W ramach zadania projektowego zrealizowano zamówienie pn. „Zakup systemu kopii zapasowych, zapór sieciowych nowej generacji oraz urządzeń do segmentacji sieci”

W ramach realizacji przedsięwzięcia doposażono infrastrukturę szpitala w nowoczesne rozwiązania poprzez:

- zakup accesspointów i kontrolerów (rozbudowa bezprzewodowych punktów dostępu do sieci Wifi - 30 szt.; Kontroler do accesponitów - 3szt.) - 1 kpl (dostawa, dokumentacja wraz z gwarancją na 36 miesięcy)
- zakup urządzenia NDR (Network Detection and Response) - służącego do automatycznego wykrywania i reakacji na zagrożenia na podstawie analizy ruchu sieciowego (dostawa, montaż, wdrożenie, szkolenie, dokumentacja- licencja wraz z gwarancją ora wsparciem na okres 36 miesięcy) - 1 szt.
- rozbudowę licencji do urządzenia Fortianalyzer. Rozbudowa o 15gb wraz ze wsparciem i licencją na okres 36 miesięcy
- zakup UTM. Dostawa/montaż/wdrożenie/gwarancja/wsparcie/szkolenie/dokume ntacja

Zakup accesspointów i kontrolerów zapewnia centralne zarządzanie, bezproblemowy roaming mobilnego sprzętu medycznego oraz wysoki poziom bezpieczeństwa danych pacjentów. Natychmiastowe powiadomienia o odłączeniu lub problemach wydajnościowych konkretnego punktu dostępowego pozwala utrzymać ciągłość pracy w opiece nad chorymi.

Zakup urządzenia NDR zapewnia ciągłe monitorowanie ruchu sieciowego, wykrywanie anomalii oraz ochronę poufnych danych medycznych. Urządzenie dodatkowo zabezpiecza wrażliwe dane pacjentów i dokumentację medyczną przed kradzieżą. Szybko wykrywa i zatrzymuje groźne ataki typu ransomware, które mogłyby sparaliżować pracę szpitala. Zapobiega przestojom w systemach IT, co gwarantuje nieprzerwane działanie aparatury medycznej i izby przyjęć.

Rozbudowa licencji do systemu FortiAnalyzer w szpitalu zapewnia kluczowe korzyści: spełnienie wymogów prawnych z zakresu cyberbezpieczeństwa, usprawnienie wykrywania zagrożeń oraz centralizację logów z systemów medycznych.

Zakup urządzenia UTM (Unified Threat Management) to kluczowa inwestycja, która zapewnia kompleksową ochronę danych oraz ciągłość działania systemów medycznych w szpitalu. Blokowanie ataków hakerskich i złośliwego oprogramowania zapobiega przestojom w pracy aparatury medycznej oraz systemów obsługi pacjentów. Ponadto urządzenie skutecznie ochronia tajemnicę medyczną oraz poufne dane osobowe pacjentów przed wyciekiem. Priorytetyzacja ruchu dla kluczowych systemów szpitalnych (np. HIS, RIS/PACS) gwarantuje stabilne działanie najważniejszych aplikacji.

Zakup współfinansowany w ramach Krajowego Planu Odbudowy i Zwiększania Odporności – „Podniesienie poziomu cyberbezpieczeństwa, cyfryzacja dokumentacji medycznej oraz rozwój e-usług i rozwiązań z zakresu sztucznej inteligencji w Katowickim Centrum Onkologii” w ramach inwestycji D1.1.2 „Przyśpieszenie procesów transformacji cyfrowej ochrony zdrowia poprzez dalszy rozwój usług cyfrowych w ochronie zdrowia”. Nr naboru KPOD.07.03-IP.10-001/25.

Data utworzenia
11-08-2026 (Michał Pisula)
Data modyfikacji
11-08-2026 (Michał Pisula)
Data publikacji
11-08-2026