Case Study

Rozbudowa infrastruktury IT oraz wdrożenie SOC w SP ZOZ w Lubaczowie

Realizacja terminowa i przeprowadzona z dużą dbałością o każdy etap projektu.(...) Rzetelny partner.

Piotr Cencora
SP ZOZ Lubaczów

01 Wyzwanie klienta – rozwój infrastruktury IT i bezpieczeństwa danych medycznych

Sektor ochrony zdrowia w Polsce jest jednym z najczęściej atakowanych przez cyberprzestępców. Według raportów publikowanych przez CERT Polska oraz NASK, liczba incydentów cyberbezpieczeństwa w Polsce rośnie z roku na rok i obejmuje dziesiątki tysięcy zgłoszeń rocznie, z czego znacząca część dotyczy podmiotów publicznych, w tym szpitali.

Placówki medyczne są szczególnie narażone ze względu na:

- przetwarzanie wrażliwych danych osobowych i medycznych,
- konieczność zapewnienia ciągłości działania systemów klinicznych,
- ograniczone zasoby wewnętrznych zespołów cyberbezpieczeństwa,
- rosnącą liczbę ataków ransomware wymierzonych w infrastrukturę medyczną.

W tym kontekście SP ZOZ w Lubaczowie realizował projekt ukierunkowany na rozwój usług cyfrowych oraz modernizację infrastruktury IT, którego kluczowym elementem było zwiększenie poziomu bezpieczeństwa danych przetwarzanych w systemach medycznych oraz zapewnienie wysokiej dostępności usług dla pacjentów i personelu. Celem przedsięwzięcia było nie tylko unowocześnienie środowiska sprzętowego i systemowego, ale przede wszystkim wdrożenie rozwiązań umożliwiających stałe monitorowanie infrastruktury oraz szybkie wykrywanie i reagowanie na zagrożenia w czasie rzeczywistym, minimalizując ryzyko zakłóceń w funkcjonowaniu placówki.

02 Potrzeby techniczne – kompleksowa modernizacja i zabezpieczenie środowiska IT02

Zamawiający potrzebował kompleksowego rozwiązania obejmującego zarówno dostawę sprzętu, jak i wdrożenie usług bezpieczeństwa:

- dostawę nowoczesnego sprzętu komputerowego i serwerowego,
- rozbudowę środowiska wirtualizacyjnego i pamięci masowych,
- wdrożenie systemów ochrony poczty e-mail,
- segmentację sieci i zwiększenie jej bezpieczeństwa,
- zapewnienie ciągłego monitorowania infrastruktury IT,
- wdrożenie usługi SOC 24/7/365 dla wykrywania i obsługi incydentów.

Kluczowym elementem projektu było wdrożenie usługi SOC (Security Operations Center).

SOC (Centrum Operacji Bezpieczeństwa) to wyspecjalizowana usługa cyberbezpieczeństwa, która działa jako zewnętrzne centrum nadzoru nad infrastrukturą IT organizacji. SOC:

- monitoruje zdarzenia bezpieczeństwa 24/7,
- analizuje logi i zachowania systemów,
- wykrywa potencjalne zagrożenia na wczesnym etapie,
- reaguje na incydenty w czasie rzeczywistym,
- wspiera organizację w ograniczeniu skutków ataku i przywróceniu bezpieczeństwa.

03 Rozwiązanie Maxto ITS – wdrożenie SOC opartego o technologie klasy światowej

W odpowiedzi na potrzeby klienta, Maxto ITS wdrożyło usługę SOC opartą o rozwiązania firmy Sophos, jednego z globalnych liderów w dziedzinie cyberbezpieczeństwa, będącego właścicielem platformy analitycznej Secureworks (Taegis XDR).

W ramach realizacji projektu Maxto ITS zapewniło:

- wdrożenie i konfigurację usługi SOC monitorującej stacje robocze i serwery,
- integrację systemów bezpieczeństwa z istniejącą infrastrukturą IT szpitala,
- uruchomienie mechanizmów ciągłego monitorowania zagrożeń 24/7,
- dostęp do zespołu analityków bezpieczeństwa monitorujących środowisko klienta,
- wsparcie wdrożeniowe oraz operacyjne,
- szkolenie administratorów w zakresie obsługi i reagowania na incydenty.

Wdrożone rozwiązanie wykorzystuje zaawansowaną analitykę behawioralną, sztuczną inteligencję oraz globalną bazę wiedzy o zagrożeniach, co umożliwia wykrywanie zarówno znanych, jak i nowych, wcześniej niezidentyfikowanych ataków.

Partnerstwo technologiczne z globalnymi liderami cyberbezpieczeństwa gwarantuje najwyższy poziom ochrony, zgodny z najlepszymi praktykami i standardami stosowanymi w sektorze ochrony zdrowia.

04 Efekty wdrożenia i korzyści dla klienta

Dzięki realizacji projektu SP ZOZ w Lubaczowie osiągnął istotny wzrost poziomu bezpieczeństwa oraz wydajności infrastruktury IT.

Najważniejsze korzyści:

- zwiększenie wydajnośc ii niezawodności systemów IT,
- poprawa bezpieczeństwa danych pacjentów,
- ciągłe monitorowanie środowiska IT 24/7,
- skrócenie czasu wykrywania i reagowania na incydenty,
- zwiększenie odporności na cyberzagrożenia,
- zapewnienie ciągłości działania systemów krytycznych,
- integracja systemów i uproszczenie zarządzania IT,
- dostęp do kompetencji ekspertów cyberbezpieczeństwa.

05 Podsumowanie

Projekt rozbudowy infrastruktury IT oraz wdrożenia usługi SOC w SP ZOZ w Lubaczowie stanowi przykład kompleksowej transformacji cyfrowej w sektorze ochrony zdrowia. Zrealizowane działania pozwoliły na jednoczesne zwiększenie poziomu bezpieczeństwa, wydajności oraz dostępności systemów IT, przy jednoczesnym zapewnieniu zgodności z rosnącymi wymaganiami w zakresie ochrony danych i cyberbezpieczeństwa.

Gwarantujemy usługi na wysokim poziomie

Jakość naszej pracy jest potwierdzona certyfikatami.

Nasi partnerzy technologiczni

Jesteśmy Tytanowym Partnerem Dell Technologies

maxtoits.pl

Maxto ITS Sp. z o.o.
+48 12 266 39 69
info@maxtoits.pl

Case Study

Wdrożenie ochrony usług pocztowych FortiMail w SP ZOZ w Lubaczowie

Realizacja terminowa i przeprowadzona z dużą dbałością o każdy etap projektu.(...) Rzetelny partner.

Piotr Cencora
SP ZOZ Lubaczów

01 Wyzwanie klienta – rozwój infrastruktury IT i bezpieczeństwa danych medycznych

Sektor ochrony zdrowia w Polsce jest jednym z najczęściej atakowanych przez cyberprzestępców. Według raportów publikowanych przez CERT Polska oraz NASK, liczba incydentów cyberbezpieczeństwa w Polsce rośnie z roku na rok i obejmuje dziesiątki tysięcy zgłoszeń rocznie, z czego znacząca część dotyczy podmiotów publicznych, w tym szpitali.

Placówki medyczne są szczególnie narażone ze względu na:

- przetwarzanie wrażliwych danych osobowych i medycznych,
- konieczność zapewnienia ciągłości działania systemów klinicznych,
- ograniczone zasoby wewnętrznych zespołów cyberbezpieczeństwa,
- rosnącą liczbę ataków ransomware wymierzonych w infrastrukturę medyczną.

W tym kontekście SP ZOZ w Lubaczowie realizował projekt mający na celu ochronę skrzynek pocztowych przed cyberatakami oraz zwiększenie bezpieczeństwa danych przetwarzanych w systemach medycznych. Kluczowym elementem było wdrożenie zaawansowanych mechanizmów zabezpieczających, takich jak filtracja wiadomości e-mail, zapobieganie phishingowi oraz ochrona przed złośliwym oprogramowaniem. Celem przedsięwzięcia było nie tylko unowocześnienie środowiska sprzętowego i systemowego, ale przede wszystkim stworzenie systemu umożliwiającego stałe monitorowanie zagrożeń oraz szybkie wykrywanie i reagowanie na próby naruszeń bezpieczeństwa, minimalizując ryzyko zakłóceń w funkcjonowaniu placówki oraz zapewniając wysoką dostępność usług dla pacjentów i personelu.

02 Potrzeby techniczne – kompleksowa modernizacja i zabezpieczenie środowiska IT02

Kluczowym elementem projektu było wdrożenie systemu ochrony poczty e-mail (FortiMail)

System ten odpowiada za zabezpieczenie komunikacji elektronicznej poprzez analizę oraz filtrowanie wiadomości przychodzących i wychodzących, minimalizując ryzyko wystąpienia incydentów bezpieczeństwa.

- ochronę przed spamem i phishingiem,
- wykrywanie zagrożeń na wczesnym etapie,
- blokowanie niebezpiecznych wiadomości przed ich dostarczeniem do użytkowników,
- analizę reputacji nadawców,
- skanowanie załączników pod kątem złośliwego oprogramowania,

Statystyki skuteczności ochrony usług pocztowych **FortiMail**

95%

skuteczność

99,84%

wykrywalność wirusów Malware

99,96%

wyłapywanie spamu

03 Rozwiązanie Maxto ITS – wdrożenie FortiMail, systemu ochrony przed cyberatakami na skrzynki mailowe

W odpowiedzi na potrzeby klienta Maxto ITS wdrożyło rozwiązanie FortiMail, oparte o zaawansowane technologie cyberbezpieczeństwa dostarczane przez globalnych liderów rynku.

W ramach realizacji projektu Maxto ITS zapewniło:

- mechanizmy antyspamowe i antyphishingowe, zaawansowaną analizę ruchu pocztowego. oraz ciągłe monitorowanie ruchu e-mail,
- integrację systemów bezpieczeństwa z istniejącą infrastrukturą IT szpitala,
- uruchomienie mechanizmów ciągłego monitorowania zagrożeń 24/7, blokowanie zagrożeń w czasie rzeczywistym,
- dostęp do zespołu analityków bezpieczeństwa monitorujących środowisko klienta,
- wsparcie wdrożeniowe oraz operacyjne,
- szkolenie administratorów w zakresie obsługi i reagowania na incydenty.

Wdrożone rozwiązanie wykorzystuje zaawansowaną analitykę behawioralną, sztuczną inteligencję oraz globalną bazę wiedzy o zagrożeniach, co umożliwia wykrywanie zarówno znanych, jak i nowych, wcześniej niezidentyfikowanych ataków.

04 Efekty wdrożenia i korzyści dla klienta

Dzięki realizacji projektu SP ZOZ w Lubaczowie osiągnął istotny wzrost poziomu bezpieczeństwa oraz wydajności infrastruktury IT.

Najważniejsze korzyści:

- zwiększenie odporności na cyberzagrożenia,
- poprawa bezpieczeństwa danych pacjentów,
- skrócenie czasu wykrywania i reagowania na incydenty,
- uproszczenie zarządzania IT,

Partnerstwo technologiczne z globalnymi liderami cyberbezpieczeństwa gwarantuje najwyższy poziom ochrony, zgodny z najlepszymi praktykami i standardami stosowanymi w sektorze ochrony zdrowia.

05 Podsumowanie

Projekt rozbudowy infrastruktury IT oraz wdrożenia systemu ochrony poczty e-mail FortiMail w SP ZOZ w Lubaczowie stanowi przykład kompleksowej modernizacji środowiska IT w sektorze ochrony zdrowia. Zrealizowane działania pozwoliły na zwiększenie poziomu bezpieczeństwa komunikacji elektronicznej, poprawę ochrony danych medycznych oraz ograniczenie ryzyka związanego z cyberzagrożeniami wykorzystującymi pocztę e-mail. Wdrożone rozwiązanie przyczyniło się także do zwiększenia stabilności i bezpieczeństwa systemów IT, przy jednoczesnym zachowaniu zgodności z rosnącymi wymaganiami w zakresie ochrony danych i cyberbezpieczeństwa.

Gwarantujemy usługi na wysokim poziomie

Jakość naszej pracy jest potwierdzona certyfikatami.

Nasi partnerzy technologiczni

Jesteśmy Tytanowym Partnerem Dell Technologies

maxtoits.pl

Maxto ITS Sp. z o.o.
+48 12 266 39 69
info@maxtoits.pl