Wdrożenie Scadvance XP® w PKP Energetyka

CASE STUDY

PKP Energetyka działa na polskim rynku od 2001 roku specjalizując się przede wszystkim w sprzedaży i dystrybucji energii elektrycznej dla kolejowych przewoźników, a także innym klientów biznesowych. Oprócz tego PKP Energetyka świadczy usługi elektroenergetyczne na terenie całego kraju i prowadzi sprzedaż paliw płynnych dla przedsiębiorstw kolejowych.

WYZWANIA

Plan rozwoju PKP Energetyka obejmuje modernizację infrastruktury sieci i wprowadzenia nowych technologii do analizowania charakterystyk ruchu sieciowego. Jego głównym celem było wdrożenie skutecznego narzędzia do identyfikacji zagrożeń cybernetycznych w sieci OT (ang. Operational Technology) w czasie rzeczywistym oraz bieżącej analizy charakterystyk sterowania obiektowego i wykrywania anomalii w ich działaniu. W efekcie system miał pozwolić na zwiększenie niezawodności infrastruktury oraz poziomu zabezpieczeń przed potencjalnymi atakami. Jednocześnie ważnym wymaganiem było dostosowanie rozwiązań do już wdrożonych i wykorzystywanych w PKP Energetyka technologii, a także zapewnienie możliwości audytu infrastruktury i generacji raportów zgodnie z wymaganiami prawnymi.

Do sterowania procesami przemysłowymi firma stosuje protokół BUSZ. Jest to unikalny protokół, wykorzystywany wyłącznie w polskiej branży energetycznej. Dlatego też, w projekcie mającym zwiększyć bezpieczeństwo systemu OT, PKP Energetyka nie mogła praktycznie skorzystać z uniwersalnych, dostępnych na rynku rozwiązań i narzędzi pozwalających na monitoring ruchu i analizy dotyczące jego charakterystyki.

ROZWIĄZANIE

Problem ten, bez nadmiernych kosztów, udało się rozwiązać korzystając z systemu do monitoringu sieci przemysłowej o nazwie Scadvance XP® firmy ICsec, który jest dostosowany do wszystkich typów sieci i różnorodnych protokołów stosowanych w systemach OT. System składa się z sond X1 odpowiedzialnych za „podsłuchiwanie" ruchu w sieci OT oraz serwera Scadvance XP®, którego zadaniem jest zbieranie danych z sond i analiza ruchu.

„Szukaliśmy dostawcy, który nie tylko zapewni obsługę protokołu BUSZ, ale również zaoferuje sniffery, które umożliwią włączenie do sieci bez zmiany jej parametrów elektrycznych, takich jak rezystancja. Oprócz tego firma ma tysiące urządzeń obsługiwanych przez kilkadziesiąt zewnętrznych firm i dlatego tylko kontrola systemu na najniższym poziomie pozwala na jego efektywne monitorowanie i wykrywanie nieprawidłowości, na które trzeba reagować" - powiedział Wojciech Kubiak - Dyrektor Biura Bezpieczeństwa Teleinformatycznego w PKP Energetyka.

Dlatego podjęto decyzję o pilotażowym wdrożeniu rozwiązania Scadvance XP® przystosowanego między innymi do obsługi protokołu BUSZ. Po przeprowadzeniu szczegółowych testów w dwóch lokalizacjach PKP Energetyka okazało się, że rozwiązanie spełnia wszystkie wymagania jakie postawiono dostawcy. Między innymi nie zakłóca i nie wpływa negatywnie na działanie sieci OT, zapewnia monitoring infrastruktury oraz wykrywanie praktycznie wszystkich urządzeń podłączonych do systemu w czasie rzeczywistym.

KORZYŚCI

Kompleksowe testy systemu Scadvance XP® wykazały, że system umożliwia:

- obserwowanie i archiwizację rzeczywistego ruchu pomiędzy sterownikami PLC,
- wykrywanie anomalii i cyberataków w monitorowanej infrastrukturze OT,
- identyfikację przekazywanych poleceń sterujących urządzeniami (między innymi przy wykorzystaniu protokołu BUSZ),
- prezentację informacji dotyczących transmisji danych pomiędzy sterownikami oraz anomalii występujących w sieci OT,
- wizualizację tzw. nodów, czyli wszystkich urządzeń logicznych biorących udział w komunikacji.

„Podczas wdrażania nie było żadnych problemów, ani zakłóceń w działaniu infrastruktury, a ma to duże znaczenie, bo obiekty kolejowe to krytyczna infrastruktura wymagająca ciągłości działania. Jednocześnie, zgodnie z zapewnieniami producenta, okazało się, że sondy X1 zapewniają pełną widoczność infrastruktury automatycznie wykrywając wszystkie podłączone do sieci urządzenia” mówi Wojciech Kubiak.

Warto też zauważyć, że PKP Energetyka zarządza infrastrukturą o krytycznym znaczeniu dla państwa i podlega przepisom ustawy o KSC (Krajowy System Cyberbezpieczeństwa). Dlatego ważne jest również to, że Scadvance XP® pomaga w zarządzaniu ryzykami oraz zapewnia obsługę występujących incydentów i ich odpowiednie dokumentowanie i zgłaszanie zgodnie z wymogami krajowych organizacji CERT.

IDS do zastosowań w sieciach przemysłowych

Scadvance XP® to specjalizowany system klasy IDS (Intrusion Detection System) przeznaczony do monitoringu sieci automatyki przemysłowej oraz wykrywania potencjalnych zagrożeń i anomalii w ruchu pomiędzy podłączonymi do niej urządzeniami. Jest to kompleksowe rozwiązanie pozwalające na wdrożenie systemu, które zapewnia bezpieczeństwo i kontrolę funkcjonowania sieci przemysłowych stosujących różne protokoły, przy użyciu zaawansowanych technologii m.in. sztucznej inteligencji (AI, ang. artificial intelligence), w tym uczenia maszynowego (ML, ang. machine learning).

Wykorzystując dane dostarczane przez sondy X1, oprogramowanie monitoruje sieci i zbiera informacje nie na ich brzegach, ale bezpośrednio z ich środka, analizując cały ruch przesyłanych w sieci pakietów. Opracowane przez ICsec interfejsy sprzętowe pozwalają na podłączenie systemu do praktycznie każdych rodzajów sieci automatyki przemysłowej, dzięki czemu powstaje wizualizacja wszystkich istniejących połączeń i urządzeń w czasie rzeczywistym w danej sieci.

Oprogramowanie informuje administratora sieci o zarejestrowanych zdarzeniach, wskazuje miejsce wystąpienia, a także cel ataku i jego prawdopodobną przyczynę.

Dzięki wykorzystaniu elastycznych modeli AI/ML, system jest zaś przygotowany do obsługi niestandardowych typów sieci przemysłowych i unikalnych aplikacji.

Podstawowe funkcje i cechy SCADVANCEXP

- obsługa protokołów z pełną analizą pakietów (DPI) i ekstrakcją danych,
- analiza NETFLOW/IPFIX dla protokołów IT,
- audyt sieci w czasie rzeczywistym,
- możliwość nagrywania rejestrowanego ruchu pakietów,
- wizualizacja mapy sieci,
- wykrywanie i prezentacja informacji o podłączonych do sieci urządzeniach,
- tworzenie mapy połączeń pomiędzy urządzeniami w sieci,
- możliwość śledzenia ruchu generowanego przez zewnętrznych dostawców,
- automatyczne wykrywanie anomalii, ataków i awarii,
- automatyczne budowanie dedykowanych modeli predykcyjno-analitycznych z osobnym zestawem parametrów dla każdego wykrytego połączenia logicznego z wykorzystaniem mechanizmów ML i AI,
- prezentacja statystyk ruchu w chronionej sieci OT / IT oraz raportów przedstawiających stan sieci.

ICsec S.A. jest liderem na rynku zabezpieczeń infrastruktury przemysłowej, w szczególności dla przedsiębiorstw z infrastrukturą krytyczną. ICsec zaprojektował i zbudował system Scadvance XP® (system klasy IDS, intrusion detection system), przeznaczony do monitoringu sieci OT. Rozwiązanie adresuje potrzeby związane z monitoringiem sieci automatyki przemysłowej, wykrywaniem potencjalnych zagrożeń i anomalii w ruchu pomiędzy podłączonymi do sieci urządzeniami.

ICsec S.A. | ul. Wichrowa 1A, 60-449 Poznań, Polska | tel. +48 506 931 953
biuro@icsec.pl | www.icsec.pl