



## Wdrożenia w Polsce

1. **NASK**
2. **Warmia i Mazury**
3. **Politechnika Krakowska**
4. **Totalizator sportowy**
5. **Uniwersytet Szczeciński**

### NASK

Naukowa i Akademicka Sieć Komputerowa (NASK) jest wiodącym polskim operatorem świadczącym usługi transmisji danych. Oferuje nowoczesne rozwiązania teleinformatyczne dla klientów biznesowych, administracji i nauki. NASK zapewnia kompleksowe rozwiązania z zakresu bezpieczeństwa teleinformatycznego. NASK poszukiwał odpowiedniego systemu do świadczenia usługi firewallingu w modelu MSS.

Po weryfikacji różnych rozwiązań wybór padł na ofertę Fortinet. Produkty firmy zapewniają wysoką elastyczność systemu i przyjazny sposób licencjonowania. Nie bez znaczenia było również profesjonalne wsparcie techniczne otrzymane od inżynierów Fortinet. Wdrożenie nowego systemu firewall zbudowanego na bazie produktów Fortinet oraz wirtualnych licencji VDOM trwało około 6 miesięcy.

W efekcie NASK jako operator sieci świadczy teraz usługi w modelu MSS w oparciu o produkty Fortinet. Usługa firewallingu realizowana na platformie operatora jest dostępna dla wszystkich klientów telekomunikacyjnych NASK. Usługa, świadczona w 3 opcjach, zapewnia klientom korzystanie z wirtualnej instancji firewalla oraz profesjonalną administrację realizowaną przez inżynierów NASK.

Dzięki korzystaniu z rozwiązania firmy Fortinet, NASK uzyskał możliwość generowania dodatkowych przychodów z nowoprowadzonej usługi. W dłuższej perspektywie zyskując elastyczne możliwości tworzenia kolejnych rozwiązań z zakresu bezpieczeństwa telekomunikacyjnego składających się na kompleksowe rozwiązanie telekomunikacyjne dla klientów.

NASK został wyróżniony przez FORTINET jako Partner Roku 2009 za największe wdrożenie w modelu MSS.

## Warmia i Mazury

Warmia i Mazury, jeden z najbardziej popularnych regionów turystycznych w Polsce, wybrał rozwiązania Fortinet do rozbudowy i zabezpieczenia infrastruktury szerokopasmowego dostępu do internetu oraz sieci publicznych punktów dostępu do internetu w Województwie Warmińsko – Mazurskim. Nowy system zaoferuje szeroki zakres usług sieciowych za pośrednictwem 640 bezpłatnych publicznych punktów dostępu do internetu. W ramach sieci powstanie 290 infokiosków, 33 telecentrów i 290 hot spotów. Wszystkie lokalizacje zostaną połączone w jedną bezpieczną sieć VPN. Rozwiązania Fortinet wybrano, aby zabezpieczyć sieć i jej użytkowników przed zagrożeniami, wirusami i robakami, niechcianą treścią, kradzieżą tożsamości, a także zapewnić ochronę poufności transmisji i treści.

Zintegrowany system bezpieczeństwa wdrożony w regionie będzie bazował na rozwiązaniach sprzętowych i oprogramowaniu Fortinet i składał się z: 246 urządzeń FortiGate 80 i jednego FortiGate 620, 289 platform FortiWiFi 80 oraz 383 bezprzewodowych punktów dostępowych FortiAP 220A. Całość będzie centralnie zarządzana przez FortiManager 300. W systemie zastosowana zostanie również aplikacja FortiAnalyzer 1000, która będzie służyć do analizy i raportowania ruchu w sieci w wielu lokalizacjach z poziomu jednej centralnej kontroli administracyjnej.

## Politechnika Krakowska

Sieć komputerowa Politechniki Krakowskiej składa się z ponad 2000 komputerów. Bezpieczeństwo danych, a także zapewnienie kontroli nad transmisją informacji w sieci, jest priorytetem dla Działu Informatyzacji uczelni. Z uwagi na konieczność skutecznej ochrony informacji szukano rozwiązania, które zagwarantuje wysoki poziom bezpieczeństwa sieci. Po analizie funkcjonalności rozwiązań dostępnych na polskim rynku, Politechnika Krakowska zdecydowała się na ofertę firmy Fortinet.

Wybrany system bezpieczeństwa firmy Fortinet składa się ze zintegrowanego urządzenia zabezpieczającego FortiGate-3810A oraz oprogramowania FortiAnalyzer. Oprócz analizy ruchu WWW, Politechnika Krakowska ma uruchomione filtrowanie poczty elektronicznej, blokowanie ruchu P2P i ochronę przed spamem. Dla zwiększenia kontroli, FortiGate-3810A pozwala na segmentację do setek wirtualnych domen (VDM) dla osobnych użytkowników, departamentów czy jakichkolwiek innych działów. Funkcjonalność ta okazała się szczególnie przydatna w projektowaniu architektury bezpieczeństwa w wielowydziałowej strukturze uczelni.

Politechnika Krakowska zdecydowała także o wdrożeniu FortiAnalyzeera - dodatkowej platformy służącej do zapisywania zdarzeń, ich analizy i raportowania. To rozwiązanie nieustannie zbiera dane przekazywane z urządzeń FortiGate, a następnie dostarcza

administratorom wyczerpujący obraz wykorzystania sieci i bezpieczeństwa informacji na całej uczelni.

## **Totalizator sportowy**

Totalizator Sportowy realizuje państwowy monopol w dziedzinie gier liczbowych i loterii pieniężnych. Jak każda firma, Lotto posiada narzędzia ochrony firmowej sieci. Jednymi z ostatnio wdrożonych są urządzenia UTM firmy Fortinet. Chronią one sieć operacyjną, niezbędną do działania spółki i połączenia oddziałów.

Wdrożono urządzenia Fortigate w jednostkach terenowych i klastrowane urządzenia z wyższej półki w centrali spółki. W skład systemu wchodzi również urządzenia do scentralizowanego zarządzania i zbierania informacji ze wszystkich urządzeń peryferyjnych tego samego producenta, z obsługą generowanych logów, w celu ich analizy. Rozwiązania innych dostawców nie zapewniały takich możliwości, jakie daje implementacja UTM wraz z ich nowymi funkcjami odpowiadającymi obecnym wyzwaniom technicznym.

Urządzenia Fortinet posiadają standardowe zabezpieczenia, takie jak antyspam, antyspyware, antywirus i filtrowanie stron WWW. Dodatkowo interesującą funkcją jest możliwość akcelerowania łączy. Siecią łatwiej jest zarządzać korzystając z jednej konsoli, co było istotnym elementem w wyborze rozwiązania.

Do wdrożenia wykorzystano prekonfigurowane urządzenia, które zainstalowano w centrali i oddziałach terenowych. Proces uruchomienia żądanej funkcjonalności zajął trzy tygodnie. Po zainstalowaniu urządzeń, centralnie zaimplementowano politykę bezpieczeństwa.

Perspektywy rozwoju Działu Informatyki ma w planach aktualizację oprogramowania do wersji 4, której nowe funkcje - m.in. inspekcja ruchu sieciowego - są bardzo istotne dla Totalizatora Sportowego.

## **Uniwersytet Szczeciński**

Uniwersytet Szczeciński jest największą uczelnią na Pomorzu Zachodnim. Uczelnia kształci obecnie 30 tysięcy studentów na 84 kierunkach studiów i specjalnościach w ramach 11 wydziałów. W ofercie studiów podyplomowych znajduje się 56 kierunków studiów. Piony naukowe, jednostki dydaktyczne, wydziały i domy studenckie są połączone akademicką i naukową siecią komputerową „Pionier”. Mając na celu zapewnienie wszystkim użytkownikom bezpiecznego i legalnego korzystania z internetu, uczelnia zdecydowała się na rozbudowę dotychczasowego systemu bezpieczeństwa.

Z sieci uniwersyteckiej korzysta obecnie 30 tysięcy studentów i 2 tysiące pracowników, a także użytkownicy z zewnątrz, studenci kierunków podyplomowych oraz osoby szukające informacji o studiach. Obciążenie serwera jest znacznie większe w trakcie konferencji organizowanych przez uczelnię. Uczelnia potrzebuje rozbudowanych rozwiązań

zabezpieczających z uwagi na skalę rozwoju sieci uniwersytetu. Ponadto podjęto decyzję o konieczności wprowadzenia działań, które miały wyeliminować nieprawidłowości związane z korzystaniem z internetu, czyli pobieranie nieautoryzowanych plików, gier i filmów. Zaistniała też potrzeba stworzenia bezpiecznego i wydajnego środowiska dla elektronicznej rekrutacji kandydatów.

W pierwszym etapie wdrożenia zostały zakupione dwa dodatkowe urządzenia Fortinet FortiGate 1000AFA2, które działały w formie klastra. Platformy te zaczęły zabezpieczać całą sieć uniwersytecką. Aby sieć uczelniana wytrzymała obciążenia związane z procesem elektronicznej rekrutacji, Uniwersytet kupił jeszcze cztery platformy Fortinet: dwa urządzenia FortiGate 3810A, FortiWeb 1000B oraz oprogramowanie do zarządzania systemem bezpieczeństwa FortiManager 300B. Rozwiązanie zostało zintegrowane z posiadaną już przez uczelnię aplikacją do zapisywania zdarzeń i raportowania FortiAnalyzer 2000B, która zbiera i analizuje dane przekazywane z różnych urządzeń FortiGate.

Jednym z głównych założeń budowanego systemu bezpiecznego dostępu do aplikacji była jego redundancja i odporność na uszkodzenia, dlatego wszystkie jego elementy zostały zdublowane. Dwie platformy FortiGate-3810A działają w klastrze Active-Active na styku z internetem (1Gbps), dwa FortiWeb 1000B pracują w klastrze Active-Passive, jako urządzenia zapewniające bezpieczeństwo aplikacji oraz równomierne rozłożenie obciążenia na serwery z zainstalowanym systemem obsługi kandydatów. Dodatkowo, aby odciążyc maszyny, szyfrowanie SSL zostało „przeniesione” na FortiWeb. Ponadto, zastosowano firewalle aplikacyjne, które zabezpieczają system.

W najbardziej „gorącym” okresie rekrutacji Uniwersytet zanotował około 200 tysięcy sesji jednocześnie. W tym samym czasie z elektronicznego systemu rekrutacyjnego korzystało od 50 do 100 tysięcy użytkowników. System wytrzymał te obciążenia, opóźnienia były rzędu 1-2 sekund, także praktycznie niezauważalne z poziomu użytkownika w momencie wprowadzania danych i wypełniania formularzy on-line.

# Fortigate w Lotku

*W Totalizatorze Sportowym niedawno ukończono wdrożenie systemu ochrony sieci firmowej, zabezpieczającego sieć w centrali i kilkunastu oddziałach terenowych.*

**T**otalizator Sportowy realizuje państwowy monopol w dziedzinie gier liczbowych i loterii pieniężnych. To główne obszary działalności spółki. Jak każda firma, Lotto posiada narzędzia ochrony firmowej sieci. Jednymi z ostatnio wdrożonych są urządzenia UTM firmy Fortinet. Chronią one sieć operacyjną, niezbędną do działania spółki i połączenia oddziałów. Ochrona nie obejmuje sieci sprzedaży (np. połączeń do jedenastu tysięcy lottomatów), gdyż jest ona realizowana w outsourcingu.

## Nowy model zarządzania bezpieczeństwem

Wdrożono urządzenia Fortigate w jednostkach terenowych i klastrowane urządzenia z wyższej półki w centrali spółki. W skład systemu wchodzi również urządzenia do scentralizowanego zarządzania i zbierania informacji ze wszystkich urządzeń peryferyjnych tego samego producenta, z obsługą generowanych logów, w celu ich analizy. Spełniają one tę samą rolę, co dotychczas wykorzystywane rozwiązania innych firm. Sam model zabezpieczeń nie uległ diametralnym zmianom, mechanizmy są te same, ale istotnie zmienił się model zarządzania. Rozwiązania innych dostawców nie zapewniały takich możliwości, jakie daje implementacja UTM wraz z ich nowymi funkcjami odpowiadającymi obecnym wyzwaniom technicznym.

*„Dział informatyki nie odpowiada za napisanie i przygotowanie polityki bezpieczeństwa. On ją realizuje. Poprzednio eksploatowano systemy, które były zarządzane zarówno centralnie, jak i lokalnie.*

*Obecnie mamy jedno centralizowane miejsce, w którym można zaimplementować zdalnie politykę bezpieczeństwa w każdym oddziale” – mówi Jacek Włoda, dyrektor działu informatyki w firmie Totalizator Sportowy sp. z o.o.*

## Modernizacja WAN

Wdrożenie nie spowodowało wyłączenia dotychczasowych urządzeń zabezpieczających, ale zmieniono niektóre ich role i funkcje. Urządzenia UTM posiadają standardowe zabezpieczenia, takie jak antyspam, antyspyware, antywirus i filtrowanie stron WWW. Dodatkowo interesującą funkcją jest możliwość akcelerowania łączy. Jest to jeden z elementów zabezpieczeń, ich obszar pokrywa się w pewnym zakresie pomiędzy urządzeniami. Siecią łatwiej jest zarządzać korzystając z jednej konsoli, co było istotnym elementem w wyborze rozwiązania. *„Część funkcjonalności jest gwarantowana przez inne systemy. Dublowanie mechanizmów ma sens, ale nie wszędzie, gdyż wtedy sieć gdzieś może działać mniej sprawnie niż byśmy sobie życzyli” – mówi Jacek Włoda.*

Wdrożenie - dostarczonych przez Veracomp urządzeń Fortigate - wykonane przez firmę Bezpieczne IT odbyło się szybko i sprawnie. Wykorzystano prekonfigurowane urządzenia, które zainstalowano w centrali i oddziałach terenowych. Proces uruchomienia żądanej funkcjonalności zajął trzy tygodnie. Po zainstalowaniu urządzeń, centralnie zaimplementowano politykę bezpieczeństwa. Firma Bezpieczne IT przeprowadziła odpowiednie testy systemu i zmian, za nim rozpoczęła się produkcyjna jego eksploatacja. Dodatkowo infrastruktura sieci Totalizatora

**MARCIN MARCINIAK**



**Polityka bezpieczeństwa Totalizatora Sportowego w zasadzie się nie zmieniła. Uruchomiono jednak narzędzie ułatwiające jej wdrożenie i dystrybucję na całą sieć firmy.**

**JACEK WŁODA**, dyrektor działu informatyki w firmie Totalizator Sportowy

Sportowego wymagała przebudowy i odświeżenia. Przeprowadzono więc modernizację sieci WAN. Zamiast tradycyjnej topologii gwiazdy w technologii Frame Relay, Totalizator Sportowy wykorzystuje nowoczesną sieć MPLS, z zarządzaniem ruchem. Łączy pochodzą od różnych dostawców, gdyż spółka posiada kilkanaście oddziałów i nie wszędzie jeden operator posiadał wystarczające warunki techniczne i nie zawsze oferował akceptowalną cenę usług o żądanej jakości. Urządzenia UTM nie są jedynym mechanizmem ochrony, ale jednym z najważniejszych.

## Drobne problemy

Pewne drobne kłopoty przy wdrożeniu dotyczyły łączy, polegały na readresacji i wymagały konsultacji z operatorem, który świadczył usługi zarządzania siecią WAN. Gdy poprzednio wykorzystywane łączy przestawało działać, uruchamiane było łączy rezerwowe. Obecnie jedną funkcją, która czasami wymaga interwencji administratorów, jest filtrowanie stron WWW. Na bieżąco zajmują się aktualizacją dozwolonych stron internetowych.

*„Czasami zdarza się, że jakaś strona błędnie znajdzie się w kategoriach blokowania, pomimo tego, że nie ma z nimi nic wspólnego. Mechanizmy Fortigate czasami «wychodzą przed szereg», blokując niektóre strony, szczególnie dotyczy to polskiej części Internetu. W razie potrzeby możemy tę klasyfikację manualnie zmienić, usuwając lub przenosząc witryny do innej grupy. Zmiany możemy sprawnie dystrybuować do sieci spółki” – mówi Jacek Włoda.*

## Perspektywy rozwoju

Dział informatyki ma w planach aktualizację oprogramowania do wersji 4, której nowe funkcje – m.in. inspekcja ruchu sieciowego – są bardzo istotne dla Totalizatora Sportowego. W tej chwili trwają testy, które mają określić zyski i potrzeby w tej dziedzinie. Nie można jednak jeszcze ocenić, która z nowych opcji tej wersji systemu będzie najbardziej przydatna dla firmy. Planowane jest także wdrożenie mechanizmów klasy SIEM, które na podstawie zgłoszeń logów z urządzeń będących w sieci, w tym również typu UTM, będą mogły automatycznie informować służby informatyczne o zdarzeniach tak, aby administratorzy mogli podejmować szybkie działania. Ponieważ w dziale pracuje kilku specjalistów, nie zawsze mogą oni odpowiednio szybko podjąć wymagane działania w przypadku ataku dnia zerowego. Możliwość szybkiej analizy tego, co się w sieci dzieje umożliwi szybszą reakcję, nawet zanim cokolwiek się stanie. *„Projekt pilotażowy chcemy uruchomić jeszcze w tym roku. Rozwiązania SIEM są konieczne już teraz. Więc pewnie zapytania ofertowe z naszej strony pojawiły się już na rynku, czekamy na odpowiedzi” – dodaje Jacek Włoda.*

## CO WIDZĄ UŻYTKOWNICY

Jednym z założeń firmowej polityki bezpieczeństwa jest blokowanie dostępu do niepożądanych stron. Filtrowane są strony, które są skategoryzowane jako pornografia, źródła nieautoryzowanego oprogramowania, nielegalne multimedia, strony dotyczące narkotyków itd. Chociaż dostęp do takich zasobów Internetu monitorowano już wcześniej, obecnie uproszczono zarządzanie, jak i wprowadzono narzędzia dotyczące kontroli aktywności użytkowników. Plusem jest też strona informująca użytkownika o fakcie zablokowania dostępu i przyczy-

nach blokady, co ma walory edukacyjne pracowników. Dotychczas przy próbie otwarcia stron uznawanych za niepożądane, wyświetlany był błąd niedostępności serwisu. Obecnie jest to korporacyjna strona z logo firmy oraz z komunikatem mówiącym o tym, jaka strona została zablokowana i co było przyczyną. Sam komunikat zablokowania konkretnego serwisu działa prewencyjnie, gdyż użytkownicy mają świadomość, że nie jest to problem techniczny, ale polityka bezpieczeństwa w firmie naprawdę zabrania dostępu do takich stron.