



veracomp

inspirujemy IT

FORTINET FortiGate, FortiAnalyzer, FortiAP

Wojewódzki Szpital Specjalistyczny we Wrocławiu

HISTORIA PLACÓWKI

Wojewódzki Szpital Specjalistyczny we Wrocławiu działa od 1984 roku. Zapewnia stałą opiekę medyczną mieszkańcom całego Dolnego Śląska. Jest nowoczesną placówką wyposażoną w aparaturę medyczną i sprzęt diagnostyczny najnowszej generacji, pozwalający na wykonywanie kompleksowych badań oraz przeprowadzanie skomplikowanych zabiegów. Rocznie na szpitalnych oddziałach leczonych jest ponad 100 000 pacjentów, a od momentu otwarcia placówki urodziło się w niej 68 000 dzieci. Dzięki wsparciu z funduszy unijnych szpital stale się rozwija. Dotychczas utworzono w nim m.in. Dolnośląskie Centrum Teleradiologii oraz uruchomiono medyczną platformę naukowo-diagnostyczną TeleMedNet. W sumie szpital zrealizował ponad 20 projektów o łącznej wartości 188 mln złotych, z czego ponad 112 mln złotych stanowiło dofinansowanie ze środków unijnych. Jedną z największych inwestycji był zakup jedyne w Polsce robota da Vinci do wykonywania operacji zdalnych. Szpital otrzymał wiele nagród i wyróżnień, w tym: Dolnośląski Certyfikat Gospodarczy, certyfikat Gazele Biznesu w kategorii Szpitalnictwo oraz Certyfikat Innowacyjności przyznawany przez Instytut Nauk Ekonomicznych PAN i Sieć Naukową Ministerstwa Szkolnictwa Wyższego i Nauki. Placówka zdobywa również czołowe miejsca w rankingach przeprowadzanych przez polskie media, uzyskała m.in. tytuł Najlepszego Publicznego Szpitala w woj. dolnośląskim w rankingu zrealizowanym na zlecenie dziennika „Rzeczpospolita” oraz tytuł Lidera Informatyki przyznawany przez redakcję „Computerworld”. Ponadto szpital otrzymał Złoty Skalpel za innowacyjne rozwiązania w medycynie.

OPIS SYTUACJI WYJŚCIOWEJ

Od 2004 roku szpital konsekwentnie realizuje strategię rozwoju systemów informatycznych. Zmodernizowano i rozbudowano serwerownię wraz z wyposażeniem, zakupiono nowe stacje robocze, zbudowano światłowodową sieć strukturalną o przepustowości 10 Gb/s, obejmującą wszystkie budynki szpitala – w tym również sale dla chorych.

case study

WYZWANIE

- Umożliwienie personelowi oraz pacjentom korzystania z zasobów internetowych przy jednoczesnym zachowaniu bezpieczeństwa przetwarzania i transmisji danych

CELE

- Zagwarantowanie bezpieczeństwa przetwarzania i transmisji danych medycznych
- Zapewnienie dostępu do rozwiązań mobilnych na terenie szpitala
- Odseparowanie fizyczne wewnętrznej sieci medycznej dla personelu od sieci ogólnodostępnej dla pacjentów i gości szpitala

ROZWIĄZANIE

- FortiGate-1240B
- FortiAnalyzer-1000C
- FortiAP-220B

BRANŻA

- Służba zdrowia

*„Wrocławski szpital rozwija się niezwykle dynamicznie...
Utworzenie Dolnośląskiego Centrum Teleradiologii
i Dolnośląskie e-Zdrowie oraz programów krajowych
związanych z dostępem do danych medycznych to tylko
niektóre efekty, jakie przyniosła kompleksowa informatyzacja
naszej placówki.”*

- prof. Wojciech Witkiewicz
Dyrektor Naczelny Wojewódzkiego Szpitala
Specjalistycznego we Wrocławiu.

FORTINET®



case study

Stały dostęp do sieci usprawnił pracę personelu medycznego, tym samym zwiększając jej efektywność. Istotny element strategii stanowiło również wdrożenie systemów informatycznych, m.in. utworzenie Dolnośląskiego Centrum Teleradiologii oraz wdrożenie systemów klasy HIS, ERP oraz BI. Przy rozbudowie infrastruktury informatycznej dużo uwagi poświęcono również bezpieczeństwu systemu. Wraz z rozwojem placówki szpital poszukiwał rozwiązania zapewniającego bezpieczeństwo wrażliwych danych (dane osobowe pacjentów oraz historie ich choroby) przetwarzanych przez pracowników medycznych przed wyciekami lub kradzieżami. Duże wyzwanie dla działu informatyki stanowił wzrost zapotrzebowania personelu medycznego na zdalny dostęp do danych medycznych znajdujących się poza szpitalem – w ramach Dolnośląskiego Centrum Teleradiologii – oraz za pośrednictwem projektu Dolnośląskie e-Zdrowie. Stały i szybki dostęp do sieci umożliwiający korzystanie z zasobów internetowych oraz komunikację za pośrednictwem sieci lokalnej na terenie placówki okazał się być niezbędnym dla personelu. Kierownictwo szpitala chciało również stworzyć możliwość dostępu do Internetu pacjentom szpitala, bez ryzyka kradzieży poufnych danych, a także ataków z zewnątrz oraz ze strony sieci lokalnej. W związku z pojawiającymi się nowymi wyzwaniami wydajność zastosowanego rozwiązania zabezpieczającego okazała się ograniczona. Dlatego dyrekcja szpitala podjęła decyzję o wdrożeniu zintegrowanej ochrony pod postacią urządzenia klasy UTM, które byłoby skuteczne i wydajne, a jednocześnie dostosowane do potrzeb placówki. Nowe rozwiązanie miało umożliwiać tworzenie reguł bezpieczeństwa zarówno dla grup komputerów, jak i pojedynczych maszyn, a także stwarzać możliwość analizy zagrożeń i na ich podstawie podejmować działania mające na celu ich wykrycie. W 2011 roku Wojewódzki Szpital Specjalistyczny we Wrocławiu ogłosił przetarg na dostawcę kompleksowego oraz elastycznego rozwiązania bezpieczeństwa sieci, które pozwoliłoby na zabezpieczenie infrastruktury IT i ochronę wrażliwych danych przed wyciekami. Spośród dostępnych na rynku UTM-ów brano pod uwagę rozwiązania firm Sonicwall, Netasq, Juniper oraz FORTINET. W przetargu wygrało kompleksowe rozwiązanie firmy FORTINET, które w pełni odpowiadało potrzebom placówki przy zachowaniu korzystnej ceny. W 2012 roku zostało ogłoszone

postępowanie przetargowe na zbudowanie sieci Wi-Fi. W tym przypadku również wygrało rozwiązanie oparte na technologii firmy FORTINET.

ROZWIĄZANIE I WDROŻENIE

Do ochrony sieci Wojewódzkiego Szpitala Specjalistycznego we Wrocławiu wybrano urządzenie zabezpieczające klasy UTM – FortiGate-1240B. Pozwala ono z dużą wydajnością wykorzystywać firewall w różnych segmentach sieci jednocześnie, oferując przy tym placówce szereg innych funkcjonalności, takich jak Antyspam, Antywirus, IPS (ang. Intrusion Prevention System – system wykrywania i zapobiegania włamaniom), kontrola aplikacji czy Web Filtering (filtrowanie zawartości stron www).

Podstawową zaletą rozwiązania FORTINET jest możliwość kontrolowania urządzeń typu access point z poziomu jednej platformy. To właśnie w oparciu o inne urządzenia FORTINET – 45 punktów dostępowych FortiAP-220B – została zbudowana sieć bezprzewodowa. Rozwiązanie umożliwia wykorzystanie w pełni możliwości tabletów, na których użytkowana jest przez personel medyczny aplikacja HIS. W szpitalu został wprowadzony elektroniczny obieg dokumentów oraz wewnętrzna wymiana informacji. Lekarze mają pełen dostęp do danych pacjenta i historii jego choroby w czasie obchodów i wizyt konsultacyjnych, co znacznie usprawnia pracę szpitala. Dzięki zintegrowanej i bezpiecznej sieci dokumentacja medyczna może być rejestrowana i przesyłana dalej pomiędzy oddziałami szpitalnymi. Sieć Wi-Fi została również udostępniona pacjentom oraz gościom. Dodatkowo do analizy ruchu w sieci oraz raportowania wykorzystany został FortiAnalyzer-1000C. Dzięki temu rozwiązaniu administrator jest w stanie wskazać, które stacje robocze generują większy ruch niż zwykle, co może oznaczać zagrożenie albo niewłaściwe użytkowanie komputerów.



case study

REALIZACJA

Wdrożenie zabezpieczające sieć intranetową Wojewódzkiego Szpitala Specjalistycznego we Wrocławiu zostało zrealizowane przez firmę Bezpieczne IT. Pracownicy przeprowadzili audyt w placówce tak, aby przygotować ofertę w pełni dostosowaną do potrzeb instytucji. Dzięki ścisłej współpracy informatyków z wrocławskiego szpitala oraz inżynierów firmy Bezpieczne IT cały proces trwał niecałe 30 dni i przebiegał bardzo sprawnie, bez konieczności ograniczania dostępu do usług IT. Obejmował instalację urządzenia UTM oraz analizatora ruchu w sieci. Następnie zainstalowano punkty dostępowe i uruchomiono bezprzewodową sieć dla pacjentów. Sam montaż i uruchomienie dostarczonego sprzętu trwał 2 dni. Ostatnim etapem była konfiguracja urządzeń oraz dostosowanie ich do wymagań szpitala. Jako część usługi firma przeprowadziła również szkolenie dla personelu działu IT.

Przed wdrożeniem rozwiązania UTM administrator odnotowywał kilka przypadków naruszenia bezpieczeństwa rocznie. Od czasu instalacji urządzenia FortiGate żadna z prób nie była udana. System FortiGate kompleksowo chroni poufne informacje o pacjentach przechowywane w bazach danych przed włamaniem lub kradzieżą, nie powodując spowolnienia działania sieci i utraty jej wydajności. Urządzenia realizują polityki bezpieczeństwa zgodne z przepisami i najlepszymi standardami oraz praktykami branży, w tym wymaganiami stawianymi przez HIPAA (Health Insurance Portability and Accountability Act).

KORZYŚCI

Wdrożenie rozwiązań jednej marki pozwoliło na optymalizację działań struktury IT w szpitalu oraz wyeliminowało problem kompatybilności urządzeń różnych producentów. Wykorzystanie zestawu komplementarnych systemów od FORTINET zredukowało koszty operacyjne, zwiększyło efektywność, zapewniło wyższy poziom bezpieczeństwa oraz ułatwiło prace związane z administracją sieci. Obecnie za funkcjonowanie systemu bezpieczeństwa odpowiedzialna jest jedna osoba – administrator systemu. Rozwiązania FORTINET pozwalają proaktywnie chronić wrażliwe dane pacjentów szpitala, dodatkowo wykrywając potencjalne zagrożenia ataków z zewnątrz lub niedobory zasobów sieci, a także analizują ruch oraz sposób użytkowania komputerów.