BUSINESS CASE

Producent nowoczesnych pojazdów kolejowych

INNERGO

aruba
a Hewlett Packard Enterprise company

Klient

Nasz Klient to jeden z najbardziej uznanych polskich producentów elektrycznych i spalinowych pojazdów pasażerskich oraz lokomotyw, a także pojazdów metra i tramwajów. Przedsiębiorstwo ma również ogromne doświadczenie w modernizacji taboru kolejowego. Pojazdy produkowane przez Klienta eksploatowane są aktualnie w Polsce i we Włoszech.

Pomimo rosnącej konkurencji firma stała się ostatnio liderem na rynku elektrycznych zespołów trakcyjnych oraz lokomotyw. Fenomen firmy wynika z niezwykłej umiejętności łączenia najnowszych osiągnięć technologicznych z doświadczeniem Zakładów, których tradycje sięgają aż XIX w. Nowoczesność stosowanych rozwiązań potwierdza m.in. tytuł „najbardziej innowacyjnej firmy kolejowej w Europie", który Klient zdobył w międzynarodowym konkursie ERCI Innovation Awards.

Potrzeby

Klient stawia na innowacyjne rozwiązania i rozumie konieczność nadążania za stale zmieniającymi się wymogami rynkowymi także w obszarach IT. Przedsiębiorstwo dostrzegło następujące potrzeby w zakresie modernizacji i optymalizacji infrastruktury informatycznej firmy:

- Potrzeba ułatwienia zarządzania i monitorowania sieci używanej w firmie oraz zwiększenia jej bezpieczeństwa. Wskazane było ujednolicenie, centralizacja i automatyzacja zarządzania oraz poprawa wydajności, niezawodności i dostępności sieci służącej pracownikom. Sprawą priorytetową było też podniesienie poziomu bezpieczeństwa systemu, co wynikało m.in. z konieczności spełnienia wymogów określonych w rozporządzeniu unijnym RODO.
- Chęć wyposażenia produkowanych zespołów trakcyjnych pasażerskich w nowoczesną infrastrukturę IT. Firma chciała zapewnić wszystkim pasażerom korzystającym z jej pojazdów dostęp do niezawodnej, wydajnej i bezpiecznej sieci na urządzeniach osobistych. Konieczne było uwzględnienie kompatybilności sieci z urządzeniami różnych producentów, o różnych systemach operacyjnych i zapewnienie jej przepustowości przy dużej liczbie użytkowników.

Firma chciała zapewnić wszystkim pasażerom korzystającym z jej pojazdów dostęp do niezawodnej, wydajnej i bezpiecznej sieci na urządzeniach osobistych.

Rozwiązanie

Aby sprostać oczekiwaniom klienta, Innergo Systems zaproponowało zintegrowane rozwiązanie technologiczne obejmujące dostawę i wdrożenie przełączników HPE Aruba, systemu do zarządzania siecią IMC (HPE IMC Standard) oraz systemu NAC (HPE Aruba ClearPass). Po przygotowaniu szczegółowego projektu technicznego, uwzględniającego także plan integracji nowych rozwiązań z zastaną infrastrukturą, rozpoczęto etap ich wdrożenia.

Przełączniki

W zakresie sprzętu konieczna była instalacja przełączników HPE Aruba. Filar sieci stanowi w tym rozwiązaniu **przełącznik szkieletowy**, który zbiera sygnał z przełączników dostępowych i zapewnia połączenia dla serwerów. Ponieważ jego działanie jest kluczowe dla całego systemu, cechuje go pełna redundantność, czyli jest w pełni zabezpieczony przed awarią. Gwarantuje to redundancja w każdym z jego elementów, a więc w przypadku niesprawności zarówno na poziomie kart liniowych, kart zarządzających, jak i zasilaczy ciągłość systemu pozostaje zachowana. Jako **przełączniki dostępowe** wykorzystano model HPE Aruba 2930F, który umożliwia łączenie maksymalnie 4 urządzeń w stos. To pozwala zarządzać nimi za pomocą jednego adresu IP i podnosi wydajność systemu.

O niezawodności rozwiązania świadczy dożywotnia gwarancja producenta, obejmująca przełącznik szkieletowy i przełączniki dostępowe. W jej zakres wchodzą również aktualizacje oprogramowania.

System zarządzający

Do zarządzania systemem użyto **HPE IMC Standard** (Intelligent Management Center), w skład którego wchodzi 50 licencji liczonych jako 50 adresów IP. Jedna licencja wystarcza do obsługi 6 urządzeń w stosie. Rozwiązanie służy uproszczeniu oraz automatyzacji zarządzania i monitorowania sieci, gdyż odbywają się one z jednego centralnego punktu. Jest to duże ułatwienie w administrowaniu siecią i zmniejsza jej złożoność, zwłaszcza że HPE IMC obsługuje urządzenia sieciowe różnych producentów. Zasilacze UPS, serwery czy routery brzegowe też mogą być monitorowane za pomocą tego narzędzia.

Jak to wygląda? Administrator może wyświetlać i monitorować sprzęt wedle urządzenia, adresu IP, topologii sieci albo wybranego niestandardowego widoku. Idąc dalej, rozwiązanie pozwala wyłapywać i zarządzać błędami, dokonuje konfiguracji elementów i prowadzi stały centralny monitoring sieci, analizując ruch bezprzewodowy i przewodowy. Jednocześnie nieprzerwanie monitorowana jest wydajność urządzenia i systematycznie tworzone są raporty.

Implementacja rozwiązania wpłynęła też pozytywnie na poziom bezpieczeństwa infrastruktury informatycznej firmy. Wzmożona została ochrona punktów końcowych, kontroli i widoczności. System wykorzystuje zdefiniowane alarmy, które włączają się w przypadku zagrożenia bezpieczeństwa sieci, np. kiedy ustawienia urządzeń nie są zgodne. Poza instalacją systemu w środowisku klienta, podłączeniem urządzeń i pełną konfiguracją, ważnym punktem wdrożenia była właśnie weryfikacja alarmów oraz ich tuning.

System kontroli dostępu

System kontroli dostępu do sieci (NAC) oparto na **HPE Aruba ClearPass**, czyli wirtualnym urządzeniu zabezpieczającym. Służy ono do centralnego uwierzytelniania urządzeń (w liczbie 5 tys.) obsługujących standard 802.1X, drukarek i telefonów (przez adres MAC). Dzięki zastosowaniu centralnej bazy oraz możliwości rozpoznawania urządzeń w przypadku prób niedozwolonych działań, system wykrywa podszywanie się pod urządzenia sieciowe. Równie skutecznie namierza aktywność urządzeń, które nie zostały wydane przez administratorów systemu.

Rozwiązanie Aruba gwarantuje wyjątkowo wysoki poziom bezpieczeństwa sieci przewodowej i bezprzewodowej, zarówno na etapie uwierzytelniania, autoryzacji, jak i kontroli dostępu użytkowników. Wśród wielu dodatkowych opcji dla klienta kluczowa okazała się realizacja dostępu dla gości oraz dostępu BYOD (Bring Your Own Device), czyli tzw. samoobsługowego dostępu do sieci na osobistym urządzeniu użytkownika przy użyciu certyfikatów. Dzięki funkcji Captive Portal strona logowania do sieci dla gości została spersonalizowana zgodnie z dyspozycjami klienta. Wszystko to przy zachowaniu najwyższych standardów bezpieczeństwa - polityki bezpieczeństwa zostają bowiem wymuszone zarówno dla użytkowników lokalnych, jak i mobilnych. Dochodzi do tego wysoka wydajność, niezawodność i skalowalność rozwiązania.

Po wdrożeniu rozwiązania przeprowadzono rygorystyczne testy odbiorcze systemu. Na koniec Innergo Systems przeszkolił pracowników klienta w zakresie obsługi nowego sprzętu i wdrożonych systemów, tak aby w pełni mogli oni wykorzystywać potencjał zastosowanych rozwiązań.

Czy wiesz że...

Rozwiązanie Aruba gwarantuje wyjątkowo wysoki poziom bezpieczeństwa sieci przewodowej i bezprzewodowej, zarówno na etapie uwierzytelniania, autoryzacji, jak i kontroli dostępu użytkowników.

Rezultat