STORMSHIELD

PRZEMYSŁ

MIEJSKI ZARZĄD GOSPODARKI WODNEJ

OPTYMALIZACJA CYBERBEZPIECZEŃSTWA

Z UWZGLĘDNIENIEM OGRANICZEŃ OPERACYJNYCH

1,3 miliona

MIESZKAŃCÓW

60

GMIN

100

WIEŻ CIŚNIEŃ

Powszechna łączność

Bezpieczeństwo instalacji wodnych jest ważnym problemem dla miast i obszarów miejskich, który stał się poważniejszy ze względu na niemal nieustanną wymianę informacji między komputerami i sieciami operacyjnymi. Pomimo niezaprzeczalnych korzyści w zakresie optymalizacji zarządzania infrastrukturą, takie rozwiązania nierozerwalnie wiążą się ze zwiększeniem liczby możliwych wektorów ataku. W marcu 2016 roku pewien haker obrał za swój cel amerykańską stację uzdatniania wody pitnej, doprowadzając do zmiany stężeń środków chemicznych dodawanych do wody. Kilka miesięcy temu, w kwietniu 2020 roku rząd Izraela podał do publicznej wiadomości informację o serii cyberataków na swoje instalacje wodociągowe i stacje uzdatniania wody. Izraelska agencja ds. cyberbezpieczeństwa poleciła wszystkim pracownikom firm działających w sektorze energetycznym i wodnym zmianę haseł do wszystkich systemów podłączonych do Internetu. To nie jedyny przypadek. W 2021 roku hakerzy włamali się do stacji uzdatniania wody na Florydzie i zmienili poziom wodorotlenku sodu do poziomu zagrażającego życiu ludzi. Na szczęście w porę udało się naprawić skutki tego ataku i nie doszło do tragedii.

Informacje ogólne

Ważny ośrodek miejski położony w jednym z większych francuskich regionów, liczący około sześćdziesiąt gmin i przeszło milion mieszkańców, ogłosił przetarg na usprawnienie zarządzania siecią dystrybucji wody pitnej, która przez kilka lat pozostawała pod kontrolą i zarządem trzech prywatnych operatorów. Celem przetargu było ograniczenie liczby operatorów do zaledwie jednego podmiotu. Poza usprawnieniem obsługi miasto chciało również zmodernizować swoją architekturę IT podnosząc jednocześnie jej poziom bezpieczeństwa.

Dotychczasowi operatorzy stanęli wówczas do rywalizacji o zarządzanie usługami publicznymi w zakresie produkcji, transportu, magazynowania i dystrybucji wody pitnej na dużym obszarze regionu.

Jednym z wymogów postawionych przez miasto było wdrożenie architektury umożliwiającej zapewnienie niezależnej ochrony poprzez wdrożenie firewalli:

- w sieci IT,
- w centralnych węzłach sieci VPN,
- w systemach informatyki przemysłowej i bezpieczeństwa,
- w zdalnych lokalizacjach,

aby w ten sposób podnieść poziom bezpieczeństwa swoich sieci.

Wybrane rozwiązanie

Zwycięzcą przetargu był czołowy operator na rynku francuskim, który zwrócił się do spółki Stormshield z prośbą o pomoc w opracowaniu systemu zabezpieczeń tego środowiska przemysłowego.

Główne oczekiwania dotyczące zabezpieczeń globalnej architektury obejmowały kontrolę oraz filtrowanie całej komunikacji (głównie protokołu Modbus) z wykorzystaniem analizy DPI, a także wdrożenie rozwiązania IPsec VPN w celu zapewnienia bezpieczeństwa komunikacji.

Kompleksowe rozwiązanie dla środowiska przemysłowego

Bezpieczeństwo centrali zostało zapewnione dzięki instalacji zapór sieciowych oddzielających sieć biurową od instalacji operacyjnych, co pozwoliło dodatkowo na ich rozdzielenie na dwie oddzielne sieci – bezpieczeństwa i przemysłową, z których każda

jest chroniona przez grupę zapór sieciowych zaprojektowanych do pełnienia funkcji koncentratorów VPN. Rozwiązanie to umożliwia również łączność aplikacji z poszczególnymi wieżami ciśnień.

W celu zabezpieczenia sieci operacyjnej i bezpieczeństwa, a także zapewnienia stabilnego działania infrastruktury operator wybrał klaster zapór sieciowych SN3100 wyposażonych w podwójne zasilacze oraz dyski twarde skonfigurowane w macierzy RAID.

Wdrożenie objęło również trzy klastry zapór SN710 w obszarze koncentratorów sieci VPN (komunikacja IT/OT). Dzięki interaktywnym raportom z możliwością dostosowania przedstawianych danych do indywidualnych potrzeb klient ma bezpośredni dostęp do istotnych informacji na temat aktywności sieci i zdarzeń związanych z bezpieczeństwem w czasie rzeczywistym. System ochrony przed włamaniami (IPS) wykorzystuje szereg behawioralnych metod wykrywania zagrożeń i jest bezpośrednio zintegrowany z produktami, dzięki czemu może zapewniać skuteczną ochronę przed zagrożeniami zero-day przy zachowaniu wysokiej wydajności.

Dodatkowo każda ze 100 wież ciśnień została wyposażona w dwa klastry obsługujące elementy sieci bezpieczeństwa i przemysłowej, obejmujące zapory sieciowe SNi40 zapewniające bezpieczeństwo przepływów danych pomiędzy poszczególnymi lokalizacjami i aplikacjami. Zapory te zostały zaprojektowane z myślą o ochronie sterowników PLC i umożliwiają tworzenie tuneli IPsec VPN w celu zapewnienia łączności z centralą.

Asortyment produktów Stormshield dla podmiotów przemysłowych doskonale wpisał się w zróżnicowane potrzeby operatora. Ważną zaletą okazały się możliwości dostosowania zaproponowanego rozwiązania, dzięki czemu sprawdziło się doskonale zarówno w standardowych lokalizacjach, jak i środowiskach przemysłowych charakteryzujących się określonymi wymaganiami w zakresie temperatury, wilgotności, instalacji na szynie DIN czy zasilania. Ponadto zastosowanie wspólnego firmware w całej gamie urządzeń Stormshield Network Security oraz konsoli centralnego zarządzania Stormshield Management Center pozwala na zarządzanie wszystkimi zaporami z jednego miejsca.

Poza doskonałym stosunkiem jakości i zestawu funkcji rozwiązania do jego ceny, a także standardowymi zabezpieczeniami takimi jak segmentacja sieci, VPN itp., nasz klient był szczególnie zainteresowany możliwościami systemu ochrony protokołów przemysłowych przed włamaniami (IPS) charakteryzujących się najlepszymi na rynku możliwościami dostosowania ich konfiguracji, pozwalających na zwiększanie bezpieczeństwa wrażliwych systemów w miarę modernizacji infrastruktury.

Usługi dostosowane do złożonych środowisk przemysłowych

Utrzymanie i eksploatacja wymagały stawienia czoła wyzwaniom związanym z utrzymaniem ruchu 24/7/365, zapewnieniem dostępność usług dla użytkowników oraz rozwiązań dostosowanych do ciężkich warunków pracy. Wyłoniony w drodze przetargu operator nawiązał w związku z tym współpracę z firmą Stormshield, by wdrożyć dostosowany do potrzeb klienta system wsparcia, obejmujący:

- Wdrożenie procedury pozwalającej pracownikowi technicznemu nieposiadającemu umiejętności w zakresie sieci/bezpieczeństwa na wymianę uszkodzonej zapory sieciowej i wznowienia działania danego obiektu z zapewnieniem odpowiedniego poziomu bezpieczeństwa;
- Aktywację trybu bezpieczeństwa (bypass) w przypadku 5% obiektów, które nie zostały wyposażone w klastry, a wyłącznie w pojedynczą zaporę, aby w ten sposób zapewnić dostępność i bezpieczeństwo systemów przemysłowych;
- Asortyment profesjonalnych usług wspierających proces industrializacji konfiguracji obiektów pilotażowych.

Dzięki silnemu zaangażowaniu oraz porozumieniu pomiędzy wszystkimi podmiotami wdrożenie projektu przebiegło pomyślnie i terminowo na wszystkich etapach realizacji. Klient docenił również wdrożenie procedur odpowiadających na wymagania biznesowe w środowisku przemysłowym.

Nawiązane w ramach projektu relacje trwają nadal – firma Stormshield zrealizowała inne projekty wspólnie z operatorem, który korzysta z usług firmy w zakresie modernizacji swojej działalności i dostosowania swojej oferty w zakresie bezpieczeństwa IT/OT.

STORMSHIELD

Obecnie przedsiębiorstwa, instytucje rządowe i organizacje obronne na całym świecie stawiają czoła wyzwaniu jakim jest zagwarantowanie cyberbezpieczeństwa kluczowych elementów infrastruktury, danych i środowisk operacyjnych. Rozwiązania Stormshield posiadające najwyższe europejskie certyfikaty spełniają wszystkie wymagania IT i OT w zakresie ochrony bezpieczeństwa. Chcemy zapewniać bezpieczeństwo naszym klientom, by dzięki temu mogli skoncentrować się na swojej podstawowej działalności – to sprawia, że instytucje i operatorzy będą w stanie funkcjonować bez zakłóceń, a społeczeństwa będą mogły korzystać z wysokiej jakości usług. Wybierając Stormshield, wybierasz zaufanego europejskiego dostawcę usług i rozwiązań w zakresie cyberbezpieczeństwa. Więcej informacji: **www.stormshield.pl**