

Kryteria doboru rozwiązań z zakresu cyberbezpieczeństwa sieci przemysłowych. Perspektywa biznesowa i techniczna

Zuzanna Wieczorek, Stefan Bednarczyk, Marcin Skórka - Tekniska

Streszczenie

Zagrożenie cyberatakami rośnie. To fakt, o którym można usłyszeć i przeczytać we wszystkich najważniejszych raportach i publikacjach dotyczących stanu cyberbezpieczeństwa infrastruktury krytycznej. Co kilka tygodni jesteśmy informowani o kolejnych atakach na infrastrukturę krytyczną lub branżę finansową, z których post-factum można wyciągnąć już tylko wnioski na temat (nie)skuteczności lub braku koniecznych zabezpieczeń. Na szczęście świadomość tego faktu również rośnie. Wiele firm oferuje już narzędzia dedykowane do zaprojektowania odpowiedniego rozwiązania i architektury cyberbezpieczeństwa dla przemysłowych sieci OT, które swoją specyfiką odbiegają od rozwiązań świata IT Telecom.

Podstawą jest dobre zaprojektowanie architektury, dopasowanej do naszych potrzeb. Tylko takie podejście sprawi, że nie będzie ona dodatkowym obciążeniem, paraliżującym lub utrudniającym realizację zadań. Staramy się znaleźć odpowiedź na pytania:

Czemu te różnice są tak istotne w aspekcie cyberbezpieczeństwa? Gdzie leżą podstawowe problemy planowania i wdrażania odpowiednich polityk bezpieczeństwa i architektury zabezpieczeń? Jak pogodzić perspektywę techniczną z perspektywą biznesową? Z jakimi kosztami musimy się liczyć? Jakie są warianty utrzymania i jakie kompetencje musimy nabyć w obrębie naszego zespołu lub zlecić na zewnątrz, jeżeli jest to zgodne z polityką firmy?, i w końcu: Które, spośród wielu, rozwiązanie będzie najlepsze dla naszego systemu i jakie postawić przed nim wymagania?

Pokazujemy przykłady wybranych rozwiązań technicznych z krótkim komentarzem, wskazującym na to, czym dobrze jest się kierować realizując konkretny cel związany ze zmniejszeniem ryzyka i podwyższeniem poziomu cyberbezpieczeństwa naszego systemu. Pokazujemy też z czym musimy się liczyć zarówno w aspekcie technicznym jak i biznesowym, podejmując decyzję o wyborze określonego rozwiązania.

1. Wstęp

W tym krótkim referacie staramy się nie powielać powtarzanych w kółko informacji, stawiamy natomiast pewne tezy i adresujemy problemy, które widzimy działając od wielu lat w różnych obszarach sieci przemysłowych. Dzielimy się doświadczeniami własnymi, tj. Zespołu ds. Cyberbezpieczeństwa firmy Tekniska Polska Sp. z o.o., jak również naszych partnerów: ScadaFence, RadiFlow, OTNSystems, Westermo, GE Digital, Teldat, MBconnect i pozostałych, zaangażowanych w tematykę cyberbezpieczeństwa systemów przemysłowych. Możecie się Państwo z nami zgodzić lub nie - zapraszamy do dyskusji, bo tylko z niej i bieżącej wymiany doświadczeń w różnych obszarach wynikać będą dobre rozwiązania. Jeżeli zauważą Państwo pewne truizmy, prosimy o wybaczenie, ale uważamy, że są na tyle istotne aby powtarzać je, za każdym razem gdy istnieje ku temu okazja.

Każde rozwiązanie cyberbezpieczeństwa musi być dobrane do konkretnych potrzeb i architektury systemu i wybrane na podstawie solidnej analizy bezpieczeństwa istniejącej infrastruktury, którą chcemy zabezpieczyć. Są rozwiązania łatwe i relatywnie szybkie do wdrożenia, funkcjonujące w obrębie fragmentu systemu oraz takie, które wymagają tygodni implementacji i współpracy różnych działów w obrębie danego przedsiębiorstwa, aby zapewnić mu kompleksową ochronę i realizację wyznaczonych polityk i procedur bezpieczeństwa.

2. Działy IT i OT – różnice do pogodzenia?

2.1. Priorytety i charakterystyka

Priorytety i charakterystyka infrastruktury sieciowej systemu OT to przede wszystkim niezawodność (dostępność) i pełna przewidywalność z punktu widzenia procesu i aplikacji krytycznych. Żadne mechanizmy bezpieczeństwa nie powinny ingerować w proces w sposób bezpośredni ani go spowalniać. Sieci OT są relatywnie małe, rozproszone, w formie „autonomicznych wysp automatyki” w obrębie przedsiębiorstwa. Wykorzystują specyficzne aplikacje i dedykowane protokoły przemysłowe (np.: sterowania to często szybka komunikacja punkt-punkt, punkt-wielopunkt), w związku z czym inne będą charakterystyki ruchu. Komunikacja nie wymaga zwykle dużych przepustowości, nie toleruje jednak dużych, zmiennych opóźnień, przerw w transmisji powyżej kilkudziesięciu ms. W przemysłowych sieciach pakietowych, w warstwie 4 najczęściej wykorzystywany jest protokół UDP. Często wykorzystuje się różne technologie transmisji: np.: połączenia szeregowo, Ethernet przemysłowy, SDH, extendery, adaptory, koncentratory.

Sieci OT często, z założenia nie miały punktu styku z sieciami zewnętrznymi, a jeżeli miały, to bardzo ograniczony. W ostatnich latach widać jednak znaczącą zmianę tej sytuacji i coraz częściej istnieją połączenia sieci OT z sieciami zewnętrznymi.

Od sieci OT wymagany jest bardzo długi „czas życia” i obsługi utrzymaniowej jeszcze po tym okresie, podczas gdy w sieciach IT częstotliwość zmian technologicznych i sprzętowych będzie wielokrotnie wyższa. Sieci OT pracują w trudnych warunkach środowiskowych, tj. często narażone są na zakłócenia elektromagnetyczne, pracę w ekstremalnych temperaturach, zapylenie etc..

Sieci OT wymagają łatwości obsługi, uruchomienia i serwisu/utrzymania. Działy Automatyki, które najczęściej są odpowiedzialne również za utrzymanie sieci OT, muszą zapewnić ciągłość i poprawne działanie procesu, bo za to ponoszą odpowiedzialność i na tym się znają. Sieć jest elementem, który „musi działać”, ale nie powinien nadmiernie „obciążać” i wymagać specjalistycznych kompetencji w przypadku serwisu, podstawowej diagnostyki, czy uruchomienia. W sieciach OT urządzenia końcowe to elementy automatyki, a użytkownicy to pojedyncze osoby z utrzymania i serwisu, zwykle systemy automatyki są autonomiczne w normalnym trybie swojej pracy.

W sieciach IT priorytetem jest natomiast przede wszystkim skalowalność, przepustowość, łatwiejsze i preferencyjnie scentralizowane zarządzanie infrastrukturą. Wykorzystywane aplikacje to najczęściej poczta email, aplikacje biurowe, bazy danych, systemy CRM i ERP, inne systemy związane ze wspomaganiem zarządzania organizacją lub specjalne aplikacje umożliwiające realizację zadań użytkowników/klientów/pracowników. Sieci IT mają bardzo dużą i zmienną liczbę użytkowników korzystających głównie z komputerów z różnymi systemami operacyjnymi. Użytkownicy mogą się często zmieniać, co wymaga odpowiednich rozwiązań związanych z autentykacją, autoryzacją, zarządzaniem hasłami etc... IT będzie się skupiać na określaniu praw i zapewnianiu dostępu tym użytkownikom do poszczególnych zasobów firmy. Będzie pilnować, aby ten dostęp realizowany był w sposób bezpieczny, aby systemy operacyjne były aktualizowane i zabezpieczone oprogramowaniem antywirusowym, aby chronić dane poufne. W wybranych przypadkach będzie logował wszelkie działania poszczególnych użytkowników. Działy IT będą dbać, aby dane krytyczne z poziomu widzenia firmy były przechowywane na odpornych na awarie, jak i ataki klastrach serwerów w centrach danych lub dobrze zabezpieczonych serwerowniach. Zespoły IT będą naturalnie zaznajomione z tematyką wydajnego, dynamicznego routingu, firewallami typu UTM (filtrujące aplikacje oraz treść do której można mieć dostęp, np.: za pośrednictwem przeglądarek oraz protokołów http i https), ochroną antywirusową stacji roboczych. Jest z tym powiązane pewne przyzwyczajenie do dużych wydajności i sztywnych procedur, które potrzebne lub nie, nie są dużym problemem na tym poziomie, ze względu na brak ograniczeń sprzętowych jeżeli chodzi o możliwości stosowania drogich podzespołów oraz wymuszonego chłodzenia mechanicznego. W sprzęcie dedykowanym do sieci OT będą występować ograniczenia wydajności, nie jest to jednak problemem ponieważ parametry wydajności sieci OT nie muszą być tak duże, biorąc pod uwagę, że jeszcze niedawno ta sama transmisja była realizowana w oparciu o technologie takie jak łącza szeregowo, pętle prądowe, modemy telefoniczne. Ważniejsza będzie konstrukcja bez elementów mechanicznych i bezprzerwowa praca (np.: szybkie przełączanie na zapasową ścieżkę w redundantnej topologii w warstwie 2).

W obydwu przypadkach, poziom usług SLA, dostępność, bezpieczeństwo, poufność i integralność danych są oczywiście bardzo istotne, mimo, że definiowane na innych poziomach i traktowane z innym priorytetem. W klasycznym IT awaria będzie miała przede wszystkim skutek finansowy i wizerunkowy, co może skutkować np. utratą zaufania klientów. Natomiast w sieciach przemysłowych atak może mieć zarówno niezwykle dotkliwy skutek finansowy i wizerunkowy, ale przede wszystkim stwarzający zagrożenie funkcjonowania krytycznej infrastruktury (np.: dostępu do energii, paliw, wody, etc.) co przekłada się na zagrożenia dla środowiska, zdrowia i życia ludzkiego.

2.2. Skala

Korporacyjne sieci IT zbudowane są często z setek urządzeń (switchy, routerów, firewalli, serwerów, komputerów z różnymi systemami operacyjnymi itd.). Sieci te mają zapewnić użytkownikom dostęp do sieci Intranet i Internet oraz sprawne funkcjonowanie narzędzi i aplikacji. Struktura jest zwykle dynamiczna - administratorzy muszą na bieżąco nadawać i zmieniać prawa dostępu do różnych zasobów, dodawać i usuwać użytkowników, dbać o zapewnienie odpowiedniej przepustowości dostępu do serwerów. Muszą również: zmieniać konfigurację segmentacji, routingu, aktualizować reguły firewalli, inwentaryzować i aktualizować sprzęt, dbać aby użytkownicy nie instalowali niedozwolonego oprogramowania i nie mogli pozyskać danych poufnych, zapewniać zdalny dostęp pracownikom pracującym spoza biur.

Sieci szkieletowe operatorów są natomiast sieciami rozległymi, które muszą gwarantować zakontraktowany poziom usług i dostępność. Te sieci są podstawą zysku, więc mogą być zrealizowane w oparciu o skomplikowane rozwiązania, wymagające ciągłego zarządzania przez sztab wyspecjalizowanych w danym zakresie fachowców. Tu krytyczna będzie wydajność, skalowalność, elastyczność i dynamika konfiguracji, możliwość zrealizowania jak największej liczby niezależnych usług, o różnych parametrach dla wielu klientów i możliwość centralizacji zarządzania ogromną infrastrukturą.

2.3. Koszty i sposób zarządzania

W świecie IT Telco (np.: sieci operatorskie) - sieć generuje zysk, wszelkie inwestycje z nią związane mają więc bezpośrednie uzasadnienie biznesowe. Korporacyjne sieci IT umożliwiają i warunkują sprawne funkcjonowanie przedsiębiorstwa, wliczane są w jego koszty operacyjne. W obydwu przypadkach zarządzanie będzie scentralizowane i oddane w ręce wyspecjalizowanych (często certyfikowanych w ramach konkretnych rozwiązań technicznych) administratorów/inżynierów sieciowych. W świecie OT infrastruktura sieciowa jest kosztem - inwestycją konieczną do zapewnienia ciągłości zautomatyzowanego procesu, nie generuje bezpośrednich zysków, natomiast źle dobrana/zaprojektowana może generować ogromne ryzyko biznesowe i techniczne oraz straty. Zarządzanie siecią często wpisywane jest w obowiązki działów automatyki (które zresztą, chcą mieć pełną kontrolę nad infrastrukturą, która ma bezpośredni wpływ na proces, za który ponoszą odpowiedzialność). Trudniejsze i nie zawsze uzasadnione (ze względów technicznych i formalnych) jest zapewnienie scentralizowanego zarządzania wszystkimi sieciami OT w danym przedsiębiorstwie. Osoba zarządzająca siecią OT musi w pełni rozumieć proces automatyki, który jest realizowany w oparciu o komunikację w tej sieci. Automatycy i inżynierowie związani z utrzymaniem ruchu i co ważniejsze, odpowiedzialni za realizowanie procesów, nie mają czasu aby nabywać dodatkowe kompetencje odpowiednie do obsługi złożonych konfiguracyjnie rozwiązań sieciowych, w związku z tym sieć przemysłowa musi być funkcjonalnie sprawna i jak najłatwiejsza w zarządzaniu i diagnostyce. Dodatkowo, tam, gdzie jest to możliwe można i należy wprowadzać elementy scentralizowanego zarządzania, monitorowania, logowania i korelowania zdarzeń sieciowo-procesowych.

2.4. Doświadczenie

Doświadczenie i perspektywa z której patrzą działy IT i OT, jak pokazano powyżej, są odmienne. Przeszkodą bywa schematyczne myślenie o słuszności podejścia bliższego naszej wiedzy, wynikające z zamknięcia w obrębie własnych doświadczeń. Częstym problemem jest jednak również (niestety) arogancja i wzajemne niezrozumienie, które utrudnia współpracę i wykorzystanie jakże cennego i nieocenionego doświadczenia obydwu stron. Żyjemy w świecie, który wymaga wysokiej specjalizacji i wysokich kompetencji. Nie ma innej drogi do sprawnego osiągnięcia celu jak wymiana doświadczeń, konsultacja ze specjalistami z poszczególnych dziedzin i uproszczony język komunikacji (umożliwiający udzielenie zrozumiałych wyjaśnień specjalistom z innych dziedzin). Tylko w ten sposób obraz sytuacji będzie pełny i możliwe będzie podjęcie odpowiednich działań i decyzji, a co za tym idzie zapewnienie należytego poziomu usług oraz bezpieczeństwa infrastruktury.

Część firm podejmuje próby oddania zarządzania sieciami OT, swoim działom IT, które często próbują narzucić swoje procedury. Zwykle spotyka się to ze sprzeciwem działów automatyki, którym komplikuje (a czasem uniemożliwia) to pracę. Zarządzanie i zabezpieczanie sieci OT nie może się odbyć bez dialogu technicznego i wymiany doświadczeń obydwu stron. Dopiero na tej podstawie można stworzyć model odpowiadający realnym potrzebom danego systemu. Projekt zarządzania cyberbezpieczeństwem sieci OT dobrze byłoby rozpocząć stworzenie zespołu, w którego skład powinny wejść osoby z działów automatyki oraz informatyki i telekomunikacji, jak również reprezentanci zarządu lub osób decyzyjnych od strony biznesowej, odpowiedzialnych za zapewnienie środków i określenie akceptowalnego poziomu ryzyka.

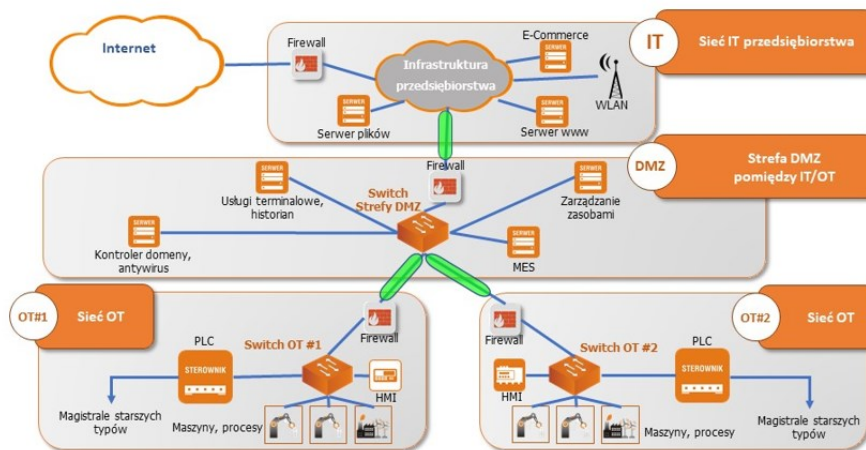
3. Perspektywa techniczna

Perspektywa techniczna będzie określać w każdym przypadku konkretne zagrożenia, podatności i ich potencjalny skutek dla ciągłości procesu. Cel systemu cyberbezpieczeństwa: zminimalizować prawdopodobieństwo wystąpienia niepożądanych incydentów (incydenty, które zaklasyfikujemy jako niepożądane będą różne dla różnych firm i osób), zminimalizować wpływ tych incydentów, zapewnić jak najszybszy powrót do poprawnej pracy systemu w przypadku wystąpienia incydentu, umożliwić analizę post-factum, która ma na celu poprawę zabezpieczeń na przyszłość.

Dobry projekt architektury zabezpieczeń powinien bazować na dogłębnej analizie istniejącego systemu przemysłowego dla którego ma być ona dedykowana. Należy poznać i zrozumieć sposób wymiany danych przemysłowych realizowany w obrębie danego przedsiębiorstwa. Możemy w tym celu wesprzeć się wybranymi standardami i narzędziami, które pomagają ten proces sprawnie zrealizować. Przykładem jest podejście iSEC firmy RadiFlow.

Jedne z najważniejszych pojęć w kontekście doboru rozwiązań to koncepcja Defence in Depth czyli warstwowa architektura zabezpieczeń (ochrona w głąb), która jest podejściem rekomendowanym przez większość standardów i organizacji zajmujących się bezpieczeństwem systemów przemysłowych. Defence in Depth polega na przeanalizowaniu podatności każdej z warstw z osobna oraz wprowadzeniu odpowiednich, niezależnych zabezpieczeń na każdym poziomie. Bardzo pomocne będzie zaznajomienie się z normą IEC62443 (ISA99), która w szerokim zakresie (począwszy od zarządzania i tworzenia polityk, aż po dobór komponentów) pokazuje tzw. „dobre praktyki”. Norma min. definiuje strefy i kanały jako elementy architektury systemu.

Strefy i kanały (zones and conduits) - przykład



Rys. 1. Podział sieci na strefy i kanały wg. normy IEC 62443

Pomiędzy poszczególnymi strefami wprowadzamy odpowiednie zabezpieczenia oraz Secure by Design czyli wykorzystanie urządzeń, zaprojektowanych i zbudowanych już z uwzględnieniem zagadnień związanych z cyberbezpieczeństwem. W części 7 omówione są konkretne rozwiązania techniczne. Poniższe punkty pokazują na które elementy systemu należy zwrócić uwagę, jako na newralgiczne z punktu widzenia zabezpieczeń.

3.1. Punkty styku z innymi sieciami

Zwyczaj się mówi, że sieci OT nie mają punktu styku z innymi sieciami (tzw. security by obscurity), ponieważ w domyśle jako „inne” czyli „obce” klasyfikuje się bezpośredni dostęp do Internetu. Tymczasem sieć OT może mieć i często ma połączenie z inną siecią - bezpośrednio (np. styk z siecią korporacyjną poprzez router z firewallem), pośrednio - przez serwery i strefę DMZ, w ograniczonym czasie - np.: zdalny dostęp serwisowy do wybranych urządzeń. Proszę pamiętać, że nawet faktyczny brak styku, lub styk wyłącznie z „bezpieczną” infrastrukturą nie gwarantują 100% bezpieczeństwa. Zawsze istnieje ryzyko skutecznego przeprowadzonego ataku socjotechnicznego, skutkującego wprowadzeniem złośliwego oprogramowania.

3.2. Protokoły przemysłowe

Protokoły używane w aplikacjach przemysłowych (np.: Modbus, DNP3, IEC103/104, IEC 61850, ProfiNet, GazModem, itd.) były projektowane bez uwzględnienia takich zagadnień jak autentykacja oraz szyfrowanie. Możemy wdrożyć rozwiązania zapewniające bezpieczną transmisję (VPN) oraz uwierzytelnianie (RadiFlow APA) poprzez wprowadzenie dodatkowych elementów infrastruktury lub oczekiwać zaimplementowania odpowiednich mechanizmów bezpośrednio w urządzeniach automatyki.

3.3. Aplikacje: serwer/klient, web based, rozproszone sterowanie

W rozproszonych przemysłowych systemach sterowania większość aplikacji (na serwerach, stacjach inżynierskich, etc.) działa na platformach opartych o różne wersje systemów Windows co powoduje, że mamy tu do czynienia z identycznymi podatnościami i lukami jak w korporacyjnych systemach IT. Dodatkowo praktyka wskazuje, że w środowiskach opartych o Windows aplikacje wykorzystują współdzielenie zasobów plikowych pomiędzy komputerami (luki właśnie w protokole SMB wykorzystywał malware Petya/NotPetya). Zastosowanie w sterownikach PLC systemów operacyjnych pochodzących od systemów ogólnego przeznaczenia może skutkować podatnościami typu „zero day”. Niektóre urządzenia posiadają interfejsy konfiguracyjne oparte o web serwer i dostęp przeglądarkowy, co wymaga szczególnej uwagi w procesie analizy podatności (OWASP Top 10).

3.4. Użytkownicy i prawa dostępu

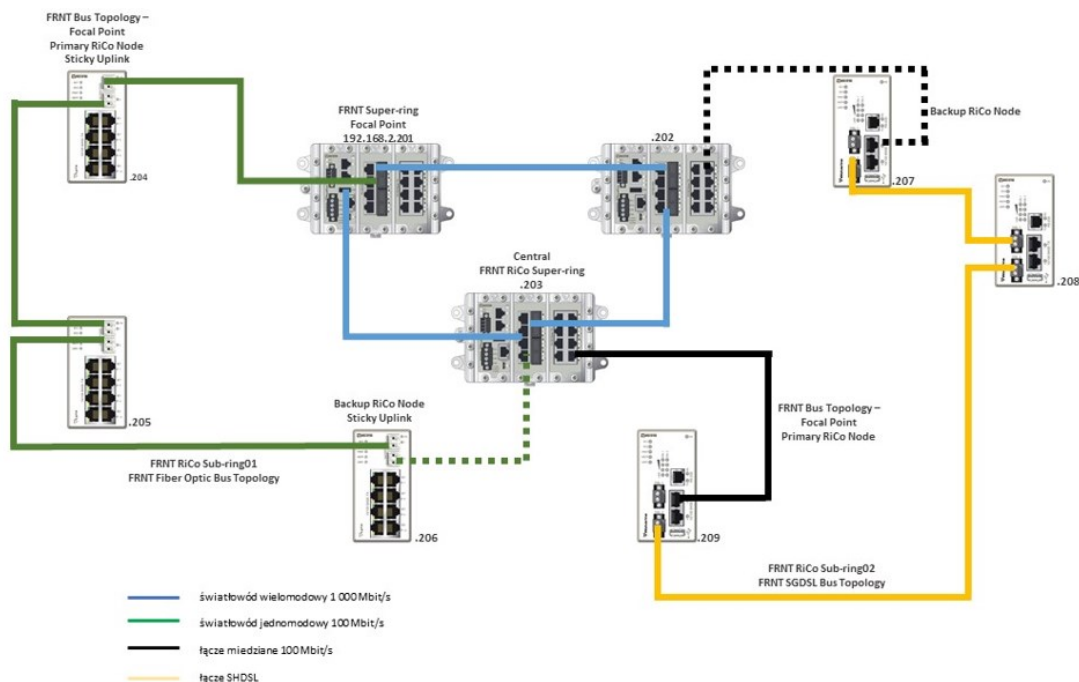
Systemem automatyki zarządzają wybrani pracownicy danej firmy, dostęp do niego mają jednak też często pracownicy firm zewnętrznych realizujący zadania związane z serwisem i utrzymaniem, którzy przyłączają do sieci OT swoje narzędzia (laptopy, smartphony, testery, zewnętrzne pamięci), o których stanie zabezpieczeń nie mamy pojęcia, ani nie mamy na ten stan specjalnego wpływu. Bardzo istotne jest aby precyzyjnie określić kto dokładnie i w jakim czasie może mieć dostęp do konkretnych zasobów i do przeprowadzenia jakich działań posiada autoryzację. Kolejny bardzo ważny aspekt to logowanie zdarzeń i wszelkich ingerencji w system i sieć OT. Dokładne logowanie jest jednym z najważniejszych kryteriów takich norm i zaleceń jak NERC-CIP.

3.5. Zintegrowany system dostępu fizycznego

Oczywiście dostęp fizyczny do sieci OT powinien być ograniczony. Istnieją rozwiązania i narzędzia umożliwiające integrację systemów udzielania dostępu fizycznego z dynamicznym przypisywaniem prawa dostępu do określonych zasobów na określony czas, w celu realizacji sprecyzowanego zadania. W sieciach operatorskich, centrach danych takie systemy stosowane są już od jakiegoś czasu.

3.6. Niezawodność

Oczywiście priorytetowym aspektem jest wysoka dostępność sieci i pewność jej działania. Powinno stosować się odpowiednio nadmiarowe topologie, z niezauważalnym czasem przełączania i przemysłowe urządzenia wysokiej klasy. Przemysłowe, czyli odporne na trudne warunki środowiskowe, oferujące długi czas życia i wysokie parametry MTBF. Przemysłowe, znaczy jednak także możliwie proste w obsłudze. Nadmierny stopień skomplikowania, będzie powodował wzrost prawdopodobieństwa popełnienia błędu.



Rys. 2. Nadmiarowa topologia „no single point of failure” na przykładzie rozwiązania Westermo i protokołu FRNT

4. Perspektywa biznesowa. Koszty i planowanie budżetu

Do perspektywy biznesowej należy szacowanie ryzyka dla organizacji, zarządzanie nim, tj. np.: określenie jaki poziom ryzyka jesteśmy w stanie zaakceptować i czy jesteśmy w stanie zapewnić odpowiedni budżet dla utrzymania go poniżej określonego poziomu. Cyberbezpieczeństwo jest tylko jednym, z elementów w całościowym szacowaniu ryzyka i musi być zbilansowane z pozostałymi wyznacznikami. W tym obszarze należy uwzględnić również stworzenie/nadanie mocy odpowiednim politykom i procedurom oraz przygotowanie scenariuszy kryzysowych, umożliwiających szybką reakcję (tu z pomocą może przyjść również norma IEC 62443 (ISA 99)).

Osoby decyzyjne będą potrzebowały bieżących informacji dotyczących realizowania procesu, stąd wystąpienie styku z siecią OT jest często odpowiedzią min. na takie zapotrzebowanie.

Perspektywa biznesowa będzie brała pod uwagę między innymi takie parametry jak RoI (Return on Investment) czyli jak inwestycja może się zwrócić (w tym przypadku nie można mówić o zwrocie z inwestycji, ale można mówić o zminimalizowaniu ryzyka strat). Bardzo ważnym pojęciem jest na pewno TCO (Total Cost of Ownership) czyli całkowity koszt utrzymania, oraz struktura kosztów składowych CAPEX (Capital Expenditures) i OPEX (Operating Expenditures).

Przykładowo: zakup serwera danych, sterowników i oprogramowania jest jednorazowym kosztem CAPEX, natomiast wszelkie koszty związane z aktualizacjami oprogramowania, serwisem, utrzymaniem, konfiguracją i obsługą to koszty kwalifikowane jako OPEX. Koszty OPEX dla czasu życia systemu często wielokrotnie przekraczają koszt CAPEX, więc warto zwrócić uwagę na rozwiązania, które będą je minimalizować. Ważne jest jednak, żeby budżetując projekty związane z cyberbezpieczeństwem pamiętać o tym, że musimy

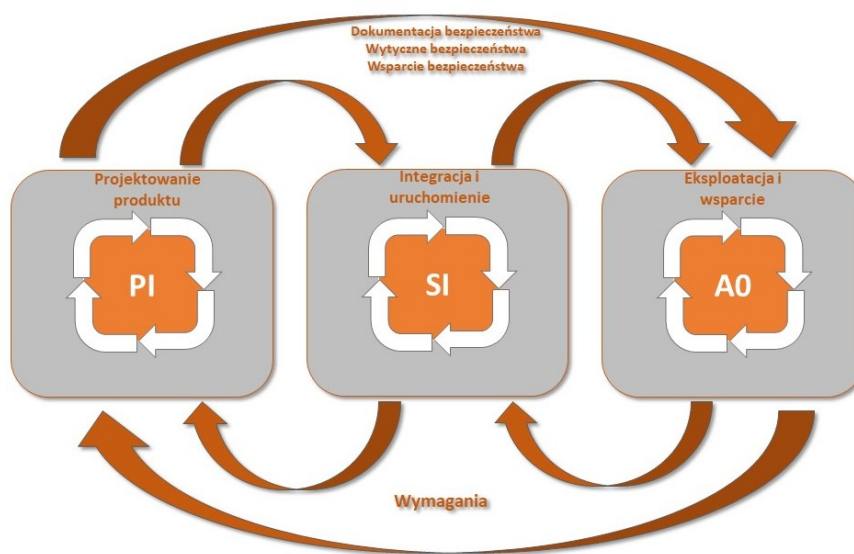
liczyć się z kosztami stałymi związanymi przynajmniej z licencjami i obsługą, ponieważ zapewnienie skutecznej ochrony nie jest równoznaczne z zakupem produktów podwyższających poziom zabezpieczeń. Każda firma powinna mieć ustalony budżet roczny na zapewnienie i utrzymanie systemów bezpieczeństwa (minimalizowanie ryzyk do oczekiwanego poziomu), a dodatkowo planować budżet inwestycyjny na wdrożenie nowych lub rozbudowę istniejących rozwiązań.

5. Problemy związane z planowaniem i wdrażaniem

Dobrze, żeby cyberbezpieczeństwo było traktowane jako projekt, modyfikowany zgodnie z metodyką „continuous improvement” czyli ciągłej poprawy. Zarządzanie projektami cyberbezpieczeństwa jest na pewno złożone i bezpośrednio powiązane z szacowaniem i zarządzaniem ryzykiem. W niniejszym artykule nie ma miejsca na szczegółowe omawianie tego zagadnienia, pozostaje nam polecić lekturę [1], [6], [7], [9]. Nadrzędnym celem projektu jest właśnie zredukowanie ryzyka, związanego z zagrożeniami i podatnościami danego systemu. Jeżeli zagrożenia, podatności i poziom akceptowalnego ryzyka będą błędnie określone, efekt zabezpieczania może różnić się z oczekiwaniami. W ramach projektu cyberbezpieczeństwa należałoby uwzględnić stworzenie odpowiednich polityk, procedur, scenariuszy kryzysowych oraz dobrać technologie adresujące konkretne, zidentyfikowane rejony podwyższonego zagrożenia. Pragniemy jednak zwrócić uwagę, że im lepiej taki projekt zostanie przygotowany od strony organizacyjnej i realizowany przez zespół posiadający kompetencje zarówno IT, jak i OT tym większa szansa, że przebiegać będzie poprawnie i spełni swoje zadanie. Poniżej omówiono krótko przykładowe zadania w takim projekcie.

5.1. Polityki, procedury, scenariusze kryzysowe

Stworzenie lub korekta procedur, polityk i scenariuszy kryzysowych jest koniecznym elementem organizacyjnym, mającym na celu egzekwowanie odpowiednich zachowań służących zmniejszeniu ryzyka i potencjalnych skutków niepożądanych incydentów. Do tworzenia takich dokumentów dobrze jest podejść biorąc pod cykl życia projektu cyberbezpieczeństwa.

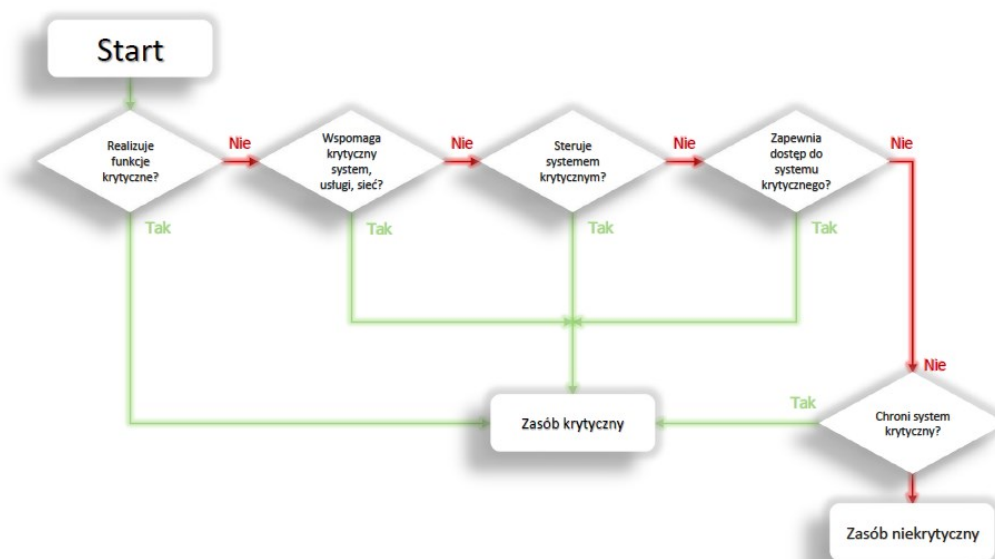


Rys. 3. Cykl życia projektu bezpieczeństwa wg. IEC 62443

5.2. Analiza bezpieczeństwa – normy, narzędzia, kompetencje

Celowo, używamy terminu „analiza bezpieczeństwa” i rozumiemy ją jako zestaw działań mających na celu zidentyfikowanie i zarządzanie ryzykiem związanym z cyberbezpieczeństwem. W skład takiej analizy będą wchodziły zadania związane ze zidentyfikowaniem zasobów krytycznych, zagrożeń i podatności. Kolejny element to szacowanie i zarządzanie ryzykiem, oraz stworzenie odpowiednich polityk i procedur. Częścią będzie również typowy audyt, sprawdzający skuteczność i sposób egzekwowania tych polityk i procedur bezpieczeństwa. Dobrze, żeby audyt bezpieczeństwa sieci OT uwzględniał rekomendacje wybrane jako wzorcowe (np. NERC-CIP, ISA99 lub inne w zależności od sektora [7]) oraz tzw. „compliance configuration auditing” czyli sprawdzenie podatności konfiguracji. Audyt może mieć formę czysto pasywną (kwestionariusze, offline test) jak i aktywną (testy). Audyt systemu OT często będzie musiał korzystać z metod offline, żeby nie zaburzać działania procesu. Taki audyt, sam w sobie, nie pokaże nam jednak obszarów ryzyka związanych z niespodziewanymi lub nowymi podatnościami i taką analizę trzeba przeprowadzić niezależnie. Wynikiem wspomnianej

analizy powinno być zestawienie wszystkich potencjalnie wrażliwych punktów w naszym systemie. Pomocne w analizie samego ryzyka będą gotowe metodologie klasyfikacji zagrożeń pod względem wpływu (np. DREAD - Damage Potential/Reproducibility/Exploitability/AffectedUsers/Discoverability) oraz standardy [10].



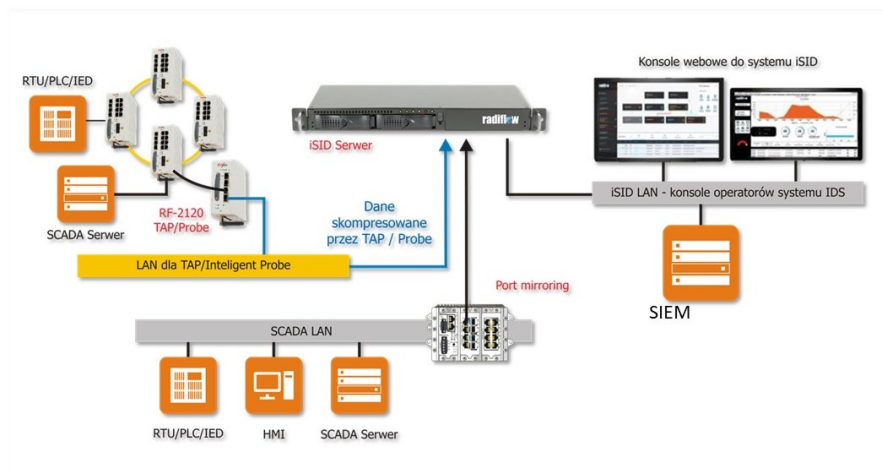
Rys. 4. Sposób zidentyfikowania zasobów krytycznych

5.3. Wdrażanie ochrony aktywnej

Przez ochronę aktywną rozumiemy wszystkie urządzenia zastosowane bezpośrednio w torze/kanale komunikacji (ang. in-line). Najważniejsze z nich to oczywiście switche/routery umożliwiające segmentację sieci. Firewallle różnego typu umożliwiające filtrowanie ruchu na poszczególnych poziomach. Pierwszy, łatwiejszy, aspekt to zidentyfikowanie i zabezpieczenie potencjalnego lub istniejącego styku z zewnętrznymi sieciami, podział na strefy (segmentacja np. w oparciu o VLAN), wprowadzenie autoryzacji dostępu do poszczególnych zasobów. Musimy najpierw dogłębnie poznać system, który ma być chroniony - jego zadania i charakterystykę tak, aby wprowadzone zabezpieczenia nie pogarszały jakości procesu (np. nie wprowadzały zbyt dużych opóźnień lub ryzyka sparaliżowania pracy). Do dyspozycji będziemy mieli takie narzędzia jak UTM, SPI, DPI firewall. Data Diode, switchy, routery, dodatkowe narzędzia wprowadzające autentykację, szyfrowanie (np. RadiFlow APA, iHUB VPN). Dobrą praktyką ochrony dla punktów styku sieci OT jest tzw. „whitelisting”, czyli zasada - wszystko co nie jest dozwolone, jest zabronione. Cała trudność wdrażania takich rozwiązań wiąże się nie tyle z ich konfiguracją od strony technicznej, a bardziej określeniem, co i w jaki sposób ma być filtrowane, logowane i przekazywane do systemów nadrzędnych. Z pomocą przyjdzie tu funkcjonalność „learning mode” czyli tryb uczenia się oferowany przez niektóre rozwiązania (patrz 7.2).

5.4. Wdrażanie oprogramowania do ciągłego monitorowania

Po zrealizowaniu podstawowej analizy i dobraniu zabezpieczeń dla punktów styku i stref, kolejnym krokiem, zgodnie z filozofią Defence in Depth, jest zabezpieczenie sieci „od dołu”. Sieć, w strefie realizującej proces jest wrażliwa i nie możemy wprowadzać w niej rozwiązań in-line. Z pomocą przyjdą więc DPI SCADA firewall off-line i systemy ciągłego monitorowania. Przykłady takich rozwiązań to SCADAfence, iSID RadiFlow, GE Digital Opshield. Takie narzędzia mogą bazować na analizie i wychwytywaniu podatności (ang. signature based, configuration compliance hardening) lub/i na analizie behawioralnej. Dobrze aby wybrane narzędzie łączyło obydwie możliwości. Wykrywanie podatności wydaje się być jasne - w tym zakresie system IDS (Intrusion Detection System) zinwentaryzuje naszą sieć (zarówno HW jak i SW), następnie będzie odnosił się do baz danych znanych podatności i zapisanych „dobrych praktyk” dotyczących konfiguracji. Analiza behawioralna jest zagadnieniem bardziej złożonym i polega na budowaniu modelu odniesienia pracy sieci OT (ang. baseline). Zbudowanie takiego modelu odbywa się automatycznie, ale wymaga dużo czasu i odpowiedniego zaimplementowania systemu IDS. Kolejny administrator, zatwierdza lub koryguje powstały model. Wszelkie zdarzenia odbiegające od zapisanych charakterystyk bazowych będą raportowane w formie alertów. Systemy IDS będą różnić się sposobem prezentacji danych, szczegółowością i trafnością analizy oraz sposobem współpracy z systemami nadrzędnymi. Wdrożenie systemów IDS wymaga zastosowania rozwiązań kierujących do nich ruch, który ma zostać poddany analizie. Do tego zadania wykorzystuje się funkcjonalność port mirroring lub specjalne sondy (ang. TAP) (patrz 7.1).



Rys. 5. Przykład wdrożenia systemu IDS - iSID RadiFlow

5.5. Wdrażanie systemów SIEM do korelacji zdarzeń i wskazywania/szacowania ryzyka

Na podstawie tego co powiedzieliśmy do tej pory i co wynika z Defence in Depth, elementów zabezpieczeń będzie wiele i nie spełnią one w pełni swojej roli bez możliwości korelacji informacji i zdarzeń, które są przez nie wychwytywane. Do takiej korelacji służą systemy SIEM. Wybór systemu SIEM będzie zależał min. od obszaru, który będzie miał on obsługiwać (tylko OT, czy OT + IT). Często systemy SIEM administrowane są już w skali przedsiębiorstwa przez dedykowane osoby z działów IT.

Dane z poszczególnych urządzeń i poziomów zabezpieczeń wysyłane są do systemów SIEM najczęściej w formie logów syslog. Część urządzeń, dodatkowo umożliwia dopasowanie formy, w jakiej wysyłane są te informacje.

6. Problemy związane z utrzymaniem

Zapewnianie ochrony wiąże się z koniecznością ciągłego monitorowania i aktualizowania systemu zabezpieczeń (min. ze względu na dynamikę podatności). Takie działania będą najbardziej efektywne, jeżeli realizowane są przez wyodrębnioną jednostkę (zespół) SOC (ang. Security Operations Center), która będzie miała możliwość korelacji informacji i zdarzeń z całego systemu objętego ochroną.

Oczywiście część wymaganych analiz, szczegółowy monitoring będzie kaskadowany na inne zespoły pomocnicze pracujące w odpowiednich strefach, ale SOC powinien mieć całościowy obraz sytuacji (poziom nadrzędny SIEM i systemy wspomagające korelację danych i analizę ryzyka). Taką usługę można realizować w obrębie własnych zasobów, coraz częściej pojawia się możliwość outsourcingu (przynajmniej w części) SOC jako usługi. Warto to przeanalizować dla inwestycji, które są na tyle małe, że koszty utrzymania własnego SOC nie mają uzasadnienia biznesowego. Niezależnie od wariantu, w kontekście TCO (Total Cost of Ownership) musimy liczyć się z kosztami aktualizacji oprogramowania, sprzętu, wsparcia technicznego oraz zarządzaniem infrastrukturą związaną z bezpieczeństwem na niższym poziomie. Wprowadzając rozwiązania powinno się oszacować przybliżony budżet na takie działania.

7. Rozwiązania techniczne, specyfikacja wymagań

7.1. Ochrona pasywna – monitorowanie, inwentaryzacja i dokumentacja sieci. Budowanie modelu odniesienia

Wdrożenie: duży projekt, wymagający od kilku do kilkunastu tygodni (zależnie od specyfiki i stopnia złożoności systemu automatyki) „uczenia się” i weryfikacji zanim zatwierdzony zostanie model odniesienia; możliwe kilka wariantów - scentralizowany, rozproszony lub mieszany; wymaga przekierowania ruchu sieciowego do serwerów IDS (port mirroring na switchach, specjalne sondy TAP).

Bez przesady można powiedzieć, że ciągłe monitorowanie jest krytyczne dla bezpieczeństwa, szczególnie w sieciach przemysłowych, w których tego typu pasywne rozwiązania spełniają zadanie kontroli, nie ingerując ani nie spowalniając krytycznych procesów.

Rzetelna dokumentacja i inwentaryzacja sieci - charakterystyki ruchu dla danych procesów, dokumentacja funkcjonalno-komunikacyjna tj. pokazująca jaki rodzaj komunikacji jest odpowiedzialny za jakie funkcje w systemie automatyki i jak powinien wyglądać – to punkt odniesienia. Musimy jednak mieć jak się do niego odnieść oraz na bieżąco go aktualizować. Tu z pomocą przychodzi nam monitorowanie sieci - absolutna podstawa bezpieczeństwa. Do dyspozycji mamy systemy IDS (Intrusion Detection System) umożliwiające bieżącą

inwentaryzację i monitorowanie w trybie ciągłym. Dobrze wybrać taki, który obok możliwości wykrywania podatności przemysłowych umożliwia analizę behawioralną. Przykładami takich rozwiązań są np.: SCADAfence CNM lub iSID RadiFlow, GE Digital Opshield. Silniki związane z wykrywaniem podatności, w przypadku tych programów, korzystają z dedykowanych baz danych podatności systemów przemysłowych. Analiza behawioralna umożliwia wychwycenie nietypowych zachowań w przemysłowych sieciach i systemach automatyki. W fazie uruchomienia zbieramy informacje i budujemy model odniesienia dla monitorowanego systemu. Wszelkie próby przekroczenia uprawnień, nietypowe komendy, ruch odbiegający od wzorcowych charakterystyk i podatności zostaną w trybie rzeczywistym wykryte, a informacja o nich może być kierowana do dowolnego systemu nadrzędnego i/lub bezpośrednio do administratora bezpieczeństwa. W przypadku takich rozwiązań należy bezwzględnie zwrócić uwagę (najlepiej w ramach testów PoC (Proof of Concept)) na skuteczność gromadzenia informacji, ilość i wiarygodność generowanych alarmów, sposób generowania alarmów i kompatybilność z systemem zarządzania wyższego poziomu. Równie ważne są zastosowane silniki analizy behawioralnej oraz i sygnaturowej, możliwość pogłębionej analizy protokołów przemysłowych, sposób instalacji w systemie, sposób zbierania danych, możliwości związane z logowaniem, automatyczny proces „uczenia się”, sposób weryfikacji ruchu, stopień szczegółowości inwentaryzacji zasobów.

7.2. Aktywna ochrona zasobów w sieciach OT – przegląd rozwiązań

7.2.1. Podstawy

Jeżeli chcemy mieć bezpieczną infrastrukturę powinniśmy zacząć od zabezpieczenia jej poprzez wszystkie warstwy, zaczynając od samego dołu – czyli urządzeń, w oparciu o które budujemy sieć oraz odpowiedniej ich konfiguracji.

Urządzenia muszą umożliwiać zarządzanie i monitorowanie. Zwykle monitorowanie realizowane jest w oparciu o protokół SNMP – jego najbezpieczniejsza wersja to SNMPv3. Wybrane przez nas rozwiązania muszą mieć odpowiednio wysoki stopień niezawodności (tu z pomocą przyjdą parametry MTBF i kalkulacje RAMS (Reliability Availability Maintainability and Safety) i odporność na warunki środowiskowe. Wszystkie nieużywane interfejsy i usługi powinny być administracyjnie wyłączone. Na wykorzystywanych interfejsach powinno w miarę możliwości stosować się mechanizmy autentykacji/autoryzacji. Przykładowo switche L2 i L3 (warstwy drugiej i trzeciej modelu OSI) Westermo umożliwiają włączenie filtrowania ruchu na każdym z portów, łańcuch autentykacji użytkowników TACACS+, Radius, 802.1x, certyfikaty, autentykację protokołów routingu MD5 RIP/OSPF. Ponadto zgodnie z zaleceniami norm takich jak IEC62443 możemy podzielić sieć na segmenty VLAN i włączyć dla nich SPI firewall jeżeli nie powinny się ze sobą komunikować. (Uwaga! Włączenie aktywnego filtrowania/blokowania w sieci przemysłowej wymaga szczegółowej analizy i pewności, że komunikacja jest bezwzględnie zabroniona i jej brak nie wpłynie na proces, gdy system będzie pracował np. w trybie awaryjnym). Urządzenia pracujące z wykorzystaniem transmisji szeregowej, w protokołach przemysłowych bez autentykacji możemy dodatkowo zabezpieczyć poprzez połączenie do sieci za pośrednictwem bram umożliwiających monitorowanie i kontrolowanie również takiego ruchu (np.: RadiFlow 3180), dzięki takim rozwiązaniom będziemy również mogli autentykację wymusić np. przy próbie nawiązania sesji do takiego urządzenia z sieci IP. Funkcjonalność ta w przypadku rozwiązań RadiFlow nosi nazwę APA (Authentication Proxy Access).

Ważne aby wybierać rozwiązania zaprojektowane i wykonane zgodnie z zasadami „secure by design”.

7.2.2. Segmentacja, VLAN-y

Wdrożenie: łatwe przy założeniu, że mamy odpowiednie urządzenia sieciowe (np. switche zarządzalne, dla których jest to standardowa funkcjonalność).

Obszar sieci i ruch związany z poszczególnymi usługami, funkcjami procesu, który nie potrzebuje szybkiej wymiany danych z innymi elementami procesu dobrze jest odseparować, np.: w ramach podsieci VLAN. Sieci VLAN można nadać odpowiedni priorytet, włączyć i wyłączyć protokoły dostępu do urządzeń sieciowych z poziomu danej podsieci, kontrolować ruch do innych VLAN (komunikacja w oparciu o routing pomiędzy VLAN) oraz filtrować dostęp z wykorzystaniem zapory firewall czy list ACL. Przykładem urządzeń przemysłowych na których jesteśmy w stanie zrealizować taką funkcjonalność są np.: switchy warstwy L2 i L3 Westermo.

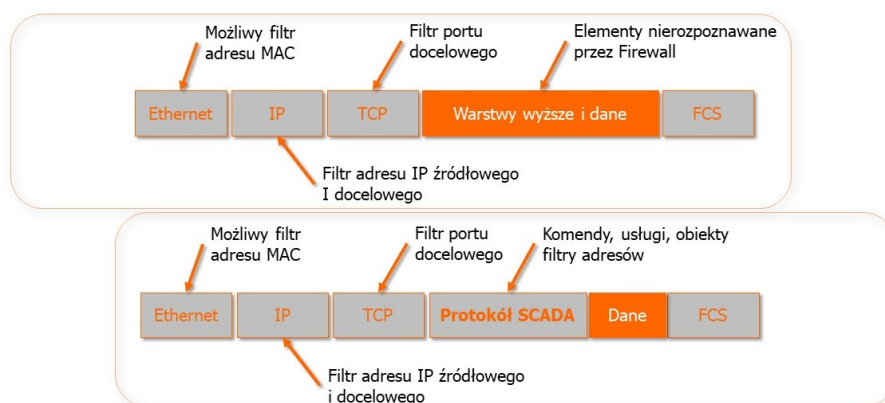
7.2.3. SPI firewall i DPI Scada firewall

Wdrożenie: w trybie monitorowania - łatwe, tryb blokowania wymaga dogłębnej analizy komunikacji. Architektura wynikająca z koncepcji Defence in Depth zakłada filtrowanie ruchu na kilku poziomach. Na poziomie sieci korporacyjnej/infrastruktury transportowej stosowane powinny być rozwiązania klasy przynajmniej IT Enterprise o dużej wydajności, umożliwiające filtrowanie i routowanie ruchu z dużą przepustowością oraz obsługę wielu kanałów VPN IPSEC i Open VPN (SSL). Firewall te za zadanie mają zabezpieczenie styku sieci od strony sieci korporacyjnej, oraz zarządzanie łączami szyfrowanymi

realizowanymi do rozproszonych lokalizacji sieci OT. Tego typu sprzęt znajdziemy w ofertach firm Cisco, Fortigate, PaloAlto, Juniper, HP i wielu innych. Od strony sieci OT musimy mieć router z firewalllem, który zapewni nam zabezpieczenie bezpośredniego styku sieci OT ze światem zewnętrznym, tj. będzie miał możliwość analizowania również protokołów przemysłowych.

Dodatkowo takie rozwiązania są zwykle kompaktowe, chłodzone pasywnie, integrujące wiele funkcjonalności, ale z limitowaną wydajnością (np. w jednym urządzeniu RadiFlow 3180 mamy funkcjonalność: bramy protokołów (na portach szeregowych), serwera/klienta VPN, uwierzytelniania APA, DPI firewall, routera z różnorodnymi opcjami interfejsów WAN, switcha, modemu LTE).

Zapory sieciowe tzw. firewall, które, oprócz funkcjonalności DPI (firewall aplikacyjny dla protokołów przemysłowych) będą miały zastosowanie na tym poziomie sieci to zapory SPI (Statefull Packet Inspection) zintegrowane z urządzeniami sieciowymi (np. switch RFIR227 lub Lynx210 Westermo) dla realizowania koncepcji Distributed Firewall i tworzenia strefy DMZ.



Rys. 6. Różnice w analizie pakietów, odpowiednio, przez SPI i DPI firewall

Firewall przemysłowy instalowany w sieci OT nie musi mieć tak dużej wydajności jak firewalles klasy Enterprise (bo nie będzie obsługiwał tak dużego ruchu), ale powinien umożliwiać pracę w trybie uczenia się, monitorowania, logowania, wysyłania alertów i ostatecznie umożliwiać blokowanie wybranego ruchu. Często tego typu urządzenia są zintegrowane z routerem i serwerem/klientem VPN, umożliwiając też realizowanie zdalnego dostępu (przewodowo lub bezprzewodowo).

7.2.4. Zdalny dostęp

Wdrożenie: łatwe od strony sieci OT, od strony sieci IT może wymagać albo routera i koncentratora (serwera) VPN albo np.: rozwiązania opartego na oprogramowaniu w chmurze. W przypadku chęci zapewnienia dostępu serwisowego punkt-punkt można rozważyć instalowanie klienta VPN bezpośrednio na komputerach osób do tego uprawnionych (tu zalecamy jednak ostrożność, znacznie łatwiej jest zapanować nad strukturą w której dostęp nie jest realizowany bezpośrednio).

Zwykle tego typu dostęp realizowany jest w oparciu o łącza bezprzewodowe. Od strony sieci OT wykorzystujemy bezprzewodowy router przemysłowy (np. Teldat, Conel, Westermo, MBconnect). Bezpieczny zdalny dostęp z wykorzystaniem dodatkowej warstwy uwierzytelniania i profilowania użytkowników APA oferuje rozwiązanie RadiFlow. Płynną agregację połączeń (wiele modemów i kart SIM) umożliwia Teldat OLA, podczas gdy w routerach Conel możemy w prosty sposób skonfigurować łącza backupowe. Do dyspozycji mamy również oprogramowanie do zarządzania dostępem zdalnym do wielu lokalizacji: Conel SmartCluster, Westermo WeConnect, RadiFlow iHUB czy MBConnect mymbConnect24. Każde z tych rozwiązań spełnia podobne zadanie, wszystkie spełniają zasadę „Secure by Design”, różnią się jednak pewnymi specyficznymi funkcjonalnościami. Dobór najlepszego rozwiązania do konkretnego zadania będzie polegał na analizie wymagań sprzętowych i funkcjonalnych, wielkości aplikacji, planach rozbudowy, a także testach PoC.

7.2.5. Sieci transportowe: bezpieczne sterowanie urządzeniami o znaczeniu krytycznym rozproszonym geograficznie systemie przemysłowym MPLS-TP

Wdrożenie: w zależności od przyjętej strategii oraz wybranego rozwiązania, wymaga odpowiedniego projektu logicznego i przewidzenia scentralizowanego zarządzania siecią i jej konfiguracją.

Przemysłowe sieci szkieletowe/transportowe również odbiegają w swojej specyfice od swoich odpowiedników w sieci IT/Telco. Wyróżniki będą podobne: mniejsza skala, mniejsza dynamika zmian konfiguracji, wymagana bezwzględna niezawodność, szybka lub bezprzerwowa protekcja dla topologii nadmiarowych,

bardzo długi okres utrzymania systemu (często >20 lat), wymagające środowisko pracy, łatwa, intuicyjna konfiguracja i diagnostyka, prosty serwis, platforma „Secure by Design”. Idealną odpowiedzią na takie wymagania wydaje się być technologia MPLS-TP. W kontekście technologii MPLS, wyznacznikiem bezpieczeństwa częściowo jest norma IETF RFC5920 (część MPLS/GMPLS Security Framework).

Norma ta określa kierunki ataków na trzech poziomach :

- Atak na warstwę kontrolną – jak hacker mógłby przejąć kontrolę nad siecią?

Problem rozwiązuje sama technologia MPLS-TP, w której sieć (w przeciwieństwie do np.: MPLS-IP czy CarrierEthernet) jest statycznie konfigurowana za pomocą systemu zarządzania siecią. Oznacza to, że nie są wykorzystywane dynamiczne protokoły sterujące zachowaniem sieci (takimi protokołami są na przykład protokoły routingu). W przypadku platformy XTran OTNSystems dodatkowo cała komunikacja związana z obsługą protekcji (topologii nadmiarowych) jest szyfrowana i odseparowana od danych transmitowanych na portach „użytkownika”.

- Atak na warstwę danych – jak hacker mógłby podsłuchać lub zaingerować w transmisję danych?

MPLS-TP zapobiega zrealizowaniu powyższego ataku poprzez wspomnianą już statyczną konfigurację i „zamknięcie” ruchu w tunelach i tzw. pseudowires. Usługi realizowane w oparciu o pseudowires są od siebie odizolowane. Niemniej jednak warto zwrócić uwagę czy platforma, na którą chcemy się zdecydować obsługuje sprzętowe szyfrowanie MACSec dla połączeń WAN (MPLS-TP) oraz czy dysponuje również możliwościami podobnymi jak w przypadku Ethernetu czyli filtrowaniem ruchu na różnych warstwach, dezaktywacją nieużywanych portów i usług.

- Atak na warstwę zarządzania siecią - jak zabezpieczony jest system zarządzania/monitoringu sieci?

W przypadku platformy służącej nam jako przykład czyli XTRAN OTNSystems komunikacja związana z zarządzaniem/monitorowaniem i konfiguracją urządzeń realizowana jest poprzez tzw. kanał DCN.

Kanał ten jest odseparowany logicznie od danych, a komunikacja w nim realizowana jest w oparciu o SNMP v3 (czyli z autentykacją oraz szyfrowaniem). Komunikacja pomiędzy systemem zarządzania siecią (NMS) TXCare, a węzłami MPLS-TP, w trybie normalnej pracy systemu odbywa się głównie w jednym kierunku i jest związana z monitorowaniem. Sieć jest w stanie pracować mimo utraty komunikacji z serwerem TXCare. Natomiast zalecana i możliwa jest redundantna praca serwerów. Samo oprogramowanie do zarządzania TXCare jest zaprojektowane zgodnie z zasadą „Secure by Design” umożliwia stworzenie kont użytkowników z różnymi uprawnieniami, bazuje na komunikacji klient-serwer.

Platforma XTRAN umożliwia realizację redundancji sprzętowej. MPLS-TP to sieć pakietowa (ze wszystkimi zaletami tej technologii takimi jak przykładowo determinizm, bezpieczeństwo, pełna kontrola, skalowalność, wysoka przepustowość, łatwość rozbudowy, modernizacji, utrzymania oraz cena). Użytkowników przyzwyczajonych do pewności sieci SDH przekona statyczny sposób konfiguracji, podobna metoda zarządzania i możliwości spokojnej migracji. Ze względu na oczekiwanie związane z bezpieczeństwem oraz determinizmem, technologią, którą często wymienia się jako rekomendowaną i przyszłościową dla szkieletowych sieci przemysłowych jest właśnie MPLS-TP.

8. Podsumowanie

„Zapewnienie cyberochrony przedsiębiorstwu to proces, a nie produkt” (Bruce Schneier) - to ciągle działanie, które wiąże się z minimalizacją ryzyka wystąpienia niepożądanego incydentu. Cel biznesowy i techniczny muszą się spotkać w racjonalnym obszarze, a określenie tego obszaru wymaga ścisłej współpracy zarządów/działów decyzyjnych z działami technicznymi. Lepsza będzie własna, wypracowana, „robocza” definicja miary cyberbezpieczeństwa dopasowana do potrzeb, specyfiki i zagrożeń realnych dla danego obszaru, niż sztywne podejście teoretyczne niedopasowane do naszych realiów. Celów technicznych, związanych z cyberbezpieczeństwem nie da się zrealizować wystarczająco dobrze przy sztywno określonych, jednorazowych budżetach, ale na pewno budżet na inwestycję w monitorowanie i zakup podstawowych systemów zabezpieczeń jest dobrym początkiem. W sposób przekrojowy staraliśmy się pokazać problematykę związaną z cyberbezpieczeństwem w sieciach przemysłowych. Celowo postawiliśmy pewne tezy, które mogą wydawać się kontrowersyjne, ale ich celem jest zwrócenie uwagi na szczególnie istotne aspekty, które gubią się niekiedy, w gąszczu innych, często sprzecznych ze sobą oczekiwań. Oczywiście mogliśmy pozwolić sobie tylko rzucić trochę światła na pewne problemy, ale zachęcamy do kontaktu i podjęcia dyskusji z całym naszym zespołem i we własnym gronie. W spisie literatury znajdują Państwo ciekawe tropy, którymi warto podążyć jeżeli tematyka cyberbezpieczeństwa w przemyśle jest dla Państwa istotna.

Kontakt do Zespołu ds. Cyberbezpieczeństwa i Integracji Sieciowej Techniska Polska Sp. z o.o.:
cybersecurityteam@techniska.pl.

Literatura

- [1] Industrial Network Security. Securing Critical Infrastructure Networks for Smart Grid, SCADA, and Other Industrial Control Systems. Second Edition @ 2015 r.
- [2] SCADAhacker
- [3] Strona Techniczna i Szkolenia z serii Akademia Techniczna: <http://tekniska.pl/know-how/>
- [4] Materiały firm: GE Digital, SCADAfence, RadiFlow, MBconnect, OTNSystems, Westermo, Teldat
- [5] iSEC <http://radiflow.com/isec-ics-security-assessment/>
- [6] Materiały i dyrektywy organizacji: ENISA, NIST, NSA
- [7] Normy dotyczące cyberbezpieczeństwa sieci przemysłowych: IEC62351, IEC61850-90-4: Rozdz.15 i 16, IEC62443/ISA 99, NERC-CIP v5, ISO/IEC 27002:2013 & ISO/IEC 27019:2013 (ISO/IEC 27011:2008)
- [8] WHITE PAPER - Juniper Networks VPN Decision Guide, 2010 r.
- [9] Interesujące spojrzenie na wprowadzenie metodyki „continuous improvement” w zakresie zarządzania cyberbezpieczeństwem: <http://www.ism3.com/node/11>
- [10] Wybrane metodologie i dobre praktyki - zarządzanie ryzykiem: BSI 100-3; CERT OCTAVE; ENISA; IEC27005, IEC31000, IEC31010; NIST800-161; NIST 800-30, 37, 39