lista znaków towarowych Cisco dostępna jest pod adresem: www.cisco.com/go/trademarks. Znaki towarowe firm trzecich są ich własnością. Użycie słowa partner nie oznacza stosunku partnerstwa pomiędzy Cisco i inną firmą.