

Atakują! Co robić?!

Kamil Kowalczyk, Adam Lisowski - PwC

Streszczenie

W referacie przedstawiono specyfikę systemów automatyki przemysłowej oraz przykłady ataków na nią. Omówiono, jak wygląda przebieg ataku w przemysłowych systemach sterowania i kontroli. W szczególności pokazano fazy takiego ataku. Wskazano sposoby ochrony przed skutecznym atakiem na przemysłowe systemy sterowania i kontroli. Opisano, jak powinna wyglądać poprawnie skonstruowana po stronie przedsiębiorstwa reakcja na atak, oraz na co należy zwrócić uwagę w przedsiębiorstwach wykorzystujących automatykę przemysłową, aby atak skutkował minimalnymi stratami firmy.

1. Wstęp

W 2014 roku świat obiegła wiadomość o kolejnym udanym ataku hakerów na instalację przemysłową. Tym razem obiektem ataku stała się niemiecka huta stali [1]. Skala spowodowanych zniszczeń była równie spektakularna, jak w przypadku Iranu i uszkodzenia wirówek do wzbogacania uranu w 2010 roku. W przypadku huty atakujący, wykorzystując socjotechnikę, skutecznie zagroził jej stabilnej pracy. Prześledźmy, jak to było możliwe. Hakerzy wysłali wiadomość e-mail adresowaną do konkretnego odbiorcy i zawierającej treść, która wzbudzi jego zainteresowanie (atak typu: spear phishing). Uzyskano dostęp do sieci biznesowej firmy, a tym samym stworzono przyczółek do dalszych działań. Umożliwiło to atakującemu, wykonanie złośliwego kodu, który uruchomił się na komputerze pracownika. Skompromitowany komputer dał atakującemu możliwości przeniknięcia do sieci przemysłowej, gdzie znajdowały się między innymi systemy sterowania i kontroli pieca hutniczego. Ciekawe w zastosowanej technice jest to, że wiadomość można wysłać do dużej grupy pracowników i wystarczy jeden odpowiedni pracownik, aby uzyskać dostęp bez potrzeby przełamывania skomplikowanych zabezpieczeń.

Instalacje przemysłowe analogiczne do wspomnianego powyżej pieca przystosowane są do pracy w procesie ciągłym, działają wiele lat bez żadnej przerwy. Bezpieczne i planowane wyłączenie takiej instalacji nie jest natychmiastowe: proces wyłączenia pieca hutniczego trwa co najmniej kilka dni. Atak doprowadził do natychmiastowego wyłączenia pieca – niezgodnie z wymogami technologicznymi. W konsekwencji spowodowało to rozległe zniszczenia, których skalę firma utajniła. Federalne Biuro ds. Bezpieczeństwa Informacji ocenia, że atakujący posiadali umiejętności techniczne obejmujące nie tylko klasyczne systemy bezpieczeństwa IT, ale także wiedzę o systemach sterowania i kontroli oraz informację o procesach, którymi te systemy zarządzały. Atakujący wiedzieli, co robili i mieli w tym konkretny cel. Niepokojące jest to, że nie udało się jasno stwierdzić, od kiedy atakujący mieli dostęp do instalacji.

Rok później...

W grudniu 2015 roku ponownie zanotowano atak hakerski – tym razem na Ukrainie skutecznie odcięto dostawę prądu [2]. Przerwa była ponownie efektem techniki „spear phishing”, połączonej z atakiem na przemysłowe systemy sterowania i kontroli. Wyłączono 7 stacji 110 kV i 23 stacje 35 kV, co w konsekwencji pozbawiło prądu ok. 225 tysięcy odbiorców.

Skoordynowano atak na 3 spółki dystrybucyjne, każda z nich musiała wdrożyć procedury przywracania zasilania przy udziale pracowników fizycznie znajdujących się na obiektach objętych atakiem. Pełne podłączenie odbiorców potrwało kilka godzin. Po tym czasie kontrola nad sieciami dystrybucyjnymi wciąż była ograniczona ze względu na potrzebę prowadzenia ruchu bez wsparcia systemów - ręcznie.

Atak objął między innymi serwery portów szeregowych, gdzie odnotowano wymianę oprogramowania na złośliwe. Atakujący nauczyli się także działać w trzech różnych i odrębnych systemach sterujących sieciami dystrybucyjnymi. Ponownie wymagało to z ich strony szerokiej wiedzy. Atakujący, czuli się tak pewnie, że na koniec posprzątali po sobie, dosłownie kasując dyski zainfekowanych komputerów sterujących oraz oprogramowanie konwerterów portów szeregowych. Szacuje się, że atakujący prowadzili działania przez przeszło pół roku infekując sukcesywnie infrastrukturę teleinformatyczną tych firm.

Bywa, że niezamierzonym atakiem jest również brak wiedzy i zrozumienia środowiska przemysłowego. Zbyt intensywne aktywne skanowanie w celu uzyskania informacji o ewentualnych podatnościach jest efektem zatrzymania sterownika i konieczność jego restartu, czy całkowite wyłączenie urządzenia.

Istnieje zasadnicza różnica w atakach pojawiających się w obszarze IT, a atakach w obszarze przemysłowym. Przemysłowe systemy sterowania i kontroli są zaprojektowane pod kątem konkretnych instalacji i procesów przemysłowych na podstawie wytycznych architektonicznych narzuconych przez producenta takiego systemu z uwzględnieniem ograniczeń finansowych inwestora – stąd skuteczny atak na infrastrukturę przemysłową

wymaga rozległej wiedzy atakującego na temat procesów przemysłowych, wpływu określonych wartości parametrów na proces.

Udany atak na systemy IT może mieć znaczący wpływ na procesy biznesowe. W przypadku udanego ataku na przemysłowe systemy sterowania i kontroli oprócz takiego wpływu dochodzą jeszcze aspekty narażenia ludzkiego zdrowia i życia oraz środowiska naturalnego. W odróżnieniu od ataków w obszarze IT, celami ataków na systemy sterowania jest nie tylko informacja, ale co najmniej utrata kontroli nad procesem technologicznym, czy też możliwość zatrzymania go lub uszkodzenia fizycznego infrastruktury przedsiębiorstwa.

Ataki na automatykę mają ogromny wpływ na życie ludzkie, zwłaszcza w obszarach infrastruktury krytycznej lub operatorów usług kluczowych zdefiniowanych i określonych w dyrektywie NIS [10]. Na dzień dzisiejszy tylko od atakujących zależy, kiedy usłyszymy o kolejnym spektakularnym ataku.

2. Model ataku

Ataki wycelowane w przemysłowe systemy sterowania i kontroli nie składają się z pojedynczych, przypadkowych incydentów – są efektem zorganizowanych i złożonych działań. Ustandaryzowany, modelowy zestaw czynności, które atakujący wykonuje podczas ataku na przemysłowe systemy sterowania i kontroli zdefiniował SANS Institute w 2015 roku pod nazwą ICS Cyber Kill Chain [9].

Model ten oparty jest o sprawdzoną koncepcję Cyber Kill Chain bazującą na spostrzeżeniu, że eliminacja lub utrudnienie wcześniejszych faz ataku powoduje wykluczenie lub ograniczenie kolejnej jego fazy. Atak składa się z dwóch etapów:

- Etap 1. Przygotowanie i realizacja cyberataku – etap ten jest podobny do standardowego ataku ukierunkowanego (APT),
- Etap 2. Zbudowanie i realizacja ukierunkowanego ataku na przemysłowe systemy sterowania i kontroli – etap zamierzonego ataku na infrastrukturę przemysłową, wykorzystującego informacje zdobyte podczas pierwszego etapu.

2.1. Etap 1. Przygotowanie i realizacja cyberataku

Każdy z etapów ataku można podzielić na mniejsze fazy. W etapie pierwszym można wyróżnić następujące:

1. Planowanie

Celem tej fazy jest identyfikacja wszystkich informacji, które mogą pomóc w dalszym ataku. Szczególne cenne informacje uzyskiwane w tej fazie to architektura sieci, rodzaje urządzeń aktywnych (firewall, router itp.), rodzaje wykorzystywanych systemów sterowania i kontroli oraz procedury postępowania.

2. Przygotowanie

W tej fazie atakujący opracowują wektory ataku na podstawie zebranych wcześniej informacji oraz znanych sobie podatności. Następnie atakujący buduje scenariusze w celu osiągnięcia jak największego efektu przy minimalnych nakładach.

3. Uzyskanie dostępu

Celem tej fazy jest uzyskanie dostępu do atakowanego systemu, sieci lub urządzenia. Przykładowo, złośliwy kod dostosowany do odkrytych wcześniej podatności podsyłany jest nieświadomym użytkownikom. Umożliwia to atakującemu skuteczne dostanie się do zaatakowanego urządzenia bez konieczności przełamывania zabezpieczeń za każdym razem tworząc przyczółek dla dalszych działań.

4. Dowodzenie i kontrola

Atakujący dobrze znający zaatakowane środowisko często budują kilka przyczółków, aby w trakcie działań obronnych przedsiębiorstwa mieć możliwość alternatywnej drogi wejścia. Atakujący do komunikacji z centrami C2 (dowodzenia i kontroli – Command and Control) potrafią stosować portale społecznościowe, dołączać swoje komunikaty do danych legalnie przesyłanych w zaatakowanej sieci (np. poprzez zapytania DNS), czy nawet podłączać własne urządzenia komunikacyjne do infrastruktury zaatakowanego przedsiębiorstwa.

5. Utrzymanie, rozwój oraz realizacja celów

W tej fazie następuje wykorzystanie potencjału zdobytego w zaatakowanym środowisku. Nowe cele między innymi to: kolejna instalacja, nowy system automatyki, lokalizacja istotnych informacji do pozyskania, wysłanie zdobytych informacji na zewnątrz zaatakowanego środowiska, zakłócanie działania mechanizmów obronnych, czy zacieranie śladów. Na tej fazie zazwyczaj kończy się standardowy atak ukierunkowany w obszarze IT. Ta część pierwszego etapu jest kluczowa dla dalszego rozwoju ataku w kierunku systemów sterowania i kontroli procesów przemysłowych. Zazwyczaj więcej wartości dla atakującego przedstawia uzyskanie danych z tego obszaru niż destruktywny atak na systemy sterowania i kontroli.

Jeśli systemy sterowania i kontroli mają bezpośrednią komunikację z Internetem, to cały powyższy etap może być pominięty. W takim przypadku atakujący nie muszą budować skomplikowanego ataku oraz przechodzić

przez monitorowany zazwyczaj obszar infrastruktury IT. Wystarczy wysłanie e-maila lub otwarcie strony na komputerze w obszarze systemów sterowania i kontroli.

Skuteczny atak na docelowe systemy sterowania i kontroli może być również przeprowadzony poprzez zrealizowanie pierwszego etapu ataku w infrastrukturze producentów, projektantów, dostawców, firm wdrożeniowych, serwisantów lub ich podwykonawców, np. poprzez modyfikacje oprogramowania produkcyjnego, w dalszym kroku podmianę oprogramowania systemowego sterownika, czy koncentratora.

2.2. Etap 2. Zbudowanie i realizacja ukierunkowanego ataku na przemysłowe systemy sterowania i kontroli

Etap 2. wykorzystuje informacje zdobyte podczas pierwszego etapu i składa się z następujących faz:

1. Rozwinięcie i dostrojenie ataku

W tej fazie atakujący buduje nowe możliwości dopasowane do specyficznego środowiska systemu sterowania i kontroli w celu osiągnięcia pożądanego efektu. Ta faza zazwyczaj realizowana jest poza środowiskiem docelowego dla atakującego systemu sterowania i kontroli poprzez przygotowanie i testowanie rozwiązań na podstawie danych wcześniej uzyskanych - z tego powodu ta faza może być znacząco opóźniona i nie zostać wykryta bezpośrednio po zakończeniu ostatniej fazy etapu 1.

2. Sprawdzenie

W przypadku chęci osiągnięcia przez atakujących znaczących i wiarygodnych efektów w tej fazie atakujący testuje swoje możliwości na podobnie lub identycznie skonfigurowanym przemysłowym systemie sterowania i kontroli. W niektórych przypadkach atakujący kupuje cały osprzęt takiego systemu.

3. Realizacja celów w systemie sterowania i kontroli

Ostatnia faza ukierunkowanego ataku na przemysłowe systemy sterowania i kontroli. W tej fazie, atakujący przeprowadza atak bezpośrednio na systemy automatyki. Atak może posiadać wiele aspektów, być wielowątkowy i obejmować także inne obszary działalności zaatakowanego przedsiębiorstwa. Ataki mogą mieć m.in. na celu: naruszenie bezpieczeństwa lub zakłócenie działania systemu sterowania i kontroli, wyciągnięcie z niego danych, jego uszkodzenie, czy w końcu mniejszy lub większy wpływ na proces obsługiwany przez dany system sterowania i kontroli, np. poprzez zmianę algorytmów, składu lub proporcji receptur, czy utratę wizualizacji czy możliwości sterowania procesem.

2.3. Jak się zabezpieczyć?

Skuteczny atak oznacza powodzenie w realizacji wszystkich poprzedzających go czynności w przedstawionym powyżej modelu ICS Cyber Kill Chain. Przerwanie któregoś z działań - ogniwa w przedstawionym powyżej łańcuchu - niweczy pozostałą część ataku. Rozsądnie zaprojektowana architektura bezpieczeństwa zawierająca zazwyczaj wiele warstw, sprzyja i umożliwia wykrycie i zidentyfikowanie działań niepożądanych, a im szybciej zostaną one wykryte przez nadzorowane mechanizmy bezpieczeństwa, tym szybciej będzie można im przeciwdziałać.

Widać również, że skuteczny atak na dobrze zaprojektowaną i chronioną infrastrukturę przemysłową sterowaną i nadzorowaną przez systemy informatyczne nie jest działaniem trywialnym. Wymaga czasu, wiedzy, dużych nakładów pieniężnych, a jego monetyzacja nie jest oczywista. Znacząco ogranicza to potencjalnie skuteczne grupy atakujących do tych najgroźniejszych: niezadowolonych lub/i byłych pracowników, szpiegostwa przemysłowego, czy wrogich państw.

3. Obsługa ataku

Potencjalnie szeroki obszar ataku, ilość użytych przez atakujących technik, różnorodność informacji niezbędnych do poprawnej identyfikacji ataku wymaga całościowego spojrzenia na organizację, źródła danych i informacje.

Tymczasem, jak wynika z badania PwC [4], prawie 20% dużych i średnich firm w Polsce nie posiada żadnego specjalisty od cyberbezpieczeństwa, a 59% przedsiębiorstw nie zatrudnia kierownika lub dyrektora do spraw bezpieczeństwa. Biorąc pod uwagę trendy w zagrożeniach opisane np. w [7] oraz nowe narzędzia i frameworki dedykowane atakowaniu przemysłowych systemów sterowania [5], [6] należy zauważyć, że standardowy dla przedsiębiorstw przemysłowych telefon do serwisu przestaje wystarczać.

Modelowy sposób obsługi ataków zawiera następujące cztery etapy:

1. Przygotowanie
2. Detekcja i analiza
3. Ograniczenie, likwidacja i przywrócenie
4. Działania po incydencie

Relacje między tymi etapami przedstawia poniższy schemat:



Rys. 1. Schemat modelowego sposobu obsługi ataków

3.1. Przygotowanie

Średni cykl życia systemu po stronie IT wynosi 4 lata, a dla przemysłowych systemów sterowania i kontroli około 15 lat [15]. Co najmniej utrudnione jest także zarządzanie aktualizacjami bezpieczeństwa po stronie systemów przemysłowych. Wymiana firmware, aktualizacja systemu operacyjnego, bazy danych, środowiska systemu SCADA / DCS, czy samej aplikacji nie jest zadaniem trywialnym i nie powinna odbywać się w sposób niekontrolowany. Często wymaga również realizacji w określonym momencie, np. w trakcie przeglądu, modernizacji, czy remontu instalacji technologicznych.

Biorąc to pod uwagę należy, oprócz mechanizmów zabezpieczających przemysłowe systemy sterowania i kontroli, obserwować symptomy incydentów / ataków, a w przypadku ich wystąpienia dysponować opracowanym planem ich obsługi [11].

Aby ograniczyć potencjalne zdarzenia bezpieczeństwa należy podjąć następujące działania:

1. Przygotowanie organizacji, infrastruktury, narzędzi oraz niezbędnej dokumentacji do obsługi incydentów / ataków.
2. Realizacja serii działań zapobiegających incydentom w takich, jak:
 - okresowa analiza ryzyka umożliwiająca określenie skutków niedostępności określonych elementów przemysłowych systemów sterowania,
 - zabezpieczenie hostów,
 - zabezpieczenie sieci i komunikacji,
 - zabezpieczenie przed malware,
 - szkolenie i uświadamianie użytkowników.

Poprawne zarządzanie bezpieczeństwem w przemysłowych systemach sterowania i kontroli uwzględnia między innymi zagadnienia: zasoby ludzkie i narzędzia techniczne, podział odpowiedzialności za systemy przemysłowe, procedury, plany odtworzenia oraz architekturę systemów, w tym ich integrację z pozostałą częścią infrastruktury informatycznej oraz niezawodność (np. redundancja).

Przygotowanie organizacji na nieuniknione, to nie tylko powołanie określonych struktur, to także ciągłe podnoszenie świadomości użytkowników w ciągle zmieniającym się środowisku zagrożeń.

3.2. Detekcja i analiza

Detekcja i analiza dla większości przedsiębiorstw jest trudnym i skomplikowanym etapem. Monitoring i zarządzanie procesem przemysłowym za pomocą systemu sterowania i kontroli nie oznacza monitorowania samego systemu. Niejednokrotnie zdarza się, że ten obszar pozostaje niezagospodarowany. Dokument NIST 800-82r2 [11] dot. przemysłowych systemów sterowania wymienia 16 symptomów incydentu / ataku. W dobrze przygotowanych przedsiębiorstwach odpowiedzialność za ich wykrycie i analizę przypada zespołowi SOC (Security Operations Center) przy wsparciu narzędzi.

Zadania zespołu to między innymi:

1. zarządzanie ryzykiem i zgodnością z przepisami,
2. dbanie o zgodność procedur i systemów z polityką bezpieczeństwa przedsiębiorstwa,
3. tworzenie i zarządzanie niezbędnymi politykami i procedurami,
4. nadzorowanie systemów monitoringu bezpieczeństwa systemów, aplikacji i użytkowników,
5. integracja systemów bezpieczeństwa,
6. zapobieganie, wykrywanie i reakcja na zagrożenia,
7. zarządzanie zagrożeniami.

Budując funkcję SOC w przedsiębiorstwie produkcyjnym należy wziąć pod uwagę m.in. jego skalę, narażenie na ryzyko ataku, możliwy wpływ ataku na organizację, wymagania prawne. Organizacja buduje rozwiązanie w warstwie procesowo-organizacyjnej oraz technicznej, adekwatnie do potrzeb i możliwości.

Decyzja wynika z prac analitycznych, pozwoli odpowiedzieć m.in. na pytania:

- Czy taniej jest zbudować osobne mechanizmy SOC dla obszaru przemysłowego i obszaru IT?
- Czy dołożyć określone mechanizmy działania, dostosowane do przemysłowych systemów sterowania i kontroli, do zazwyczaj już istniejących po stronie obszaru IT?
- Czy zlecać realizację tych działań w całości lub w części na zewnątrz?
- Czy zastosować inne mechanizmy wynikające z wypracowanej analizy?

Podstawowym narzędziem komórki pełniącej zadania SOC jest system klasy SIEM (Security Information and Event Management) integrujący i wstępnie interpretujący wg zadanych reguł dane spływające z systemów obejmujących obszary umożliwiające identyfikację ataku we wszystkich etapach określonych w ICS Kill Chain. Sygnały incydentu / ataku można uzyskać z powszechnie dostępnych narzędzi o dobrze określonym działaniu i jego wpływie na pozostałą część środowiska przemysłowego. Takimi źródłami danych dot. bezpieczeństwa są m.in.: IDSy, oprogramowanie antywirusowe, antyspamowe i antymalware, oprogramowanie weryfikujące integralność plików, oprogramowanie monitorujące, logi urządzeń sieciowych, w tym firewalli, logi systemów operacyjnych, logi usług, logi aplikacji. Dobrze wyszkolony i przygotowany operator systemów sterowania i nadzoru w zakresie cyberzagrożeń, również może być źródłem informacji o podejrzanym zachowaniu się systemu.

Oczywiście nie oznacza to, że każdy z pojawiających się sygnałów należy od razu zignorować. Dobrze wyszkolony i zaznajomiony z infrastrukturą zespół SOC jest w stanie ocenić, czy dane zdarzenie ma związek z naruszeniami bezpieczeństwa. Nawet jeśli sygnały o ataku są niejasne lub jeśli zespołowi po prostu brakuje informacji do podjęcia decyzji, to zespół SOC powinien być w stanie je uzupełnić kierując zapytanie do znanych mu osób odpowiedzialnych za określone fragmenty infrastruktury przedsiębiorstwa. Między innymi dlatego w ocenie i klasyfikacji incydentu / ataku po stronie przemysłowych systemów sterowania i kontroli powinny uczestniczyć takie osoby jak serwisanci, administratorzy techniczni, dyspozytorzy czy operatorzy poszczególnych procesów technologicznych a nawet technologowie.

Niezależnie od sposobu prowadzenia analizy poszczególnych zestawów sygnałów istotnym aspektem jest czas. Skuteczne organizacje bezpieczeństwa dążą do jego minimalizacji, tak aby jak najszybciej przerwać opisany powyżej ICS Kill Chain i nie dopuścić do rozbudowania i zwiększenia skali incydentu / ataku. Nie pomaga w tym ilość zdarzeń do przeanalizowania. W dużych organizacjach mogą to być nie tysiące, ale miliony sygnałów dziennie do przeanalizowania.

W efekcie analizy wstępnej organizacja powinna określić zakres i zasięg incydentu / ataku (konkretnie jakich sieci, komputerów lub systemów dotyczy), kto spowodował pojawienie się incydentu / ataku, w jaki sposób się on objawia w infrastrukturze przedsiębiorstwa oraz jakie metody i podatności zostały wykorzystane przy jego budowie. To pozwala na określenie istotności danego incydentu / ataku i określenie pilności i sposobu realizacji kolejnego etapu.

Istotność ataku powinna uwzględniać co najmniej następujące obszary:

1. Wpływ incydentu / ataku na funkcjonalność przemysłowego systemu sterowania i kontroli.
2. Wpływ incydentu / ataku na sterowanie, przetwarzane dane i informacje.
3. Ilość zasobów niezbędnych, aby powrócić do stanu sprzed wystąpienia incydentu / ataku.

Każda z organizacji powinna już na etapie planowania określić, jak należy postępować z incydentami / atakami o określonym wpływie na jej funkcjonowanie.

W dojrzałych organizacjach opisaną powyżej analizą i określeniem priorytetów oraz zarządzaniem wykrytym incydem / atakiem zajmuje się zespół CSIRT (Computer Security Incident Response Team). Jeśli zespół taki nie jest formalnie powołany, wówczas to zadanie realizowane jest przez SOC. Jeśli przedsiębiorstwo posiada formalnie powołany CSIRT, to wówczas SOC pomaga zespołowi CSIRT w zgromadzeniu wszystkich niezbędnych informacji w celu efektywnej odpowiedzi na atak i zagrożenie.

Typowymi zadaniami zespołu CSIRT są:

1. przeciwdziałanie, wykrywanie i odpowiedź na trwające ataki i naruszenia bezpieczeństwa,
2. określanie priorytetu incydentu / ataku,
3. przeprowadzanie bardziej dogłębnej analizy i śledztwa w zakresie incydentu / ataku,
4. realizacja planów komunikacji o incydencie / ataku,
5. koordynacja i realizacja strategii odpowiedzi na atak,
6. utrzymywanie repozytoriów zebranych informacji dla celów zabezpieczenia organizacji przed podobnymi atakami zachowując zgodność z uwarunkowaniami prawnymi.

Aby zespół CSIRT wiedział, z kim należy współpracować i kogo należy powiadamiać istotne jest również opracowanie skutecznych mechanizmów działania i przepływu informacji o zdarzeniu bezpieczeństwa. Należy odpowiedzieć na pytania:

- Których zasobów incydent dotyczy?
- Jakie są możliwe ścieżki eskalacji?
- Kto powinien się o nim dowiedzieć?
- Kto podejmuje decyzje np. o wyłączeniu części lub w całości systemu?
- Kto będzie uczestniczył w ograniczeniu skutków?
- Kto będzie informował wewnątrz i na zewnątrz o zdarzeniu?
- Kto podejmie decyzje o uruchomieniu planów awaryjnych?

Odpowiedź na te pytania w dużej mierze zależy od organizacji, jednak powinna znaleźć się w opracowanym planie komunikacji o incydencie / ataku.

W celu usystematyzowania kogo należy powiadamiać można skorzystać z poradników opracowanych w ramach Rządowego Centrum Bezpieczeństwa [13] i [14], gdzie zdefiniowano zestaw ról w obszarze przemysłowym niezależny od organizacji, które powinny zostać jednoznacznie przypisane do osób, komórek organizacyjnych lub firm trzecich:

1. Właściciel biznesowy systemu OT.
2. Administrator merytoryczny systemu OT.
3. Administrator techniczny systemu OT.
4. Użytkownik systemu OT.
5. Koordynator ds. bezpieczeństwa systemów OT.
6. Architekt systemów OT.
7. Audytor bezpieczeństwa systemów.

Ilość ról nie oznacza ilości osób niezbędnych do obsługi systemów przemysłowych. Role mogą być łączone z innymi obowiązkami – wszystko zależy od skali i złożoności firmy. Generalną zasadą jest unikanie sytuacji, w której osoba będzie sama siebie kontrolować, czyli nie można łączyć roli realizacyjnych z kontrolną.

3.3. Ograniczenie, likwidacja i przywrócenie (Containment, Eradication & Recovery)

W tym punkcie realizowane są następujące działania:

1. Ograniczenie incydentu / ataku.
2. Zbieranie dowodów – dokumentowanie przebiegu incydentu.
3. Ewentualna identyfikacja atakujących hostów.
4. Likwidacja / ograniczenie ataku i przywrócenie.

Powyższe punkty realizowane są przez zespół CSIRT i stanowią kontynuację podjętych wcześniej działań.

Ograniczenie incydentu / ataku pozwala uniknąć sytuacji, w której skala i niekorzystne efekty przekraczają możliwości organizacji i daje czas na zbudowanie skutecznej i dopasowanej strategii naprawy sytuacji stworzonej przez incydent / atak. W przemysłowych systemach sterowania i kontroli ta taktyka powinna być nie tylko spisana, ale również dopasowana i przetestowana w planowanym czasie i w kontrolowanym środowisku określonego przemysłowego systemu sterowania i kontroli – analogicznie do testów i sprawdzeń poprawności działania samego przemysłowego systemu sterowania i kontroli. Nie oznacza to konieczności działania na środowisku produkcyjnym. Przy współpracy z producentami, dostawcami lub wykorzystując dedykowane usługi możliwe jest stworzenie tymczasowego środowiska testowego i zrealizowanie w nim podobnych scenariuszy. Paradoksalnie ograniczenie incydentu / ataku np. poprzez wyłączenie zidentyfikowanego komputera systemu sterowania i kontroli zarażonego ransomware, czy odłączenie całego systemu od komunikacji zewnętrznej może nie mieć żadnego wpływu na ten system i realizowane przy jego pomocy sterowania. Zastosowanie tej strategii nie oznacza także zamrożenia działania ataku – może zaistnieć dokładnie odwrotna sytuacja: możliwe są ataki, w których proste zamknięcie komunikacji z serwerami kontroli (C2) spowoduje reakcję malware osadzonego na zarażonych hostach w postaci np. wyczyszczenia lub zaszyfrowania całego dysku.

Oczywiście decyzja o realizacji takiego, czy innego scenariusza działań musi zostać podjęta przy wcześniejszej akceptacji określonych ryzyk przez zidentyfikowane w organizacji osoby. W przypadku przemysłowych systemów sterowania i kontroli będą to dyspozytorzy, operatorzy, ich kierownicy lub dyrektorzy departamentów technicznych.

O ile podstawowym celem zbierania dowodów podczas incydentu / ataku jest przyspieszenie rozwiązywania problemu przez niego powstałego, o tyle może być ono również wymuszone przez prawo bądź procedury obowiązujące w organizacji.

Najczęstszą metodą gromadzenia dowodów jest wykonywanie kopii dysku lub uruchamianie dedykowanych narzędzi. W przemysłowych systemach sterowania i kontroli należy zweryfikować możliwość zastosowania takich metod, tak aby w przypadku realnego ataku nie trzeba było tracić czasu na dodatkową weryfikację poprawności działania zarówno narzędzia, jak i przemysłowego systemu sterowania i kontroli. Oczywiście takie działanie powinno być przeprowadzone albo w kontrolowanych warunkach, albo od razu opisane i zweryfikowane przez dostawcę / producenta.

Po ograniczeniu incydentu / ataku oraz zebraniu dowodów następuje czas na degradację ataku i przywrócenie bezpieczeństwa kontrolowanego środowiska. Likwidacja lub degradacja skali i zakresu ataku może być konieczna, aby skutecznie przeprowadzić proces przywrócenia bezpieczeństwa i polega np. na usunięciu zidentyfikowanego malware, wyłączeniu skompromitowanych kont użytkowników, czy załataniu podatności wykorzystywanych w ataku. Likwidacja / degradacja ataku najczęściej jest od razu połączona z przywróceniem środowiska, które ma na celu eliminację komponentów wykorzystanych przez atakującego.

3.4. Działania po incydencie (Post-Incident Activity)

Aby powyższe pracochłonne i kosztowne działania nie okazały się bezowocne, każda z organizacji po obsłudze incydentu / ataku powinna wyciągnąć z niego wnioski i ulepszyć stosowane mechanizmy bezpieczeństwa. Obszary do udoskonalenia mogą być różne - od technicznych, np. dołożenie kolejnych źródeł informacji, zmiana sposobu logowania, zbudowanie kolejnych reguł, poprzez proceduralne, np. zmiany w obowiązujących procedurach postępowania przy zgłaszaniu incydentu / ataku, czy w procedurach zarządzania zmianą, po organizacyjne: powołanie dedykowanych komórek CSIRT, zmiany w zakresach odpowiedzialności, itp. Istotnym elementem służącym do zbudowania wiedzy może być stworzenie raportu opisującego sposób, w jaki organizacja poradziła sobie z incydemem i wskazującego miejsca, w których można było zrobić coś lepiej.

4. Podsumowanie

Przeciętny czas przebywania intruzów w zaatakowanym środowisku to 106 dni [8]. Atakującymi są zazwyczaj aktualni pracownicy (33%), hakerzy (28%) oraz byli pracownicy (13%) [4].

W tym aspekcie trzeba ostrożnie podchodzić do integracji funkcjonalności lub samych systemów, np. należy rozważyć pod kątem potencjalnego ryzyka integrację systemów zabezpieczeń z systemami sterowania i kontroli. Takiego podejścia, które uwzględnia aspekty bezpieczeństwa przemysłowych systemów sterowania i kontroli, wymaga także sposób przesyłania danych procesowych z obszarów produkcyjnych do obszarów biznesowych, czy też zabezpieczenie kanałów serwisowych. Należy także przeanalizować, gdzie w informatycznej architekturze przedsiębiorstwa ulokowane są przemysłowe systemy sterowania i kontroli, tak aby ograniczyć możliwość wystąpienia niezamierzonych ataków skutkujących np. zaszyfrowaniem dysków stacji wizualizacji sterowania procesem.

Określone powyżej sposoby postępowania z atakiem oraz techniki, technologie i mechanizmy bezpieczeństwa składają się na poziomie przedsiębiorstwa w dedykowane usługi bezpieczeństwa. Przy takim podejściu odpowiedź na tytułowe pytanie „Atakują, co robić?” jest prosta: należy być przygotowanym, aby w chwili ataku adekwatnie reagować przy użyciu wcześniej zbudowanych i przetestowanych mechanizmów, a po odparciu ataku wyciągnąć wnioski i zaimplementować je w swoich systemach ochrony.

Literatura

- [1] „The State of IT Security in Germany 2014” - Bundesamt für Sicherheit in der Informationstechnik
- [2] “Analysis of the Cyber Attack on the Ukrainian Power Grid” – SANS ICS, E-ISAC
- [3] NotPetya cyber-attack cost TNT at least \$300m – BBC: <http://www.bbc.com/news/technology-41336086>
- [4] „Cyber-ruletka po polsku. Dlaczego firmy w walce z cyberprzestępcami liczą na szczęście” – raport PwC: <https://www.pwc.pl/badaniebezpieczenstwa>
- [5] “Threat Landscape for Industrial Automation Systems in H1 2017” - Kaspersky Lab
- [6] “WIN32/INDUSTROYER - A new threat for industrial control systems” - ESET
- [7] “Kaspersky Security Bulletin: Kaspersky Lab Threat Predictions for 2018” - Kaspersky Lab
- [8] “M-TRENDS® 2017 - A View From the Front Lines” - Mandiant
- [9] “The Industrial Control System Cyber Kill Chain” - SANS Institute
- [10] Dyrektywa NIS - Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii
- [11] “NIST Special Publication 800-82 Revision 2 - Guide to Industrial Control Systems (ICS) Security” - National Institute of Standards and Technology

- [12] "NIST Special Publication 800-61 Revision 2 - Computer Security Incident Handling Guide" - National Institute of Standards and Technology
- [13] Standardy i dobre praktyki ochrony infrastruktury krytycznej - Automatyka przemysłowa w sektorze elektroenergetycznym – Dokument Rządowego Centrum Bezpieczeństwa
- [14] Standardy i dobre praktyki ochrony infrastruktury krytycznej - Automatyka przemysłowa w sektorze ropy i gazu – Dokument Rządowego Centrum Bezpieczeństwa
- [15] Kubiak W. – PwC: XIX Seminarium Energotestu, „Podejście do monitorowania cyberbezpieczeństwa systemów OT w energetyce, czyli praktyczna implementacja standardu branżowego NIST SP 800-82”
- [16] Gęborys P., Kowalczyk K., Sobczyk Sz - PwC, XX Seminarium Energotestu: „Zasada Pareto w cyberbezpieczeństwie OT, czyli jak maksymalnie zwiększyć ochronę systemów OT przy minimum kosztów”