Infrastruktura sieciowa Extreme Networks gwarantuje szybkie i bezpieczne przesyłanie medycznych danych pacjentów Centralnego Szpitala Klinicznego MSW.

W SKRÓCIE

Liczby:

- 852 lekarzy
- ok. 279 tys. pacjentów w 2013 r.
- 2 serwerownie
- 48 punktów LPD
- 1500 portów Ethernet

Branża:

- ochrona zdrowia

Wyzwania:

- stworzenie wydajnej, niezawodnej i stabilnej infrastruktury sieciowej
- uproszczenie zarządzania środowiskiem sieciowym
- zapewnienie pełnej ochrony danych przed dostępem osób niepowołanych

Zastosowane produkty:

- przełączniki rdzeniowe serii S4 z modułami S155
- przełączniki dostępowe L3 B5G/B5K
- system zarządzania NMS
- system dostępu do sieci NAC
- system sieci bezprzewodowej IdentiFi 802.11n
- system wykrywania intruzów w sieci przewodowej IDS
- system SIEM

O firmie

Centralny Szpital Kliniczny MSW w Warszawie to nowoczesny ośrodek diagnostyczno-leczniczy, przyjazny pacjentom i ich rodzinom. Placówka w 2013 r. udzieliła ponad pół miliona wysokospecjalistycznych porad i hospitalizowała 56 tys. osób.

Nie ma dziś szpitala, który nie korzystałby z nowoczesnych rozwiązań teleinformatycznych. Wymaga tego przede wszystkim bardzo szybki rozwój technologii obrazowania medycznego, dzięki którym możliwe jest postawienie dokładnej diagnozy. Dlatego od kilkunastu lat w szpitalach widać dynamiczny wzrost obecności sprzętu komputerowego (stacji roboczych i maszyn diagnostycznych, ale także tradycyjnych profesjonalnych serwerów i pamięci masowych). Transmisja wszystkich danych pomiędzy tymi systemami musi być pewna i bezpieczna, bez jakichkolwiek przestojów, czy ryzyka przedostania się informacji w niepowołane ręce.

Przed takim samym wyzwaniem stanął Centralny Szpital Kliniczny MSW: - Musieliśmy przesyłać coraz więcej danych diagnostycznych, a w związku z nieustannym wzrostem ich objętości, zwiększał się czas transmisji między sprzętem medycznym, a serwerami i stacjami roboczymi. Przez to transmisja wyników badań trwała dłużej, co opóźniało diagnozę - wspomina Marcin Oleksiński administrator sieci i koordynator sekcji informatyki w CSK MSW.

Każda próba rozwoju infrastruktury LAN związana była wówczas z wieloma problemami. Część posiadanych przez szpital przełączników nie była zarządzalna. Coraz częściej w wybranych miejscach infrastruktury pojawiały się małe przełączniki, gdy potrzebne było zapewnienie dodatkowych portów sieciowych. - Zdarzało się też, że któryś z pracowników przypadkowo rozłączył kabel sieciowy i później podłączył go do dowolnego, innego portu - dodaje Marcin Oleksiński. - W ten sposób często powstawały pętle w sieci, których ręczne wykrycie graniczyło z cudem. Posiadane przez nas przełączniki zaczęły też coraz częściej ulegać awariom w związku z wysłużeniem mechanicznym sprzętu. Musieliśmy pilnie dokonać wymiany sprzętu sieciowego.

Niezawodnie i bezpiecznie

W 2009 r. został zorganizowany przetarg, w ramach którego zaplanowano wymianę wszystkich urządzeń sieciowych, jak też wybranych elementów okablowania strukturalnego. Zaplanowano podwojenie liczby dostępnych portów sieciowych, jak też zapewnienie możliwości szybkiej rozbudowy infrastruktury, gdy zaistnieje taka potrzeba. Pozostawiono jednak także fragmenty wcześniej używanego okablowania światłowodowego, które wciąż jest wykorzystywane do projektów o mniejszych wymaganiach związanych z dostępnością i niezawodnością, np. do wideokonferencji.

Zorganizowany przez CSK MSW przetarg obejmował kompleksową wymianę infrastruktury, okablowania, światłowodów, dostawę przełączników sieciowych, centrali telefonicznej, telefonów IP i innych elementów. Wśród wskazanych wymagań były kwestie związane z niezawodnością, politykami bezpieczeństwa

i systemem zarządzania wszystkimi sieciowych urządzeniami aktywnymi (przewodowymi i bezprzewodowymi). Pojawił się także wymóg wieczystej gwarancji i nieograniczonej dostępności aktualizacji. Przetarg wygrało konsorcjum firm Siemens Enterprise Communication i Telsar, które zaproponowały m.in. rozwiązania sieciowe Extreme Networks.

- Samo wdrożenie i konfiguracja systemów trwały krócej niż trzy miesiące - mówi Marcin Oleksiński. - Wszystko odbyło się zupełnie bezproblemowo, pracownicy praktycznie nie odczuli żadnych niedogodności, zauważyli natomiast znaczny wzrost wydajności.

Obecnie w szpitalnej sieci pracuje ok 900 komputerów, 200 terminali (ich liczba cały czas rośnie), ok. 100 punktów dostępowych WLAN i 200 drukarek. Wszystkie medyczne urządzenia diagnostyczne są podłączone do sieci, gdzie mają swoją wydzieloną wirtualną sieć VLAN.

Przyrost danych to nie problem

Obecnie w ramach infrastruktury IT szpitala funkcjonują dwie serwerownie w odległości ok. 250 metrów od siebie, są połączone ze sobą światłowodem, każda z nich ma też oddzielne połączenie z Internetem. W niedalekiej przyszłości będą pracowały w trybie active-active. W jednej z serwerowni zainstalowany jest przełącznik rdzeniowy ze zdublowanymi wszystkimi komponentami (zasilaczami, modułami przełączającymi itd.), zaś w planach jest instalacja drugiego w zapasowej serwerowni.

- Naszym podstawowym wyzwaniem jest ogromna i nadal rosnąca ilość danych - mówi Marcin Oleksiński. - Gdy rozstrzygaliśmy przetarg to urządzenia diagnostyczne generowały w jednym badaniu średnio 300-800 obrazów. Dziś jest ich ok. 1000-2500 i to w znacznie większej rozdzielczości. Na razie mamy duży komfort pracy, ponieważ przepustowość sieci jest wykorzystana w ok. 35%. Mamy też plany dalszego rozwoju, np. na blokach operacyjnych chcemy zainstalować kamery 3D i prowadzić transmisję obrazu z prowadzonych zabiegów.

Szpital korzysta też z bezpiecznej sieci bezprzewodowej. Jest ona dostępna zarówno dla pacjentów, ale też dla lekarzy, którzy dzięki niej podczas obchodu mogą pracować w szpitalnej aplikacji na tabletach. Wykorzystanie urządzeń mobilnych zdecydowanie poprawia skuteczność procesu leczenia pacjenta

- lekarz może mieć bieżący dostęp do wszystkich wyników badań, może też na miejscu zlecać dodatkowe badania lub zabiegi. O bezpieczeństwo przesyłanych danych dbają zarówno urządzenia w infrastrukturze sieciowej (autentykacja adresów MAC karty bezprzewodowej w tabletach), jak też sama aplikacja szpitalna, do której każdy użytkownik musi zalogować się swoim indywidualnym hasłem.

Obcym wstęp wzbroniony

Specyfika pracy szpitala i konieczności serwisowania medycznych urządzeń diagnostycznych charakteryzuje się tym, że do sieci dostęp muszą uzyskiwać także ekipy serwisowe. Brak możliwości centralnego egzekwowania działań zgodnych z politykami bezpieczeństwa doprowadzał do sytuacji, gdzie do sieci często podłączane były routery serwisantów z włączonym serwerem DHCP i bez jakichkolwiek polityk bezpieczeństwa. Dziś ten problem jest wyeliminowany.

- Dzięki wdrożeniu zarządzalnej sieci zyskaliśmy możliwość centralnego wglądu w całą infrastrukturę, bez konieczności ręcznego identyfikowania ewentualnych problemów lub anomalii - podsumowuje Marcin Oleksiński. - Nie ma już możliwości podłączenia do sieci nieautoryzowanego przez nas urządzenia. Wspólny, zintegrowany interfejs graficzny dla wszystkich urządzeń Extreme Networks powoduje też, że nie muszę wprowadzać tych samych danych konfiguracyjnych sieci wirtualnych lub polityk bezpieczeństwa w wielu miejscach, co zwiększałoby ryzyko popełnienia błędu.

Administratorzy działu IT szpitala samodzielnie zarządzają całą infrastrukturą - podkreślają przejrzystość interfejsu urządzeń. Ukończyli oni odpowiednie szkolenia i chwalą sobie też zaangażowanie działu wsparcia technicznego Extreme Networks. Posiadana przez nich infrastruktura jest też rozbudowywana od czasu do czasu w związku z trwającymi wdrożeniami terminali do obsługi aplikacji medycznych i koniecznością udostępnienia użytkownikom dodatkowych portów sieciowych.

Istnieje kilka cech, które nie były wymagane w przetargu, ale systemy, które zostały dostarczone posiadają je i używamy ich niemal codziennie. Funkcje te to np Compas, jest on w stanie znaleźć urządzenie w sieci w oparciu o nazwę hosta, nazwę użytkownika, Mac lub adres IP. Wynik wyszukiwania jest poszerzony o status portu, statystyki(w tym błędy transmisji) ruchu na porcie i wiele innych przydatnych informacji. Kolejna funkcja to Polityki Bezpieczeństwa. Profile te pozwalają nam na zdefiniowanie dozwolonych aplikacji dla każdego rodzaju systemu końcowego. Reguły w polityce są stosowane zarówno w sieci przewodowej i bezprzewodowej dla wszystkich systemów końcowych. Wszystko jest centralnie zarządzane. Mamy pełną widoczność, kiedy i gdzie każdy system końcowy jest podłączony i możemy go kontrolować, z perspektywy uprawnień wcześniej zdefiniowanych w systemie. Jest to bardzo przydatne, zwłaszcza z szerokiej różnorodności systemów końcowych. Otrzymaliśmy to w pakiecie wraz z systemem zarządzania NetSight.

Extreme networks

http://www.extremenetworks.com/contact / Phone +1-408-579-2800