veracomp
inspirujemy IT

case study

Extreme Networks oraz Fortinet na straży danych tour operatora Grecos Holiday

Biuro Podróży Grecos Holiday

W czasach rozwijającej się w błyskawicznym tempie digitalizacji dbanie o bezpieczeństwo w sieci stało się jednym z kluczowych elementów ochrony w każdej firmie.
Tą myślą kierował się również tour operator Grecos Holiday – specjalizujący się w organizowaniu wakacji w Grecji – który podjął decyzję o rozbudowaniu infrastruktury sieciowej i wdrożeniu kompleksowego systemu bezpieczeństwa IT.

- Większość usług w naszej firmie świadczona jest przez Internet, w tym kluczowy dla funkcjonowania biura internetowy system rezerwacji. Codziennie przetwarzamy duże ilości istotnych danych, których ochrona jest dla nas absolutnym priorytetem – mówi Filip Kielban, CIO w firmie Grecos. – *Jeśli dodać do tego obowiązki wynikające z przepisów ustawowych związane z koniecznością odpowiedniego zabezpieczenia przetwarzanych danych osobowych, to mamy jasność, że warto spojrzeć na bezpieczeństwo jako na jeden z kluczowych obszarów wymagających całościowego i kompleksowego zarządzania w przedsiębiorstwie.*

Rozstrzygający wpływ na decyzję o wzmocnieniu bezpieczeństwa sieciowego miała aranżacja drugiego, nowego oddziału firmy. Potrzebna była infrastruktura, która nie tylko ochroni systemy przed zaawansowanymi wirusami i ukierunkowanymi atakami, ale też zapewni pełną kontrolę dostępu dla określonych grup użytkowników.
O specjalistyczne wsparcie w zakresie integracji rozwiązań IT tour operator zwrócił się do poznańskiej firmy VOL, która działa na rynku od 18 lat i cieszy się statusem Extreme Networks Platinum Partner oraz Gold Partner firmy Fortinet.

Grecos Holiday oczekiwał przede wszystkim wysokowydajnych, zintegrowanych rozwiązań, których wdrożenie zakończy się w krótkim czasie. Przeprowadzony audyt umożliwił wybór urządzeń spełniających wszystkie oczekiwania klienta.

Firma zaufała rozwiązaniom oferowanym przez Extreme Networks i Fortinet dostarczonych przez autoryzowanego dystrybutora, Veracomp SA.

INFRASTRUKTURA BEZPIECZEŃSTWA. DYNAMICZNE PRZEPISYWANIE POLITYK

Właściwa administracja bezpieczeństwem firmowych danych to rozbudowany proces zachodzący na każdym poziomie funkcjonowania przedsiębiorstwa. Aby zwiększyć bezpieczeństwo firmy w Internecie, należy w pierwszej kolejności zadbać o ustanowienie odpowiednich standardów i kształtowanie pożądanych zachowań wszystkich użytkowników sieci.

- Wzrost ukierunkowanych ataków hakerskich to problem dotyczący coraz większej liczby przedsiębiorstw. Zapobieganie zagrożeniom związanym z utratą biznesowych danych wymaga nieustannego rozbudowywania systemowych zabezpieczeń i stosowania wielu kompatybilnych rozwiązań jednocześnie – tłumaczy Filip Kielban CIO z Grecos Holiday.

Do standardów należy już zabezpieczanie stacji roboczych (ochrona antywirusowa, antyspamowa, przed oprogramowaniem szpiegującym), firewall, bramka do tworzenia kanałów VPN (w tym SSL VPN), system wykrywania i prewencji włamań IPS, kontrola treści ładowanych z Internetu, ochrona poczty elektronicznej, system AAA (Administracja, Autoryzacja i Uwierzytelnienie) czy zabezpieczanie poufnych danych przed wyciekiem (szyfracja + DLP). Rozwiązania te mogą występować jako osobne programy lub w formie jednego, wielofunkcyjnego systemu UTM.

Extreme networks

FORTINET

veracomp
inspirujemy IT

case study

Poza odpowiednim doborem rozwiązań hardware'owych – przełączników, firewalli oraz punktów dostępowych – zespół pracujący nad wdrożeniem w Grecos musiał zaprojektować także kompleksową infrastrukturę bezpieczeństwa firmowego składającą się z wielopoziomowych polityk bezpieczeństwa. Działania te obejmowały m.in. zdefiniowanie sieci VLAN wraz z zasadami określającymi ruch w sieci; zaprojektowanie polityki dotyczącej korzystania z Internetu wraz z wdrożeniem filtrów AV, IPS, WEB; wprowadzenie kilku poziomów dostępności sieci Wi-Fi (dla pracowników, gości oraz urządzeń mobilnych); budowę tuneli IPSec (dla dostawców firmy) oraz wdrożenie systemu loadbalancing.

ZASTOSOWANE ROZWIĄZANIA

W nowo tworzonej infrastrukturze projektanci zastosowali wysokowydajne przełączniki marki Extreme Networks.

- Zastosowane rozwiązanie to gigabitowe przełączniki brzegowe. Poza inteligentną obsługą ruchu sieciowego posiadają funkcjonalność PoE w celu zasilania podpiętych punktów dostępowych. Jak przystało na przedstawiciela technologii ExtremeSwitching™ umożliwiają pełną kontrolę nad zasobami sieci – tłumaczy Maciej Stawiarski, Product Manager z firmy Veracomp SA. – *Dzięki możliwości dynamicznego nadawania polityk bezpieczeństwa administrator IT może precyzyjnie przepisywać dostęp do sieci i nadawać uprawnienia określonym grupom użytkowników w zgodzie z przyjętą polityką cyfrowego bezpieczeństwa. Zdefiniowane role lub profile reprezentują firmowe grupy operacyjne, takie jak BOK, IT czy HelpDesk.*

Najważniejszym elementem integrującym system zarządzania bezpieczeństwem jest urządzenie typu UTM (Unified Threat Management). Pozwala ono na integrację

z wieloma elementami infrastruktury celem budowy ekosystemu bezpieczeństwa. Dzięki temu rozwiązanie jest nie tylko wszechstronne, ale też proste w obsłudze. UTM ułatwia prowadzenie jednolitej polityki bezpieczeństwa we wszystkich obszarach komunikacji w firmie.

Do zabezpieczenia opisywanej inwestycji wybrano urządzenie UTM FORTIGATE-140D marki Fortinet, nazywane firewallem nowej generacji (NGFW), które zapewnia bezpieczeństwo sieci w trybie end-to-end i chroni przed najbardziej zaawansowanymi zagrożeniami i ukierunkowanymi atakami.

KORZYŚCI Z WDROŻENIA

Wdrożenie systemów Extreme Networks i Fortinet wprowadziło szereg korzystnych zmian wpływających na wzrost poziomu bezpieczeństwa firmy w Internecie. Grecos Holiday może teraz zarówno monitorować, jak i kontrolować wszystkie urządzenia, użytkowników i działania prowadzone w sieci – a to wszystko z poziomu jednej aplikacji, dzięki czemu administrowanie bezpieczeństwem firmy jest sprawne i proste. (pracownikom i gościom) oraz urządzeniom (komputerom, laptopom, tabletom, smartfonom, telefonom IP, drukarkom itp.).

Extreme networks

FORTINET

veracomp
inspirujemy IT

case study

- Dzięki zintegrowanym rozwiązaniom Fortinet i Extreme Networks zabezpieczyliśmy wszystkie systemy informatyczne działające w oparciu o nasze zasoby biznesowe. Zapewniliśmy ochronę przed atakami z zewnątrz i kontrolę dostępu użytkowników. Wdrożyliśmy także odpowiednią priorytetyzację ruchu wynikającą z przyjętej polityki bezpieczeństwa. Mogę spokojnie teraz powiedzieć, że w pełni kontrolujemy bezpieczeństwo sieciowe w naszej organizacji – podsumowuje Filip Kielban, CIO w Grecos Holiday.

PODSUMOWANIE

Zespół projektujący i wdrażający system zarządzania bezpieczeństwem sieciowym w firmie Grecos Holiday kierował się przekonaniem, że rozwiązania systemowe marki Extreme Networks oraz Fortinet nie tylko w pełni zabezpieczą środowisko sieciowe w firmie, ale będą też stanowić przyjazną i intuicyjną infrastrukturę, która przyczyni się do kształtowania bezpiecznych praktyk wśród wszystkich użytkowników firmowej sieci – pracowników, partnerów i kontrahentów.

Extreme networks

FORTINET