veracomp
inspirujemy IT

case study

FORTINET
FortiGate, FortiAP

Szpital Specjalistyczny Św. Zofii
w Warszawie

OPIS SYTUACJI WYJŚCIOWEJ

Szpital Specjalistyczny św. Zofii w Warszawie jest jednym z najstarszych ośrodków położniczoginekologicznych w Warszawie i placówką medyczną, w która w ostatnich latach notuje największą liczbę urodzeń w stolicy. Jest pierwszym publicznym szpitalem położniczym w Warszawie, którego początek działalności sięga 1912 roku. Placówka rozwija się bardzo dynamicznie, co ma swoje potwierdzenie w skali popularności wśród pacjentek. Szpital otrzymał również wiele nagród i wyróżnień, w tym wyróżnienie XII Edycji Polskiej Nagrody Jakości w 2006 roku oraz czwarte miejsce w organizowanym przez dziennik „Rzeczpospolita" Rankingu Szpitali i pierwsze wśród szpitali położniczo-ginekologicznych w Polsce. Placówka zdobyła również tytuł „Szpitala Przyjaznego Dziecku".

W związku z koniecznością dbania o ochronę danych pacjentów i historii ich choroby, szpital zdecydował się na zakup zintegrowanego urządzenia UTM, zapewniającego bezpieczeństwo lokalnej sieci na wysokim poziomie. Drugim powodem było stworzenie możliwości szybkiego dostępu do internetu personelowi medycznemu szpitala, bez ryzyka ataków z zewnątrz i kradzieży poufnych danych. W związku z intensywnym rozwojem placówki potrzebna była zintegrowana struktura ochrony, która byłaby wydajna, skuteczna i jednocześnie odpowiednio dostosowana do potrzeb dużego przedsiębiorstwa. Szpital zatrudnia 375 pracowników, z których zdecydowana większość to personel medyczny. Dokumentacja lekarska, w którą - z racji konieczności - wgląd ma wielu pracowników szpitala, prowadzona jest elektronicznie.

Dodatkowo personelowi niezbędny jest stały dostęp do sieci, umożliwiający korzystanie z zasobów internetowych oraz komunikacja za pośrednictwem lokalnej sieci na terenie szpitala. Sprostanie tym potrzebom wymagało wyposażenia placówki w strukturę bezpieczeństwa o wysokim poziomie ochrony sieci, która gwarantowałaby sprawne działanie bez opóźnień i pozwalała na łatwe zarządzanie systemem.

WYZWANIE

- Zwiększenie ochrony sieci lokalnej oraz umożliwienie personelowi i pacjentom korzystania z zasobów internetowych i komunikacji za pomocą sieci

CELE

- Wzmocnienie bezpieczeństwa lokalnej sieci.
- Zapewnienie poufności danych.
- Zabezpieczenie przed atakami i wirusami.
- Zintegrowanie systemu uwierzytelniania oraz zarządzania zabezpieczeniami sieci.

ROZWIĄZANIE

- FortiGate
- FortiAP

BRANŻA

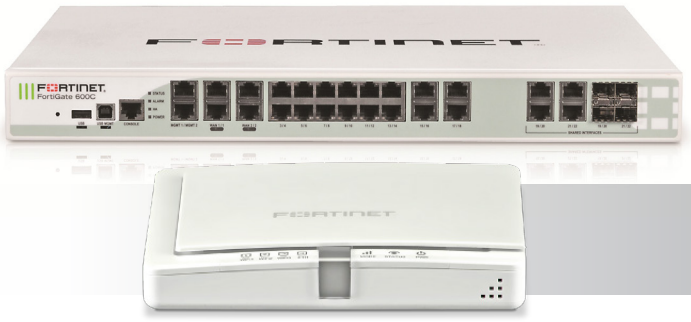
- Służba zdrowia

"Szpitale muszą zapewniać wysoki poziom ochrony informacji dotyczących przebiegu leczenia pacjentów, które są przechowywane w sieciach komputerowych. Stąd decyzja o zakupie urządzenia klasy UTM wspomagającego bezpieczeństwo sieci."

- Pawel Frączak,
Kierownik Sekcji Informatyki
Szpital Specjalistyczny Św. Zofii w Warszawie

FORTINET®

veracomp
inspirujemy IT



case study

ROZWIĄZANIE

Do ochrony sieci szpitala wybrano urządzenie zabezpieczające FortiGate-200B, które zapewnia przepustowości firewalla na poziomie 5 Gbps oraz zintegrowane mechanizmy ochronne.

Dedykowane układy scalone pozwalają również na zabezpieczenie sieci bez negatywnego wpływu na jej efektywność. Podstawową zaletą rozwiązania Fortinet jest możliwość kontrolowania urządzeń typu access point z poziomu jednej platformy. Dlatego zdecydowano równocześnie o instalacji drugiego rozwiązania tego samego producenta, FortiAP-220B, w liczbie 14 sztuk. FortiAP-220B oraz kontroler FortiGate-200B automatycznie wykrywają siebie nawzajem w sieci oraz dokonują automatycznego przesłania i załadowania konfiguracji do punktu dostępowego.

Wspólna i zcentralizowana platforma zarządzania oraz brak późniejszych opłat licencyjnych umożliwiły obniżenie kosztów utrzymania rozwiązania. Cały proces implementacji trwał około jednego miesiąca, a prace wdrożeniowe przeprowadziła firma Maxto.

KORZYŚCI

Zaimplementowany zintegrowany system ochrony sieci lokalnej szpitala firmy Fortinet pozwala na kontrolę na poziomie warstwy aplikacyjnej, priorytetyzację ruchu, ochronę przed wyciekiem danych poufnych oraz kontrolę dostępu do sieci. Urządzenia zapewniają wysoki poziom bezpieczeństwa. Rozwiązanie charakteryzuje duża przepustowość i skalowalność.

„Z racji tego, że codziennie pojawiają się coraz to nowocześniejsze techniki stosowane przez hakerów do ataków i wyłudzania poufnych informacji, instytucje, zwłaszcza te z sektora publicznego, stoją przed koniecznością ciągłej modernizacji swoich zabezpieczeń. Szpitale muszą zapewniać wysoki poziom ochrony informacji dotyczących przebiegu leczenia pacjentów, które są przechowywane w sieciach komputerowych. Stąd decyzja o zakupie urządzenia klasy UTM wspomagającego bezpieczeństwo sieci. Drugim naszym problemem był brak ciągłego dostępu do sieci dla naszego personelu. Implementacja 14 urządzeń typu access point umożliwia korzystanie z zasobów internetowych oraz komunikację na terenie szpitala, co jest koniecznością dla pracowników naszej placówki,"
– podkreśla Paweł Frączak, kierownik Sekcji Informatyki w Szpitalu Specjalistycznym Św. Zofii w Warszawie.

Wdrożenie rozwiązania Fortinet przebiegło pomyślnie i bezproblemowo. Obecnie szpital testuje skuteczność urządzeń, dzięki którym administratorzy mogą centralnie zarządzać siecią szpitala i na bieżąco kontrolować jej poziom bezpieczeństw .

Wdrożenie zabezpieczające sieć internetową Szpitala Specjalistycznego św. Zofii w Warszawie zostało zrealizowane przez firmę Maxto, która funkcjonuje w obszarze kompleksowej realizacji systemów teletechnicznych i teleinformatycznych. Zajmuje się analizą, projektowaniem, dystrybucją, instalacją oraz integracją rozwiązań zarówno dla administracji publicznej jak i sektora prywatnego.

Sprzęt wraz ze wsparciem technicznym dostarczył Veracomp SA, autoryzowany dystrybutor Fortinet w Polsce.

FORTINET®