Bezpieczeństwo technologii OT

Spis treści

Charakterystyka pracy środowisk OT i CPS

Systemy cyberfizyczne (*ang. Cyber-Physical Systems - CPS*) wykorzystywane w technologiach operacyjnych (*ang. Operational Technology - OT*) i infrastrukturze krytycznej stają się coraz częstszym celem cyberataków, co skutkuje znaczącymi stratami finansowymi, przerwami w świadczeniu kluczowych usług oraz potencjalnymi zagrożeniami dla bezpieczeństwa publicznego. W obliczu wzmożonego ryzyka bezpieczeństwo środowisk OT stało się kluczowym elementem strategii korporacyjnej, a wiele organizacji powierza tę odpowiedzialność kluczowej osobie w jednostce organizacyjnej odpowiedzialnej za bezpieczeństwo informacji (*ang. Chief Information Security Officer - CISO*). Zmiana ta wymusza na działach odpowiedzialnych za cyberbezpieczeństwo głębsze zrozumienie zagrożeń dla przemysłowych systemów sterowania (*ang. Industrial Control Systems - ICS*). Jednocześnie organizacje muszą opanować zaawansowane technologie i strategie obronne dedykowane środowiskom OT, aby chronić się przed rosnącym spektrum cyberataków skierowanych na infrastrukturę krytyczną.

Znaczenie bezpieczeństwa systemów cyberfizycznych i konwergencji IT/OT

Środowiska operacyjne (OT) różnią się fundamentalnie od klasycznych sieci informatycznych (*ang. Information Technology - IT*). Zamiast tradycyjnych serwerów, rozległy ekosystem OT składa się ze sterowników przemysłowych, sensorów, regulatorów oraz innych specjalistycznych urządzeń, które zarządzają procesami fizycznymi na linach produkcyjnych, w systemach energetycznych i infrastrukturze krytycznej. Właśnie dlatego bezpieczeństwo systemów cyberfizycznych wymaga unikalnego podejścia, które uwzględnia zarówno zagrożenia bezpieczeństwa, jak i operacyjne priorytety, takie jak ciągłość produkcji i bezpieczeństwo personelu. Jednocześnie wiele organizacji stoi wobec wyzwania konwergencji technologii IT i OT – integracji tradycyjnych systemów informatycznych z systemami operacyjnymi. Integracja ta przynosi wiele korzyści w zakresie efektywności i centralizacji zarządzania, lecz jednocześnie znacznie zwiększa powierzchnię ataku. Kluczowe osoby odpowiedzialne za bezpieczeństwo muszą zarządzać nie tylko rozproszonym zestawem dostawców zabezpieczeń, ale również pogodzić inne priorytety operacyjne takie jak ograniczone zasoby personelu zajmującego się cyberbezpieczeństwem oraz konieczność ochrony systemów, które często działają bez aktualnych poprawek (nakładek) bezpieczeństwa.

Ponadto zaawansowane technologie, takie jak sztuczna inteligencja (*ang. Artificial Intelligence - AI*) i rosnąca moc obliczeniowa, ułatwiają potencjalnym atakującym łamanie tradycyjnych zabezpieczeń i włamywanie się do systemów. Również rosnące wymagania regulacyjne — w tym dyrektywa unijna NIS2 (*ang. Network and Information Security Directive 2*) czy rozporządzenie CRA (*ang. Cyber Resilience Act*) komplikują krajobraz bezpieczeństwa dla organizacji zarządzających infrastrukturą krytyczną.

Wyzwania w zabezpieczaniu środowisk OT

Zespoły ds. cyberbezpieczeństwa odpowiedzialne za ochronę środowisk OT stają przed kilkoma istotnymi wyzwaniami. Po pierwsze, wiele urządzeń i systemów OT działa bez aktualnych poprawek bezpieczeństwa z powodu braku dostępnych aktualizacji od producentów lub ze względu na konflikty z priorytetami produkcyjnymi – przerwy w działaniu systemu mogą oznaczać znaczne straty finansowe. Po drugie, tradycyjne rozwiązania bezpieczeństwa opracowane dla środowisk IT nie są przystosowane do specyficznych wymagań systemów OT, które posiadają inną architekturę, protokoły komunikacyjne i kryteria niezawodności. Po trzecie, konsolidacja dostawców zabezpieczeń i wdrażanie technologii takich jak SSE (*ang. Secure Service Edge*) w środowiskach OT stanowi wyzwanie ze względu na wrażliwość krytycznych systemów i brak znormalizowanych rozwiązań zgodnych z modelem zerowego zaufania dla środowisk operacyjnych. Po czwarte rosnąca liczba wymagań legislacyjnych wywiera coraz większą presję w zakresie modernizacji zabezpieczeń i monitoringu instalacji o wysokim długu technologicznym co jest dużym wyzwaniem.

Główne elementy kompleksowego podejście do ochrony systemów OT

Skuteczna ochrona systemów OT wymaga wielowarstwowego podejścia, które łączy bezpieczną łączność sieciową, usługi bezpieczeństwa brzegu sieci i urządzeń końcowych oraz zaawansowane centrum zarządzania bezpieczeństwem (*ang. Security Operations Center - SOC*) dostosowane do specyfiki OT. Równie ważne jest wdrożenie szeregu procedur bezpieczeństwa oraz szkoleń pogłębiających wiedzę personelu na temat cyberbezpieczeństwa OT w przedsiębiorstwie. Podejście to powinno obejmować:

1. **Zabezpieczenie komunikacji sieciowej na styku środowisk OT/IT**

   Zapewnienie bezpiecznej konwergencji między systemami cyberfizycznymi i infrastrukturą IT przedsiębiorstwa jest obecnie niezbędne dla większości

organizacji. Wymaga ona zastosowania zaawansowanych zapór sieciowych nowej generacji (*ang. Next-Generation Firewall - NGFW*), które muszą rozpoznawać zarówno rodzaj, jak i kontekst monitorowanej komunikacji, aby skutecznie chronić połączone systemy OT.
Efektywna ochrona wymaga stosowania zapór NGFW obsługujących specjalistyczne sygnatury umożliwiające interpretację protokołów przemysłowych (takich jak IEC104, Profinet czy OPC UA) oraz wyposażonych w moduły IPS (*ang. Intrusion Prevention System*) i AV (*ang. Antivirus*) zdolne do blokowania zewnętrznych ataków na instalacje OT.
Dodatkowo urządzenia te muszą pracować niezawodnie w wymagających warunkach środowiskowych charakteryzujących się szerokim zakresem temperatur, zapyleniem oraz ekspozycją na wilgoć i drgania. W takich warunkach zaleca się wybierać warianty zapór NGFW ze wzmocnioną konstrukcją, które zapewniają wysoką niezawodność tego krytycznego elementu infrastruktury przez wiele lat.

2. **Segmentacja i mikrosegmentacja sieciowa**

   Dzielenie sieci OT na mniejsze, izolowane podsieci znacznie ogranicza rozprzestrzenianie się zagrożeń w przypadku naruszenia bezpieczeństwa i zwiększa odporność systemu na potencjalne ataki zarówno z zewnątrz, jak i z wewnątrz sieci. Zgodnie z normą IEC 62443 dobrą praktyką jest segmentacja sieci OT na strefy funkcjonalne, które mogą działać autonomicznie nawet w przypadku kompromitacji jednej z sąsiednich stref. Ruch między strefami jest nadzorowany poprzez zapory NGFW lub zarządzalne przełączniki sieciowe ze zdefiniowanymi sieciami wirtualnymi (ang. Virtual Area Network - *VLAN*).

   W przypadku konieczności wdrożenia szczególnie ścisłej kontroli ruchu na niższych poziomach sieci można zastosować mikrosegmentację. Technika ta umożliwia precyzyjne określenie dozwolonych ścieżek komunikacji między wybranymi urządzeniami już na poziomie przełączników dostępowych, zapewniając tym samym bardziej szczegółową kontrolę i hermetyzację ruchu między krytycznymi urządzeniami w instalacjach OT.

3. **Wirtualne wprowadzenia poprawek (patchowanie)**

   Ze względu na częsty brak możliwości regularnego instalowania aktualizacji na urządzeniach OT [np. sterownikach PLC (*ang. programmable logic controller*), regulatorach], organizacje muszą wdrażać proaktywne mechanizmy ochrony kompensacyjnej. Wirtualne wprowadzanie poprawek to technika "osłaniająca" luki

w zabezpieczeniach – pozwala na blokowanie na poziomie sieci prób wykorzystania znanych podatności bez konieczności zatrzymania urządzenia i aktualizacji jego oprogramowania. Nowoczesne platformy zabezpieczeń, takie jak NGFW, oferują tysiące reguł wirtualnych poprawek chroniąc przed zagrożeniami podatne urządzenia OT.

4. **Ochrona punktów dostępowych na brzegu sieci**

   Rozszerzenie modelu zerowego zaufania na środowiska OT wymaga integracji zarządzania dostępem uprzywilejowanym (*ang. Privileged Access Management - PAM*) i kontroli dostępu do sieci (*ang. Network Access Control - NAC*). Systemy te weryfikują tożsamość oraz zapewniają, że tylko autoryzowani użytkownicy oraz urządzenia mogą uzyskać dostęp do wrażliwych zasobów OT.
   Nowoczesne rozwiązania takie jak SASE (*ang. Secure Access Service Edge*), ZTNA (*ang. Zero Trust Network Access*), PAM umożliwiają bezpieczny i kontrolowany dostęp do sieci korporacyjnej. Są szczególnie ważne przy udzielaniu dostępu pracownikom i podwykonawcom pracującym zdalnie, chroniąc krytyczne systemy przed zagrożeniami związanymi z niezaufanymi sieciami i urządzeniami.
   Uwierzytelnianie użytkowników uzyskujących dostęp do sieci OT powinno obowiązkowo obejmować uwierzytelnianie wieloskładnikowe (*ang. Multi-Factor Authentication - MFA*). Mechanizm MFA zapewnia dodatkową warstwę ochrony przed dostępem nieautoryzowanym i znacznie wzmacnia bezpieczeństwo całego systemu.

5. **Pasywne systemy monitoringu ruchu sieciowego IDS (*ang. Intrusion Detection System*), NDR (*ang. Network Detection and Response*)**

   Obserwacja i analiza ruchu sieciowego w systemach OT stanowi zadanie wymagające, ale jednocześnie umożliwiające głębokie zrozumienie komunikacji sieciowej. Ze względu na to, że ruch w środowiskach OT jest zazwyczaj nieszyfrowany, analiza jest bardziej przejrzysta, choć jednocześnie systemy są bardziej narażone na ataki typu MITM (*ang. Man-in-the-Middle*). Brak szyfrowania ułatwia integrację systemów OT, jednak zmniejsza ich bezpieczeństwo.
   Systemy monitoringu sieci OT muszą rozumieć kontekst komunikacji przemysłowej na takim samym poziomie co zapory sieciowe, a nawet bardziej zaawansowany. Wykorzystanie sygnatur DPI (*ang. Deep Packet Inspection*) pozwala tym systemom budować zaawansowane wzorce behawioralne z użyciem sztucznej inteligencji i uczenia maszynowego (*ang. Machine Learning / Artificial Intelligence - ML/AI*),

umożliwiając obserwację odchyleń od wybranych wartości bazowych w komunikacji między elementami systemów OT.
Kluczową cechą systemów monitoringu jest zdolność do pracy na pełnej kopii ruchu sieciowego, zapewniając operatorom kompletny przegląd wszystkich procesów zachodzących w sieci OT oraz zidentyfikowanych urządzeń. Dane z tych systemów są krytyczne dla centrów SOC OT, umożliwiając wykrywanie i reagowanie na zagrożenia w czasie poniżej jednej sekundy, co zapewnia natychmiastową ochronę środowisk OT.

6. **Zabezpieczanie stacji roboczych i serwerów w OT**

W wielu systemach OT krytyczną rolę pełnią stacje operatorskie, panele HMI (*ang. Human-Machine Interface*), serwery SCADA (*ang. Supervisory Control And Data Acquisition*), historiany i stacje programistyczne. Niestety bardzo często urządzenia te działają na już nieobsługiwanych systemach operacyjnych (takich jak Windows XP czy Windows 7), które zawierają liczne luki bezpieczeństwa, których nie można bezpośrednio wyeliminować. Dodatkowo serwery i stacje robocze w środowiskach OT zazwyczaj nie są przystosowane do instalowania standardowego oprogramowania antywirusowego (AV) lub oprogramowania typu EDR (*ang. Endpoints Detection and Response*), ze względu na ograniczone zasoby obliczeniowe ilość pamięci.

Wyzwania te wymagają wdrożenia specjalistycznego oprogramowania zabezpieczającego urządzenia końcowe – rozwiązań AV lub EDR zoptymalizowanych do pracy na starszych systemach operacyjnych. Oprogramowanie to musi pracować z minimalnym zużyciem zasobów systemowych oraz nie może wpływać negatywnie na działanie krytycznych systemów sterowania. Jednocześnie musi zapewniać skuteczną ochronę przed zagrożeniami oraz ciągłe monitorowanie aktywności chronionych urządzeń.

7. **Pułapki sieciowe imitujące systemy przemysłowe**

W przypadku, w którym mamy ograniczone możliwości monitorowania ruchu sieciowego w infrastrukturze OT [zamknięte systemy DCS (*ang. Distributed Control Systems*), brak możliwości wykonania kopii ruchu, niezarządzane przełączniki warstw dostępowych] skutecznym rozwiązaniem pozwalającym na monitorowanie atypowej aktywności w sieci OT są pułapki sieciowe, tzw. honeypot-y. Honeypot-y symulują popularne urządzenia przemysłowe, które powszechnie występują w sieciach OT. Pułapki w sposób aktywny reagują na akcje wykonywane

przez skanery sieciowe, reagując w sposób analogiczny do autentycznych urządzeń przemysłowych (np. te same otwarte porty i usługi sieciowe) dzięki czemu mogą zostać zinterpretowane przez atakujących jako prawdziwe urządzenia OT. Informacje zgromadzone przez pułapki sieciowe powinny być przekazywane do zespołów SOC w celu szybkiej identyfikacji naruszeń bezpieczeństwa oraz ewentualnej odpowiedzi na incydenty.

8. **Centra operacji bezpieczeństwa (SOC) zoptymalizowane pod kątem OT**

Efektywność działania centrów SOC w obszarze OT wymaga integracji danych z wielu różnorodnych źródeł (m.in. zapór sieciowych, systemów monitorowania sieci czy punktów końcowych) co umożliwia korelację zdarzeń i wykrywanie zagrożeń oraz pozwala na automatyzację reakcji na incydenty.
Źródła zintegrowane w ramach SOC powinny w jak największym stopniu uwzględniać kontekst związany z systemami OT, które mają chronić (np. DPI protokołów przemysłowych, wzorce behawioralne sieci OT).
Platformy nadrzędne stosowane w SOC, takie jak kolektory, systemy SIEM (*ang. Security Information and Event Management*) czy SOAR (*ang. Security Orchestration, Automation and Response*), powinny obsługiwać mapę topologii sieci zgodnie z modelem Purdue oraz macierz MITRE ATT&CK dla systemów ICS pozwalające zespołom SOC na szybką i skuteczną identyfikację zagrożeń, taktyk i technik ataku oraz odparcie tego ataku.
Integracja z zaawansowanymi technologiami monitoringu ruchu sieciowego OT jak systemy IDS czy NDR, jest kluczowa dla ochrony całego systemu i powinna być obligatoryjna.
Rozwiązania SIEM i SOAR stosowane w SOC OT powinny również oferować łatwą i płynną integracje z dostawcami rozwiązań specyficznych dla OT opisywanych wyżej oraz umożliwiać wykorzystanie predefiniowanych playbook-ów dostosowanych do potrzeb reagowania w środowiskach OT oraz infrastrukturze krytycznej, gdzie schematy operacyjne są inne niż w klasycznych systemach IT.
Innym istotnym aspektem jest zdolność systemów osadzonych w SOC do generowania raportów. Raporty te powinny być zdolne do weryfikacji aktualnej zgodności systemu OT z wymaganiami wynikającymi z norm oraz standardów branżowych takich jak IEC62443, NIST 800-82, NERC CIP czy zgodności względem wymogów dyrektywy NIS2 i ustawy o KSC (Krajowy System Cyberbezpieczeństwa).

9. **Regularne szkolenia i audyty systemów i procedur bezpieczeństwa**

W każdej metodologii związanej z cyberbezpieczeństwem podstawowymi obszarami do zaadresowania, poza technologią, pozostają ludzie i procesy. Nie inaczej jest w przypadku systemów OT.
Cyberbezpieczeństwo OT pozostaje procesem, którego częścią jest ciągła ocena skuteczności wprowadzonych procedur, systemów i rozwiązań cyberbezpieczeństwa oraz ich ciągłe dostrajanie, modyfikacja i ewolucja pozwalające dostosować się do bieżących zagrożeń. Każde przedsiębiorstwo posiadające systemy OT jest zobowiązane do przeprowadzania regularnych audytów również ze względu na zachowanie zgodności z wymaganiami prawnymi wynikającymi z ustawy o KSC oraz dyrektywy NIS2.
Kluczowym elementem jest również proces ciągłej edukacji pracowników obsługujących systemy OT na temat ryzyk oraz cyber-higieny. Jest on równie krytyczny jak aktualność systemów technicznych zabezpieczeń i stanowi nieodzowny komponent całościowej strategii bezpieczeństwa, co jest wyraźnie wskazane w ustawie o KSC.

10. **Centralizowanie zarządzania systemami bezpieczeństwa**

W poprzednich punktach wskazanych zostało kilkanaście różnych systemów i rozwiązań technicznych budujących cyberbezpieczeństwo środowisk OT. Mnogość tych rozwiązań bez ich spójnej i efektywnej integracji może pomimo dużego potencjału nie spełnić pokładanych w nich oczekiwań ze względu na skomplikowaną i czasochłonna obsługę oraz konieczność ciągłego przełączania się pomiędzy nimi.
W celu pełnego wykorzystania tych rozwiązań należy pamiętać o jakościowej integracji lub skorzystaniu z rozwiązań platformowych oferujących natywną integrację systemów oraz automatyzację reakcji nawet na niskich poziomach.
W takim wariancie, poza uzyskaniem wysokiej efektywności detekcji i szybkości reakcji na incydenty, uzyskujemy jedną z najcenniejszych rzeczy dla centrów SOC – czas który możemy poświęcić na głębszą inwestygację incydentów czy mitygację skutków ataków.