

Zakłócanie Cyber Kill Chain w środowiskach OT i nie tylko

Piotr Urbańczyk – Techniska Polska

Streszczenie

W referacie przedstawiony został optymalny sposób ochrony przed atakami cybernetycznymi. Został pokazany ciąg czynności, które składają się na atak cybernetyczny. Przed właściwym atakiem występuje szereg inwigilacyjnych działań przygotowawczych. Udaremnienie ataku jest warunkowane skutecznym wykrywaniem tych działań przygotowawczych.

1. Wstęp

Coraz częściej media donoszą o nowym ataku na sieci różnych firm. Każdy z tych ataków wydaje się być unikalny, wykorzystuje inne podatności [1] i kończy się w inny sposób. Dociekliwy słuchacz może zastanawiać się, czy jest między nimi jakieś podobieństwo i dlaczego część organizacji jest w stanie poradzić sobie z tymi atakami, a część nie, części zajmuje to mniej czasu, a części więcej. Ten referat ma na celu odpowiedzieć na najczęściej zadawane członkom naszego Cybersecurity Team (CST Techniska) pytania odnośnie przyczyn, procesu i metod atakowania sieci organizacji. Czytelnik znajdzie w nim również porady, jak walczyć z zagrożeniami nawet zanim jeszcze atakujący zapukają do wrót sieci czytelnika.

Wszystkie inne skróty i terminy z żargonu opisane są w przypisach na końcu referatu.

2. Definicje wstępne

Rozpocząć należy od zdefiniowania tytułowego Kill Chainu i kilku podstawowych terminów, którymi posługujemy się w tym referacie. Ten złowrogo brzmiący „łańcuch zabijania” jest po prostu cyklem działań, które musi wykonać atakujący, żeby skutecznie infiltrować sieć. Ciekawostką jest, że nazwa ta została zapożyczona z czasów II Wojny Światowej, kiedy dotyczyła prawdziwych działań wojennych. Żeby uściślić terminologię, kiedy w referacie wspominamy o IT [2], lub ICT [3], będzie to dotyczyło ogółu usług mających za zadanie zapewnić stały przepływ informacji, w postaci komunikacji telekomunikacji VoIP [4], e-mail, stron WWW, systemów billingu, sprzedaży, ERP [5] itp. Kiedy natomiast wspominamy o OT [6], lub ICS [7], będziemy mieli na myśli systemy i sieci monitorujące i zarządzające procesem produkcji. Należy w tym momencie zrozumieć kilka podstawowych różnic pomiędzy systemami IT i OT. Przede wszystkim systemy OT są wrażliwe na opóźnienia i zakłócenia w komunikacji. W skrajnych przypadkach system sterowania procesem może przestać działać w przypadku opóźnień rzędu kilkudziesięciu milisekund, które są niezauważalne dla standardowego użytkownika sieci IT. Inną cechą systemów ICS jest brak aktualizacji lub opóźnienia w ich nakładaniu na systemy, spowodowane często brakiem okien serwisowych w czasie normalnej produkcyjnej pracy systemu. Inną przyczyną braku aktualizacji mogą być też wymagania producenta systemu automatyki, który mógł nie zdążyć certyfikować nowych aktualizacji. W sieciach OT rzadko kiedy można pozwolić sobie na nieplanowane przestoje związane z aktualizacjami. W sieciach IT niemal standardem stały się już comiesięczne lub częstsze aktualizacje. Różnic jest sporo. Zainteresowanym proponujemy lekturę literatury fachowej [8]. W referacie celowo nie porusza się szczegółowo zagadnień związanych z IoT, IIoT, czy też Industry 4.0, które w dużej mierze mają wiele wspólnego z OT w chmurze, czyli m.in. bezpośrednio podłączonym do Internetu, sieci WAN lub w przyszłości sieci 5G. Warto jednak wiedzieć, że część propozycji i problemów, które opisano w referacie będzie miało wpływ również w tych środowiskach, choć skala problemu może być zupełnie inna.

3. Cyber Kill Chain



Rys. 1. Elementy IT/OT cyber kill chain

Cyber Kill Chain to blokowy algorytm przeprowadzania ataków na dowolną infrastrukturę sieciową dowolnej organizacji. Wszystkie elementy tego łańcucha są na tyle ogólne, że za ich pomocą można opisać dowolną stosowaną metodologię ataku. Różne grupy przestępcze, szpiegowskie lub całkowicie legalne zespoły pentesterów [9], takie jak działający w ramach CST Techniska, którego członkiem jest autor, 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. Podobnie jak w przypadku gotowania potraw, każdy z przepisów może różnić się od innego, ale każdy przepis można podzielić na grupy: zbierania składników, wstępnej obróbki, przygotowania dania, konsumpcji dania, odebrania pochwały i smutnego obowiązku posprzątania kuchni.

W przypadku Cyber Kill Chain również do czynienia będziemy mieć z kilkoma standardowymi krokami, które atakujący będzie musiał wykonać, aby włamać się do sieci organizacji.

I tak, jednym z pierwszych kroków w planowanym ataku jest rekonesans. Nieważne jest czy planuje się atak na sieć przeciwnika czy wyprawę w nieznane, rekonesans jest podstawowym krokiem. Planując wycieczkę w nieznane należy wiedzieć mniej więcej czego możemy się spodziewać. Sprawdza się więc prognozę pogody, studiuje mapy, bada możliwości dojazdu, czyta o niebezpieczeństwach lokalnej fauny i robi listę atrakcji, które warto zwiedzić. Nie inaczej jest w przypadku ataku na sieć przeciwnika. Zanim atakujący rozpocznie swój właściwy atak, musi wiedzieć m.in., co jest dla niego celem głównym (tzw. Klejnoty koronne), co broni tego celu, jakie adresy IP prowadzą do sieci organizacji, którą atakujący ma na celowniku.

Internet i sieci społecznościowe ułatwiają oba zadania. W przypadku wycieczki, wystarczy zapytać kogoś, kto już zwiedził te rejony. W przypadku ataku na systemy IT/OT organizacji, same organizacje lub ich pracownicy dzielą się informacjami, które najlepiej byłoby zachować dla siebie. Drastycznym przykładem takiego zjawiska, niech będzie ceremonia uroczystego przecięcia wstęgi w nowym Centrum Przetwarzania Danych Policji w 2012 r. W trakcie ceremonii ogłoszono szereg przemówień, oprowadzono gości po obiekcie, zaproszono media i księdza, który pobłogosławił obiekt. Problem w tym, że centrum to miało być z założenia tajne, nawet funkcjonariusze pracujący w obiekcie pracowali w nim ubrani po cywilnemu [10].

Co ma to wspólnego z organizacją czytelnika? Warto zastanowić się, czy informacje opublikowane przez dział komunikacji z mediami [11] są odpowiednio autoryzowane. Czy w materiałach foto/video nie da się zauważyć żółtych karteczek z hasłami do systemów? Atak na jedną z telewizji francuskich rozpoczął się właśnie od takiego zdarzenia (czyli taki był wektor ataku) – w materiałach udostępnionych w Internecie możliwe było odczytanie haseł zapisanych właśnie na kartkach widocznych w tle. Temat ujawniania danych logowania na wizji pojawia się co jakiś czas, np. w trakcie powodzi w Wielkiej Brytanii w 2014 r. kamery telewizyjne zarejestrowały hasła do sieci sztabu kryzysowego [12]. Jak wiele zła mogło wyrządzić złośliwe wykorzystanie tych danych? Na szczęście nie dane było tego doświadczyć. Innym aspektem, który należy rozważyć jest czy pracownicy organizacji lubią dzielić się informacjami w sieciach społecznościowych. Czy na swoich profilach chwalą się zdaniem ciężkiego egzaminu z zarządzania nowym systemem, który zainstalowano w sieci wewnętrznej?

Poszukując w ramach rekonesansu przed testem penetracyjnym 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 również informacje dostępne publicznie w Internecie, niezbędne do zapewnienia organizacji widoczności w Internecie, takie jak wpisy DNS [13], informacje o adresach poczty elektronicznej itp. W środowisku pentesterów mówi się o takich działaniach „Biały wywiad” (ang. OSINT - czyli Open Source Intelligence). Większość tych informacji można uzyskać w zasadzie nie pozostawiając żadnych śladów na serwerach organizacji. Stąd też inna nazwa tej techniki – rekonesans pasywny.

Kiedy atakujący upewni się, że nic już więcej nie uzyska za pomocą białego wywiadu, skategoryzuje uzyskane dane pod kątem ich przydatności i przeanalizuje je dokładnie, przejdzie do skanowania sieci swojego celu. Pozostając wiernym analogii, porównać to można do zadzwonienia do wszystkich numerów w miejscowości, do której planuje się wycieczkę. Sporo numerów odpowie komunikatem „nie ma takiego numeru”, część abonentów nie odbierze, część przekaże jakieś użyteczne informacje, część z nich okaże się hotelami, być może uda się dodzwonić również na komisariat. Na gruncie informatyki, zanim rozpocznie się fazę ataku, najczęściej wykonuje się skanowanie adresów IP organizacji. Na podstawie takiego skanowania uzyskać można informację o tym, jakie zasoby organizacja udostępnia w Internecie. Znaleźć można serwery WWW, e-mail i wszystkie inne usługi, które są widoczne z sieci publicznej, nawet te, o których IT celu nie wie, lub zapomniało.

Po wykonaniu rekonesansu atakujący zaczyna przygotowywać atak. Tak jak wybierając się na wycieczkę i znając warunki pogodowe, lokalowe itp. rozpoczyna się pakowanie, tak atakujący wiedząc czego może się spodziewać w środowisku atakowanej organizacji, zaczyna przygotowywać oprogramowanie, które będzie mu niezbędne w trakcie atakowania organizacji na jego celowniku. Analogicznie, kiedy z rekonesansu wycieczkowego okaże się, że w całej okolicy nie ma bazy noclegowej, a jedyny sklepik zamykany jest tuż po otwarciu, warto wiedzieć, że należy spakować namiot, śpiwór i zapas jedzenia. Z kolei atakujący, kiedy dowie się, że administratorzy organizacji popełnili pomyłkę w czasie konfiguracji serwera WWW, to przygotowuje cały

zestaw programów, które tę podatność wykorzystuje. Jeśli z rekonesansu wywnioskować można, że w organizacji stosuje się rozwiązanie antywirusowe konkretnego dostawcy i konkretną wersję systemu operacyjnego, można przygotować swój podręczny zestaw złośliwego oprogramowania, w taki sposób, aby nie został wykryty przez żaden z komponentów bezpieczeństwa obecny w organizacji. Cały ten proces, trwający czasem całkiem 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 przygotować można również fałszywe strony, którymi będzie wabić się pracowników organizacji. Jest to proces bardzo żmudny i choć technicznie bardzo ciekawy, to dla większości społeczeństwa bardzo nudny. Dlatego pominiemy szczegóły i przejdziemy do opisu następnego etapu. Pamiętać należy, że choć żmudny, często proces ten kończy się wygenerowaniem „gotowców”, które można dostosować do użycia w następnych atakach, co z kolei wprawnym pentesterem i atakującym skraca następne fazy zbrojenia.

Turysta ze spakowanym plecakiem i atakujący z gotowym arsenałem, mogą przejść do właściwych etapów swoich przedsięwzięć. Nastął czas na fazę dostawy na miejsce. Turysta w jakiś sposób musi dostać się do wymarzonego celu. Może wykorzystać każdy środek transportu – może na przykład spróbować wysiąść na najbliższej stacji kolejowej i autostopem zbliżyć się do celu. Atakujący musi w jakiś sposób uzyskać kontrolę nad choć jednym komputerem w sieci organizacji. Do tego celu może wykorzystać podatne oprogramowanie obecne w sieci organizacji, a zwłaszcza dostępne w Internecie. Opiszemy pokrótce taki atak, jednak zapamiętać warto analogię podróży autostopem. Jeszcze do niej wrócimy. Wiedząc o podatnym oprogramowaniu dostępnym z Internetu, atakujący może spróbować ataku bezpośrednio na nie. W tym celu dostarcza się takiemu celowi exploita – czyli sklejone ze sobą części wykorzystujące podatność i zawierające komendy atakującego. Jeśli atak się uda, system wykona zestaw komend atakującego. Ta faza (faza uruchomienia) zazwyczaj wykonuje się autonomicznie, a atakujący może jedynie mieć nadzieję, że poprawnie przygotował kod exploita, który uzyska w ten sposób jakąś formę kontroli nad działaniem podatnego systemu.

Użyta powyżej analogia do podróży autostopem bardzo pasuje do metody ataku, o której czytelnik pewnie już słyszał. Mowa tu o atakach z wykorzystaniem socjotechniki (ang. Social engineering-inżynieria społeczna). Ta metoda polega na wykorzystaniu ludzi i ich cech do osiągnięcia swoich celów. Ludzie najczęściej chcą czynić dobro, chcą pomóc osobie w potrzebie i lubią czuć się docenionymi. Najczęściej więc atakujący wysyła do pracownika organizacji wiadomość z prośbą o pomoc, np.

„właśnie się zorientowałem, że w umowie podałem Państwu niewłaściwy numer konta. Proszę o zmianę go na ten: [tu numer konta oszustaj]”.

W podobny sposób kradziono pieniądze z urzędów i firm na całym świecie. Pentestera zwanego czasem etycznym hakerem, nie interesują jednak takie oszustwa. Jego celem jest zainfekować komputer w organizacji w ramach testu. Wykorzystuje on socjotechnikę w celu skłonienia pracownika do uruchomienia programu, który mu wyśle. Popularne treści wiadomości, które mają za zadanie skłonić użytkownika do kliknięcia w link, pod którym znajdować się będą złośliwe elementy jego arsenału, to m.in. „Czy to ty jesteś na tym zdjęciu? [złośliwy link]”, „Nie spodziewałem się tego po tobie – cały artykuł o tym co zrobiłeś napisałeś[...].”, „Gratulacje! Szkoda, że dowiedziałem się o tym dopiero z tej strony[...], a nie od Ciebie...”. Metody socjotechniki są w zasadzie niegraniczone. Jeśli atakujący chciałby, żeby pracownik uruchomił program, który będzie załącznikiem do wiadomości, spróbuje wmówić mu, że to zalega faktura, której nie zapłacił, list przewoźowy, wezwanie do zapłaty, inny ważny dla niego dokument, lub przypadkowo wysłana lista płac, którą dział kadr omyłkowo wysłał do niego. W tym zakresie – treści e-maila i sposobu na podejście do pracownika organizacji, pentester w ramach umowy zazwyczaj zapewnią ma spora dozę autonomii, a atakujący najczęściej nie mają żadnych skrupułów. Dodatkowo informacje zebrane z kont sieci społecznościowych w fazie rekonesansu tylko ułatwiają dobranie właściwej treści. Jeśli pracownik udostępnia zdjęcia z dalekich podróży, przygotowuje się dla niego ciekawą ofertę wyjazdu ze zniżką dla pierwszych 1000 osób. Jeśli zatrudniony ćwiczy karate, zaprosi się go na zlot i turniej w znanym dojo w Japonii, ale pod warunkiem, że wypełni „tę skromną ankietę”. Inną metodą dostarczenia złośliwego oprogramowania są podrzucane nośniki – wystarczy, że na parkingu w okolicy organizacji firmy pracownik znajdzie pendrive z breloczkiem i kluczykiem samochodowym. Najczęściej osoba ta zacznie współczuć niezdarze, która kluczyk zgubiła, więc aby jej pomóc sprawdzi, co jest na znalezionym nośniku, bo często są tam zdjęcia, dokumenty, być może jakieś CV?

Obie metody – z wykorzystaniem socjotechniki i ta, z wykorzystaniem exploita, kończą z grubsza fazę dostawy. W tym momencie zaczyna 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 exploita, powoduje najczęściej wykonanie złośliwego kodu (faza uruchomienia) i w kilka chwil później radość atakującego, ponieważ jak napisano powyżej, atakujący potrzebuje przejąć kontrolę tylko nad jednym komputerem w organizacji, a każda ze wspomnianych powyżej akcji zakończona udanym uruchomieniem kodu w ostatecznym rozrachunku umożliwia mu to.

Faza uruchomienia jest najkrótsza w tym opisie, a także w rzeczywistości, ale jest kluczowa dla powodzenia dalszego ataku. Momentalnie po uruchomieniu złośliwego oprogramowania następuje faza instalacji, która

ma na celu pobranie reszty wymaganych narzędzi niezbędnych atakującemu do wprawnej pracy w systemie organizacji. Narzędzia te przygotowane w fazie zbrojenia czekają 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 oprogramowanie raz stworzone w fazie zbrojenia można wykorzystywać ponownie podczas atakowania innego celu, agresor często będzie wykorzystywał ten sam zestaw narzędzi do atakowania różnych środowisk [14]. Dla atakującego ważne jest precyzyjne przygotowanie ataku, bo każde dodatkowe pobrane narzędzie może powodować wcześniejsze wykrycie obecności atakującego, identyfikację jego TTP [15], właściwą reakcję organizacji na atak, eliminację reszty arsenału atakującego i w konsekwencji potrzebę rozpoczęcia całego procesu od początku fazy dostawy lub nawet fazy rekonesansu.

Fazy uruchomienia i instalacji można porównać do rozbicia namiotu/zameldowania się w hotelu i rozpakowania plecaka, a następnie pójścia na zakupy po rzeczy, których celowo turysta nie zapakował, żeby ograniczyć masę jego plecaka. Turysta jest już o krok od rozpoczęcia wakacyjnych przygód!

Kiedy już system w organizacji zostanie przejęty, pobierze z serwera atakującego dodatkowe oprogramowanie i zainstaluje je bez problemu, pozostaje już jeden krok, który należy wykonać. Oprogramowanie nawiązuje połączenie z serwerem zarządzającym (ang. Command and Control), który ma za zadanie ułatwić sprawowanie kontroli nad większą ilością przejętych systemów. Tutaj jedyne porównanie do wycieczki w nieznane, jakie przychodzi do głowy, to wysłanie wiadomości do najbliższych o treści: „Jestem na miejscu! Mogę zwiedzać! Przywieźcie wam jakieś pamiątki?”. I w ten płynny sposób przejść można do ostatniego elementu Cyber Kill Chain jakim jest misja właściwa.

W obu opisanych powyżej przypadkach sam proces włamania się do systemu lub wycieczki w nieznane nie jest przecież tym co planowano osiągnąć! Turysta chce zwiedzić okolicę, zrobić zdjęcia, stworzyć wspomnienia i mieć o czym opowiadać znajomym. Pentester żmudnie dąży do wykonania misji jaką dla niego jest zdefiniowany w zleceniu cel (klejnoty koronne). W tym celu ponownie wykonuje cały Cyber Kill Chain, z tym, że już wewnątrz sieci organizacji. Dla złośliwych atakujących celem może być upublicznienie poufnych informacji na temat organizacji lub żądanie okupu za dane, które przejęto. Agresorzy będą chcieli najczęściej zarobić na włamaniu do organizacji i w tym celu też będą powtarzać części Kill Chainu od wewnątrz.

Jest jeszcze jedna różnica. Pentester pod koniec testu musi dokładnie opisać, jakiej metody użył, żeby zaatakować system organizacji. Musi również przygotować dla organizacji zalecenia, które należy wdrożyć, żeby atak na jej systemy przeprowadzony w taki i podobne sposoby był utrudniony lub niemożliwy. Złośliwy atakujący musi w jakiś sposób z włamania uzyskać wartość pieniężną, musi więc zażądać okupu, sprzedać uzyskane z organizacji dane i wyprać te pieniądze. A turysta z wycieczki musi koniecznie przywieźć zdjęcia i pamiątki!

3.1. Przykłady

Żeby lepiej zobrazować Cyber Kill Chain, przedstawić można typowy atak na system firmy z sektora produkcyjnego. W dniu „zero” ataku kilkuset użytkowników firmy otrzymało e-mailem fałszywe wezwania do zapłaty faktury (**faza dostawy**). Większość z nich, nie będąc bezpośrednio odpowiedzialnych za faktury, po otwarciu załącznika stwierdziło, że należy tego e-maila przesłać do działu księgowości. Na każdym z komputerów, na którym otwarto załącznik, został uruchomiony mały program (**faza uruchomienia**), który zidentyfikował oprogramowanie antywirusowe, pobrał właściwy moduł (**faza instalacji**), który tego antywirusa wyłączył, połączył się z serwerem zarządzającym i otrzymał serię rozkazów (**faza przekazania kontroli**). Następnie w wyniku tych rozkazów pobrał kolejny moduł złośliwego oprogramowania, który za pomocą podatności w systemie Microsoft Windows rozprzestrzenił się po całej sieci organizacji i zaszyfrował dane zgromadzone na stacjach roboczych i serwerach (**misja właściwa**). Po wykonaniu tej akcji, oprogramowanie wyświetliło żądanie okupu za odblokowanie dostępu do danych. Firma okupu nie zapłaciła, jednak przywracanie danych z kopii zapasowych i czyszczenie systemów z infekcji zajęło sporą część miesiąca. Przez ten czas zdolność produkcyjna firmy była solidnie ograniczona, a nawet kiedy przywrócono już działanie stacji operatorskich, część danych, w tym zapotrzebowanie na produkty było w trakcie odzyskiwania z kopii zapasowych.

Innym przykładem, który warto przedstawić jest chyba najgłośniejszy ostatnimi czasy atak na ukraiński zakład energetyczny z 2015 r. W tym przypadku atakujący również dostali się do sieci za pomocą złośliwego załącznika dostarczonego za pomocą e-maila (**faza dostawy**). Po jego uruchomieniu i pobraniu komponentów, złośliwe oprogramowanie przekazało kontrolę swoim twórcom. **Misja właściwa** w tym przypadku polegała na infiltracji sieci zakładu i dostaniu się do sieci przemysłowej. Po uzyskaniu tego dostępu, atakujący przygotowali dodatkowe komponenty (**ponowna faza zbrojenia**) w postaci złośliwego oprogramowania, które miało utrudnić pracownikom firmy odzyskanie kontroli nad swoim systemem. Zastosowano m.in. oprogramowanie, które wymazało dane z systemów operatorskich i serwerów, uszkodziło zasilacze awaryjne, modemy i terminale zdalne (RTU), a nawet przygotowano atak uniemożliwiający dodzwonienie się klientów, w celu powiadomienia o usterce [16]. Całość tej fazy trwała

ponad pół roku, aż do kulminacyjnego momentu 23 grudnia 2015 r, kiedy to wyłączono zdalnie podstacje energetyczne i jednocześnie uruchomiono wszystkie opisane powyżej komponenty uniemożliwiające zdalną pracę. W wyniku tego ataku około 230 tys. odbiorców pozbawiono zasilania na 6 godzin, wyłączono 30 podstacji, zmuszając pracowników firmy do przejścia na ręczne sterowanie [17], [18], [19].

W obu tych przykładach nie widać elementów wstępnej fazy rekonesansu, jednak taka musiała mieć miejsce, ponieważ atakujący wysłali złośliwe e-maile [20] 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, przedstawione w pierwszym przykładzie, nazywane jest „ransomware” i w ostatnich latach jest zdecydowanie najpopularniejszą metodą wykorzystywaną przez grupy przestępcze, ostatnimi czasy (początek 2020 r.) wykryto obecność tej klasy zagrożenia, które celowo poszukuje komponentów systemów ICS. W drugim przykładzie zastosowano oprogramowanie o nazwie BlackEnergy.

Warto zwrócić również uwagę na fakt, że czas trwania ataków, czyli de facto wykonania całości Cyber Kill Chain nie jest stały dla każdej grupy atakujących. W niektórych przypadkach całość ataku trwa kilkanaście godzin – np. w przypadku masowych kampanii phishingowych, które ze względu na ich widoczność w sieci często są blokowane już po kilku godzinach, po czym atakujący zmuszeni są rozpocząć nową kampanię. W innych przypadkach wykonywanie ataku trwa tygodniami lub nawet miesiącami. Tak długie kampanie określa się atakami APT (ang. Advanced Persistent Threat – czyli Zaawansowane Trwałe Zagrożenie). Atak na Ukrainie, opisany powyżej należy do tej drugiej grupy, atak za pomocą ransomware z pierwszego przykładu raczej zaklasyfikować można do pierwszego typu szybkiego ataku.

4. Zrywanie łańcucha

W tym miejscu można byłoby zakończyć artykuł, ale przecież jego tytuł zawiera frazę „zakłócanie Cyber Kill Chain”. Należy się zatem zastanowić jak można przerwać tę wycieczkę w nieznane, jaką jest atak na system organizacji. Poniżej opiszemy metody jakie można zastosować, aby przerwać Cyber Kill Chain, ze szczególnym uwzględnieniem specyfiki środowisk automatyki przemysłowej.

Metody przerywania Cyber Kill Chain można pogrupować w sześć kategorii:

Wykrywanie

Blokada

Przerywanie

Degradacja

Oszustwo

Ograniczenie

Rys. 2. Metody przerywania Kill Chain

Każda z tych kategorii pozwala grupie obrońców sieci rozpocząć działania, które uniemożliwią atakującym skuteczny atak na systemy w sieci organizacji.

Przed przejściem do opisu każdej z tych kategorii, zacytować warto truizm, który dotyczy nie tylko świata bezpieczeństwa IT/OT, ale w zasadzie każdego aspektu życia.

„Nie możesz zabezpieczyć czegoś, o czym nie wiesz”

To bardzo ważne, żeby zapamiętać go jako dogmat bezpieczeństwa. W kontekście systemów z którymi automatycy stykają się na co dzień, maksyma ta sprowadza się do żmudnego obowiązku wykonania rzetelnej inwentaryzacji komponentów systemu, który należy zabezpieczyć. Oczywiście nie ma obowiązku wykonywania tej pracy samodzielnie.

Istnieją systemy i usługi, które mogą wesprzeć organizację w tym zadaniu. Na przykład odpowiednio zasilony ruchem system Radiflow iSID [21], zinwentaryzuje wszystkie widziane w sieci urządzenia i komunikację między nimi. Raport wygenerowany z tego procesu w połączeniu z wiedzą ekspercką, pozwoli stworzyć solidną dokumentację, potrzebną do podjęcia dalszych kroków, opisanych poniżej.

Wykrywanie jest jedną z najważniejszych metod. Choć sama w sobie nie zablokuje żadnego ataku, to jednak w środowiskach sieci przemysłowych, cechę tę widzi się raczej jako zaletę, ponieważ błędne

zablokowanie komunikacji pomiędzy elementami sieci przemysłowej może przerwać działanie procesu. Pasywne wykrywanie pozwoli obrońcom sieci przygotować się na atak lub rozpocząć procedury reakcji na incydenty w momencie wykrycia podejrzanego zachowania w sieci, bez ryzyka zakłócenia pracy sieci procesowej OT.

Detekcja może wykryć każdą z faz Kill Chainu, począwszy od wykrywania pasywnego rekonesansu za pomocą właściwie przeprowadzonej analityki wykorzystania serwerów WWW lub przeszkolonego personelu, który rozpozna działania fazy rekonesansu. Brzegowe IDSy [22] wykrywające skanowanie granicy sieci to również ważny element wykrywania. Faza zbrojenia zostanie wykryta przez sieciowy IDS, kiedy atakujący będzie musiał zweryfikować czy program, który pisze działa poprawnie w środowisku celu. Szkolenie personelu skutecznie podnosi umiejętności wykrywania metod socjotechniki, co wpływa na wykrywanie fazy dostawy. Fazy uruchomienia i instalacji zostaną wykryte przez IDS zainstalowany na atakowanym systemie, próba podłączenia się do serwera zarządzającego zostanie wykryta przez sieciowy IDS, a działania na przejętych systemach zostaną wykryte przez analizę dzienników audytu. Co ważne – wykrywanie zazwyczaj jest procesem pasywnym, którego wdrożenie i używanie nie będzie mieć negatywnego wpływu na obserwowaną sieć. To jest krytyczny argument w kontekście sieci ICS.

Jak można zauważyć sama obserwacja sieci i systemów daje sporą przewagę nad atakującym. Nasze doświadczenie wielokrotnie pokazało nam skuteczność monitoringu w kontekście ochrony sieci OT. Wykorzystanie narzędzi pasywnych, nieingerujących w infrastrukturę, umożliwiających wykrycie i tym samym skrócenie czasu reakcji daje solidny fundament do budowania kolejnych elementów ochrony aktywnej. Tę samą opinię wyraził regulator, w postaci ustawy o Krajowym Systemie Cyberbezpieczeństwa [23]. W ofercie Tekniska Polska znajdują się usługi polegające na wdrożeniu jednego z przemysłowych IDS z naszej oferty i przygotowaniu raportu o znalezionych problemach w sieci. Taki raport bardzo często jest pierwszym krokiem do solidnej poprawy bezpieczeństwa sieci organizacji.

Blokowanie ma równie mocny, jeśli nie mocniejszy, wpływ na przerwanie Kill Chain. Podstawą jego działania jest wymuszanie polityk bezpieczeństwa. I tak w fazie rekonesansu skutecznie wymuszona polityka na firewallu brzegowym ograniczy bardzo mocno skuteczność skanowania sieci i portów. Podczas testowania oprogramowania w fazie zbrojenia, IPS [24] na brzegu sieci uniemożliwi atakującemu przeprowadzenie skutecznych testów, co w ostatecznym rozrachunku może znaczyć tyle, że nawet z przygotowanym oprogramowaniem idealnym, które zaatakuje system celu i pozwoli agresorowi przejść nad nim kontrolę, IPS uniemożliwi mu jego wykorzystanie w trakcie fazy dostawy. Odpowiednio skonfigurowany filtr proxy [25] uniemożliwi infekcję systemu przez kliknięcie w złośliwy odnośnik. Fazę uruchomienia złośliwego oprogramowania, a w szczególności exploita, skutecznie utrudni wdrożenie rygorystycznej polityki nakładania łątek [26] na oprogramowanie. Fazę instalacji dodatkowego oprogramowania można skutecznie zakłócić poprzez właściwe ograniczenie uprawnień użytkownika, uniemożliwiające mu pobieranie i uruchamianie oprogramowania, zwłaszcza na wysokim poziomie uprawnień. Fazy przekazania kontroli i działania na zainfekowanym systemie w ramach **misji właściwej** zablokować można stosując firewalle i ich właściwą konfigurację. Działania ostatniej fazy Kill Chain można zablokować stosując polityki ograniczające ruch wychodzący z systemu.

Obie powyższe metody ograniczania Kill Chain stanowią absolutne minimum, warto jednak zauważyć, że w przypadku błędnej konfiguracji którejkolwiek z metod 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 taka przerwa lub opóźnienie komunikacji może mieć opłakane skutki dla ciągłości procesu, a w najgorszym przypadku może skutkować wypadkiem i uszczerbkiem na zdrowiu personelu. Dlatego też prace, które wykonujemy w zakresie konfiguracji urządzeń z tej grupy w sieciach OT oraz jakiegokolwiek podjęte akcje poprzedzone są dogłębną analizą ruchu sieciowego pomiędzy komponentami systemu i konsultacjami z właścicielem systemu, a w razie wątpliwości z producentami systemu. Urządzenia IPS, firewall i proxy powinny zostać gruntownie przeanalizowane, ich konfiguracja przetestowana w różnych stanach pracy systemu ICS.

Należy rozważyć miejsce w architekturze, gdzie lepiej zastosować jest systemy aktywne (brzeg sieci, segmentacja fragmentów sieci) oraz pasywne (blisko procesu, czyli typowa sieć ICS).

Dobrze jest chronić aktywnie sieć na jej brzegu oraz w newralgicznych kanałach komunikacyjnych – stosując firewalle, IPS lub diody i monitorować całość sieci (ochrona pasywna) odpowiednimi narzędziami dla IT i OT.

Przerwanie to metoda, która ma za zadanie przerwać trwający już atak. Nie ma ona wpływu na fazy rekonesansu i zbrojenia. W odosobnionych przypadkach niektóre metody blokowania dostawy mogą okazać się nieskuteczne. W tych sytuacjach dobrze jest mieć dodatkową warstwę obrony w postaci systemu antywirusowego inline, czyli skanującego przechodzący przez niego ruch. Jeśli filtr proxy nie zablokuje złośliwego odnośnika, Antywirus inline wykryje zagrożenie i uniemożliwi mu dostanie się do atakowanego systemu. Jeśli szkolenie zawiedzie, i użytkownik podłączy zainfekowany pendrive do stacji roboczej, odpowiednio skonfigurowane DEP [27] i ASLR [28] przerwą fazę uruchamiania się exploita, a gdyby okazało się, że i one zawiodą, lub są nieodpowiednio skonfigurowane, to fazę instalacji powstrzyma zainstalowany antywirus. Faza przekazania kontroli zostanie zatrzymana przez poprawnie

skonfigurowany IPS sieciowy, a misja właściwa, polegająca na wykradaniu danych zostanie skutecznie przerwana przez wdrożony i poprawnie skonfigurowany system DLP [29]. Należy zauważyć jednak, że systemy przerywające połączenia tak samo jak systemy blokujące opisane akapit wyżej, najbezpieczniej wdrożyć na granicy sieci IT i OT. Wewnątrz sieci ICS pomiędzy strefami bezpieczeństwa wdrożenie musi być poprzedzone dogłębną analizą w celu weryfikacji, czy wdrożony system nie przerwie istotnej komunikacji pomiędzy elementami procesu.

Na rynku dostępne są systemy klas Inline AV, IPS sieciowy i DLP. Wdrożenie każdego z tych systemów poprzedzone musi być wnikliwą analizą. Dla każdej z tych klas należy wykonać wiele prac przygotowawczych, których ciężar najczęściej leży po stronie zamawiającego. Poprawne wdrożenie każdego z tych systemów jest trudną i żmudną pracą, ale niesie za sobą oczywiście dodatkowe korzyści. Zawsze istotne jest spojrzenie z perspektywy ryzyka, czyli jak bardzo wdrożenie danego elementu infrastruktury wpłynie na minimalizację całościowego ryzyka organizacji i ile tą organizację będzie kosztowało uwzględniając koszty CAPEX, OPEX i jej przygotowanie do poprawnej obsługi danego systemu. Nawet najlepszy system - jeżeli nie zostanie poprawnie wdrożony i skonfigurowany nie tylko nie wpłynie na efektywne ograniczenie ryzyka, a może to ryzyko podwyższyć dając fałszywe „poczucie bezpieczeństwa”. Ten sam efekt powstanie w sytuacji, kiedy system powinien być jednym z wielu elementów, a wykorzystuje większość budżetu organizacji przeznaczonego na zabezpieczenia, uniemożliwiając zakup reszty komponentów. Cyberbezpieczeństwo wymaga strategicznego podejścia i planowania popartego rzetelną analizą ryzyka i powinno stanowić na nią odpowiedź poprzez minimalizację kolejnych, największych ryzyk w organizacji.

Degradacja to metoda mająca największy potencjał wywołania u atakujących napadu furii. W skrócie polega ona na tym, że uniemożliwia im pracę z zainfekowanym systemem w sposób łatwy i szybki. Najczęściej degradacja dotyczy trzech faz. Fazy dostawy, podczas której złośliwe oprogramowanie zostaje dodane do kolejki, co powoduje znaczne opóźnienie w jego wykonaniu, a u atakującego nagły brak wiary w sukces przedsięwzięcia. Faza przekazania kontroli i misja właściwa to kolejne dwie, które można skutecznie zdegradować, np. stosując systemy klasy tarpit, które spowolnią złośliwą pracę w sieci organizacji na tyle, że obrońcy będą mieli czas na wykrycie ruchów agresorów. Inną skuteczną metodą jest wdrożenie QoS w sieci, skutecznie ograniczając pasmo przydzielone na komunikację nieznanego pochodzenia. W tym układzie złośliwe działania, będą obciążone sporym opóźnieniem w transmisji, a to nigdy nie sprzyja komfortowi pracy atakujących.

Oszustwo to nie tylko domena atakujących – obrońcy również mogą oszukiwać wroga. Do tego celu służą głównie dwie klasy rozwiązań. Pierwsza to DNS Redirect – powodujący, że faza przekazania kontroli i dostawy mogą zostać przekierowane do środowisk analitycznych stworzonych przez obrońców. Druga klasa rozwiązań to honeypot, który ma za zadanie udawać łakomy dla atakującego kąsek. Atakując system w trakcie testów poszukuje się najciekawszych dalszych celów – kiedy zauważony zostanie tak wspaniale wyglądający system, na pewno agresor zwróci na niego uwagę. Honeypot najczęściej jest pod ścisłą obserwacją obrońców, przez co zdarza się, że działając na nim, atakujący ujawnia swoje techniki, pokazuje im na co się przygotować, nie uzyskując nic w zamian.

Ostatnia, lecz nie najmniej ważna metoda to **ograniczenie**. Jest to metoda, która ma za zadanie zmniejszyć wpływ każdej z faz Cyber Kill Chain na wynik ataku. W gronie technik stosowanych w celu ograniczenia możliwości atakujących stosuje się prostą segmentację sieci, czyli podzielenie sieci organizacji na wycinki o konkretnych funkcjach np. księgowość, automatycy, zarząd, proces. Taki podział na strefy bezpieczeństwa pozwala bardzo mocno utrudnić pracę atakującego. Zastosowanie firewalla z ACL ograniczy mu widoczność podczas fazy rekonesansu. Zastosowanie IPS sieciowego skutecznie obniży wiarę atakującego w jego przygotowany arsenał, ponieważ nie będzie miał go jak przetestować. Zastosowanie firewalla aplikacyjnego zmusi go do dokładnego trzymania się specyfikacji protokołów, przez co zwiększa się prawdopodobieństwo popełnienia przez atakującego błędu. IPS pomiędzy strefami bezpieczeństwa bardzo utrudni mu uruchomienie exploita na kolejnych systemach, zastosowanie antywirusa na stacjach roboczych i serwerach praktycznie utrudni agresorowi instalację dodatkowych programów. Zastosowanie stref, w połączeniu z zdefiniowanymi poziomami zaufania do każdej z nich spowoduje, że komunikacja do serwera zarządzającego będzie utrudniona lub niemożliwa. Dokładnie ten sam efekt będzie widoczny dla dalszych działań, które atakujący będzie usiłował wykonać w zaatakowanym systemie w ramach misji właściwej.

Inwentaryzacja, separacja sieci OT od sieci IT i zapewnienie sobie widoczności zdarzeń za pomocą IDS, to fundamenty, które należy posiadać w sieci przemysłowej. Dalsza kolejność wdrażania technologii ochronnych w zasadzie nie ma znaczenia, bo każda technologia dodaje kolejną warstwę, której atakujący będzie musiał sprostać. Zapamiętać należy jednak, że każda z nich ma konkretne zastosowanie i skuteczność w przerywaniu konkretnych faz Kill Chain. Niektóre z nich – takie jak monitoring ICS warto wdrożyć w pierwszej kolejności, ponieważ przekazywane informacje o wykrytych podatnościach i próbach ich wykorzystania stanowią nieocenioną pomoc dla zespołu obrońców i mogą być pomocne w planowaniu

kolejnych kroków. Warto też dość wysoki priorytet nadać podstawowym metodom blokującym takim jak firewall, które pozwolą złapać oddech i przygotować dalsze metody w sposób w miarę systematyczny i zorganizowany.

Wiele uwagi w tej części artykułu poświęcono obrońcom. W żargonie cyberbezpieczeństwa mówi się o nich „Blue Team” [30], niebieski kolor tego zespołu, kojarzony z policją, która ma za zadanie chronić nie jest przypadkowy. Najczęściej, zespoły Blue Team to wydzielone w organizacjach komórki SOC [31], których zadaniem jest koordynacja działań związanych z cyberbezpieczeństwem organizacji. Zespoły te najczęściej wyposażone są w systemy klasy SIEM [32], które zbierają informacje z chronionej infrastruktury, korelują je w czasie, wykrywają symptomy ataków i pozwalają obrońcom na sprawną reakcję na incydenty. Systemy te mogą mieć postać gotowych platform, stosowanych w środowiskach korporacyjnych lub systemów open source [33], stosowanych w mniejszych środowiskach, bądź w przypadku ograniczonego budżetu. Najczęściej te drugie wymagają sporo pracy zespołu SOC w celu dostosowania ich do potrzeb organizacji, a te pierwsze zawierają gotowe moduły, które zapewniają Blue Teamowi zestaw podstawowych narzędzi pozwalających na rozpoczęcie właściwej pracy. Dodatkowo, zakup SIEM klasy korporacyjnej najczęściej dostarcza usługi wsparcia, z których obrońcy mogą skorzystać w przypadku wystąpienia problemów z działaniem systemu. Systemy open source, stosowane często ze względu na brak 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 systemów i sieci organizacji.

Systemy IDS dla OT przykładowo wspomniani już iSID RadiFlow czy SCADAFence umożliwiają integrację z systemami klasy SIEM/SOAR takimi jak popularne QRadar, CyberArk, Demisto, a nawet polskim SECUREVisio firmy eSECURE. Jest również możliwa integracja (jeżeli istnieje dla niej uzasadnienie) z istniejącymi firewallami i elementami infrastruktury.

Zespoły SOC najczęściej składają się ze specjalistów, znających doskonale architekturę swojej sieci i systemów, posiadających obszerną wiedzę z zakresu cyberbezpieczeństwa teleinformatycznego, najczęściej wywodzących się z zespołów IT organizacji. Te cechy pozwalają im rozpoznawać ataki na infrastrukturę swoich organizacji, często już na samym początku. Do obowiązków SOC należy również przygotowywanie i wykonywanie planów reakcji na incydenty, a nawet skomplikowane analizy TTP atakujących. Ich możliwości są tym większe, im więcej metod przerywania Cyber Kill Chain wdroży organizacja, ale nawet w bardzo ograniczonym, podstawowym środowisku, sama obecność osób, które śledzą zapisy monitoringu i są w stanie rozpoznać atak, zapewnia minimalną możliwość reakcji na incydent, choćby jedyną reakcją jaką SOC będzie w stanie zastosować będzie odłączenie sieci organizacji od Internetu. W przypadku, kiedy organizacja nie ma zasobów, które pozwalają na zbudowanie własnego zespołu SOC, może posilkować się usługami SOC as a Service. Usługi te pozwalają skorzystać z już działającego zespołu SOC organizacji świadczącej usługi dla swoich kontrahentów. Należy jednak pamiętać, że skorzystanie z takiej usługi będzie wymagało czasu, w którym zespół usługodawcy pozna działanie i architekturę sieci zamawiającego.

Idealnym rozwiązaniem jest budowanie zespołów SOC wewnątrz organizacji, bazujących na jej zasobach. Takie rozwiązanie jest najlepsze, ponieważ znajomość procesów zachodzących wewnątrz sieci organizacji jest kluczowym elementem. Często zdarza się też, że w gronie personelu organizacji odnaleźć można pracowników, którzy wymagają zaledwie kilku szkoleń, które odpowiednio wyposażą ich w wiedzę niezbędną do utworzenia zespołu SOC. Niestety, realnie jest to często bardzo trudne, ponieważ wymaga dodatkowych etatów lub stworzenia warunków (np. przekierowania innych obowiązków) do realizacji nowych działań. Istnieje całe spektrum możliwości wdrożenia SOC w organizacji. Pomiedzy bardzo kosztownym własnym SOC 24h organizacji, wykorzystaniem SOC 24h as a Service firm świadczących takie usługi lub brakiem SOC jest jeszcze kilka opcji wartych przemyślenia, które mogą być korzystne dla mniejszych organizacji.

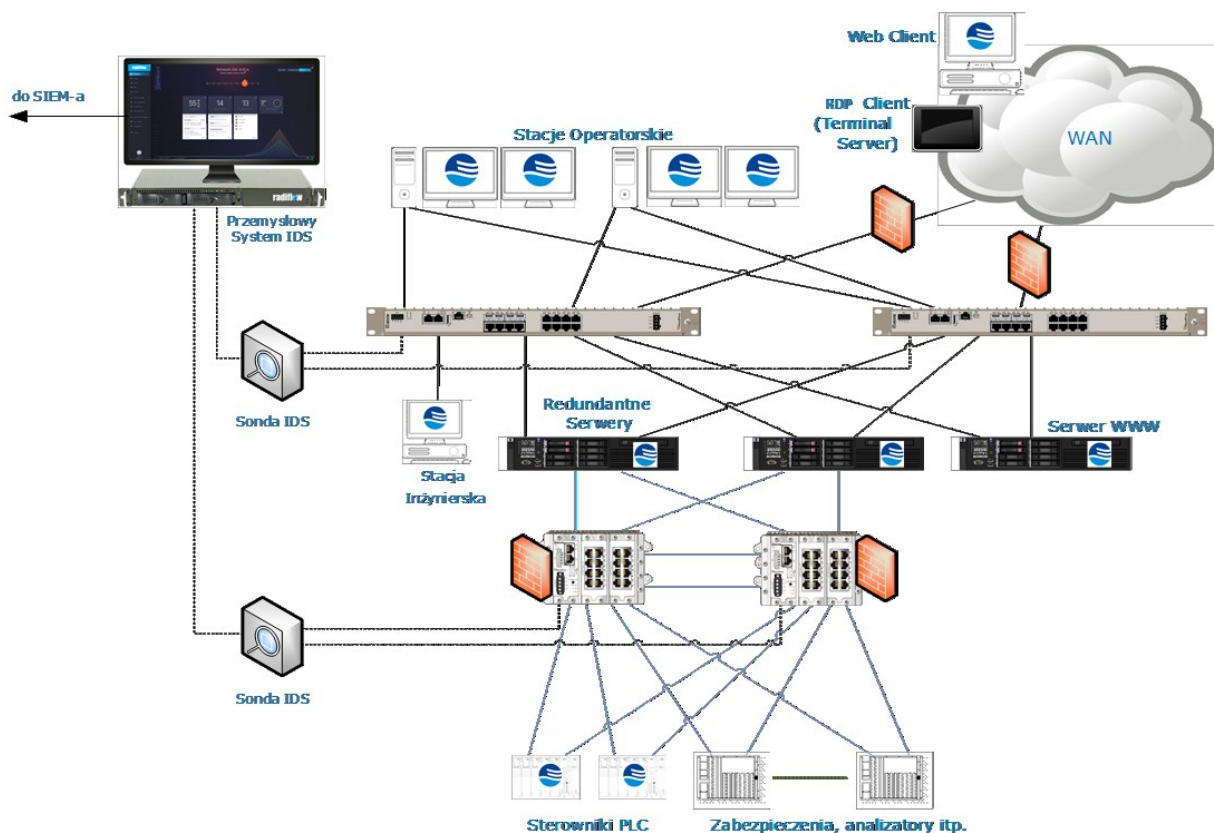
Przykładem może być oddelegowanie pracowników odpowiedzialnych za dany system do współpracy z firmą zewnętrzną, która będzie wspierać ich w analizie zachowania sieci i incydentów w trybie cyklicznym w wybranym modelu. Analiza sieci nawet w trybie raz na 2 czy 3 tygodnie jest lepsza niż brak analizy, którego uzasadnieniem jest brak funduszy na SOC. Pamiętajmy, że Kill Chain wymaga czasu.

Wspomniana powyżej procedura reakcji na incydenty to materiał na niejeden artykuł, lub nawet całą książkę. W skrócie można opisać ten proces jako wszystkie działania niezbędne do przywrócenia prawidłowej pracy systemów organizacji po incydencie bezpieczeństwa. Najważniejszymi elementami tej procedury jest identyfikacja wektora ataku, tzw. „pacjenta zero”, od którego rozpoczął się incydent, a także ograniczenie skutków incydentu i ostateczna naprawa dotkniętych komponentów systemu. Procedura ta

wymaga od zespołu SOC zrozumienia incydentu, właściwego zakresu wiedzy odnośnie systemów – w szczególności informacji o osobach, które mogą być kluczowe w jego przywróceniu. Krytyczne jednak jest zidentyfikowanie wektora ataku i uniemożliwienie ponownego wykorzystania jego wykorzystania. W przeciwnym wypadku nawet najszybciej wykonana procedura reakcji nie powstrzyma atakującego od powtórzenia fazy dostawy i ponownego uruchomienia złośliwego oprogramowania.

Tekniska Polska oferuje usługi szkoleniowe, badania bezpieczeństwa, wdrożeń i modernizacji aż po prowadzenie procesu analizy i reakcji na incydenty.

W trakcie konferencji na połączonym stanowisku ekspozycyjnym firm Tekniska Polska i Energotest, zaprezentowana zostanie przykładowa architektura łącząca technologie i wiedzę obu firm. Na rysunku 3 można zapoznać się z uproszczonym schematem tej prezentacji. Znaleźć można na nim podstawowe elementy zabezpieczeń, takie jak Przemysłowy IDS, jego sondy, a także firewalle chroniące segmenty sieci przemysłowej. Wspomniane elementy stanowią fundament zabezpieczenia sieci. Atakujący od strony sieci WAN spotka się z oporem już na granicy WAN/Sieć OT. Pierwsze firewalle widoczne na schemacie to firewalle aplikacyjne Stormshield, które mogą dostarczać ochronę antywirusową inline, system IPS/IDS dedykowany dla protokołów IT, podstawowe funkcje DLP, filtr proxy, a jako firewalle aplikacyjne zapewniają wykrywanie i możliwość blokowania anomalii protokołów. Samo zastosowanie takich firewalli na granicy sieci IT/OT wyraźnie wpływa na postawę bezpieczeństwa sieci [34] Następną linię obrony stanowią same serwery i stacje robocze o właściwej konfiguracji i aktualizowane do najnowszych wersji oprogramowania. Kolejną warstwą zabezpieczeń są firewalle wbudowane w urządzenia typu router-switch Westermo Redfox. Właściwa konfiguracja, dopuszczająca jedynie uprawnione serwery do odpowiednich usług udostępnionych przez sterowniki i elementy zabezpieczeń przemysłowych, stanowi kolejne ograniczenie możliwości atakującego. Wszystkie przełączniki sieciowe (switch) monitorowane są przez sondy systemu Radiflow iSID zbierające dane z wszystkich portów sieciowych i przesyłające ten ruch do centralnego analizatora przemysłowego IDS, który może przysyłać informacje o wszystkich wykrytych nieprawidłowościach do systemu SIEM. Ten ostatni może zbierać dane również z każdego wspomnianego w tym podrozdziale elementu cyberbezpieczeństwa. Firewalle, switchy, routery, serwery i stacje robocze, mogą (i powinny) być skonfigurowane w taki sposób, aby przysyłać dzienniki systemowe do SIEM. Taka konfiguracja zapewnia zespołowi SOC właściwą widoczność zdarzeń w sieci.



Rys. 3. Przykładowa architektura zabezpieczenia środowiska OT

5. Podsumowanie

Mamy nadzieję, że wiedza zawarta w artykule pozwoliła pogłębić Państwa wiedzę na temat zagrożeń cyberbezpieczeństwa takich jak sposób w jaki przeprowadzany jest typowy atak na typowe sieci IT i OT. Staraliśmy się zaznaczyć różnice dzielące sieci IT od sieci OT. Artykuł miał również na celu wyjaśnić jakie metody mogą uniemożliwić lub skutecznie utrudnić atakującemu przeprowadzenie udanego ataku. Jeśli temat jest dla Państwa interesujący lub chcą Państwo pogłębić swoją wiedzę w tym zakresie, a w szczególności w zakresie bezpieczeństwa sieci OT, serdecznie zapraszamy do kontaktu lub do udziału w szkoleniach z zakresu cyberbezpieczeństwa organizowanych w Techniska Polska.

Przypisy

- [1] Podatność to każdy błąd w konfiguracji, lub kodzie oprogramowania, lub nawet w konstrukcji urządzenia, który powoduje, że istnieje możliwość wykorzystania urządzenia, lub oprogramowania w sposób nieprzewidziany przez twórcę, lub nawet przeciwko jego użytkownikowi.
- [2] Information Technologies – Technologia informatyczna
- [3] Information and Communication Technologies – Teleinformatyka
- [4] Voice over IP, czyli telefonia z wykorzystaniem sieci komputerowych np. Skype lub Asterisk
- [5] Enterprise Resource Planning, czyli systemy wspomagające Planowanie Zasobów Przedsiębiorstwa. Klasa systemów, ułatwiających planowanie produkcji, inwentaryzację zasobów lub nawet współpracę z innymi firmami
- [6] Operational Technology – technologie operacyjne
- [7] Industrial Control System – System kontroli przemysłowej
- [8] Bodungen C.: „Hacking Exposed Industrial Control Systems: ICS and SCADA Security Secrets & Solutions”
- [9] Specjaliści wykonujący testy penetracyjne systemów i sieci komputerowych. Testy te polegają na zleconym przez klienta włamaniu się do jego systemów, tak aby ujawnić możliwe do wykorzystania podatności i metody ataku. (<https://pl.wikipedia.org/wiki/pentester>)
- [10] <https://niebezpiecznik.pl/post/tym-zdjeciem-zdekonspirowano-tajna-jednostke-policji-centrum-przetwarzania-danych/>
- [11] ang. Public Relations (PR)
- [12] <https://www.grahamcluley.com/passwords-leaked-live-tv-flood-emergency/>
- [13] Domain Name System – system nazw domenowych, który umożliwia wykorzystywanie łatwych do zapamiętania domen np. www.techniska.pl, zamiast topornych adresów IP
- [14] Nawiasem mówiąc, czasami na podstawie charakterystycznych wykorzystywanych narzędzi i technik możliwe jest określenie, że niektóre ataki wykonuje ta sama grupa. W żargonie bezpieczeństwa mówi się o tych charakterystycznych cechach „TTP”, czyli Taktyki, Techniki i Procedury
- [15] Patrz przypis 14
- [16] Atak DDoS – Distributed Denial of Service – czyli Rozproszony atak Odmowy Usługi, w tym przypadku polegał na wykonywaniu tysięcy połączeń telefonicznych na infolinię obsługi klienta
- [17] <https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/>
- [18] <https://www.fireeye.com/blog/threat-research/2016/01/ukraine-and-sandworm-team.html>
- [19] https://ics.sans.org/media/E-ISAC_SANS_Ukraine_DUC_5.pdf
- [20] Phishing – zniekształcona forma zapisu słowa fishing – czyli łowienie ryb. W kontekście tego typu ataków jest to wdzięczne porównanie, ponieważ zarzucamy wędkę (e-mail) z haczykiem (złośliwy załącznik), przynętą (właściwa treść e-maila). Nie do końca celujemy w konkretną osobę, bo wtedy byłoby to spear phishing – czyli harpunnictwo – jak widać analogia w dalszym ciągu jest spójna
- [21] <https://techniska.pl/isid>
- [22] IDS – Intrusion Detection System, czyli system wykrywający włamania do sieci lub hostów (komputerów) w organizacji. Dobrze zaprojektowany IDS wykrywa anomalie sieciowe i wzorce ruchu wykonywane przez włamywacza. IDS to rozwiązanie pasywne, które po wykryciu włamania, może jedynie zareportować o tym fakcie, ale nie zablokuje tego ataku
- [23] <http://prawo.sejm.gov.pl/isap.nsf/download.xsp/WDU20180001560/U/D20181560Lj.pdf>
- [24] IPS – Intrusion Prevention System – system zapobiegający włamaniom, czyli IDS, który może zablokować ruch wykryty jako złośliwy
- [25] Proxy – system pośredniczący w połączeniach do innych hostów. 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

- [26] Łatka/Patch – poprawka programistyczna usuwająca wykryte błędy i podatności
- [27] DEP – Data Execution Prevention jest metodą ochrony systemów operacyjnych przed exploitami wykorzystującymi podatność przepełnienia bufora
- [28] ASLR – Address Space Layout Randomisation – kolejna metoda ochrony systemów, chroniąca przed atakami nadpisującymi pamięć aplikacji
- [29] DLP – Data Loss Protection, czyli system zapobiegający wyciekowi danych. Zasada jego działania opiera się na klasyfikacji poufności danych i systemów, a następnie blokowaniu przepływu danych poufnych do systemów o niższej klasyfikacji
- [30] ang. „Niebieski zespół”
- [31] Security Operations Centres
- [32] Security Information and Event Management
- [33] Oprogramowanie Open Source (ang. Otwarte źródło), licencjonowane jest najczęściej w taki sposób, że pozwala na darmowe wykorzystywanie i modyfikację oprogramowania przez użytkownika
- [34] ang. security posture

