Cyberbezpieczeństwo w przemyśle. Skuteczny monitoring sieci OT

SCADVANCE XP podnosi poziom bezpieczeństwa sieci przemysłowych. Pozwala wykryć anomalie oraz cyberzagrożenia w sieciach automatyki przemysłowej w czasie rzeczywistym. Informuje o niepożądanym zdarzeniu, wskazując miejsce wystąpienia zagrożenia, cel ataku i jego prawdopodobną przyczynę.

Systemy OT/SCADA zostały zaprojektowane na długo przed rozwojem bezprzewodowego internetu czy zdalnego dostępu do systemów i sieci. Projektowane były do długotrwałego działania, nie uwzględniano w tych rozwiązaniach aspektów bezpieczeństwa. Podstawowym zadaniem urządzeń automatyki przemysłowej była ich wieloletnia użyteczność. Dynamiczny rozwój technologii siłą rzeczy nie objął sfery bezpieczeństwa sieci OT.

Aktualizacja urządzeń w systemach OT jest dużo trudniejsza niż w systemach IT. W zakładach przemysłowych wymagana jest bowiem wysoka dostępność usług i narzędzi. Często zdarza się też, że aktualizacje sterowników i systemów SCADA powodują zatrzymanie programów systemów automatyki i tym samym błędne działania. Sterowniki i urządzenia komunikują się za pośrednictwem starych i niebezpiecznych protokołów. Można je podsłuchiwać lub hakować. Z drugiej strony, systemy OT/SCADA, przez wzgląd na oczekiwania biznesowe, są włączane do infrastruktury przedsiębiorstw w celu optymalizacji obsługiwanych przez nie procesów. Tym samym nie da się w pełni odizolować sieci, w której pracują, od środowisk publicznych.

Mocne strony SCADVANCE XP

- **Pasywność**
- **Skalowalność systemu**
- **Krótki czas wdrożenia**
- **Przewaga nad komputerami przemysłowymi**
- **Polska wersja językowa**
- **Odporność na czynniki zewnętrzne**
- **Polski zespół wsparcia**
- **Integracja z zewnętrznymi systemami**

Główne wyzwania, przed jakimi stoją dzisiaj zakłady przemysłowe, to:

01 Podatność na cyberzagrożenia, która jest spowodowana:

- brakiem znajomości aktualnej mapy sieci;
- komunikacją w sieci za pomocą przestarzałych protokołów;
- brakiem całkowitego oddzielenia sieci OT od IT;
- nieprawidłową aktualizacją sterowników.

02 Konieczność wypełnienia obowiązków wynikających z:

- ustawy o krajowym systemie cyberbezpieczeństwa;
- ustawy o zarządzaniu kryzysowym.

SCADVANCE XP

INTRUSION DETECTION SYSTEM DLA SIECI PRZEMYSŁOWYCH

Pasywna sonda X1 oraz kompletne rozwiązanie do monitoringu sieci OT

Polskie słowo „bezpieczeństwo" ma w języku angielskim co najmniej dwa odpowiedniki: „safety" i „security". Pierwsze z nich oznacza ograniczanie możliwości negatywnego wpływu systemu na jego otoczenie. Drugie natomiast określa ograniczenia związane z negatywnym wpływem otoczenia na system. Różnice można zobrazować na przykładzie budynku wyposażonego w wyjście awaryjne. Z punktu widzenia „safety" chcielibyśmy, aby wszystkie drzwi były otwarte, a dostępu do nich nic nie ograniczało. Bezpieczeństwo w rozumieniu „security" oznacza zamknięcie, a najlepiej zamurowanie niektórych przejść.

Różne priorytety uwidaczniają się, kiedy mówimy o bezpieczeństwie sieci przemysłowych. Sieci te są projektowane ze szczególnym uwzględnieniem ochrony życia, zdrowia i środowiska naturalnego. Przez dziesiątki lat były odizolowane, a „security" oznaczało stosowanie fizycznych środków zabezpieczeń przed niepowołanym dostępem. Nowe technologie i uwarunkowania biznesowe łączą zamknięte środowiska z sieciami IT oraz internetem. Dlatego bezpieczeństwo nabiera nowego wymiaru, a „security" może mieć wpływ na „safety". Nadszedł czas, abyśmy do słownika bezpieczeństwa sieci przemysłowych dodali definicję słowa „cyberbezpieczeństwo"...

Michał Horubała

Senior Security Consultant

W JAKI SPOSÓB SCADVANCE XP WSPIERA BEZPIECZEŃSTWO INFRASTRUKTURY KRYTYCZNEJ?

Monitoring sieci

SCADVANCE XP monitoruje sieci przemysłowe nie na ich brzegach (jak robią to standardowe systemy informatyczne), lecz zbiera informacje bezpośrednio z ich środka, analizując cały ruch przesyłanych pakietów. Zastosowane interfejsy sprzętowe pozwalają na podłączenie i monitorowanie wszystkich popularnych sieci automatyki przemysłowej. Dzięki temu osoby odpowiedzialne za bezpieczeństwo w przedsiębiorstwie mają w czasie rzeczywistym dostęp do wizualizacji informacji na temat wszystkich istniejących połączeń oraz urządzeń. Tym samym widzą od razu niepożądaną komunikację w sieci OT. System umożliwia wizualizację statystyk ruchu w chronionej sieci OT/IT za pomocą wbudowanego oraz konfigurowalnego dashboardu.

Zarządzanie aktywami

SCADVANCE XP wykrywa urządzenia podłączone do chronionej sieci na podstawie obserwowanego ruchu. W ten sposób powstaje mapa chronionej sieci w postaci grafu połączeń pomiędzy urządzeniami na poziomie urządzeń logicznych.

Wykrywanie anomalii i cyberataków

Dzięki analizie pakietów, wykorzystaniu charakterystyk NetFlow i zastosowaniu korelacji system pozwala na wykrycie anomalii (czyli niepożądanej pracy systemów sterowania i niepożądanych połączeń), w tym najbardziej niebezpiecznych cyberataków (np. zero day, man in the middle, blackhole attack). Rozwiązanie posiada mechanizmy pozwalające na zbudowanie modeli predykcyjnych przeznaczonych dla monitorowanej sieci (nie korzysta z gotowych modeli dostarczanych przez producentów), co pozwala na wyeliminowanie błędów false-positive. System oparty jest o moduły analityczne uczenia maszynowego (ML) oraz sztucznej inteligencji (AI) odpowiedzialne za wykrywanie sytuacji odbiegających od normy.

Monitoring procesów

SCADVANCE XP posiada moduł pozwalający na przechwycenie wartości zmiennych fizycznych występujących w procesach rzeczywistych. Pozwala także na śledzenie ich zmian niezależnie od systemu SCADA.

ICsec SA jest producentem rozwiązań z obszaru cyberbezpieczeństwa dla przemysłu, w szczególności dla przedsiębiorstw z infrastrukturą krytyczną. Zaprojektował i zbudował polski system SCADVANCE XP. Jest to system klasy IDS (Intrusion Detection System), przeznaczony do monitoringu sieci OT. Rozwiązanie odpowiada na potrzeby związane z monitoringiem sieci automatyki przemysłowej. W czasie rzeczywistym umożliwia wykrywanie potencjalnych zagrożeń i anomalii w ruchu między podłączonymi do sieci urządzeniami.

www.icsec.pl