POLITECHNIKA KRAKOWSKA

KLIENT

Politechnika Krakowska im. Tadeusza Kościuszki w Krakowie, która od 60 lat kształci kadrę inżynierską kraju, należy dziś do ścisłej czołówki technicznych ośrodków naukowych zarówno w Polsce, jak i za granicą. Na uczelni rozwijane są takie dyscypliny naukowe jak: architektura i urbanistyka, budownictwo i transport, elektrotechnika, inżynieria środowiska, mechanika, budowa i eksploatacja maszyn. W ofercie edukacyjnej Politechniki znajduje się 20 kierunków na 7 wydziałach: Architektury, Fizyki, Matematyki i Informatyki, Inżynierii Elektrycznej i Komputerowej, Inżynierii i Technologii Chemicznej, Inżynierii Lądowej, Inżynierii Środowiska oraz Mechanicznym. Mury Politechniki Krakowskiej opuściło już ponad 60 tys. absolwentów. Obecnie uczelnia kształci ponad 16 tys. studentów na studiach stacjonarnych i niestacjonarnych I i II stopnia oraz doktoranckich i podyplomowych, a także zatrudnia ok. 2 tys. pracowników. Studenci i wykładowcy wykorzystują do swojej pracy naukowej i dydaktycznej informacje zgromadzone w sieci oraz na bieżąco korzystają z internetu.

POTRZEBA

Sieć komputerowa Politechniki Krakowskiej składa się z ponad 2000 komputerów. Otwarta sieć uczelniana oferuje studentom i pracownikom swobodny dostęp do zasobów, dlatego notuje spory ruch wychodzący i przychodzący na poziomie 100 Mbit/ sekundę. Sieć jest ogólnodostępna, więc istnieje duże ryzyko utraty poufnych danych i łatwego rozprzestrzeniania się infekcji. Dlatego wymaga szczególnych zabezpieczeń, ponieważ są do niej podpięte komputery pracowników i 39 specjalistycznych laboratoriów, w których realizowane są ogólnopolskie i międzynarodowe projekty badawczo-rozwojowe oraz naukowe przedsięwzięcia innowacyjne. W laboratoriach wykonywane są analizy i ekspertyzy dla przemysłu oraz trwają prace nad nowymi rozwiązaniami chronionymi prawem własności intelektualnej. Badania przeprowadzane na aparaturze i urządzeniach laboratoryjnych Politechniki Krakowskiej są wykorzystywane w ramach projektu komercjalizacji wyników badań naukowych dla przemysłu. 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.

ROZWIĄZANIE

Wybrany system bezpieczeństwa firmy Fortinet składa się ze zintegrowanego urządzenia zabezpieczającego FortiGate-3810A oraz oprogramowania FortiAnalyzer. Rozwiązanie działa na platformie systemowo - sprzętowej składającej się z przełączników i routerów Allied Telesis.

FortiGate-3810A jest modularną platformą integrującą wiele funkcji bezpieczeństwa w jednym urządzeniu, które można aktywować stosownie do potrzeb organizacji. Początkowo uczelnia korzystała z podstawowych funkcji systemu Fortinet, w styczniu tego roku włączone zostały kolejne moduły zabezpieczające. Teraz, oprócz analizy ruchu WWW, Politechnika Krakowska ma uruchomione filtrowanie poczty elektronicznej, blokowanie ruchu P2P i ochronę przed spamem. Dla zwiększenia kontroli, FortGate-3810A pozwala na segmentację do setek wirtualnych domen (VDOM) 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 FortiAnalyzer'a - 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. FortiAnalyzer pobiera i przetwarza pełny zakres informacji dostarczanych przez system FortiGate dotyczących ruchu, zdarzeń, wirusów, ataków, e-maili. Ponadto, rozwiązanie realizuje zaawansowane funkcje zarządzania bezpieczeństwem, takie jak: kwarantanna antywirusowa, korelacja zdarzeń, ocena podatności na zagrożenia, analiza ruchu, czy archiwizacja treści. FortiAnalyzer informuje też na bieżąco o wydajności i wykorzystaniu sieci, co pozwala administratorom sieci uczelnianej na efektywniejsze planowanie i zarządzanie zasobami. System wyposażono w ponad 400 predefiniowanych raportów, które w czytelny sposób obrazują pracę sieci. Dodatkowo, każdy administrator może też budować własne zestawienia.

KORZYŚCI

Wdrożony system spełnił wymagania Politechniki Krakowskiej dotyczące zarówno bezpieczeństwa, jak i wydajności. Uczelniana sieć komputerowa musi służyć całemu środowiskowi akademickiemu. Dziś to jeden z najważniejszych sposobów zbierania informacji, wymiany doświadczeń i wyników badań naukowych. Platforma Fortinet wyposażona jest w cztery akcelerowane przez układ ASIC porty SFP. Rozwiązanie pozwala na monitoring sieci, nie powodując przy tym utraty jej wydajności, a więc użytkownicy nie odczuwają skutków kontroli bezpieczeństwa. Maksymalna przepustowość na poziomie zapory ogniowej wynosi 7 Gbps, dla IPS - 4 Gbps, a przy włączonej ochronie antywirusowej - 500 Mbps (HTTP).

Jeśli chodzi o względy bezpieczeństwa najbardziej przydatne okazały się kwestie związane z monitoringiem ruchu w sieci i utrzymaniem polityki wykorzystania zasobów. Pakiet FortGate-3810-A plus FortiAnalyzer pozwala łatwo zidentyfikować zagrożenia i wyciągnąć konsekwencje wobec osób naruszających prywatność i bezpieczeństwo poufnych danych. Według Rafała Przybylskiego, administratora sieci komputerowej Politechniki Krakowskiej, atutem wdrożonego systemu jest możliwość prewencji i szybkiej reakcji. „Dzięki dobrej analizie ruchu zarówno wychodzącego, jak i przychodzącego, można podjąć odpowiednie działania zarówno wobec użytkowników wewnętrznych, jak i zewnętrznych i w porę zareagować na wypadek ataku lub podejrzanego zachowania" – mówi Przybylski.

REALIZACJA

Projekt dla Politechniki Krakowskiej został zrealizowany przez Zakład Systemów Komputerowych ZSK Sp. z o.o., firmę dostarczającą kompleksowe rozwiązania informatyczne, teleinformatyczne oraz związane z automatyką budynkową. Sprzęt wraz ze wsparciem technicznym dostarczył Veracomp SA, autoryzowany dystrybutor Fortinet w Polsce.