Case Study

Urząd Marszałkowski Województwa Kujawsko-Pomorskiego

Opis sytuacji wyjściowej

Urząd Marszałkowski Województwa Kujawsko-Pomorskiego stanowi jednostkę organizacyjną samorządu województwa i jest aparatem pomocniczym dla realizowania zadań Marszałka Województwa Kujawsko-Pomorskiego oraz Zarządu i Sejmiku Województwa. Główna siedziba Urzędu znajduje się w Toruniu, natomiast jednostki podległe rozlokowane są w kilku miastach na terenie województwa: Bydgoszczy, Włocławku, Inowrocławiu i Grudziądzu.

Biorąc pod uwagę charakter działalności urzędu, kwestie bezpieczeństwa danych są dlań kluczowe. W związku z potrzebą zabezpieczenia danych poufnych, a także zapewnienia kompleksowej ochrony sieci komputerowej, odpowiedniej dla rozbudowanej infrastruktury, Urząd Marszałkowski zdecydował się na zakup zintegrowanego urządzenia UTM. Wcześniej korzystał z urządzenia firmy Checkpoint oraz rozwiązań OpenSource opartych na systemach z rodziny Linux. W związku z gwałtownym rozwojem Urzędu Marszałkowskiego konieczne było wdrożenie rozwiązania trwałego, o dużej skalowalności, takiego które będzie można dostosować do zmieniającej się sytuacji lokalowej i personalnej.

Poszukiwaliśmy systemu o szerokim zakresie funkcjonalności. Jednym wdrożeniem chcieliśmy objąć wiele obszarów związanych z bezpieczeństwem sieci zarówno lokalnej, jak i sieci WAN. Ważne dla nas było również, aby system posiadał rozwiązanie umożliwiające centralne zarządzanie wieloma urządzeniami oraz zbieranie i przechowywanie wszystkich informacji ze wszystkich urządzeń z możliwością tworzenia zaawansowanych raportów – mówi Wojciech Rzemykowski, Kierownik Biura Oprogramowania Urzędu Marszałkowskiego Województwa Kujawsko-Pomorskiego. *Poza wdrożeniem systemu bezpieczeństwa planowaliśmy zastosowanie systemu zarządzającego siecią bezprzewodową. Początkowo myśleliśmy nad osobnym rozwiązaniem dedykowanym tylko sieciom bezprzewodowym, jednak po zapoznaniu się z możliwościami, jakie oferuje FortiGate, podjęliśmy decyzję, że w tym obszarze oprzemy się na kontrolerze wbudowanym w to urządzenie, wykorzystując punkty dostępowe FortiAP. Po prawie dwóch latach użytkowania utwierdziliśmy się w przekonaniu, że była to słuszna decyzja* – dodaje Wojciech Rzemykowski.

Rozwiązanie

Wdrożenie zostało przeprowadzone przez firmę XCOMP, Złotego Partnera i jedną z trzech firm w Polsce o najwyższym statusie kompetencji technologicznych Partner of Excellence firmy Fortinet. Rozwiązanie wybrane zostało w drodze postępowania przetargowego, które poprzedzone zostało wnikliwymi badaniami dotyczącymi rozwiązań wielu producentów dostarczających urządzania klasy UTM. Oferta FORTINET zawsze osiągała wysoką pozycję w porównaniu z produktami innych producentów. O wyborze najkorzystniejszej oferty zadecydowała najniższa cena.

Wyzwanie

- wdrożenie elastycznego i trwałego rozwiązania zwiększającego wydajność sieci komputerowej oraz podniesienie poziomu bezpieczeństwa w perspektywie rozwoju urzędu

Cele

- zapewnienie bezpieczeństwa ochrony sieci komputerowej klasy UTM, które objęłoby swoim zasięgiem wszystkie lokalizacje UMWKP
- zarządzanie wszystkimi urządzeniami bezpieczeństwa sieci z jednego miejsca, przy jednoczesnym ograniczeniu do minimum czasu koniecznego do konfiguracji urządzeń oraz zmniejszeniu liczby punktów potencjalnej awarii
- zbudowanie sieci bezprzewodowej w oparciu o nowoczesny kontroler zintegrowany z systemem bezpieczeństwa

Rozwiązanie

FortiGate
FortiAnalyzer
FortiManager
FortiAP

Branża

Administracja publiczna

Bezpieczeństwo sieci jest priorytetem dla każdej organizacji, a szczególnie dla instytucji publicznych. Specjaliści FORTINET posiadają specjalistyczną wiedzę oraz bogate doświadczenie w zakresie oceny i optymalizacji bezpieczeństwa w rozproszonych, skomplikowanych architekturach sieci oraz w zakresie usług IT. Potrafią doskonale ocenić ryzyko, na jakie narażona jest dana instytucja oraz tak dopasować rozwiązanie, aby spełniało wymagania w zakresie bezpieczeństwa informacji – mówi Mariusz Rzepka, Fortinet Territory Manager na Polskę, Białoruś i Ukrainę.

Proces wdrożenia został podzielony na dwa etapy. W grudniu 2011 roku zakupiono dwa urządzenia FortiGate-621B, które skonfigurowano w klaster HA (Active-Active). Urządzenia wykorzystane zostały do zabezpieczenia sieci komputerowej w głównym budynku Urzędu Marszałkowskiego oraz do zabezpieczenia serwerów (w tym serwera poczty elektronicznej, serwerów www, serwera obiegu dokumentów i innych usług świadczonych przez Urząd). Wraz z tym zakupem dostarczone zostało urządzenie FortiAnalyzer- 1000C oraz FortiManager-100C.

W maju 2012 roku zrealizowany został drugi etap wdrożenia systemu bezpieczeństwa sieci komputerowej. Zakupione zostały urządzenia do pozostałych dziewięciu jednostek Urzędu Marszałkowskiego, zarówno na terenie Torunia, jak i do Przedstawicielstw Urzędu Marszałkowskiego w Bydgoszczy, Włocławku, Inowrocławiu i Grudziądzu. Zakupione zostały 2 urządzenia FortiGate-200B, 2 FortiGate-111C oraz 5 FortiGate-40C. Wszystkie urządzenia ustawione zostały tak, aby ich konfiguracja odbywała się za pomocą FortiManagera, a informacje o zdarzeniach z wszystkich urządzeń zbierane były w jednym miejscu, czyli wysyłane do FortiAnalyzer. Podczas prac wdrożeniowych opracowany został model konfiguracji zakładający, że ruch wychodzący z wszystkich lokalizacji odbywa się poprzez urządzenie FortiGate-621B, zlokalizowane w głównym budynku Urzędu Marszałkowskiego Województwa Kujawsko-Pomorskiego, co jeszcze bardziej ułatwiło zarządzanie i reagowanie na niebezpieczne zdarzenia.

Dodatkowo w drugim etapie wdrożenia zakupiono 12 sztuk FortiAP-220B. Sieć bezprzewodowa pokrywa swoim zasięgiem wszystkie sale konferencyjne w głównym budynku (6 sal), salę posiedzeń Sejmiku Województwa oraz salę posiedzeń Zarządu. Po jednym FortiAP umieszczono również w budynku Przedstawicielstwa we Włocławku oraz w innym budynku na terenie Torunia. Wszystkie urządzenia FortiAP podłączone zostały do FortiGate-621 i konfigurowane są z jednego miejsca. Sieć została skonfigurowana tak, by umożliwić pełen dostęp do sieci wewnętrznej pracownikom urzędu przy wykorzystaniu serwera Radius i mechanizmu SSO. Dla gości urzędu przygotowana została natomiast sieć z ograniczeniami, do której dostęp mają wszyscy odwiedzający pod warunkiem akceptacji regulaminu korzystania z sieci.

Urządzenia FORTINET rozmieszczone są w 10 punktach, połączonych ze sobą siecią VPN. Cały ruch odbywa się przez urządzenia FortiGate-621B zlokalizowane w głównym budynku Urzędu Marszałkowskiego w Toruniu. Wszystkie urządzenia konfigurowane są za pomocą FortiManager i podłączone do FortiAnalyzer. Dzięki takiemu kierowaniu przepływem danych cała polityka bezpieczeństwa skonfigurowana jest w jednym miejscu, co pozwala w krótkim czasie zdiagnozować nieprawidłowości i zdarzenia bezpieczeństwa występujące w sieci. Urządzenia FortiGate używane są zarówno do ochrony systemów serwerowych jak i do zabezpieczenia ruchu użytkownika z Internetem poprzez konfiguracje Firewall, Web Filtering, antywirus oraz DLP. Wykorzystywana jest również funkcja tuneli VPN, które łączą wszystkie lokalizacje. Dodatkowo wdrożone zostało uwierzytelnianie Two-Factor Authentication z wykorzystaniem hasła oraz FortiToken. Takie rozwiązanie pozwoliło wzmocnić poziom bezpieczeństwa.

Kompleksowe rozwiązanie firmy FORTINET zabezpieczyło sieć, z której na co dzień korzysta blisko 950 pracowników w 10 placówkach Urzędu Marszałkowskiego, rozmieszczonych na terenie całego województwa kujawsko-pomorskiego. Ochroną objęta została również praca administratorów sieci komputerowej.

Korzyści

Wdrożenie rozwiązania jednego producenta we wszystkich lokalizacjach Urzędu Marszałkowskiego pozwoliło w ramach wszystkich budynków na stworzenie wspólnej sieci dla wszystkich komputerów. Dzięki temu udało się scentralizować systemy informatyczne w jednej lokalizacji (głównej serwerowni) i co za tym idzie, zmniejszyć konieczność odbywania częstych wizyt w serwerowniach zlokalizowanych w innych budynkach. Pozwoliło to zaoszczędzić czas, jak również zmniejszyć liczbę punktów, w których mogą pojawić się awarie.

Wdrożenie zabezpieczające sieć internetową Urzędu Marszałkowskiego Województwa Kujawsko-Pomorskiego zostało zrealizowane przez firmę XCOMP, oferującą kompleksową obsługę IT oraz dostawy sprzętu i oprogramowania najwyższej klasy. Sprzęt wraz ze wsparciem technicznym dostarczył Veracomp SA, autoryzowany dystrybutor FORTINET w Polsce. Dodatkowo pracownicy działu IT odbyli szkolenia w certyfikowanym ośrodku szkoleniowym – Compendium Centrum Edukacyjne.

GLOBAL HEADQUARTERS
Fortinet Inc.
1090 Kifer Road
Sunnyvale, CA 94086
United States
Tel: +1.408.235.7700
Fax: +1.408.235.7737
www.fortinet.com/sales

EMEA SALES OFFICE
120 rue Albert Caquot
06560, Sophia
Antipolis, France
Tel: +33.4.8987.0510
Fax: +33.4.8987.0501

APAC SALES OFFICE
300 Beach Road 20-01
The Concourse
Singapore 199555
Tel: +65.6513.3730
Fax: +65.6223.6784

LATIN AMERICA SALES OFFICE
Prol. Paseo de la Reforma 115 Int. 702
Col. Lomas de Santa Fe,
C.P. 01219
Del. Alvaro Obregón
México D.F.
Tel: 011-52-(55) 5524-8480

Copyright© 2012 Fortinet, Inc. All rights reserved. Fortinet®, FortiGate®, and FortiGuard®, are registered trademarks of Fortinet, Inc., and other Fortinet names herein may also be trademarks of Fortinet. All other product or company names may be trademarks of their respective owners. Performance metrics contained herein were attained in internal lab tests under ideal conditions, and performance may vary. Network variables, different network environments and other conditions may affect performance results. Nothing herein represents any binding commitment by Fortinet, and Fortinet disclaims all warranties, whether express or implied, except to the extent Fortinet enters a binding written contract, signed by Fortinet's General Counsel, with a purchaser that expressly warrants that the identified product will perform according to the performance metrics herein. For absolute clarity, any such warranty will be limited to performance in the same ideal conditions as in Fortinet's internal lab tests. Fortinet disclaims in full any guarantees. Fortinet reserves the right to change, modify, transfer, or otherwise revise this publication without notice, and the most current version of the publication shall be applicable.