Cyberbezpieczeństwo w środowiskach OT

Stefan Bednarczyk, Krzysztof Kawecki – Tekniska
Michał Zając – SPIE Energotest

Streszczenie

Informacje zawarte w niniejszym referacie pozwolą czytelnikowi na usystematyzowanie lub pogłębienie wiedzy dotyczącej zagrożeń w zakresie cyberbezpieczeństwa sieci przemysłowych, a także bezpieczeństwa systemów OT w odniesieniu do normy IEC 62443 i funkcjonalności ECONTROLplus.

1. Wstęp

Świadomość, oraz zainteresowanie zagadnieniami związanymi z cyberbezpieczeństwem zdecydowanie wzrasta. Można z dużą dozą pewności powiedzieć, że jeszcze kilkanaście lat temu bardzo nieliczne instytucje i organizacje uznawały bezpieczeństwo procesów i własnych danych za jeden z kluczowych aspektów dotyczących ich funkcjonowania. Przez ostatnie kilka lat zarówno na poziomie świadomości jak i podejmowanych działań następują jednak znaczące zmiany. Tematy związane z cyberbezpieczeństwem cieszą się sporym zainteresowaniem nawet wśród osób, które na co dzień nie mają bezpośredniej styczności ze środowiskiem czy otoczeniem IT bądź OT.

Media coraz częściej informują o atakach i agresywnych działaniach wobec sieci i zasobów firm czy instytucji. Każdy z nas zapewne zastanawia się, jakie jest między nimi podobieństwo i dlaczego część organizacji jest w stanie poradzić sobie z tymi atakami, a część nie. Zagadką pozostaje również to, o jakiej części zdarzeń w ogóle nie posiadamy wiedzy – ile z wrogich aktywności pozostaje nieskutecznych czy bez efektu – bądź z drugiej strony, ile przypadków pozostaje wciąż niewykrytych i poza świadomością zaatakowanych.

Ten artykuł stanowi próbę udzielenia odpowiedzi na pytania odnośnie przyczyn, procesu i metod atakowania sieci w organizacji, szczególnie z sektora OT. Przedstawia jednocześnie porady i wskazówki, jak walczyć z zagrożeniami nawet zanim jeszcze atakujący podejmą swoje starania.

2. Definicje

Każdy atak stanowi swego rodzaju ciąg zdarzeń. W szerszym kontekście można podjąć się dokonania pewnego opisu i odszukania prawidłowości, logicznej kolejności, oraz nazwania.

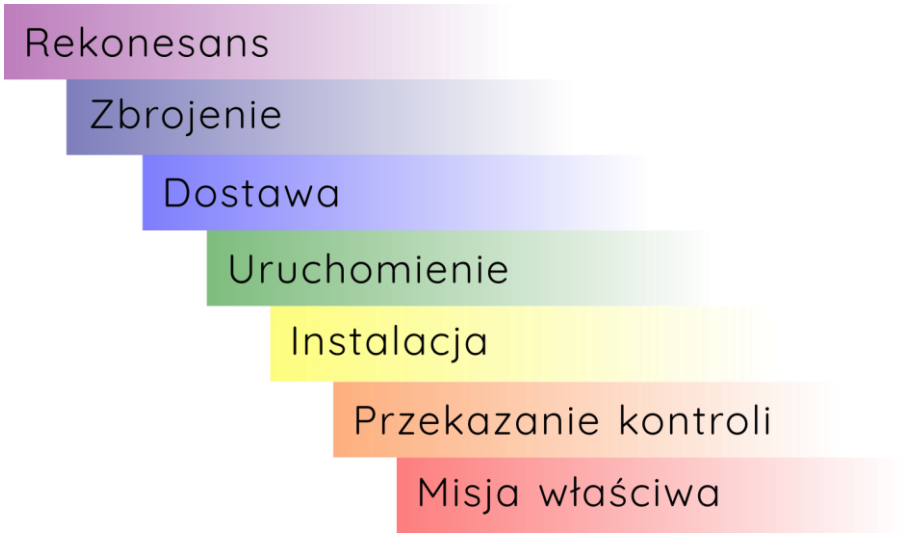
Rozpocząć należy od zdefiniowania pojęcia „Kill Chain” i kilku związanych z nim podstawowych terminów. „Kill Chain” to zatem cykl działań, jakie musi podjąć i wykonać atakujący, aby skutecznie zinfiltrować sieć zaatakowanego. W tym momencie ważne jest uściślenie zastosowanego w dalszej części nazewnictwa. Odniesienia IT lub ICT dotyczą ogółu usług mających za zadanie zapewnić stały przepływ informacji – w postaci komunikacji (telekomunikacji), łączności e-mail, uruchamiania stron WWW, systemów billingu, sprzedaży, ERP itd. Odniesienia OT lub ICS dotyczą natomiast systemów i sieci wykorzystywanych do monitorowania i zarządzania szeroko rozumianym procesem produkcji.

Istotnych jest kilka podstawowych różnic między systemami IT i OT. Przede wszystkim systemy OT są wrażliwe na opóźnienia i zakłócenia w komunikacji. W skrajnych przypadkach system sterowania procesem może przestać funkcjonować, jeśli dojdzie do opóźnień rzędu kilkudziesięciu milisekund. Opóźnienia takie są natomiast niezauważalne dla standardowego użytkownika sieci IT. Inną cechą systemów ICS jest brak aktualizacji lub opóźnienia w ich nakładaniu na systemy. Spowodowane jest to często brakiem okien serwisowych podczas normalnej produkcyjnej pracy systemu. Inną przyczyną braku aktualizacji mogą być też wymagania producenta systemu automatyki, który mógł nie zdążyć certyfikować nowych aktualizacji. W sieci OT rzadko kiedy można pozwolić sobie na przestoje związane z aktualizacjami, a w sieciach IT niemal standardem stały się już comiesięczne lub częstsze aktualizacje. Różnic jest zatem sporo.

3. Cyber Kill Chain

„Cyber Kill Chain” to blokowy algorytm prowadzenia ataków na dowolną infrastrukturę sieciową dowolnej organizacji. Wszystkie elementy tego łańcucha są na tyle ogólne, że za ich pomocą można opisać dowolną stosowaną technikę ataku. Różne grupy przestępcze, szpiegowskie bądź całkowicie legalne zespoły pentesterów mają utartą ścieżkę przeprowadzania ataków. Każda z nich różni się od siebie

w szczegółach, ale możliwe jest opisanie poszczególnych kroków i zgrupowanie ich w większe bloki dla zapewnienia przejrzystości. Wszystkie działania obserwowane czy analizowane na pewnym poziomie wykazują wspólne cechy i prawidłowości.



Rys. 1. Elementy „Cyber Kill Chain”

W odniesieniu do „Cyber Kill Chain” można powiedzieć o kilku standardowych krokach, które atakujący musi wykonać, aby włamać się do sieci organizacji. Jedną z pierwszych czynności w planowanym ataku stanowi w zdecydowanej większości rekonesans. Niezależnie od planowanego celu działań i oczekiwanego efektu, to właśnie rekonesans jest podstawowym ruchem „zaczepnym”. Zanim atakujący rozpocznie swoje właściwe działanie, musi wiedzieć między innymi co jest dla niego celem głównym, co stanowi przeszkodę w jego osiągnięciu, w jaki sposób jest chroniony obiekt docelowy czy – w odniesieniu do szczegółów – na przykład jakie adresy IP prowadzą do sieci organizacji, którą atakujący ma na celowniku.

Internet i sieci społecznościowe mogą stanowić spore ułatwienie w realizacji powyższego zadania. W przypadku ataku na systemy IT/OT organizacji, same organizacje lub ich pracownicy często dzielą się informacjami, które powinni zachowywać w tajemnicy. Nierzadko pokusa „pochwalenia się” na niwie prywatnej jest silniejsza od rekomendacji i potrzeb definiowanych na poziomie firm czy instytucji.

Co ma to wspólnego z organizacją OT? Warto zastanowić się na przykład, czy informacje opublikowane przez dział komunikacji z mediami są odpowiednio autoryzowane. Czy w materiałach prasowych przypadkiem nie pojawiają się wrażliwe dane. Czy przez nieuwagę nie są „odsłaniane” słabości lub nie pozwala się na identyfikację „czułych punktów”. Atak na jedną z francuskich telewizji rozpoczął się właśnie od analogicznego zdarzenia – w materiałach udostępnionych w Internecie możliwe było odczytanie haseł zapisanych na słynnych żółtych karteczkach”, widocznych w tle. Warto rozważyć jakie informacje przekazywane są w sieciach społecznościowych, nawet w dobrej wierze. „Kamyczkiem do ogródka” może być choćby pochwalenie się pozytywnym wynikiem trudnego i wymagającego egzaminu z zarządzania nowym systemem, który właśnie zainstalowano w sieci wewnętrznej danej jednostki.

Poszukując w ramach rekonesansu informacji na temat organizacji, pentester podobnie jak atakujący sprawdzi wszystkie możliwe ślady. Przejrzy stronę WWW, zobaczy artykuły na temat celu, spróbuje pobrać z Internetu wszystkie dokumenty o organizacji, które znajdzie, a nawet spróbuje się zaprzyjaźnić z jej pracownikami i przejrzy ich profile. Sprawdzi informacje dostępne publicznie w Internecie, a niezbędne do zapewnienia widoczności – takie jak wpisy DNS, dane o adresach poczty elektronicznej itp. Tego typu czynności noszą miano „Białego wywiadu” (OSINT - czyli *Open Source Intelligence*). Większość tych informacji można uzyskać właściwie nie pozostawiając żadnych śladów na serwerach organizacji. Stąd też inna nazwa tej techniki – rekonesans pasywny.

Kiedy atakujący upewni się, że za pomocą białego wywiadu nie jest w stanie uzyskać więcej danych, skategoryzuje te już posiadane pod kątem ich przydatności. Przeanalizuje je dokładnie i przejdzie do skanowania sieci swojego celu. Innymi słowy, na gruncie informatycznym, zanim jeszcze dojdzie do fazy właściwego ataku, najczęściej nastąpi skanowanie adresów IP organizacji. Na podstawie takiego skanowania uzyskać można informacje o tym, jakie zasoby organizacja udostępnia w Internecie. Możliwe jest znalezienie serwerów WWW, e-mail i wszystkich innych usług, które są widoczne w sieci

publicznej. Nawet tych, które z perspektywy instytucji zostały zapomniane, lub o których istnieniu nie posiada ona wiedzy.

Po wykonaniu rekonesansu atakujący zaczyna szykować uderzenie. Wiedząc, czego może się spodziewać w środowisku wybranej organizacji, przygotowuje oprogramowanie, które będzie mu niezbędne w trakcie wrogiego działania skierowanego przeciw konkretnej instytucji. Jeśli na przykład dowiedział się, że administratorzy organizacji popełnili błąd w czasie konfiguracji serwera WWW, przygotowuje zestaw programów, które tę podatność wykorzystują. Jeśli z wykonanego rekonesansu wnioskuje, że w organizacji stosuje się rozwiązanie antywirusowe konkretnego dostawcy i konkretną wersję systemu operacyjnego – może przygotować własny zestaw złośliwego oprogramowania, który nie zostanie wykryty przez żaden z zastosowanych wewnątrz firmy komponentów bezpieczeństwa.

Cały wyżej opisany proces, trwający niekiedy dość długo, nazywa się fazą zbrojenia. W jego trakcie wykorzystuje się każdy skrawek informacji, jaki dotychczas uzyskano o celu. Przygotowuje się całość arsenału i rozważa wszystkie metody dostarczenia tego arsenału do organizacji, która ma zostać zaatakowana. W trakcie tego kroku możliwe jest choćby przygotowanie fałszywych stron, którymi będzie „wabić się" pracowników organizacji. Jest to proces bardzo żmudny i choć technicznie bardzo ciekawy, to jednak stosunkowo mało interesujący – stąd pominięcie już dalszych szczegółów. Niemniej należy pamiętać, że choć jest pracochłonny i czasochłonny, to często proces ten kończy się wygenerowaniem „gotowców", które można dostosować do wykorzystania w następnych atakach. Pozwala to zarówno wprawnym pentesterom, jak i atakującym na skrócenie następnych fazy zbrojenia.

Po realizacji wcześniej opisanych działań, nastaje czas „wejścia". Atakujący musi w jakiś sposób uzyskać kontrolę nad choćby jednym komputerem / jedną stacją w sieci organizacji. Do tego celu może wykorzystać wykryte podatne oprogramowanie, obecne w sieci organizacji i zwłaszcza to dostępne w Internecie. Wiedząc o podatnym oprogramowaniu dostępnym z poziomu Internetu, atakujący może podjąć próbę uderzenia bezpośrednio w ten punkt. W tym celu dostarczy wybranemu obiektowi tak zwany „exploit" – czyli spreparowane fragmenty oprogramowania, wykorzystujące podatność i zawierające polecenia atakującego. Jeśli cios okaże się skuteczny, system wykona zestaw komend przygotowanych przez napastnika. Ta faza, czyli faza uruchomienia, zazwyczaj wykonuje się autonomicznie. Atakujący może jedynie mieć nadzieję, że poprawnie przygotował kod „exploit", który uzyska w ten sposób formę kontroli nad działaniem podatnego systemu.

Jednym ze sposobów uzyskania nieautoryzowanego dostępu do chronionej sieci jest uderzenie z wykorzystaniem inżynierii społecznej (*social engineering*). Metoda ta polega na wykorzystaniu ludzi, oraz ludzkich cech do osiągania zakładanych celów. Najczęściej bazuje na zaangażowaniu emocji.

Większość osób zwykle kieruje się chęcią dobrego postępowania. Wobec tego chce pomóc osobie w potrzebie, albo też lubi czuć się docenianymi. W takiej sytuacji atakujący może wysłać do pracownika organizacji wiadomość z prośbą o pomoc:

„Przepraszam, ale właśnie uświadomiłem sobie, że podałem Państwu w umowie niewłaściwy numer konta. Proszę o pilną zmianę na niżej podany: [tu numer konta oszusta]. Bardzo dziękuję za sprawną pomoc i reakcję!"

W podobny sposób atakowano i wykradano pieniądze lub dane z urzędów i firm na całym świecie. Schemat takiego ataku wykorzysta także pentester, zwany czasem etycznym hakerem. Takiej osoby oczywiście nie interesują oszustwa, natomiast jego celem jest w ramach testu właśnie zainfekowanie komputera wewnątrz organizacji. Pentester również wykorzystuje inżynierię społeczną w celu skłonienia pracownika do uruchomienia wysłanego mu programu. Popularne treści wiadomości, które mają za zadanie skłonić użytkownika do uruchomienia „złośliwego" odnośnika, to między innymi:

„Czy to ty jesteś na tym zdjęciu?", „Nie spodziewałem się tego po tobie – cały artykuł o tym co zrobiłeś napisali[...]", „Gratulacje! Szkoda, że dowiedziałem się o tym dopiero z tej strony[...], a nie od Ciebie...". Metody i sformułowania są w zasadzie niegraniczone. W tym zakresie, co do treści e-maila i sposobu na „podejście" pracownika organizacji, pentester w ramach umowy zazwyczaj zapewnioną ma sporą dozę autonomii – a już na pewno realny atakujący nie ma żadnych skrupułów.

Informacje zebrane z kont sieci społecznościowych w fazie rekonesansu ułatwiają dobranie właściwej treści. Jeśli pracownik udostępnia zdjęcia z dalekich podróży, otrzymuje przygotowaną dla niego ciekawą ofertę wyjazdu z atrakcyjną propozycją. Jeśli zatrudniony trenuje konkretny sport, zostaje zaproszony na pokaz lub zajęcia pod warunkiem wypełnienia „króciutkiej ankiety". I tak dalej.

Inną metodą dostarczenia złośliwego oprogramowania jest podrzucenie nośnika. Przykładowo, pracownik znajduje pendrive z wartościowym breloczkiem lub kluczykiem. Osoba, ponownie kierowana współczuciem, ciekawością lub chęcią działania, sprawdzi co znajduje się na znalezionym nośniku. Przynęta działa!

Obie metody inżynierii społecznej co do istoty stanowią zakończenie fazy dostawy. W tym momencie rozpoczyna się faza uruchomienia: podłączenie takiego urządzenia do komputera w sieci firmowej lub otwarcie jakiegokolwiek pliku na nim. Kliknięcie w linka w spreparowanym e-mailu, wejście na złośliwą stronę, czy też udane wykonanie kodu exploit'a powoduje najczęściej wykonanie złośliwego kodu

(faza uruchomienia) i pierwszy poważny sukces atakującego. Atakującemu wystarczy przejąć kontrolę tylko nad jednym komputerem w organizacji, a każda ze wspomnianych powyżej akcji zakończona udanym uruchomieniem kodu w ostatecznym rozrachunku umożliwia mu to.

Zarówno w niniejszym opracowaniu jak i w rzeczywistości sama faza uruchomienia jest najkrótszą, ale jednocześnie kluczową dla powodzenia dalszego ataku. W momencie uruchomienia złośliwego oprogramowania następuje faza instalacji, która ma na celu pobranie pozostałych niezbędnych narzędzi, potrzebnych napastnikowi do sprawnej pracy w systemie zaatakowanej organizacji. Narzędzia te przygotowane w fazie zbrojenia czekają najczęściej na pobranie na przygotowanym wcześniej serwerze. Część z tych narzędzi ma za zadanie dać pełne uprawnienia w zaatakowanym systemie, część z nich ma zapewnić, że zostanie wyłączona ochrona antywirusowa. Zestaw narzędzi do pobrania może być inny dla każdego celu, ale ponieważ narzędzia raz stworzone w fazie zbrojenia można wykorzystać ponownie podczas atakowania innego celu, agresor często będzie wykorzystywał ten sam zestaw narzędzi do atakowania różnych środowisk

Dla atakującego ważne jest precyzyjne przygotowanie. Każde dodatkowo pobrane narzędzie może spowodować wcześniejsze wykrycie obecności, oraz identyfikację jego tak zwanych TTP (*tactics, techniques and procedures*). W konsekwencji (oczywiście z perspektywy napastnika) może to spowodować właściwą reakcję organizacji na atak, eliminację pozostałego arsenału atakującego i w efekcie potrzebę cofnięcia się w całym procesie do początku fazy dostawy lub nawet do fazy rekonesansu.

W sytuacji, w której system organizacji zostanie „przejęty”, nastąpi pobranie z serwera atakującego dodatkowego oprogramowania, oraz skuteczna instalacja tego „software’u”, pozostaje już tylko jeden krok do wykonania. Mianowicie, krok ten stanowi nawiązanie przez oprogramowanie połączenia z serwerem zarządzającym (*Command and Control*), który ma za zadanie ułatwić sprawowanie kontroli nad większą liczbą przechwyconych systemów. W ten płynny sposób możliwe jest przejście do ostatniego elementu łańcucha „Cyber Kill Chain”, czyli do właściwej misji.

Nawiązując do ogółu dotychczas przedstawionych działań należy pamiętać, że sam proces włamania do systemu w zdecydowanej większości przypadków nie jest jeszcze celem samym w sobie i tym, do czego dąży „intruz”! Pentester wciąż żmudnie zmierza do wykonania misji, jaką dla niego stanowi zdefiniowane w zleceniu zadanie. Wykonuje zatem ponownie cały proces „Cyber Kill Chain”, z tym że już wewnątrz sieci organizacji. Natomiast dla realnych atakujących, których intencje są nakierowane na wyrządzenie szkód, czy wymuszenie profitów, celem może być upublicznienie poufnych informacji na temat organizacji, żądanie okupu za przechwycone dane, wyrządzenie nieodwracalnych strat czy zakłócenie ciągłości funkcjonowania. Agresorzy, aby osiągnąć większy efekt włamania do organizacji, będą powtarzać elementy łańcucha „Kill Chain” już od wewnątrz.

W tym momencie warto wspomnieć o ogromnej różnicy w skutkach działania obu wspominanych wcześniej jednostek. Pentester pod koniec prowadzonego testu dokładnie opisuje metody, wykorzystane do zaatakowania systemu / systemów organizacji. Przygotowuje również dla tej organizacji zalecenia, które należy wdrożyć, aby atak na jej struktury przeprowadzony we wskazany lub pokrewny sposób był utrudniony lub niemożliwy. Działa zatem przede wszystkim na rzecz danej instytucji. Złośliwy atakujący natomiast dąży do osiągnięcia własnych korzyści, na przykład w postaci uzyskania „nagrody” pieniężnej, wartości materialnej lub niematerialnej, bądź spowodowanie strat po stronie zaatakowanego.

3.1. Przykład

W celu lepszego zobrazowania działań w ramach „Cyber Kill Chain”, przedstawiony zostanie typowy atak na system firmy z sektora produkcyjnego. W dniu „zero” ataku, kilkuset użytkowników firmy otrzymuje e-mailem fałszywe wezwania do zapłaty faktury (faza dostawy). Część z nich, nie będąc bezpośrednio odpowiedzialnych za faktury, po otwarciu załącznika stwierdza, że należy tego e-maila przesłać do działu księgowości. Na każdym z komputerów, na którym otwarto załącznik, zostaje jednak uruchomiony mały program (faza uruchomienia). Identyfikuje on oprogramowanie antywirusowe, pobiera właściwy moduł wyłączający tego antywirusa (faza instalacji), oraz łączy się z serwerem zarządzającym i otrzymuje serię rozkazów (faza przekazania kontroli). Następnie w wyniku tych rozkazów pobiera kolejny moduł złośliwego oprogramowania, który za pomocą podatności w systemie operacyjnym rozprzestrzenia się po całej sieci organizacji i szyfruje dane zgromadzone na stacjach roboczych i serwerach (misja właściwa).

Po wykonaniu powyższej akcji, oprogramowanie wyświetla żądanie okupu za odblokowanie dostępu do danych. Firma decyduje się nie ulegać bezpośrednim żądaniom i nie opłaca okupu, jednak przywracanie danych z kopii zapasowych i czyszczenie systemów po infekcji zajmuje wiele czasu. Przez ten czas, zdolność produkcyjna organizacji jest znacząco ograniczona. Nawet jeśli przywrócono już poprawne działanie stacji operatorskich, część danych – na przykład przedstawiających zapotrzebowanie na produkty firmy – jest nadal w trakcie odzyskiwania z kopii zapasowych.

W przedstawionym przykładzie nie są w sposób jawny widoczne elementy wstępnej fazy rekonesansu. Musiała mieć ona jednak miejsce, ponieważ atakujący wysłali złośliwe e-maile do konkretnych osób w firmie. Faza zbrojenia również została wykonana wcześniej, ponieważ pobrane moduły wykorzystywały relatywnie nowe podatności w systemach operacyjnych. Złośliwe oprogramowanie szyfrujące dane użytkowników nosi miano „ransomware" i w ostatnich latach jest zdecydowanie najpopularniejszą metodą wykorzystywaną przez grupy przestępcze.

Warto zwrócić uwagę na fakt, że czas trwania ataków, czyli właściwie czas wykonywania całości działań „Cyber Kill Chain" nie jest stały dla każdej grupy atakujących. W niektórych przypadkach pełen atak trwa kilkanaście godzin, na przykład przy masowych kampaniach „phishing'owych". Te, ze względu na ich widoczność w sieci, często są blokowane już po kilku godzinach, po czym intruzi zmuszeni są rozpoczynać nową kampanię. W innych przypadkach wykonywanie napadu trwa tygodniami lub nawet miesiącami. Tak długie kampanie określa się atakami APT (*Advanced Persistent Threat* czyli Zaawansowane Trwałe Zagrożenie). Tego typu atakami mogą być szczególnie działania ukierunkowywane na infrastrukturę krytyczną w postaci elektrowni czy sieci energetycznych. Opisana natomiast wroga akcja wobec firmy produkcyjnej to raczej działanie klasyfikowane do pierwszego typu szybkiego ataku.

4. Zrywanie łańcucha

Z perspektywy napastnika możliwe jest już zakończenie niniejszego opracowania… Niemniej, dla środowiska użytkowników sieci OT, właściwie dopiero teraz zaczyna się działanie! Aktywność tę stanowi zakłócanie łańcucha „Cyber Kill Chain".

W jaki sposób możliwe jest przerywanie tej „wycieczki" w nieznane, którą stanowi atak na system organizacji?

W dalszym toku dokumentu przedstawione są czynności, które można wykonać, aby zakłócić i powstrzymać wrogie działanie – ze szczególnym uwzględnieniem specyfiki środowisk automatyki przemysłowej. Metody przerywania „Cyber Kill Chain" można pogrupować w sześć kategorii:

- wykrywanie,
- blokowanie,
- przerywanie,
- degradacja,
- oszustwo,
- ograniczenie.

Każda z tych kategorii pozwala grupie obrońców sieci na rozpoczęcie działań, które w efekcie uniemożliwią atakującym przeprowadzenie skutecznego ataku na systemy w sieci organizacji. Przed przejściem do opisu każdej z tych kategorii, na wstępie należy jednak przytoczyć hasło dotyczące nie tylko świata bezpieczeństwa IT/OT. Hasło, które z pozoru wydaje się oczywiste…

„Nie można zabezpieczyć czegoś, czego się nie zna".

To bardzo ważne, by mieć w pamięci rzeczone hasło jako punkt wyjścia. W kontekście systemów, z którymi automatycy stykają się na co dzień, maksyma ta sprowadza się do żmudnego obowiązku wykonania rzetelnej inwentaryzacji komponentów zabezpieczanego systemu. Oczywiście nie oznacza to obowiązku wykonywania pracy samodzielnie! Istnieją systemy i usługi, które wspierają przedstawicieli firm i instytucji w realizacji już tego pierwotnego zadania. Przykładem takiej platformy jest Radiflow iSID, umożliwiający zinwentaryzowanie wszystkich widocznych w sieci urządzeń wraz z następującą między nimi komunikacją. Raport wygenerowany w oparciu o powyższy proces, połączony z właściwym know-how, pozwala na stworzenie solidnej dokumentacji, która staje się niezbędną bazą do podjęcia dalszych, opisanych poniżej, kroków.

Wykrywanie. Wykrywanie jest jedną z najważniejszych metod działania. Choć samo w sobie nie prowadzi do zablokowania żadnego ataku, to jednak w środowiskach sieci przemysłowych właściwość tę przyjmuje się w kontekście zalet. Powodem takiej oceny jest świadomość, że błędne wstrzymanie komunikacji między elementami sieci przemysłowej może przerwać działanie procesu. Pasywne wykrycie pozwala natomiast obrońcom sieci przygotować się na atak, lub rozpocząć procedury reakcji na incydent w momencie stwierdzenia podejrzanego zachowania w infrastrukturze OT. Następuje to bez ryzyka zakłócenia pracy sieci procesowej.

Detekcja. Detekcja może ujawnić każdą z faz „Cyber Kill Chain". Począwszy nawet od wykrywania pasywnego rekonesansu – za pomocą właściwie przeprowadzonej analityki wykorzystania serwerów WWW, lub za pośrednictwem przeszkolonego personelu, który rozpoznaje działania związane z fazą rekonesansu. Jednym z istotnych elementów detekcji są urządzenia brzegowe funkcjonujące w ramach IDS (*Intrusion Detection System*). IDS to system wykrywający włamania do sieci lub hostów (komputerów) w organizacji. Dobrze zaprojektowany IDS ujawnia anomalie sieciowe i wzorce ruchu

wykonywanego przez włamywacza. Sam IDS to również rozwiązanie pasywne, które po wykryciu włamania zgłasza ten fakt, ale nie blokuje ataku ani procesu.

Sieciowy IDS pozwala na wykrycie fazy zbrojenia, kiedy to atakujący musi zweryfikować czy program, który przygotował, działa poprawnie w docelowym środowisku. Szkolenie personelu skutecznie podnosi umiejętności wykrywania metod związanych z socjotechnikami, co dodatkowo wpływa na odkrywanie fazy dostawy.

Fazy uruchomienia i instalacji zauważane są przez system IDS zainstalowany w atakowanym środowisku. Sieciowy IDS nie jest także obojętny na próbę podłączenia się złośliwego oprogramowania do serwera zarządzającego, a działania na przejętych systemach są wykrywane przez analizę dzienników audytu. Co ważne – ma to miejsce zazwyczaj w sposób pasywny, którego wdrożenie i używanie nie ma negatywnego wpływu na obserwowaną sieć. To krytyczny argument w kontekście sieci ICS.

Jak można wywnioskować na podstawie powyższych zapisów, sama obserwacja sieci i systemów daje sporą przewagę nad atakującym. To siła monitoringu w kontekście ochrony sieci OT. Wykorzystanie narzędzi pasywnych, nie ingerujących w infrastrukturę OT, a umożliwiających wykrycie i tym samym skrócenie czasu reakcji, daje solidny fundament do budowania kolejnych elementów ochrony aktywnej. Tę samą opinię wyraża regulator w postaci ustawy o Krajowym Systemie Cyberbezpieczeństwa. W tym kontekście warte uwagi są usługi polegające na wdrożeniu przemysłowej platformy IDS i przygotowaniu raportu o stwierdzonych problemach w sieci. Taki raport bardzo często jest pierwszym krokiem do znaczącej poprawy bezpieczeństwa sieci organizacji.

Blokowanie. Blokowanie ma równie mocny, jeśli nie mocniejszy, wpływ na przerwanie łańcucha „Kill Chain". Podstawą jego działania jest wymuszanie polityk bezpieczeństwa. I tak, w fazie rekonesansu skutecznie wymuszona polityka na firewall'u brzegowym ograniczy bardzo mocno skuteczność skanowania sieci i portów. Podczas testowania oprogramowania w fazie zbrojenia, urządzenia zwane IPS (*Intrusion Prevention System* – to jest zapobiegające włamaniom, mogące zablokować ruch wykryty jako złośliwy) umieszczone na brzegu sieci uniemożliwiają atakującemu przeprowadzenie skutecznych testów. W ostatecznym rozrachunku oznacza to, że nawet z przygotowanym idealnym oprogramowaniem, atakującym system „ofiary" i pozwalającym agresorowi przejąć nad nim kontrolę, IPS uniemożliwia intruzowi wykorzystanie tego oprogramowania w trakcie fazy dostawy.

Wspomagającym elementem składowym jest także „proxy" – czyli system pośredniczący w połączeniach do innych urządzeń (host'ów). Najczęściej spotyka się serwery proxy, które pośredniczą w komunikacji do serwerów WWW. Proxy może filtrować taki ruch na podstawie wbudowanych list reputacji danego adresu, pobieranych w czasie rzeczywistym od producenta lub utrzymywanych lokalnie. Odpowiednio skonfigurowany filtr proxy uniemożliwia infekcję systemu przez kliknięcie w złośliwy odnośnik.

Fazę uruchomienia złośliwego oprogramowania, a w szczególności „exploit'a", skutecznie utrudnia wdrożenie rygorystycznej polityki nakładania łatek (poprawek) dla oprogramowania. Fazę instalacji dodatkowego oprogramowania można skutecznie zakłócić przez właściwe ograniczenie uprawnień użytkownika – uniemożliwiające mu pobieranie i uruchamianie oprogramowania, zwłaszcza na wysokim poziomie przywilejów. Fazy przekazania kontroli i działania na zainfekowanym systemie w ramach misji właściwej zablokować można natomiast stosując firewall'e z ich właściwą konfiguracją. Wreszcie działania ostatniej fazy „Kill Chain" przerywa się, stosując polityki ograniczające ruch wychodzący z systemu.

Opisane powyżej metody ograniczania łańcucha „Kill Chain" stanowią absolutne minimum. Warto jednak zauważyć, że w przypadku błędnej konfiguracji któregokolwiek ze sposobów blokowania, istnieje ryzyko uszkodzenia kontroli procesu. O ile w sieciach ICT przerwa w działaniu systemu będzie miała co najwyżej skutki finansowe, to w przypadku sieci ICS takie przerwanie lub opóźnienie komunikacji może mieć fatalne skutki dla ciągłości procesu. W najgorszym przypadku może nawet skutkować wypadkiem i uszczerbkiem na zdrowiu personelu. Dlatego też prace wykonane w sieciach OT w zakresie konfiguracji urządzeń z tej grupy i jakiekolwiek podjęte akcje muszą być poprzedzone dogłębną analizą wymiany danych między komponentami systemu, oraz konsultacjami z właścicielem systemu, a w razie wątpliwości z jego producentami. Urządzenia IPS, firewall i proxy należy dokładnie przeanalizować, a ich konfigurację przetestować w różnych stanach pracy systemu automatyki.

Istotnym zagadnieniem w odniesieniu do całości opisywanych metod i systemów jest rozważenie miejsca w architekturze, w którym zastosowanie systemów aktywnych (brzeg sieci, segmentacja fragmentów sieci), oraz pasywnych (blisko procesu czyli typowa sieć ICS) jest najlepsze. Dobrze jest chronić aktywnie sieć na jej brzegu, oraz w newralgicznych kanałach komunikacyjnych – stosując firewall'e, IPS, diody, oraz monitorowanie całości sieci (ochrona pasywna) z zastosowaniem odpowiednich narzędzia dla IT i OT w odpowiednich okolicznościach. Co ciekawe, niekiedy mniej istotna jest natychmiastowa reakcja, a wyraźnie ważniejszy krok stanowi efektywne, a więc bezpieczne dla procesu, wykrycie ataku.

Przerwanie. Przerwanie to metoda, która ma za zadanie zatrzymać trwający już atak. Nie ma ona wpływu na fazy rekonesansu i zbrojenia. Zdarzają się sytuacje, w których niektóre metody blokowania dostawy

okazują się nieskuteczne. W tych momentach przydatne okazuje się posiadanie dodatkowej warstwy obrony w postaci systemu antywirusowego „inline", czyli skanującego przechodzący przez niego ruch. Jeśli filtr proxy nie blokuje złośliwego odnośnika, antywirus inline wykrywa zagrożenie i uniemożliwia przeniknięcie do atakowanego systemu. Jeśli pamięć po szkoleniu zawodzi lub użytkownik ulega pokusie łącząc zainfekowany pendrive do stacji roboczej, odpowiednio skonfigurowane urządzenia DEP i ASLR przerywają fazę uruchamiania „exploit'a". Co to jest DEP i ASLR? DEP (*Data Execution Prevention*) to metoda ochrony systemów operacyjnych przed exploit'ami wykorzystującymi podatność przepełnienia bufora. ASLR (*Address Space Layout Randomisation*) to natomiast metoda ochrony systemów, strzegąca przed atakami nadpisującymi pamięć aplikacji. Gdy okazuje się, że i one zawodzą, lub są nieodpowiednio skonfigurowane, fazę instalacji powstrzymuje zainstalowany antywirus.

Faza przekazania kontroli jest zatrzymywana dzięki poprawnie skonfigurowanemu IPS'owi sieciowemu, a misja właściwa, polegająca na wykradaniu danych, jest skutecznie przerywana przez wdrożony i poprawnie skonfigurowany system DLP (*Data Loss Protection*). DLP to platforma zapobiegająca wyciekowi danych. Jej zasada działania opiera się na klasyfikacji poufności danych i systemów, a następnie blokowaniu przepływu danych poufnych do systemów o niższej klasyfikacji. Należy zauważyć jednak, że systemy przerywające połączenia – tak samo jak systemy blokujące opisane nieco wcześniej – najbezpieczniej wdrożyć na granicy sieci IT i OT. Wewnątrz sieci ICS między strefami bezpieczeństwa wdrożenie musi być poprzedzone szczegółową analizą. Jej celem jest weryfikacja czy wdrożony system nie przerywa istotnej komunikacji między elementami procesu.

Łączność sieci ICS ze światem zewnętrznym co do zasady powinna być maksymalnie ograniczona. Niemniej w pewnym aspekcie stanowi to kolejne wyzwanie. Mianowicie wyzwanie to dotyczy konieczności systematycznej aktualizacji opisywanych zabezpieczeń – bez niej mogą okazać się nieskuteczne. Oczywiście istnieją sposoby zaplanowania aktualizacji w sposób kontrolowany i bezpieczny, niemniej jest to kolejny element architektury, który wymaga innego podejścia zarówno we wdrożeniu, jak i w trakcie eksploatacji.

Na rynku dostępne są systemy klas inline AV, IPS sieciowy i DLP. Wdrożenie każdego z tych systemów poprzedzone musi być wnikliwą analizą. Dla wszystkich tych klas należy wykonać wiele prac przygotowawczych, których ciężar najczęściej leży po stronie zainteresowanego. Poprawne wdrożenie każdego z tych systemów jest trudnym i żmudnym działaniem, ale niesie za sobą oczywiście dodatkowe korzyści. Zawsze istotne jest spojrzenie z perspektywy ryzyka. Polega ono na ocenieniu z jednej strony w jakim stopniu wdrożenie danego elementu infrastruktury wpłynie na minimalizację całościowego ryzyka organizacji, oraz z drugiej strony ile będzie organizację kosztowało. Co do strony finansowej, należy uwzględnić koszty CAPEX, OPEX, oraz przygotowania instytucji do poprawnej obsługi danego systemu. Najlepszy bowiem system, jeżeli nie zostanie poprawnie wdrożony i skonfigurowany, lub jeżeli powinien być tylko jednym z wielu elementów, a już wykorzystuje większość budżetu przeznaczonego na cyberbezpieczeństwo – nie tylko nie wpłynie na efektywne ograniczenie ryzyka, ale może to ryzyko podnieść przez wprowadzenie złudnego „dobrego samopoczucia". Cyberbezpieczeństwo wymaga strategicznego podejścia i planowania popartego rzetelną analizą ryzyka i powinno stanowić odpowiedź na tę analizę w postaci minimalizacji kolejnych, największych ryzyk stwierdzonych w organizacji.

Degradacja

Degradacja to w skrócie metoda polegająca na tym, że uniemożliwia atakującym pracę z zainfekowanym systemem w sposób łatwy i szybki. Najczęściej degradacja dotyczy trzech faz. Pierwszy przypadek to faza dostawy, podczas której złośliwe oprogramowanie zostaje dodane do kolejki. Może to powodować znaczne opóźnienie w jego wykonaniu, a u atakującego sprowokować myśl o braku sukcesu przedsięwzięcia. Faza przekazania kontroli i misja właściwa to kolejne dwie, które można skutecznie zdegradować. Może to mieć miejsce na przykład przez zastosowanie systemów klasy tarpit, które spowalniają złośliwą pracę w sieci na tyle, że obrońcy mają czas na wykrycie ruchów agresorów. Inną skuteczną metodą jest wdrożenie polityk QoS w sieci, skutecznie ograniczające pasmo przydzielone na komunikację nieznanego pochodzenia. W tym układzie złośliwe działania będą obarczone sporym opóźnieniem w transmisji, a to nigdy nie sprzyja komfortowi pracy atakujących.

Oszustwo

Wprowadzanie w błąd to nie tyko domena atakujących – obrońcy również mogą oszukiwać wroga. Do tego celu służą głównie dwie klasy rozwiązań. Pierwsza to DNS Redirect, czyli ośrodek powodujący, że realizacja fazy przekazania kontroli i dostawy zostaje skierowana do środowisk analitycznych, stworzonych przez obrońców. Druga klasa rozwiązań to „honeypot", który ma za zadanie udawać łakomy dla intruza kąsek. Podczas ataku na system, w trakcie testów poszukujących najciekawszych dalszych celów, zauważenie tak wspaniale wyglądającego obiektu przyciąga uwagę agresora. Honeypot najczęściej jest pod ścisłą obserwacją obrońców, przez co zdarza się, że działając na nim, atakujący ujawnia swoje techniki i zdradza, na co należy się przygotować, a sam nie uzyskuje nic w zamian.

Ograniczenie. Ostatnia, lecz nie najmniej ważna metoda to ograniczenie. Jest to mechanizm, który ma za zadanie zmniejszyć wpływ każdej z faz „Cyber Kill Chain" na końcowy rezultat ataku. Wśród technik stosowanych w celu ograniczenia możliwości niepowołanego działania występuje między

innymi prosta a skuteczna segmentacja sieci – czyli podzielenie sieci organizacji na wycinki o konkretnych funkcjach, na przykład księgowość, automatyka, zarząd, proces. Taki podział na strefy bezpieczeństwa bardzo mocno utrudnia pracę atakującemu. Zastosowanie firewall'a z ACL zawęża widoczność podczas fazy rekonesansu. Wykorzystanie IPS sieciowego obniża skuteczność przygotowanego arsenału, ponieważ nie pozostawia pola do testowania. Użycie firewall'a aplikacyjnego zmusza do dokładnego trzymania się specyfikacji protokołów, co zwiększa prawdopodobieństwo popełnienia przez atakującego błędu. Wprowadzenie IPS między strefami bezpieczeństwa bardzo utrudnia uruchomienie „exploit'a" na kolejnych systemach. Zastosowanie antywirusa na stacjach roboczych i serwerach praktycznie utrudnia agresorowi instalację dodatkowych programów. Wdrożenie stref w połączeniu ze zdefiniowanymi poziomami zaufania do każdej z nich powoduje, że komunikacja do serwera zarządzającego jest utrudniona lub niemożliwa. Dokładnie ten sam efekt jest widoczny dla dalszych działań, które atakujący usiłuje wykonać w zaatakowanym systemie w ramach misji właściwej.

Inwentaryzacja, separacja sieci OT od sieci IT, oraz zapewnienie widoczności zdarzeń za pomocą platformy IDS to fundamenty, które należy stworzyć w sieci przemysłowej. Dalsza kolejność wdrażania technik ochronnych w zasadzie ma już niewielkie znaczenie, ponieważ każda metodyka dodaje kolejną warstwę, której atakujący musi sprostać. Zapamiętać należy jednak, że każda z nich ma konkretne zastosowanie i określoną skuteczność w przerywaniu konkretnych faz łańcucha „Kill Chain". Niektóre z działań – takie jak monitoring ICS – warto wdrożyć w pierwszej kolejności, bowiem przekazywane informacje o wykrytych podatnościach, oraz próbach ich wykorzystania stanowią nieocenioną pomoc dla zespołu obrońców i są pomocne w planowaniu kolejnych kroków. Warto też dość wysoki priorytet nadać podstawowym metodom blokującym, takim jak firewall. Pozwalają wszak „złapać oddech" i przygotować dalsze metody w sposób w miarę systematyczny i zorganizowany.

Wiele uwagi w tej części artykułu jest poświęcone obrońcom. W żargonie cyberbezpieczeństwa obrońców określa się mianem „Blue Team". Niebieski kolor tego zespołu, kojarzony z policją mającą za zadanie chronić obywateli, nie jest oczywiście przypadkowy. Najczęściej zespoły Blue Team to wydzielone w organizacjach komórki SOC (*Security Operations Centres*), których zadaniem jest koordynacja działań związanych z cyberbezpieczeństwem organizacji. Zespoły te przeważnie wyposażone są w systemy klasy SIEM (*Security Information and Event Management),* zbierające informacje z chronionej infrastruktury, korelujące je w czasie, wykrywające symptomy ataków i pozwalające obrońcom na sprawną reakcję na incydenty. Systemy te mają postać gotowych platform, stosowanych w środowiskach korporacyjnych, lub postać platform „open source", stosowanych w mniejszych środowiskach, albo w przypadku ograniczonego budżetu. Te drugie zwykle wymagają sporo pracy zespołu SOC w celu dostosowania ich do potrzeb organizacji. Te pierwsze zawierają natomiast gotowe moduły, które zapewniają Blue Team'owi zestaw podstawowych narzędzi, pozwalających na rozpoczęcie właściwej pracy. Co więcej, zakup systemu SIEM klasy korporacyjnej najczęściej połączony jest z usługami wsparcia, z których obrońcy mogą skorzystać w przypadku wystąpienia problemów z jego działaniem. Platformy open source, stosowane zazwyczaj ze względu na nieposiadanie budżetu, bez wykupienia dodatkowej usługi wsparcia pozostawiają całość prac konfiguracyjnych na barkach zespołu SOC. Systemy SIEM zasilone odpowiednim strumieniem informacji, z opracowanymi regułami korelacji dla interesujących Blue Team zdarzeń, stanowią potężne wsparcie – wymagane do skutecznego zabezpieczenia sieci i narzędzi organizacji.

Zespoły SOC najczęściej składają się ze specjalistów znających doskonale architekturę swoich sieci i systemów, oraz posiadających obszerną wiedzę z zakresu cyberbezpieczeństwa teleinformatycznego. Przeważnie wywodzą się z personelu IT organizacji. Te cechy pozwalają im rozpoznawać ataki na infrastrukturę instytucji często już na ich samym początku. Do obowiązków SOC należy również przygotowanie i wykonywanie planów reakcji na incydenty, a także skomplikowane analizy TTP atakujących. Ich możliwości są tym większe, im więcej metod przerywania „Cyber Kill Chain" wdroży organizacja.

Nawet w bardzo ograniczonym podstawowym środowisku, sama obecność osób śledzących zapisy monitoringu i będących w stanie rozpoznać atak, zapewnia minimalną możliwość reakcji na incydent. Także wtedy, gdy tą jedyną reakcją, jaką jest w stanie zastosować grupa SOC jest odłączenie sieci organizacji od Internetu. W przypadku, kiedy organizacja nie ma zasobów, które umożliwią zbudowanie własnego zespołu SOC, może posiłkować się rozwiązaniem „SOC as a Service". Możliwość ta daje szansę na skorzystanie z już działającego zespołu SOC w ramach jednostki świadczącej usługi dla swoich kontrahentów. Należy jednak pamiętać, że skorzystanie z takiej usługi wymaga czasu, w którym zespół usługodawcy pozna działanie i architekturę sieci zlecającego.

Optymalnym rozwiązaniem jest zbudowanie zespołów SOC wewnątrz organizacji, bazując na jej zasobach. Takie podejście jest zdecydowanie uzasadnione, ponieważ znajomość procesów zachodzących we własnej sieci jest kluczowym czynnikiem. Dodatkowo zdarza się, że w gronie personelu instytucji są już obecni utalentowani lub merytorycznie świadomi pracownicy, którzy stosunkowo szybko i umiarkowanym kosztem pozyskują i uzupełniają wiedzę, niezbędną do utworzenia zespołu SOC.

Niestety, należy jednak być świadomym, że realnie stworzenie działu SOC jest często bardzo trudne i wymaga dodatkowych etatów lub zmiany warunków (przekierowania innych obowiązków), dążących do realizacji nowych działań.

Poza już zarysowanymi opcjami bardzo kosztownego „SOC 24h", usługą „SOC 24h as a Service", oraz całkowitym brakiem SOC jest jeszcze kilka alternatyw do rozważenia, mogących być korzystnymi dla średnich i mniejszych organizacji. Przykładem może być oddelegowanie pracowników odpowiedzialnych za dany system do współpracy z firmą zewnętrzną, która będzie wspierać ich w analizie zachowania sieci i incydentów w trybie cyklicznym w wybranym modelu. Analiza sieci nawet w trybie raz na dwa czy raz na trzy tygodnie zawsze jest lepsza niż zupełny brak analizy – uzasadniany upraszczająco brakiem funduszy na SOC. Należy mieć na względzie, że czynności „Kill Chain" wymagają czasu. Niewiele ataków w obszarze OT charakteryzuje się natychmiastowym działaniem. Wiele z nich natomiast pozostaje zupełnie niezauważonych przez wszystkie pierwsze a nieagresywne fazy.

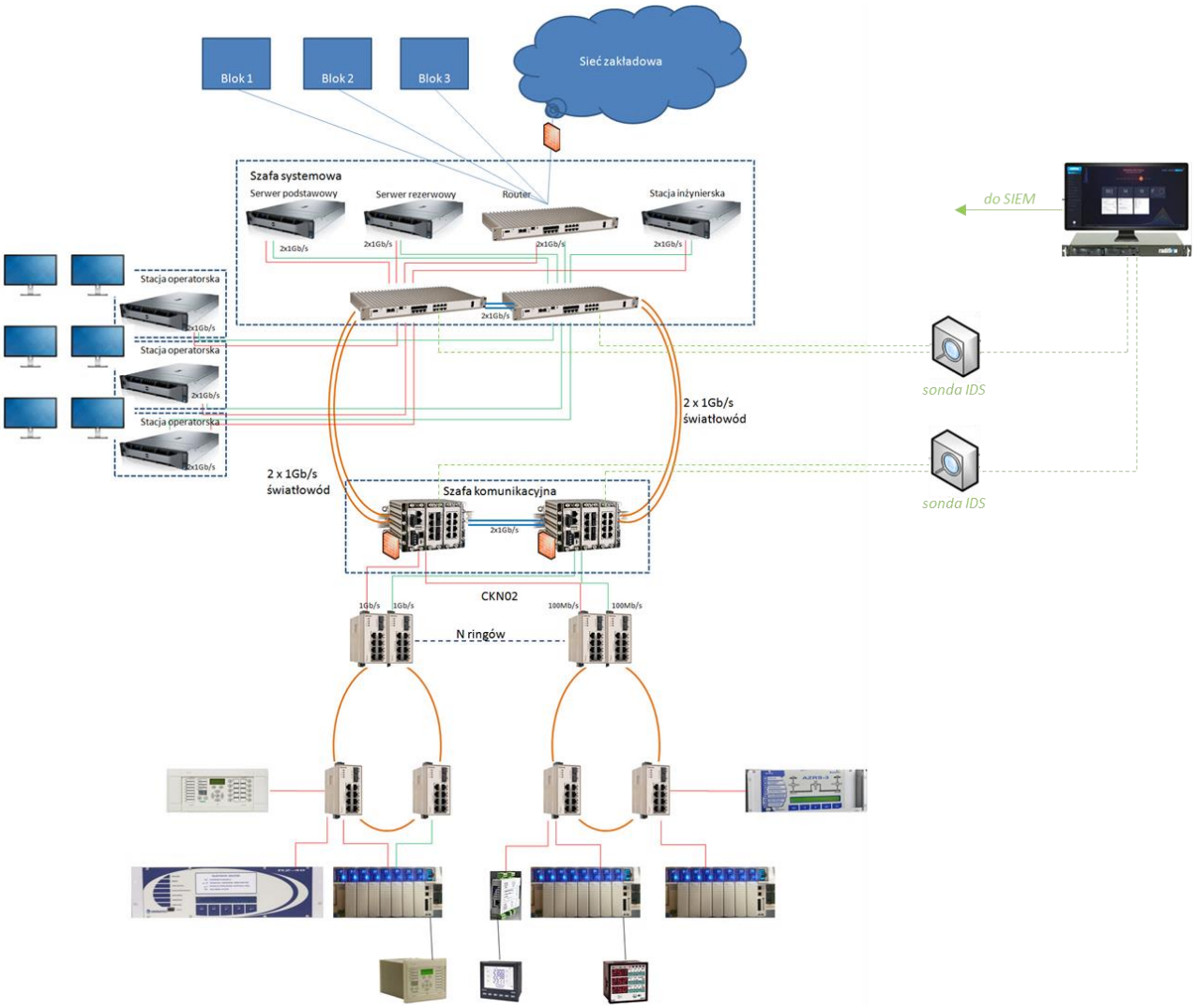
Procedura reakcji na incydenty to zagadnienie, którego omówienie może stanowić odrębne opracowanie. W skrócie, można opisać ten proces jako ogół działań niezbędnych do przywrócenia prawidłowej pracy systemów organizacji po mającym miejsce incydencie bezpieczeństwa. Najważniejszymi elementami tej procedury są identyfikacja wektora ataku i określenie tak zwanego „pacjenta zero", od którego rozpoczął się incydent, a także ograniczenie skutków incydentu i ostateczna naprawa naruszonych komponentów systemu. Reakcja wymaga od zespołu SOC zrozumienia incydentu, właściwego zakresu wiedzy odnośnie systemów i w szczególności posiadania informacji o osobach, które mogą być kluczowe w przywróceniu poprawnego funkcjonowania. Należy jednak jeszcze raz podkreślić – krytyczne jest zidentyfikowanie wektora ataku i uniemożliwienie ponownego jego wykorzystania. W przeciwnym wypadku, nawet najszybciej zrealizowana procedura reakcji nie powstrzyma atakującego przed powtórzeniem fazy dostawy i ponownym uruchomieniem złośliwego oprogramowania.

Za pośrednictwem firmy Tekniska Polska możliwe jest skorzystanie z usług szkoleniowych, zrealizowanie badania bezpieczeństwa sieci, wykonanie wdrożenia i modernizacji systemu, aż po prowadzenie przez proces analizy i reakcji na incydenty. W trakcie konferencji, na połączonym stanowisku ekspozycyjnym firm Tekniska Polska i SPIE Energotest, prezentowane są przykładowe architektury łączące techniki i wiedzę obu firm. Rysunek przedstawia uproszczonym schemat tego pokazu. Konfiguracja zawiera podstawowe elementy omawianych w opracowaniu zabezpieczeń, takie jak przemysłowy system IDS wraz z sondami, a także firewall'e chroniące segmenty sieci OT.

Wspomniane komponenty stanowią fundament bezpieczeństwa sieci organizacji. Atakujący od strony infrastruktury WAN spotyka się z oporem już na granicy sieć WAN / sieć OT. Pierwsze zabezpieczenia widoczne na schemacie to firewall'e aplikacyjne (tu marki „Stormshield"). Dostarczają one ochronę antywirusową inline, system IPS/IDS dedykowany dla protokołów OT, podstawowe funkcje DLP, filtr proxy, a jako firewalle aplikacyjne zapewniają wykrywanie i możliwość blokowania anomalii protokołów. Samo zastosowanie takich urządzeń na granicy sieci IT / OT wyraźnie wpływa na postawę bezpieczeństwa sieci (*security posture*).

Kolejną linię obrony stanowią same serwery i stacje robocze o właściwej konfiguracji, aktualizowane do najnowszych wersji oprogramowania. Następną warstwą zabezpieczeń są natomiast firewall'e wbudowane we właściwe urządzenia komunikacyjne, takie jak rutery czy przełączniki przemysłowe (tu marki „Westermo"). Odpowiednia konfiguracja, dopuszczająca jedynie uprawnione serwery do właściwych usług udostępnionych przez sterowniki i elementy zabezpieczeń przemysłowych, stanowi kolejny poziom ograniczający możliwości atakującego.

Wszystkie urządzenia sieciowe monitorowane są przez sondy systemu (tu marki „Radiflow"), zbierające dane z wszystkich portów sieciowych i przesyłające te informacje do centralnego analizatora przemysłowego IDS. Ten z kolei może przekazywać dane o wszystkich wykrytych nieprawidłowościach do systemu SIEM. System SIEM może gromadzić dane z każdego wspomnianego powyżej modułu cyberbezpieczeństwa. Firewall'e, switch'e, router'y, serwery i stacje robocze mogą – i powinny – być skonfigurowane w taki sposób, aby przesyłać dzienniki systemowe do platformy SIEM. Taka konfiguracja zapewnia zespołowi SOC właściwą widoczność zdarzeń w sieci.



Rys. 2. Komunikacja między elementami systemu wraz z modułami cyberbezpieczeństwa

5. Norma IEC62443 a integrator systemu – SPIE Energotest

Norma IEC62443 wyjaśnia jakie obowiązki ciążą na poszczególnych interesariuszach wdrażanego systemu. Zainteresowane strony to:

- producent platformy systemowej (np. zenon, Ascom, Siemens, itp.),
- integrator – firma wdrożeniowa lub zespół firm (SPIE Energotest, Tekniska),
- użytkownik końcowy / inwestor.

W poszczególnych rozdziałach ww. normy możemy natknąć się na szereg wymogów stawianych przed poszczególnymi interesariuszami. Ogólnie mówiąc, każdorazowo, gdy wdrażany jest system, równolegle powinien powstać dokument opisujący stopień zgodności poszczególnych cech i funkcjonalności systemu z zapisami normy, obowiązki poszczególnych stron (aktualizacja oprogramowania, przegląd, kopia zapasowa, zasady nadawania uprawnień itd.). Nie jest konieczne, aby za każdym razem zastosować najostrzejsze i często najdroższe zabezpieczenia dla poszczególnych z tych punktów. Kluczem do optymalnego doboru zabezpieczeń jest analiza ryzyka dla każdego przypadku (rodzaju zagrożenia) z osobna. Taka analiza pozwoli ocenić, czy mamy pełną świadomość na temat potencjalnego zdarzenia czy możemy w jakiś sposób mu zapobiec? Jeżeli nie to czy jesteśmy w stanie w jakiś sposób ograniczyć prawdopodobieństwo jego wystąpienia lub ograniczyć skutki, jeżeli się ono zrealizuje? W ostateczności można podjąć decyzję o akceptacji ryzyka. Kwintesencją dobrego wdrożenia systemu jest zadania sobie szeregu pytań j.w. dla poszczególnych zagrożeń i stworzenia dokumentu opisującego stan końcowy. Zarówno użytkownik końcowy jak i integrator systemu powinni mieć pełną świadomość w zakresie potencjalnych luk systemu, wdrożonych zabezpieczeń, procedur. Świadomość ta często jest najskuteczniejszym zabezpieczeniem. Tak przygotowany dokument powinien być zgodny z obowiązującą polityką bezpieczeństwa informacji użytkownika końcowego, jeżeli takowa istnieje, co może oznaczać konieczność dokonania zmian w tejże

polityce. Nie odbędzie się to bez ścisłej współpracy na linii integrator – inwestor / użytkownik. Cel dla obydwu stron powinien być jasny i zrozumiały. Stworzenia takiego dokumentu nie wyczerpuje tematyki cyberbezpieczeństwa. Zapewnienie bezpieczeństwa jest procesem ciągłym co oznacza, że jak każdy proces musi być w sposób ciągły udoskonalany. Wszelkie zastosowane zabezpieczenia powinny być okresowo przeglądane i w razie pojawienia się nowych możliwości technicznych - udoskonalane.

Na bazie przeprowadzonych wdrożeń systemu ECONTROLplus, zebranych doświadczeń, oceniamy, że minimalne wymagania, jakie powinien spełniać system, opracowany w oparciu o normę IEC 62443, przedstawiają się następująco:

- dwustopniowe logowanie dla osób, które łączą się do systemu z tego samego komputera,
- blokowanie konta użytkownika w przypadku kilkukrotnego błędnego logowania,
- pełna lista zdarzeń w zakresie działań podejmowanych przez użytkownika,
- ograniczenie możliwości działania użytkownika do zakresu przydzielonych uprawnień (odczyt, sterowanie, dostęp, zarządzanie itp.),
- automatyczne wylogowania użytkownika,
- lista użytkowników pracujących z systemem SCADA, wraz z opisem poziomu uprawnień przydzielonemu każdemu z użytkowników,
- lista urządzeń z których użytkownicy systemu łączą się do systemu,
- lista procesów i usług, które również mają dostęp do systemu,
- lista innych systemów (oprogramowanie), które wymieniają dane z systemem SCADA,
- rozbudowane funkcje zarzadzania użytkownikami (dostępne dla administratora),
- silne hasła, minimalna długość hasła, konieczność zastosowania znaków specjalnych, cyfr, małych i dużych liter, maskowanie hasła,
- białe listy, MAC adres,
- monitoring sesji RDP,
- monitoring obciążenia procesora, dysku twardego i pamięci RAM,
- wybrane zdarzenia są zapisywane do pliku syslog,
- możliwość wskazania dodatkowego serwera czasu,
- stosowanie protokołów zgodnych z IEC 62351,
- ukrycie na liście zdarzeń adresów IP i MAC poszczególnych urządzeń,
- wewnętrzna aplikacja wryfikująca poprawność działania systemu, jego komponentów i niezbędnych procesów w tle,
- szyfrowanie przechowywanych danych,
- możliwość pracy w środowisku zwirtualizowanym,
- segmentacja systemu zgodnie ze strategią DMZ,
- ciągły monitoring ruchu sieciowego po zastosowaniu rozwiązań firm zewnętrznych,
- zewnętrzna kopia zapasowa po zastosowaniu rozwiązań firm zewnętrznych.

Cyberbezpieczeństwo to proces, to analiza, to świadomość, to współpraca i systematyczność. Dobierajmy odpowiednich partnerów biznesowych podczas wdrożeń systemów takich jak SPIE Energotest i Tekniska Polska.

6. Podsumowanie

Informacje zawarte w niniejszym artykule powinny pozwolić czytelnikowi na usystematyzowanie, lub pogłębienie wiedzy dotyczącej zagrożeń w zakresie cyberbezpieczeństwa sieci przemysłowych. Opracowanie przedstawia metodykę i sposób, w jaki przeprowadzany jest typowy atak na sieci IT I OT. Kilkukrotnie podkreśla się przy tym różnice co do zachowania i oczekiwań charakteryzujących reakcję w kontekście sieci OT i sieci IT. Dokument ma również na celu wyjaśnienie, jakie metody i działania mogą uniemożliwić, lub skutecznie utrudnić atakującemu przeprowadzenie udanego ataku.

Na koniec raz jeszcze przypomnienie punktu wyjścia dla podejmowania zagadnień z zakresu cyberbezpieczeństwa sieci przemysłowych: „Nie można zabezpieczyć czegoś, czego się nie zna”. Kluczowa jest świadomość dotycząca zachodzących procesów, wymiany informacji, danych I stawianych celów organizacji w kontekście systemów ICS, oraz merytoryczne i godne zaufania źródła wiedzy i wsparcia!

Literatura

[1] Materiały wewnętrzne Tekniska Polska
[2] Materiały wewnętrzne SPIE Energotest