FUNDACJA bezpieczna cyberprzestrzeń

CERT PSE computer emergency response team

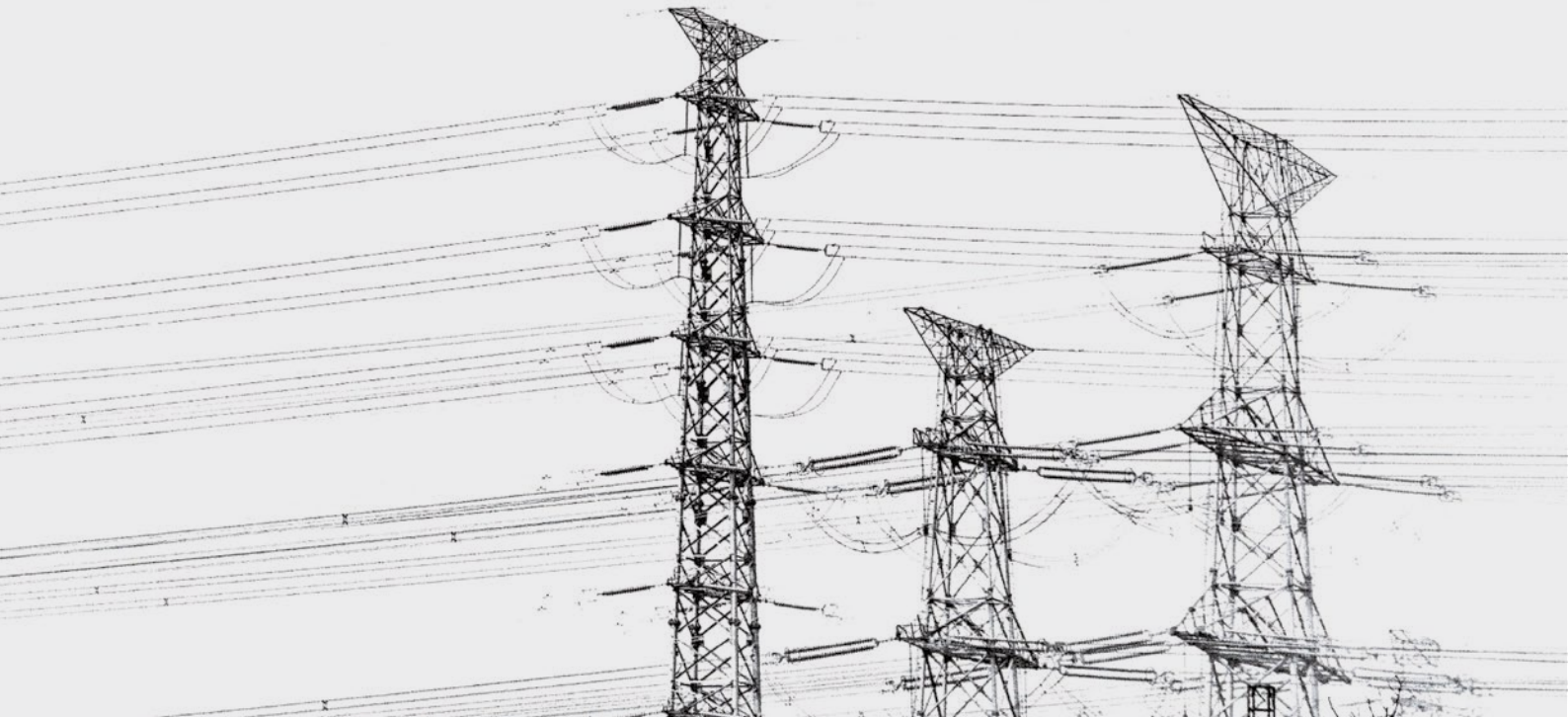
CYBER-EXE POLSKA 2017

ENERGY BLACK SHIELD

CYBER-EXE™ POLSKA 2017 – Energy Black Shield

RAPORT Z ĆWICZEŃ W ZAKRESIE OCHRONY PRZED ZAGROŻENIAMI Z CYBERPRZESTRZENI DLA POLSKIEGO SEKTORA ENERGETYCZNEGO

PRZYGOTOWANIE, PRZEBIEG, ANALIZA, WNIOSKI I REKOMENDACJE



Spis treści

1 Wstęp

Ćwiczenia są jedną z najskuteczniejszych form przygotowania organizacji do reakcji na zagrożenia. Umożliwiają uzyskanie i utrzymanie wysokiego poziomu wiedzy i praktycznych umiejętności. Służą wyrabianiu, utrwalaniu i doskonaleniu nawyków niezbędnych w procesie kierowania realizacją zadań z zakresu zarządzania kryzysowego przez osoby funkcyjne i zespoły ludzkie wszystkich szczebli. Ponadto stwarzają warunki do trafnego wyboru skutecznych form i metod działania w różnorodnych sytuacjach.

W raporcie znajdą Państwo odpowiedź na pytanie, w jaki sposób praktycznie przygotowano i przeprowadzono ćwiczenia, jak one przebiegały, oraz wnioski i rekomendacje, sformułowane na podstawie zaobserwowanych reakcji ćwiczących na zdarzenia zaplanowane w scenariuszu.

Pomimo tego, że do tej pory w Polsce nie odnotowano przypadków zmasowanych, równolegle przeprowadzanych w tym samym czasie ataków na wielu operatorów infrastruktury krytycznej, zagrożenia z cyberprzestrzeni nie są dla sektora energetycznego nowością. Od wielu lat w sektorze tym można zaobserwować większe lub mniejsze ataki, na poszczególne podmioty, które w przypadku zmasowanego charakteru mogą zagrozić bezpieczeństwu nie tylko klientów korzystających z usług operatorów, ale również bezpieczeństwu państwa. Doświadczenie to pozwoliło na wypracowanie szeregu procedur oraz technicznych systemów zabezpieczeń.

Dodatkowym elementem, który był ćwiczony podczas Cyber-EXE™ Polska 2017 Energy Black Shield (dalej: CEP17-EBS), jest zdolność funkcjonowania podmiotów sektora energetycznego w przestrzeni medialnej oraz odporność na występujące w niej na operacje informacyjne.

2 Podsumowanie menadżerskie

Ćwiczenia z cyklu Cyber-EXE™ Polska po raz kolejny udowodniły, że sprostanie zaawansowanemu i wielowektorowemu atakowi teleinformatycznemu, nie jest proste i nawet istniejące i wdrożone w organizacjach procedury mogą być zawodne. Podczas reakcji na cyberatak, który choćby trochę odbiega od przewidzianych procedurami i standardowo realizowanych schematów, istotną rolę odgrywa doświadczenie pracowników, ich kreatywność i osobiste zaangażowanie, a także zdolność do koordynacji działań wewnątrz samej organizacji. W związku z tym kompetencje pracowników odpowiedzialnych za reagowanie na zdarzenia związane z cyberatakiem powinny iść w parze z poziomem wiedzy atakujących i rozwojem technologicznym. W trakcie całodniowych ćwiczeń CEP17-EBS symulowano skoordynowany atak teleinformatyczny na firmy z sektora energetycznego. Podczas ćwiczeń przyglądaliśmy się podejmowanym przez organizacje działaniom oraz ich komunikacji z innymi podmiotami, dla których atak ten mógł mieć znaczenie. Monitorowanie zachowania organizacji dotyczyło również warstwy komunikacji medialnej. W trakcie ćwiczenia, organizacje w nim uczestniczące, pracowały w oparciu o wewnętrzne regulacje dotyczące postępowania w sytuacjach kryzysowych. Bez pełnej identyfikacji narzędzi wykorzystywanych przez atakujących, organizacja może nie mieć możliwości oszacowania realnego wpływu incydentu na bezpieczeństwo oraz przygotowania odpowiednich metod przeciwdziałania.

Niniejszy raport stanowi sprawozdanie z ćwiczeń CEP17-EBS, a także zawiera podsumowanie kluczowych spostrzeżeń i rekomendacji dla firm sektora energetycznego w obszarze bezpieczeństwa teleinformatycznego.

Należy podkreślić, że wszyscy uczestnicy ćwiczeń wskazali na korzyści wyniesione z udziału w tym przedsięwzięciu. Z pewnością, regularnie przeprowadzane ćwiczenia są szansą na osiągnięcie większej dojrzałości organizacji biorących w nich udział, zaś wyciągnięte wewnętrznie wnioski mogą przyczynić się do udoskonalenia stosowanych procedur, zarówno tych dotyczących bezpośredniej reakcji na incydenty, jak i komunikacyjnych. Raport zawiera spostrzeżenia i wnioski, które dotyczą wszystkich uczestników ćwiczeń. Niezależnie od nich i przedstawionego raportu, Fundacja Bezpieczna Cyberprzestrzeń, współpracując z poszczególnymi organizacjami, zaprezentowała szczegółowe spostrzeżenia i rekomendacje dla uczestników ćwiczeń.

3 Ćwiczenia Cyber-EXE™ Polska 2017 Energy Black Shield

3.1 Idea ćwiczeń w zakresie ochrony w cyberprzestrzeni

Ćwiczenia CEP17-EBS są kontynuacją inicjatywy organizacji polskich ćwiczeń z ochrony w cyberprzestrzeni, które po raz pierwszy zorganizowane zostały w 2012 roku. Warto przypomnieć, że pierwsza edycja ćwiczeń organizowana była właśnie dla sektora energetycznego.

Organizacja ćwiczeń, które mają podnosić zdolność organizacji i struktur państwowych do skutecznej ochrony przed atakiem z cyberprzestrzeni stała się koniecznym elementem działań na rzecz poprawy bezpieczeństwa. Organizatorzy cyklu ćwiczeń Cyber-EXE™ Polska ponad pięć lat temu zdecydowali, by w sposób aktywny realizować takie zadanie. Bezpośrednią zachętą i inspiracją do podjęcia się organizacji były rekomendacje Europejskiej Agencji Bezpieczeństwa Sieci i Informacji (ENISA), które zostały przygotowane po przeprowadzeniu ćwiczeń Cyber Europe 2010, a następnie miały kontynuację w roku 2012, 2014 i 2016. Wśród wyżej wspomnianych rekomendacji znalazły się takie, które zachęcały do organizacji podobnych ćwiczeń na poziomie krajowym, jak również do działań na rzecz udziału w ćwiczeniach – obok przedstawicieli sektora publicznego – podmiotów reprezentujących sektor prywatny. Dodatkową motywacją okazały się udane poprzednie edycje ćwiczeń Cyber-EXE™ Polska; w 2012 roku w sektorze energetycznym, w 2013 roku w sektorze bankowym, w 2014 roku w sektorze telekomunikacyjnym, oraz w 2015 roku w sektorze finansowym, w których do banków dołączyły również firmy ubezpieczeniowe.

Fot. 1: Centrum koordynacji ćwiczeń CEP17

3.2 Geneza ćwiczeń Cyber-EXE™ Polska 2017 Energy Black Shield

Po pozytywnych doświadczeniach związanych z ćwiczeniami Cyber-EXE™ Polska 2012 – 2015, w sposób oczywisty powstała chęć kontynuacji tej inicjatywy. Powrócono do ćwiczeń dla sektora energetycznego, po raz pierwszy zorganizowanych w roku 2012.

Przychylne wsparcie ćwiczeń przez współorganizatora – spółkę Polskie Sieci Energetyczne S.A., oraz przez podmioty publiczne, takie jak Rządowe Centrum Bezpieczeństwa, przy jednoczesnym zainteresowaniu organizacji uczestnictwem w tym przedsięwzięciu sprawiło, że pomysł organizacji ćwiczeń mógł być zrealizowany.

3.3 Organizatorzy

Organizatorem ćwiczeń CEP17-EBS była Fundacja Bezpieczna Cyberprzestrzeń. Współorganizatorem i jednocześnie uczestnikiem ćwiczeń były Polskie Sieci Elektroenergetyczne S.A.

3.4 Uczestnicy ćwiczeń

Do ćwiczeń przystąpiło 6 kluczowych podmiotów, przedstawicieli sektora energetycznego. W ćwiczeniu aktywnie wzięło udział ponad 200 osób.

W ćwiczeniach wzięły udział następujące podmioty:

- Polskie Sieci Elektroenergetyczne S.A.
- Grupa Energa
- Grupa Kapitałowa Polska Grupa Energetyczna S.A.
- Grupa Kapitałowa TAURON
- PERN S.A.
- PGNiG TERMIKA S.A.

3.5 Zespół projektowy

Zespół projektowy stanowili przedstawiciele Fundacji Bezpieczna Cyberprzestrzeń oraz wszystkich pozostałych podmiotów ćwiczących. Zespół projektowy miał przed sobą zadania związane z przygotowaniami w czterech istotnych obszarach projektowych:

- zadania związane z wypracowaniem scenariusza ćwiczeń,
- zadania związane z koncepcją i przeprowadzeniem warstwy medialnej ćwiczeń,
- zadania związane z przygotowaniem warstwy technicznej ćwiczeń, w tym systemu raportowania oraz wizualizacji przebiegu ćwiczeń,
- zadania związane z przygotowaniem zaplecza logistycznego do przeprowadzenia ćwiczeń.

Fot. 2: Centrum Koordynacji Ćwiczeń CEP17

4 Cele ćwiczeń Cyber-EXE™ Polska 2017 Energy Black Shield

Celem głównym ćwiczeń było zbadanie oraz doskonalenie zdolności i przygotowania organizacji do identyfikacji zagrożeń w obszarze bezpieczeństwa teleinformatycznego, odpowiedzi na te zagrożenia oraz skutecznej współpracy w ramach sektora energetycznego. Poza celem głównym konieczne stało się sformułowanie celów szczegółowych, obejmujących:

A. **Sprawdzenie zdolności reakcji organizacji na atak teleinformatyczny:**

- sprawdzenie istniejących planów i procedur zarządzania, identyfikacja potrzeb ich uzupełnienia, aktualizacji lub stworzenia nowych,
- sprawdzenie współpracy i komunikacji wewnątrz i na zewnątrz organizacji.

B. **Sprawdzenie zdolności reagowania organizacji w przypadku szantażu i żądania okupu.**

C. **Sprawdzenie komunikacji zarówno pomiędzy podmiotami ćwiczącymi, jak również organami administracji publicznej oraz innymi podmiotami zewnętrznymi odgrywanymi w ćwiczeniach:**

- sprawdzenie, czy występuje wymiana informacji o zagrożeniach i czy ma ona realny wpływ na zarządzanie nimi,
- sprawdzenie jakości i przydatności wymienianych informacji w reakcji na zagrożenie,
- sprawdzenie komunikacji z producentami sprzętu i oprogramowania.

D. **Sprawdzenie zdolności komunikacyjnych organizacji w warstwie medialnej w związku z incydentem.**

Dodatkowo ćwiczenia były dobrą okazją do sprawdzenia, czy sektor energetyczny potrzebuje i w jak dużym stopniu, wspólnych działań koordynacyjnych? Próba odpowiedzi na tak sformułowane pytanie wpisuje się doskonale w rozważania na temat konieczności istnienia i zakresu funkcjonowania tzw. CERT-u sektorowego dla energetyki.

5 Proces organizacji ćwiczeń

5.1 Faza identyfikacji

W tej fazie zostały ustalone podstawowe cele ćwiczeń oraz lista jego uczestników. W sformułowaniu celów ćwiczeń bardzo pomocne okazały się podmioty biorące udział w ćwiczeniach, zidentyfikowały one szczegółowe obszary, które chciały sprawdzić przystępując do ćwiczeń. Wszystko to w naturalny sposób pomogło wyznaczyć ramy i zakres tematyczny CEP17-EBS. Faza ta obejmowała również określenie przybliżonego obszaru tematycznego ćwiczeń, czyli omówienie wstępnych założeń scenariusza.

5.2 Faza Planowania

W trakcie fazy planowania dokładnie określono obszar tematyczny ćwiczeń, który następnie został opisany szczegółowo w postaci scenariusza. W tej fazie został wybrany przez uczestników ostateczny model przeprowadzenia ćwiczeń i lista uczestniczących wewnętrznie komórek organizacyjnych i stanowisk. Bardzo ważnym elementem fazy planowania było ustalenie organizacyjnych i technicznych zasad przeprowadzenia ćwiczeń, w tym przydzielenia ról związanych z zarządzaniem ćwiczeniami oraz opracowanie instrukcji ćwiczeń. Warto wspomnieć, że uczestnicy mieli dowolność w wyborze modelu przeprowadzenia ćwiczeń wewnątrz swoich organizacji. Przyjęty model był konsultowany z organizatorem ćwiczeń tak, aby mógł być sprawnie włączony w ogólny model organizacji ćwiczeń CEP17-EBS.

5.3 Faza przeprowadzenia ćwiczeń

W trakcie tej fazy przeprowadzono zasadnicze ćwiczenia. Ćwiczenia były poprzedzone próbą generalną (tzw. dry run), podczas której dokonano sprawdzenia kluczowych elementów organizacyjnych oraz scenariusza ćwiczeń, dokonując ostatnich korekt, a przede wszystkim przygotowując ostatecznie organizacje do uczestnictwa w ćwiczeniach. Przetestowano również rozwiązania techniczne, które posłużyły do przeprowadzenia ćwiczeń – przede wszystkim system zarządzania zdarzeniami (ang. injects) – EXITO (the EXercise event Injection TOolkit)[1]. W trakcie próby „dry run" wszystkie osoby zaangażowane w przygotowanie ćwiczeń zasymulowały jego przebieg, odgrywając według swojej najlepszej wiedzy potencjalne zachowania poszczególnych osób i komórek organizacyjnych, których uczestnictwo było przewidziane w ćwiczeniu. Wnioski wyciągnięte z próby generalnej miały istotny wpływ na ostateczny kształt ćwiczenia.

1 https://ec.europa.eu/jrc/en/scientific-tool/exito-exercise-event-injection-toolkit

5.4 Faza oceny

W trakcie tej fazy dokonano podsumowania ćwiczeń i przygotowano końcowy raport. Istotnym elementem tej pracy było przygotowanie i przekazanie uczestnikom ćwiczeń ankiety ewaluacyjnej. Ankiety stały się podstawą do opracowania wniosków i wynikających z nich rekomendacji. Oprócz ankiety zorganizowano spotkanie podsumowujące, w którego trakcie przedyskutowane zostały wszystkie zgłaszane przez uczestników oraz proponowane przez organizatorów wnioski. Materiał dotyczący sporządzenia raportu końcowego został przygotowany przede wszystkim przez organizatora. Został on również uzupełniony o wnioski zgłoszone przez uczestników ćwiczeń. Wszyscy uczestnicy mieli prawo zgłaszać zarówno swoje uwagi, jak i zatwierdzać całość dokumentacji końcowej.

Fot. 3: Centrum koordynacji ćwiczeń CEP17

6 Scenariusz ćwiczeń

Scenariusz ćwiczeń został opracowany przez zespół projektowy, składający się z przedstawicieli podmiotów biorących udział w ćwiczeniach oraz ekspertów merytorycznych specjalizujących się w bezpieczeństwie firm sektora energetycznego. Scenariusz ćwiczeń został oparty na aktualnych i przewidywanych trendach dotyczących złożonych cyberataków.

Założono, że charakter zdarzeń powinien dotyczyć całego sektora oraz doprowadzić do poważnej sytuacji kryzysowej w organizacjach, na którą nie ma gotowych szczegółowych planów postępowania. Wykreowana w scenariuszu sytuacja wymagała od uczestników podejmowania szybkich decyzji oraz umiejętności trafnej diagnozy – tak by nie doprowadzić swym działaniem do eskalacji problemu.

W praktyce scenariusz zakładał, że każda z organizacji stanie się obiektem kilku ataków. Pierwszą zdarzeń był atak DDoS na strony WWW organizacji, biorących udział w ćwiczeniach. Atak ten osiągał nawet 100% wysycenia łącza. W późniejszym etapie ćwiczeń, atak ten został również przeprowadzony na serwery pocztowe, powodując identyczne wysycenie łącza.

Drugą grupą zdarzeń był phishing, a w zasadzie dwa jego rodzaje, które pojawiły się niemal równocześnie. Phishing skierowany był w pierwszej kolejności do działów finansowych a w drugiej do działów IT wszystkich organizacji ćwiczących.

Kolejny etap ćwiczeń stanowiły problemy związane z automatyką przemysłową i wynikające z tego zagrożenia, które mogą pojawić się w organizacjach zarówno bezpośrednio, jak i za pośrednictwem vendora.

Należy podkreślić, że scenariusz mimo swojego charakteru sztabowego, zakładał również element analizy prawdziwego złośliwego oprogramowania, którego próbki zostały przekazane podmiotom ćwiczącym, by sprawdzić gotowość uczestników do przeprowadzenia jego analizy. Zadanie to miało na celu nie tylko sprawdzenie przygotowania proceduralnego, ale również sprawdzenie, czy uczestnicy posiadają stosowne zaplecze techniczne w postaci odpowiednio przeszkolonego personelu i dedykowanego laboratorium umożliwiającego przeprowadzenie w bezpieczny sposób badania złośliwego kodu. Ze względu na swoją odmienność, zdarzenie to zostanie szerzej omówione wraz z wnioskami w tym rozdziale.

Dla uczestników przygotowana została dedykowana próbka złośliwego oprogramowania będąca plikiem wykonywalnym przeznaczonym na platformę Windows. Do próbki dołączony był zestaw pytań mający na celu weryfikację stopnia przeanalizowania przez uczestników przygotowanej próbki. Zadaniem poszczególnych zespołów było najpierw pozyskać próbkę, następnie przeprowadzić jej analizę, a na koniec odpowiedzieć na dołączone do niej pytania.

Należy w tym miejscu zaznaczyć, że zarówno sama próbka, jak i zestaw pytań przygotowane były w taki sposób, że skorzystanie z komercyjnych rozwiązań typu Sandbox pozwalało odpowiedzieć tylko na część załączonych pytań i nie było wystarczające, by udzielić pełnej odpowiedzi na wszystkie pytania. W celu

odpowiedzi na wszystkie pytania konieczne było przeprowadzenie deasemblacji złośliwego kodu i zastosowanie technik inżynierii wstecznej.

W dniu ćwiczeń, około godziny 11:00 w mediach społecznościowych (symulowanych podczas ćwiczeń) zaczęły się pojawiać informacje, że pewien badacz bezpieczeństwa natknął się na próbkę złośliwego oprogramowania prawdopodobnie mogącego być użytym w aktywnych atakach na polskie firmy z sektora energetycznego. Badacz oferował możliwość przekazania próbki wszystkim zainteresowanym stronom.

Po przekazaniu zespołom próbki w późniejszym terminie, zespoły rozpoczęły analizę. Na tym etapie obserwowane były trzy zasadnicze podejścia:

a) rozpoczęcie samodzielnej analizy,
b) przekazanie próbki do zespołu CERT, mogącego pełnić rolę CERT-u sektorowego,
c) przekazanie próbki do zewnętrznych podmiotów – komercyjnych firm i CERT-ów.

Ostatecznie pomimo drobnych niedociągnięć w postaci opóźnionego startu analizy i ograniczonej wymiany informacji o zagrożeniu, końcowy rezultat przeprowadzonych analiz był zadowalający – większość organizacji dostarczyła odpowiedzi, na zasadnicze pytania, które pozwalały na rozpoznanie i identyfikację zagrożenia w sieci wewnętrznej.

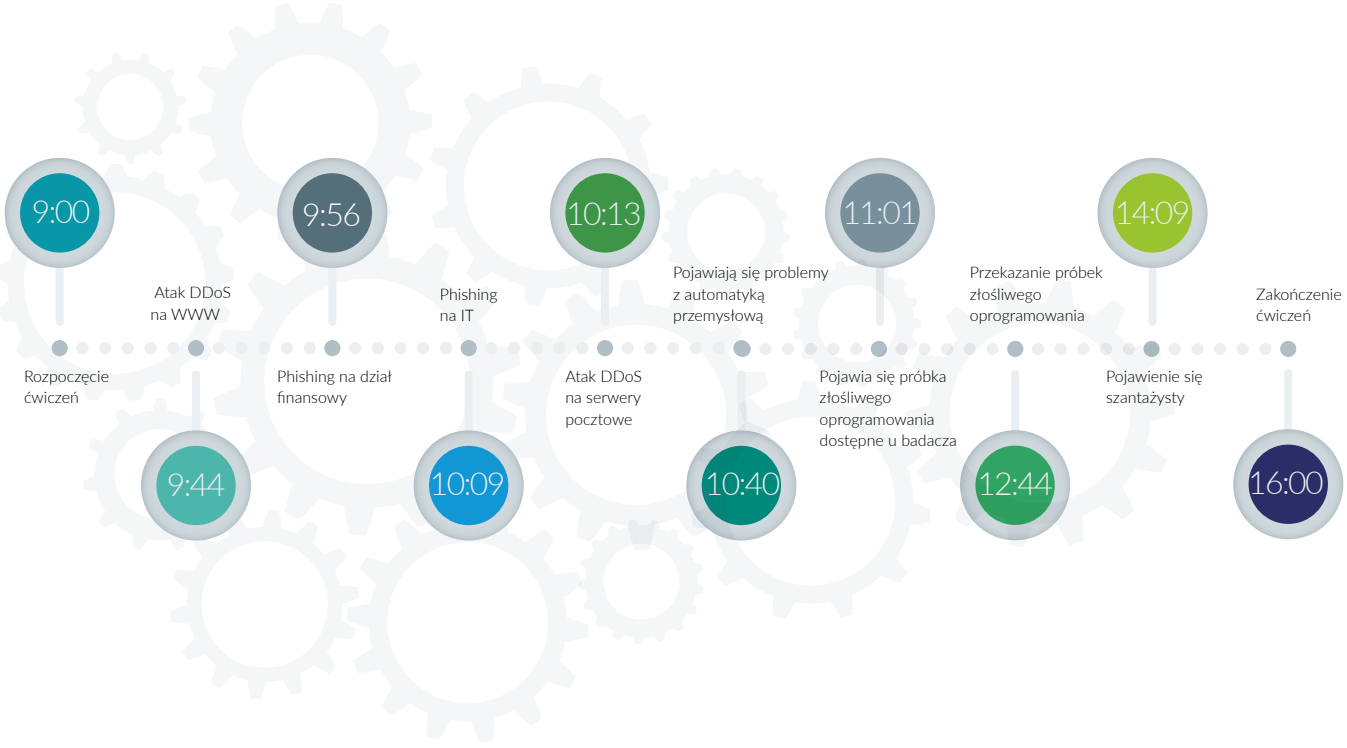
Fot. 4: Organizatorem ćwiczenia CEP15 była FBC, współorganizatorem PSE S.A.

W scenariuszu pojawił się również szantażysta posiadający dane, które wyciekły z organizacji, Groził on udostępnieniem danych publicznie w wypadku niespełnienia jego żądań.

Równolegle do części organizacyjnej ćwiczeń, rozgrywana była również warstwa medialna oraz elementy operacji informacyjnej. W warstwie medialnej, uczestnicy musieli w odpowiedzi na zdarzenia ze scenariusza, przygotować politykę informacyjną i odpowiadać na zapytania dziennikarzy. Pojawił się również element mający sprawdzić zrozumienie komunikatów ukazujących się w warstwie medialnej przez działy PR, jak również ich współpracę i komunikację z działami odpowiadającymi w organizacjach za bezpieczeństwo. Wykorzystując platformę CISKOM, zamieszczono informację o nowym zidentyfikowanym malware, wymierzonym w sektor energetyczny. W informacji tej zachęcano do kontaktu z analitykiem, który owe złośliwe oprogramowanie rozpoznał. W przypadku kontaktu z nim organizacje otrzymałyby jego próbkę do analizy o wiele wcześniej, niż zakładał to scenariusz. W warstwie operacji informacyjnej uczestnicy ćwiczeń musieli zmierzyć się z procesami manipulacji przekazem informacyjnym w mediach społecznościowych oraz podejmować działania mające ograniczać efekty takiej operacji.

Poniższy diagram przedstawia odgrywaną w scenariuszu sekwencję zdarzeń zarówno technicznych, jak i medialnych. Łącznie w scenariusz przygotowano niemal 20 zdarzeń, co oznaczało, że do organizacji ćwiczących trafiało w ciągu godziny około 3–4 komunikatów.

Rysunek 1.
Linia czasu CEP17 EBS



7 Przebieg ćwiczeń

7.1 Informacje podstawowe

Faza przeprowadzenia ćwiczeń CEP17-EBS miała miejsce w dniu 4 stycznia 2018 r. w godzinach 9:00 – 16:00. CEP17-EBS były rozproszonymi ćwiczeniami sztabowymi. Uczestnicy ćwiczeń podzieleni byli na dwie grupy. Pierwsza grupa znajdowała się w Centrum Koordynacji Ćwiczeń (CKC) w siedzibie Polskich Sieci Elektroenergetycznych. Druga pozostawała we własnych lokalizacjach.

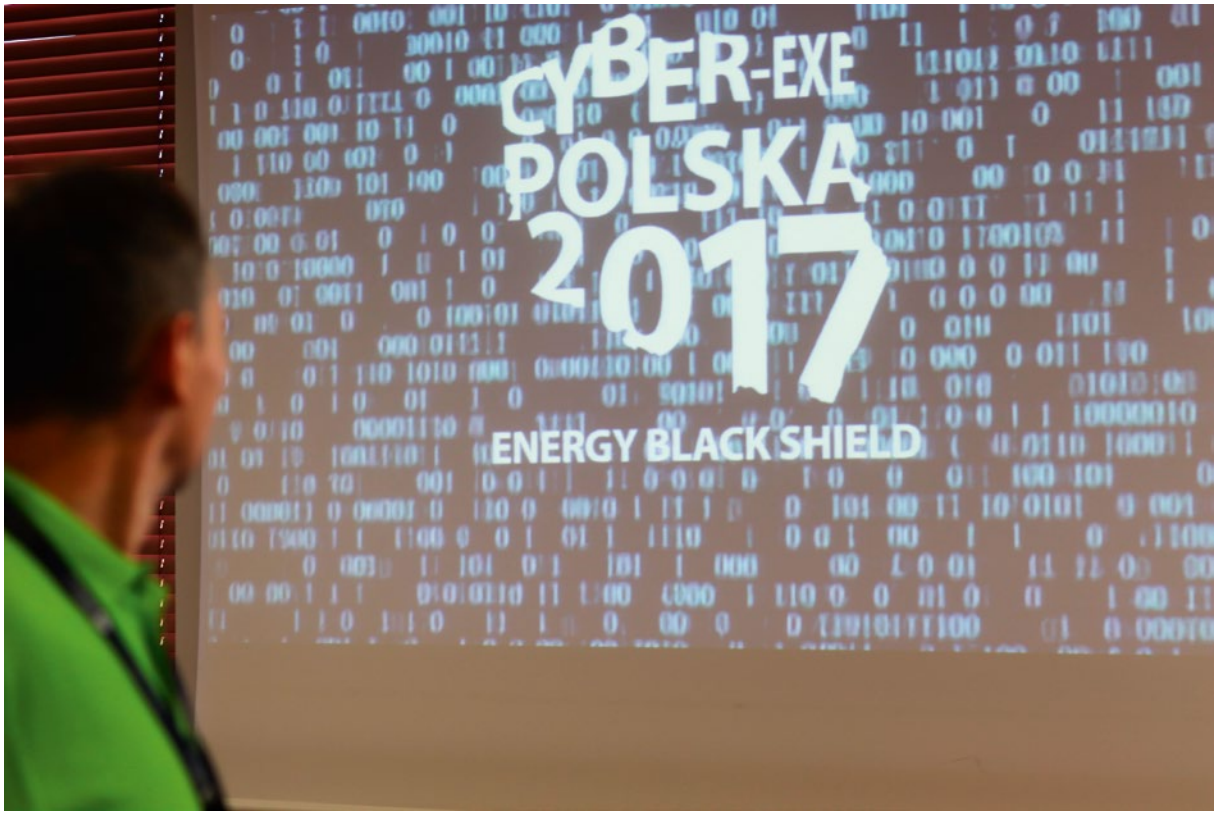
Skład Centrum Koordynacji Ćwiczeń

- moderator główny,
- koordynator zarządzania zdarzeniami,
- koordynator oceny (ewaluator),
- moderatorzy organizacyjni,
- zespół techniczny (2 osoby),
- zespół medialny (5 osób),
- obserwatorzy.

Skład zespołów ćwiczących w organizacjach

- ćwiczący,
- zespoły CERT,
- służby prasowe organizacji.

Fot. 5: Centrum koordynacji ćwiczeń CEP17



7.2 Struktura organizacyjna ćwiczeń

Role poszczególnych uczestników ćwiczeń omówione zostały poniżej.

Rysunek 2.
Struktura organizacyjna ćwiczeń Cyber-EXE™ Polska 2017

7.2.1 Moderator główny

Moderatorem głównym CEP17-EBS był przedstawiciel Fundacji Bezpieczna Cyberprzestrzeń. Osobie moderatora przypisane były następujące zadania:

- koordynacja całości przebiegu CEP17-EBS,
- współpraca z moderatorami organizacyjnymi poszczególnych organizacji w celu przekazywania informacji o przebiegu zdarzeń oraz reakcjach na nie, w oparciu o ustalony zakres informacji,
- rozstrzyganie wątpliwości dotyczących przebiegu CEP17-EBS,
- odbieranie raportów z przebiegu CEP17-EBS od moderatorów organizacyjnych,
- podgrywanie działań podmiotów nieuczestniczących w ćwiczeniach.

Ważną rolę wspierającą pracę moderatora głównego pełniły osoby mające za zadanie podgrywanie niektórych podmiotów uczestniczących w ćwiczeniach.

7.2.2 Koordynator zarządzania zdarzeniami

Koordynatorem zarządzania zdarzeniami był przedstawiciel Fundacji Bezpieczna Cyberprzestrzeń. Osobie koordynatora zarządzania zdarzeniami przypisane były następujące zadania:

- podejmowanie decyzji o uruchamianiu kolejnych zdarzeń scenariusza. W przypadku zdarzeń warunkowych decyzja jest podejmowana w porozumieniu z moderatorem organizacyjnym,
- współpraca z moderatorami organizacyjnymi poszczególnych organizacji w celu przekazywania informacji o przebiegu zdarzeń oraz reakcjach na nie, w oparciu o ustalony zakres informacji,

7.2.3 Ewaluator

Ewaluatorem CEP17-EBS był przedstawiciel Fundacji Bezpieczna Cyberprzestrzeń. Osobie ewaluatora przypisane były następujące zadania:

- stała obserwacja przebiegu ćwiczeń,
- rejestracja przebiegu zdarzeń służących przyszłej ocenie ćwiczeń,
- wsparcie moderatora głównego w realizacji jego zadań,
- współpraca z moderatorami organizacyjnymi w celu zebrania obserwacji związanych z oceną przebiegu CEP17-EBS.

7.2.4 Zespół techniczny

Zespół techniczny składał się z przedstawicieli Fundacji Bezpieczna Cyberprzestrzeń. Zadaniem zespołu technicznego było przygotowanie techniczne i logistyczne ćwiczeń. W szczególności zespół techniczny był odpowiedzialny za:

- utrzymanie systemu EXITO służącego do komunikacji w trakcie ćwiczeń,
- utrzymanie systemu mailowych skrzynek kontaktowych służących do komunikacji w trakcie ćwiczeń,
- organizacja logistyczna ćwiczeń (przygotowanie sali i urządzeń koniecznych do ich przeprowadzenia),
- przygotowanie i obsługa systemu wizualizacji CEP17-EBS,
- stała współpraca z moderatorem głównym i ewaluatorem CEP17-EBS, w celu prezentowania w systemie wizualizacji bieżącego przebiegu ćwiczeń dla poszczególnych organizacji,
- odnotowanie szczegółów dotyczących przebiegu ćwiczeń, tj. czasów wystąpienia poszczególnych zdarzeń reprezentowanych w systemie wizualizacji CEP17-EBS,
- wsparcie moderatora w przygotowaniu technicznych szczegółów wprowadzeń scenariusza i ewentualnie odpowiedzi zewnętrznych systemów teleinformatycznych,
- wsparcie dla zespołu medialnego przy technicznym utrzymaniu systemu CISKOM[2].

7.2.5 Zespół medialny

Zespół medialny składał się z przedstawicieli Fundacji Bezpieczna Cyberprzestrzeń. Był on odpowiedzialny za:

- przygotowanie komunikatów medialnych związanych ze scenariuszem ćwiczeń CEP17-EBS,
- współpracę z moderatorem głównym w celu publikowania komunikatów medialnych w systemie CISKOM, zgodnie z przebiegiem zdarzeń,
- reagowanie na komunikaty publikowane przez służby PR organizacji biorących udział w ćwiczeniach, poprzez odpowiednie publikacje oraz bezpośrednie kontakty z tymi służbami.

7.2.6 Moderatorzy organizacyjni

Moderatorami organizacyjnymi były osoby wyznaczone do tej funkcji przez poszczególne organizacje biorące udział w ćwiczeniach CEP17-EBS. Osobie moderatora organizacyjnego przypisana była:

- koordynacja ćwiczeń CEP17-EBS w danej organizacji, a w szczególności:
  - przekazywanie wprowadzeń (kolejnych zdarzeń) ze scenariusza ćwiczeń, uruchamianych przez moderatora głównego,
  - symulowanie działania wewnętrznych systemów teleinformatycznych danej organizacji w oparciu o wcześniej przygotowane założenia komunikatów technicznych,

2 System CISKOM jest platformą należącą do Rządowego Centrum Bezpieczeństwa..

- monitorowanie przebiegu ćwiczeń w danej organizacji oraz reakcja na ewentualne zakłócenia jego przebiegu,
- przekazywanie informacji o przebiegu ćwiczeń w danej organizacji w oparciu o ustalony zakres informacji, współpraca z moderatorem głównym oraz ewaluatorem ćwiczeń CEP17-EBS.

7.2.7 Służby Public Relations

Służby Public Relations (dalej: PR) to koordynatorzy PR wyznaczeni w organizacjach uczestniczących w ćwiczeniach CEP17-EBS, do zapewnienia obsługi warstwy medialnej danej organizacji. Służby PR w realizacji swoich zadań korzystały z dostępu do systemu CISKOM, co zapewniało, że informacja o konsekwencjach zdarzeniach, które wystąpiły w trakcie ćwiczeń, będą docierały do nich niezależnie od informacji, które przekazywali im moderatorzy organizacyjni oraz ćwiczący w ich organizacjach. Dzięki temu, Służby PR w poszczególnych organizacjach mogły materializować swoje decyzje zarówno poprzez publikacje własne w systemie CISKOM, będące symulacją ich zachowań na zewnątrz organizacji, jak również przekazywać informacje o swoich decyzjach do innych uczestników ćwiczeń oraz własnych moderatorów organizacyjnych.

7.2.8 Zespoły CERT

Z założenia ćwiczeń CEP17-EBS, każda organizacja biorąca udział w ćwiczeniu posiada wyznaczony wewnątrz organizacji zespół CERT na potrzeby ćwiczeń. Rolę tę mogły odgrywać inne komórki organizacyjne, odpowiadające za bezpieczeństwo teleinformatyczne organizacji (w szczególności za reagowanie na incydenty), które nie są formalnie zespołami CERT.

7.2.9 Ćwiczący

Ćwiczącymi byli przedstawiciele wyznaczonych komórek organizacyjnych lub pracownicy poszczególnych organizacji tworzący zespoły CERT i PR, którzy zostali zaangażowani w realizację działań przewidzianych w scenariuszu CEP17-EBS.

7.2.10 Obserwatorzy

Obserwatorami byli przedstawiciele podmiotów związanych z cyberbezpieczeństwem i sektorem energetycznym, którzy obserwowali przebieg ćwiczeń:

- Agencja Bezpieczeństwa Wewnętrznego
- ENEA S.A.
- Ministerstwo Cyfryzacji
- Rządowe Centrum Bezpieczeństwa

7.2.11 Inne podmioty

Innymi podmiotami były organizacje niebiorące aktywnego udziału w ćwiczeniach, a które zdaniem danej organizacji lub organizatora, mogły wziąć udział w rozwiązaniu problemu zarysowanego w scenariuszu ćwiczeń. Komunikacja z tymi organizacjami była realizowana z udziałem moderatora głównego ćwiczeń, którego zadaniem było podgrywanie (symulowanie) działań takich podmiotów.

Podmiotami tymi były przykładowo:

- dostawca kluczowego rozwiązania, producent rozwiązania (tzw. vendor),
- CERT.GOV.PL – rządowy zespół reagowania na incydenty komputerowe,
- Policja
- szantażysta,
- inne zespoły wspierające działalność organizacji, np.: CERT-y komercyjne,
- organizacje i środowiska współdziałające w rozwiązywaniu incydentów teleinformatycznych.

7.3 Zarządzanie zdarzeniami i komunikacja w trakcie ćwiczeń

Ćwiczenia przebiegały zgodnie z wcześniej przygotowanym scenariuszem. Zaplanowane w scenariuszu zdarzenia wraz z rozwojem ćwiczeń były systematycznie uruchamiane przez koordynatora zarządzania zdarzeniami, z wykorzystaniem narzędzia EXITO.

Zdarzenia przewidziane w scenariuszu podzielone były na dwie grupy:

- zasadnicze – zdarzenia mające wywołać określoną reakcję ćwiczących,
- warunkowe – zdarzenia proceduralne uruchamiane w sytuacji, kiedy ćwiczący nie podejmowali sami akcji, które były przewidziane lub których uruchomienie zależało od reakcji uczestnika.

W trakcie ćwiczeń przewidziano, że uczestnicy będą wykorzystywać standardowe, na co dzień stosowane w ich organizacjach środki komunikacji.

7.3.1 Komunikacja pomiędzy moderatorem głównym a moderatorami organizacyjnymi

Komunikacja pomiędzy moderatorem głównym a moderatorami organizacyjnymi prowadzona była dla każdej z organizacji oddzielnie. Przybierała ona następujące formy:

Forma komunikacji	Kierunek komunikacji	Opis
Wprowadzenie (z ang. inject)	Moderator główny  Moderator organizacyjny	Podstawowa informacja dotycząca zdarzeń przewidzianych w scenariuszu. Stanowiła podstawę do dalszego postępowania moderatora organizacyjnego wobec innych uczestników ćwiczeń z organizacji, którą reprezentował. Dalszy sposób procedowania zdarzenia realizowany był metodami przyjętymi przez każdą z ćwiczących organizacji.
Konsultacja	Moderator główny  Moderator organizacyjny	Komunikacja mająca na celu rozwiewanie wątpliwości dotyczących przebiegu ćwiczeń i odpowiedzi na szczegółowe pytania dotyczące przebiegu ćwiczeń.
Komunikat	Moderator organizacyjny  Moderator główny	Przekazywany w sytuacji, kiedy moderator organizacyjny uzna, że konkretna informacja dotycząca przebiegu ćwiczeń w danej organizacji może mieć istotny wpływ na dalszy przebieg ćwiczeń, a jej przekazanie w postaci raportu może negatywnie wpłynąć na przebieg ćwiczeń, głównie ze względu na opóźnienie przekazania tej informacji.
Raport	Moderator organizacyjny  Moderator główny	Podstawowy sposób komunikacji pomiędzy moderatorem głównym i moderatorem organizacyjnym. Wzór raportu stanowił formularz dostępny w systemie EXITO.

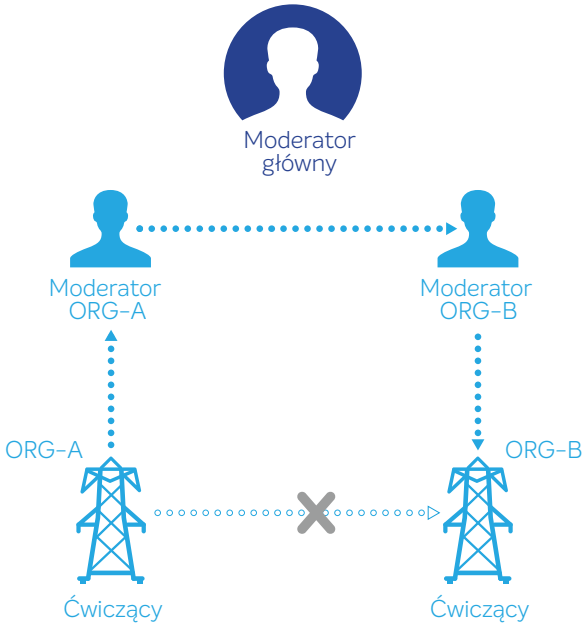
7.3.2 Komunikacja pomiędzy ćwiczącymi organizacjami

W trakcie ćwiczeń CEP17-EBS dopuszczalna była komunikacja pomiędzy organizacjami ćwiczącymi. Jednak ze względu na zróżnicowaną formę wykorzystywanych w poszczególnych przypadkach narzędzi komunikacji, założono możliwość takiej komunikacji tylko poprzez korzystanie z oficjalnych kont mailowych przygotowanych na potrzeby ćwiczenia.

Podczas ćwiczeń CEP17-EBS wyróżniało się dwa podstawowe rodzaje komunikacji pomiędzy organizacjami i jeden dotyczący kontaktów z „innymi podmiotami":

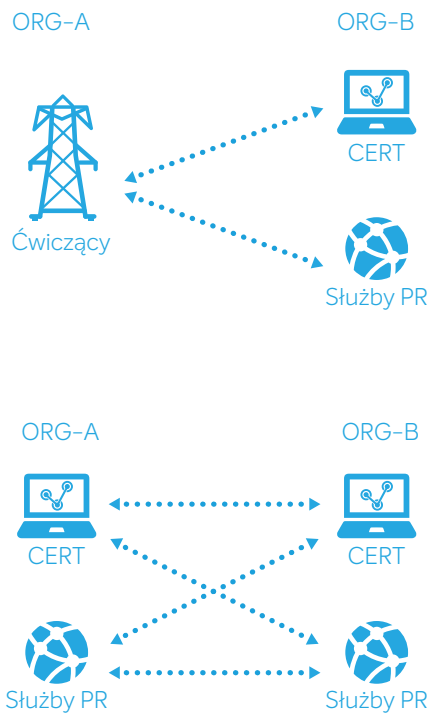
- Komunikacja za pośrednictwem moderatorów organizacyjnych. Ten model komunikacji dotyczył sytuacji, w której ćwiczący z organizacji A chciał skomunikować się z ćwiczącym z organizacji B. W tym celu ćwiczący z organizacji A przekazywał swoją wiadomość w postaci maila do moderatora organizacyjnego organizacji A. Informacja taka powinna zawierać dane dotyczące konkretnego adresata (organizacja, stanowisko lub podmiot wewnątrz struktury organizacyjnej) oraz treść wiadomości. Moderator organizacyjny organizacji A przekazywał otrzymaną informację moderatorowi organizacyjnemu organizacji B, który z kolei przekazywał ją adresatowi tj. ćwiczącemu w organizacji B.

Rysunek 3.
Komunikacja pomiędzy ćwiczącymi



- Komunikacja bez pośrednictwa moderatorów organizacyjnych. Ten model komunikacji dotyczył kontaktów pomiędzy ćwiczącymi z danej organizacji a zespołami CERT oraz Służbami PR z innej organizacji, a także komunikacji zespołów CERT i Służb PR pomiędzy sobą. Komunikacja taka przebiega bezpośrednio z wykorzystaniem dedykowanych kont pocztowych dla zespołów CERT i Służb PR w domenie cyberexepolska.pl i nie wymagała informowania moderatorów organizacyjnych.
- W trakcie ćwiczeń dopuszczono również komunikację pomiędzy organizacjami ćwiczącymi a innymi podmiotami zewnętrznymi, które nie były uczestnikami ćwiczeń. Komunikacja taka odbywała się z wykorzystaniem dedykowanych kont pocztowych w domenie cyberexepolska.pl. W sytuacji, kiedy ćwiczący z organizacji A chciał skomunikować się z podmiotem X, to informację tę przekazywał bezpośrednio do tego podmiotu, korzystając z oficjalnego konta z listy kontaktowej. Informacja ta powinna zawierać dane dotyczące konkretnego adresata (Nazwa podmiotu X, stanowisko lub podmiot wewnątrz struktury organizacyjnej), jeśli taka jest potrzeba, oraz treść komunikatu. Przykładowo, chcąc skontaktować się z Komendą Główną Policji, ćwiczący kontaktował się mailowo z wykorzystaniem swojego dedykowanego konta, na odgrywane w ćwiczeniach konto KGP w domenie cyberexepolska.pl.

Rysunek 4.
Zasady komunikacji pomiędzy organizacjami (komunikacja bez pośrednictwa moderatorów organizacyjnych.



7.3.3 System komunikacji w organizacji

Organizacje uczestniczące w ćwiczeniach CEP17-EBS wykorzystywały w ich trakcie standardowe i na co dzień stosowane w organizacjach środki komunikacji.

7.3.4 Kluczowe decyzje podejmowane w trakcie ćwiczeń

Organizatorzy w trakcie ćwiczeń monitorowali wystąpienie kilku ważnych zdarzeń, które w ich opinii mogły świadczyć o przebiegu ćwiczeń w poszczególnych organizacjach.

Monitorowano następujące zdarzenia:

- podjęcie działań minimalizujących skutki ataku DDoS,
- poinformowanie przez służby PR organizacji o wystąpieniu cyberataku,
- próbę nawiązania kontaktu z analitykiem, posiadającym informację o malware wymierzonym w sektor energetyczny,
- reakcję służb PR na operacje informacyjne w przestrzeni medialnej,
- reakcję organizacji na próbę phishingu,
- komunikację z vendorem, odpowiedzialnym za automatykę przemysłową,
- analizę próbki złośliwego oprogramowania,
- podjęcie negocjacji z szantażystą,
- zgłoszenie przypadku cyberataku do RCB,
- zgłoszenie przypadku cyberataku i szantażu na Policję.

7.4 Dokumentacja i monitoring przebiegu ćwiczeń

Podstawową formę dokumentacji i obserwacji przebiegu ćwiczeń stanowiły raporty sytuacyjne oraz monitoring kontaktów pomiędzy poszczególnymi podmiotami. Począwszy od godziny 9:00, wszyscy moderatorzy organizacyjni przekazywali swoje raporty sytuacyjne do moderatora głównego. Zawierały one między innymi:

- informację o wewnętrznych komórkach organizacyjnych, uczestniczących w reagowaniu na dane zdarzenie i dystrybucji informacji o zdarzeniu,
- informacje ogólne o podjętych działaniach,
- przewidywany rozwój wydarzeń,
- informację o wykorzystaniu zewnętrznych klas rozwiązań systemów teleinformatycznych,
- opis komunikacji na zewnątrz organizacji.

W przypadku wyboru modelu symulacji moderatorzy organizacyjni mieli zapewnioną kontrolę nad przebiegiem ćwiczeń, poprzez możliwość obserwacji całości korespondencji wymienianej pomiędzy uczestnikami. Ponadto, w związku z możliwością użycia w komunikacji wewnętrznej komunikacji telefonicznej, szczególne znaczenie miało informowanie moderatora organizacyjnego o jej wykorzystaniu. Rozmowa telefoniczna

pomiędzy uczestnikami ćwiczeń wewnątrz organizacji była udokumentowana poprzez wiadomość e-mail do moderatora organizacyjnego. W wiadomości uczestnik podawał następujące informacje:

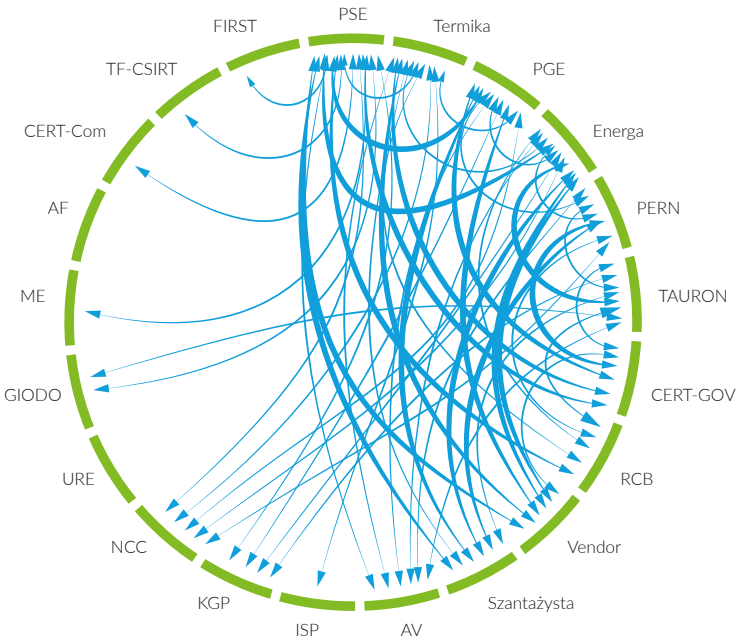
- Do kogo został wykonany telefon,
- W jakiej sprawie (np. przekazanie polecenia, informacja, pytanie, prośba o wsparcie) połączenie telefoniczne zostało wykonane.

Dodatkowo, dla zobrazowania przebiegu ćwiczeń, w trakcie jego trwania przygotowano wizualizację, na której były prezentowane w uproszczonej formie, raporty sytuacyjne, przekazywane moderatorowi głównemu ćwiczeń.

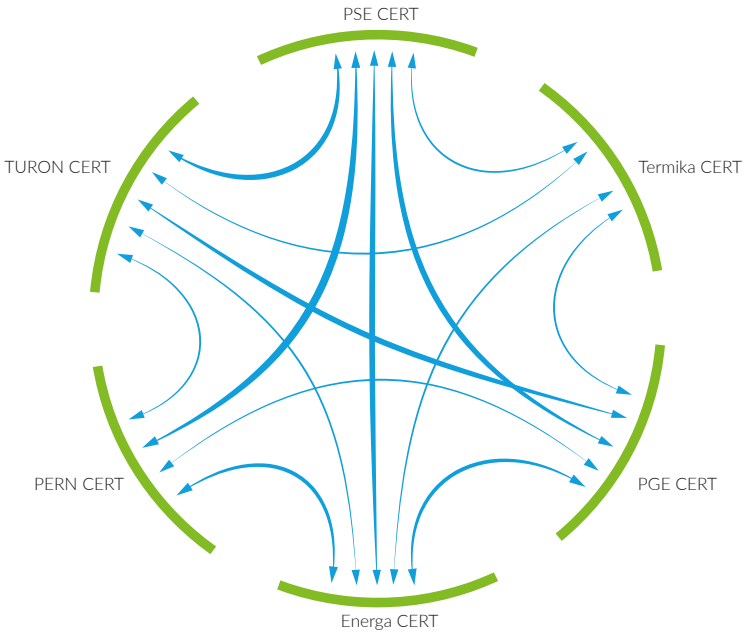
Komunikacja pomiędzy poszczególnymi podmiotami, a w szczególności ta pomiędzy ćwiczącymi a podmiotami administracji publicznej, mogła być obserwowana dzięki monitoringowi korespondencji pomiędzy moderatorami reprezentującymi poszczególne organizacje. Specjalny skrypt odnotowywał wszystkie fakty połączeń pomiędzy tymi podmiotami, co skutkowało pojawieniem się tej relacji na mapie wizualizacji połączeń.

Fot. 6: Screenshot zwiastuna wideo ćwiczeń Ćwiczenie Cyber-EXE™ Polska 2017 https://youtu.be/Mxq0w61im30

Rysunek 5.
Mapa relacji pomiędzy uczestnikami



Relacje pomiędzy podmiotami (skumulowane)



Relacje pomiędzy CERTami (skumulowane)

7.5 Przebieg ćwiczeń w warstwie komunikacji medialnej

Zdarzenia z warstwy komunikacji medialnej podczas ćwiczeń CEP17-EBS miały za zadanie sprawdzić przygotowanie działów PR oraz rzeczników prasowych organizacji ćwiczących na komunikację w sytuacji nietypowej lub takiej, która może doprowadzić do kryzysu. W trakcie ćwiczeń podgrywani dziennikarze komunikowali się z działami PR telefonicznie, za pomocą poczty e-mail, platformy imitującej komunikację w internecie: (strony www danych firm, media społecznościowe).

Organizacja ćwiczeń w warstwie komunikacji medialnej i włączenie do nich służb prasowych okazała się bardzo cenna. Prace grupy symulującej działania mediów urealniają sytuację ćwiczebną i wywierają presję, stymulując ćwiczących do działania.

Fot. 7: Zespół medialny ćwiczeń CEP17

8 Obserwacje, wnioski i rekomendacje

Na podstawie przeprowadzonej wśród organizacji ankiety ewaluacyjnej ćwiczeń, można zdecydowanie stwierdzić, że istnieje potrzeba przeprowadzania ćwiczeń sektorowych. Organizacje zgodnie uznały, że udział w ćwiczeniach CEP17-EBS wpłynie na procesy cyberbezpieczeństwa w firmie, a także doprowadzi do usprawnienia współpracy pomiędzy podmiotami z sektora energetycznego w zakresie cyberbezpieczeństwa.

Poniżej przedstawione zostały najistotniejsze obserwacje i rekomendacje wynikające z ćwiczeń CEP17-EBS, analizowane w dwóch warstwach, w zakresie obsługi incydentów:

- Komunikacji wewnętrznej, proceduralnej i technicznej,
- komunikacji medialnej, w tym w obszarze operacji informacyjnych.

8.1 Rekomendacje w zakresie warstwy komunikacyjnej, proceduralnej i technicznej

W odniesieniu do warstwy komunikacyjnej, proceduralnej i technicznej w zakresie obsługi incydentów, zaobserwowano m.in.:

- Pomiędzy niektórymi spółkami sektora są zawarte porozumienia, które bardzo usprawniają komunikację i współpracę w zakresie obsługi incydentów.
- Wszystkie organizacje w miarę sprawnie wykryły zagrożenie infekcji malware'em w sieci wewnętrznej.
- Część organizacji wykorzystała komunikację mobilną, podczas ataku DDoS na serwery pocztowe, aby zapewnić wewnętrzny przepływ informacji.
- Część organizacji skontaktowała się w Vendorem z prośbą o sprawdzenie laptopa technika, jak również aktualizacji sterownika przed jej wgraniem, a także zażądała natychmiastowego zaprzestania prac technika po oświadczeniu Vendora o infekcji komputera technika i potencjalnie także systemów biznesowych.

Na podstawie obserwacji przebiegu ćwiczeń CEP17-EBS, sformułowano następujące rekomendacje, w następujących obszarach:

- komunikacji i współpracy wewnątrz spółek sektora energetycznego,
- współpracy pomiędzy spółkami sektora,
- współpracy pomiędzy spółkami sektora a podmiotami zewnętrznymi.

8.1.1 Rekomendacje dotyczące współpracy wewnątrz spółek sektora energetycznego

Sformułowano następujące rekomendacje w odniesieniu do komunikacji i współpracy wewnątrz spółek w zakresie cyberbezpieczeństwa:

1. Ćwiczenia wskazały, że w przypadku niektórych spółek sektora konieczna jest dalsza rozbudowa ich struktur cyberbezpieczeństwa.

2. Ćwiczenia sektorowe powinny być przeprowadzane regularnie, żeby testować wdrożone zmiany oraz sprawdzać, czy cele postawione po ćwiczeniach, zostały osiągnięte.

3. Odpowiednio skonfigurowane i przetestowane techniczne kanały komunikacji wewnątrz organizacji mają zasadniczy wpływ na efektywność reakcji na zdarzenie. Zwiększenie liczby ćwiczeń próbnych, typu dry-run, podczas których organizacje mogą przetestować techniczne kanały komunikacji, komunikację alarmową, dostęp do poczty oraz poprawność konfiguracji swoich systemów (odnośnie obsługi injectów), może usprawnić przeprowadzenie ćwiczeń.

4. Ważne jest dopracowanie wewnętrznych procedur reakcji na incydenty od strony komunikacyjnej. Ustrukturyzowane sposoby komunikacji, szablony dotyczące alertów i powiadamiania, karty incydentów są niezbędne do efektywnej obsługi incydentów.

5. Ważne jest uzgodnienie i zapewnienie dodatkowych – alternatywnych kanałów wymiany informacji w organizacji na wypadek ataków DDoS na usługi internetowe i SMTP. Komunikacja mobilna może być ważnym elementem wsparcia komunikacji w przypadku sytuacji kryzysowej.

6. Organizacje powinny dopracować podejście do monitorowania informacji o nowych zagrożeniach, pojawiających się w mediach społecznościowych. Może być to robione niezależnie na poziomie każdej organizacji z osobna lub oddelegowane do jednej wybranej organizacji, której rolą byłoby wyszukiwanie informacji o zadanych typach zagrożeń. Dodatkowo dobrą praktyką dla działów technicznych jest korzystanie z forów wymiany informacji o zagrożeniach, np. FIRST, GEANT, Abuse Forum.

7. Istnieje potrzeba zweryfikowania wewnętrznych regulacji oraz podjęcie działań związanych z dopracowaniem procedur na wypadek wystąpienia próby wymuszenia okupu.

8. Dwustronny kontakt pomiędzy działem technicznym i działem PR jest konieczny w celu ustalenia postępowania w zakresie informowania o incydencie opinii publicznej i klientów. Ponadto, rola działów PR nie powinna ograniczać się tylko do obsługi kryzysów medialnych i komunikacji na zewnątrz. W przypadku niektórych incydentów bezpieczeństwa dział PR, poza ochroną marki i dbałością o wizerunek może przyczynić się do lepszej obsługi incydentów, jeszcze zanim kryzys medialny powstanie, przekazując napływające informacje z otoczenia oraz prowadząc działania medialne po uzyskaniu informacji, co do pożądanych kierunków i celów prowadzenia komunikacji.

9. Kontakt działów bezpieczeństwa z działem prawnym jest niezbędny w przypadku niektórych incydentów, w celu ustalenia, jakie konsekwencje prawne mogą wyniknąć np. w przypadku upublicznienia określonych danych oraz podejmowania przez firmę właściwych decyzji. Istotne jest uzgodnienie odpowiedzialności za komunikację z instytucjami zewnętrznymi (np. policja, prokuratura), gdzie niezbędna jest wiedza prawna i procesowa, której działy techniczne mogą posiadać.

10. Powinny zostać dopracowane regulacje, które pozwolą na skrócenie formalnej ścieżki decyzyjnej, w sytuacjach kryzysowych dotyczących cyberbezpieczeństwa.

11. W przypadkach, gdy aktualizacja oprogramowania sterowników wymaga obecności zewnętrznego technika, konieczne jest zadbanie o techniczne i fizyczne bezpieczeństwo wnoszonego do organizacji sprzętu.

12. Spółki sektora powinny organizować własne laboratoria badania automatyki przemysłowej.

13. Zaleca się nawiązanie bliższych relacji pomiędzy działami utrzymania sieci przesyłowej a działami bezpieczeństwa IT, w celu uruchomienia wspólnych środków w trybie kryzysowym.

8.1.2 Rekomendacje dotyczące współpracy w ramach polskiego sektora energetycznego

Do najważniejszych rekomendacji, wynikających z przeprowadzonych ćwiczeń CEP17-EBS, należy zaliczyć przede wszystkim **postulaty współpracy pomiędzy spółkami sektora energetycznego w zakresie cyberbezpieczeństwa**. W tym zakresie sformułowano następujące rekomendacje:

1. Utworzenie formalnej grupy, zrzeszającej polskie spółki sektora energetycznego.

Wspólna platforma organizacyjna mogłaby usprawnić współpracę w zakresie cyberbezpieczeństwa w sektorze, a także reprezentować sektor na zewnątrz, w kontaktach z administracją rządową oraz vendorami. Członkostwo w takiej organizacji byłoby dobrowolne, ale wiązałoby się ze spełnieniem szeregu formalnych wymagań przede wszystkim dotyczących dojrzałości zespołów zajmujących się obsługą incydentów bezpieczeństwa. W ramach takiej grupy, istotne byłoby podjęcie w szczególności następujących działań:

- Organizowanie regularnych spotkań przedstawicieli zespołów reagujących i działów bezpieczeństwa IT poszczególnych spółek. Spotkania miałyby na celu:
  - nawiązanie bezpośrednich kontaktów i relacji pomiędzy osobami odpowiedzialnymi za cyberbezpieczeństwo,
  - dzielenie się informacjami dotyczącymi między innymi;
    - występujących problemów bezpieczeństwa w obszarze ICT i ICS,
    - opinii o wykonawcach i produktach bezpieczeństwa,
    - szkoleń i certyfikacji,
    - oceny vendorów i integratorów,
    - audytów bezpieczeństwa.

  - omawianie „planu rozwoju i współpracy sektora energetycznego w zakresie cyberbezpieczeństwa",
  - podejmowanie wspólnych działań, żeby zacieśnić i usprawnić współpracę wewnątrz sektora.
- Usprawnienie relacji z vendorami. Wspólne działanie wszystkich spółek mogłoby poprawić relacje z vendorami, w zakresie komunikowania, lobbowania za określonymi rozwiązaniami bezpieczeństwa oraz współpracy z nimi w tym obszarze.

2. Utworzenie technicznej platformy wymiany informacji (Forum Bezpieczeństwa) dla podmiotów z sektora energetycznego.

Ćwiczenia pokazały, że istnieje potrzeba uregulowania w sektorze energetycznym, komunikacji dotyczącej incydentów, wypracowania wspólnych dla sektora standardów komunikacji, systemu powiadamiania oraz sposobów dzielenia się wiedzą nt. zagrożeń cyberbezpieczeństwa.

- Organizacje powinny uzgodnić bezpieczny kanał wymiany informacji o zagrożeniach oraz uzgodnić sposób publikowania i rodzaje publikowanych w nim informacji. Informacje przekazywane takim kanałem powinny podlegać wcześniejszej pobieżnej weryfikacji oraz mieć przypisane stosowne poziomy istotności.
- W ramach sektora, powinien powstać uregulowany system wymiany informacji dotyczącej obsługi incydentów, w oparciu o wspólny dla sektora katalog incydentów. Znormalizowane podejście do klasyfikacji incydentów może być wprawdzie utrudnione z uwagi na różną specyfikę organizacji, np. wynikającą z różnych rodzajów klientów i sposobu komunikacji z nimi. Dlatego, szablon incydentu powinien zawierać „część wspólną", która umożliwi statystyczne raportowanie, dające obraz występowania zagrożeń w sektorze.
- Sektor potrzebuje usprawnień w zakresie komunikacji w obszarze cyberbezpieczeństwa, zwłaszcza do przekazywania informacji w trybie kryzysowym. Warto rozważyć uzupełnienie środków technicznych wymiany informacji o bezpieczny kanał komunikacji typu chat oraz dodanie do wewnętrznych procedur organizacji usługi telefonicznej, działającej 24h/dobę; numer telefoniczny, do którego mogłyby mieć dostęp wszystkie organizacje.
- Sektor potrzebuje wspólnej „zamkniętej" platformy wymiany informacji o zagrożeniach typu MISP[3] (ang. Malware Information Sharing Platform & Threat Sharing). W ramach platformy mogłyby być wymieniane wskaźniki kompromitacji (tzw. IoC – Indicators of Compromise).

3 https://www.misp-project.org

3. **Opracowanie formalnego dokumentu, regulującego współpracę w ramach sektora energetycznego w zakresie cyberbezpieczeństwa.**

Uregulowanie współpracy i polityki wymiany informacji w zakresie cyberbezpieczeństwa w sektorze powinno być zrealizowane w oparciu o formalne porozumienia i umowy bilateralne. Taki formalny dokument powinien obejmować regulacje dotyczące m.in.

- wymiany informacji,
- wymiany doświadczenia operacyjnego,
- wsparcia procesu wykrywania i reagowania na incydenty,
- zasilania wiedzą/wskaźnikami systemów bezpieczeństwa.

8.1.3 Rekomendacje dotyczące współpracy polskiego sektora energetycznego z podmiotami zewnętrznymi

W zakresie współpracy zewnętrznej sektora, sformułowano następujące rekomendacje:

1. **Zapewnienie dwustronnej wymiany informacji w zakresie incydentów cyberbezpieczeństwa pomiędzy spółkami sektora a podmiotami administracji rządowej[4].**

W celu usprawnienia wymiany informacji na temat incydentów z podmiotami administracji rządowej, zaleca się zawarcie specjalnych porozumień pomiędzy spółkami a odpowiednimi podmiotami, takimi jak: Rządowe Centrum Bezpieczeństwa, Agencja Bezpieczeństwa Wewnętrznego czy działające w ramach NASK – Narodowe Centrum Cyberbezpieczeństwa. Ważne jest ustalenie sposobu relacji z ww. podmiotami, które będą miały praktyczne konsekwencje w realnej komunikacji i wymianie informacji i zakresie pomocy i wsparcia, jakie sektor energetyczny uzyska od tych organizacji.

2. **Sektor potrzebuje sprecyzowanych ustaleń co do sposobu raportowania incydentów do podmiotów administracji rządowej.**

W tym zakresie konieczne jest doprecyzowanie pełnionych funkcji podmiotów administracji publicznej w zakresie zgłaszania incydentów dotyczących np. sytuacji wymuszania okupu przez szantażystę. Nie powinno to jednak spoczywać wyłącznie na firmach, a odbyć się przy pełnej współpracy z odpowiednimi instytucjami państwowymi, które powinny dać odpowiednie wytyczne podmiotom z sektora infrastruktury krytycznej. Sektor oczekuje, że wymiana informacji będzie dwustronna.

4 Ćwiczenie CEP17-BSE nie uwzględniało aktywnej roli podmiotów administracji rządowej. Relacje z ćwiczącymi ze strony tych podmiotów były w większości podgrywane, uwzględniając doświadczenia ćwiczących z tego typu relacji.

8.2 Obserwacje, wnioski i rekomendacje dotyczące warstwy komunikacji medialnej

1. Biura prasowe organizacji reagowały na kontakt telefoniczny ze strony dziennikarzy. W przypadku braku możliwości odebrania połączenia oddzwaniały.

2. Pozytywnie należy ocenić fakt, że część organizacji ćwiczących w wydanych komunikatach zawarło przeprosiny „za utrudnienia i obniżenie jakości usług".

3. Służby PR trzech organizacji przy komunikacie w CISCOM lub kontakcie telefonicznym z dziennikarzami powtarzały zapewnienie, że przeprowadzona analiza zaistniałej sytuacji nie wykazała żadnego zagrożenia dla bezpieczeństwa danych klientów oraz funkcjonowania systemów teleinformatycznych.

4. Przedstawiciele wszystkich firm reagowali na kontakt za pośrednictwem poczty e-mail. Zawsze, choć nie od razu, odpisywali na zadawane przez dziennikarzy pytania. Każda z ćwiczących firm wspomniała o tym, że weryfikują problem i odpowiedzą w najbliższym czasie.

5. Zespoły prasowe mają wypracowane standardy komunikacji z dziennikarzami. Zostały one zachowane także podczas krytycznych etapów w odgrywanym scenariuszu.

Rekomendacje:

1. Ze względu na duże ryzyko naruszeń, biura prasowe powinny mieć opracowane dedykowane procedury postępowania w odniesieniu do komunikacji kryzysowej związanej z cyberbezpieczeństwem. Tego typu procedury mogą być oparte na kilku najczęściej występujących scenariuszach ataków, np. blokady usług, włamania do systemu, kradzieży danych.

2. W celu skrócenia czasu przygotowania odpowiedzi dla dziennikarza, warto skorzystać z wcześniej opracowanych „głównych przekazów" (ang. key messages) dotyczących naruszeń bezpieczeństwa. Przebieg większości ataków jest podobny, a zatem tego typu dokumenty są przydatne w pierwszej fazie zbierania materiału i opracowania komunikatu.

3. Niezależnie od przyjętej struktury działu komunikacji w danej firmie, niezbędna jest stała współpraca i wymiana informacji pomiędzy biurem prasowym, a specjalistami ds. mediów społecznościowych. Ci ostatni, w sytuacji krytycznej, powinni być włączeni w działania sztabu kryzysowego PR i być w komunikacji z zespołem CERT.

4. Należy rozważyć zastąpienie pasywnej komunikacji zewnętrznej aktywnymi działaniami. Jeśli dany problem występuje w organizacji, istnieje małe prawdopodobieństwo, że nie zostanie upubliczniony, nawet jeśli w tym samym czasie dotyczy on całego sektora. Jest to także dobry moment na uruchomienie współpracy z mediami na zasadach komercyjnych, zazwyczaj jednak współpraca ta bazuje na wcześniejszych ustaleniach i stosownych umowach.

5. Nawet jeśli podawanie nieprawdziwych przyczyn problemów było zamierzonym działaniem i stanowiło element przyjętej strategii komunikacyjnej, jest to niezgodne z najlepszymi standardami informowania o naruszeniach bezpieczeństwa, które rządzą się prostą regułą: „informuj rzetelnie, ale bez szczegółów".

6. W celu uniknięcia negatywnego oddziaływania szumu informacyjnego, niezbędna jest budowa kompetencji biur prasowych i rzeczników w zakresie operacji Info Ops. Na wypadek kryzysu warto rozważyć zaangażowanie usług specjalistów od informacji operacyjnych.

7. Media społecznościowe powinny być kluczowym elementem procesu komunikacji w organizacji. W organizacjach należy przeanalizować możliwość stworzenia nawet jednoosobowego stanowiska ds. obsługi mediów społecznościowych.

8. Spójność komunikacji jest najważniejsza w sytuacjach kryzysowych. Wypracowane główne przekazy zawsze powinny być wyznacznikiem w kontakcie z mediami, również z uwzględnieniem mediów społecznościowych.

8.3 Obserwacje, wnioski i rekomendacje dotyczące warstwy Info Ops

Po raz pierwszy w ćwiczeniach z cyklu CYBER-EXE™ Polska w warstwie komunikacji medialnej w mediach społecznościowych przeprowadzone były ćwiczenia z obszaru Info Ops (tj. operacji informacyjnych).

Komunikacja prowadzona w medium społecznościowym „Dwitter" była zaplanowanym działaniem informacyjnym, którego przebieg odnosił się do przebiegu scenariusza technicznego i następował w korelacji z elementami obsługi incydentów realizowanej przez zespoły CERT oraz bieżących wydarzeń, w tym działań komunikacyjnych podejmowanych przez zespoły PR biorące udział w ćwiczeniu.

Podstawowym założeniem operatora prowadzącego ćwiczenie było prowadzenie działań dezawuujących wizerunek podmiotów biorących udział w ćwiczeniu, wprowadzenie w błąd „odbiorców" wpisów, w tym posługiwanie się wykorzystaniu komunikatów publikowanych w związku z obsługiwanym incydentem komputerowym oraz odseparowaniem użytkowników medium społecznościowego od kanałów komunikacji spółek. Kampania zawierała również element dezinformacji polegający na stworzeniu odbiorcom warunków do podjęcia decyzji o niekorzystaniu z oficjalnych kont i stron www uczestników ćwiczeń w celu odseparowania ruchu „naturalnego" od dostępu do wiarygodnego obiektu informacyjnego (oficjalna strona podmiotu, kanału komunikacji w mediach społecznościowych).

Rekomendacje:

1. Zaleca się budowę procesu rozpoznania środowiskowa informacyjnego kształtowanego w mediach społecznościowych w celu identyfikacji i analizy zachodzących zjawisk.

2. Rekomenduje się opracowanie metodyki rozpoznania potrzeb informacyjnych jako jedno z kryteriów planowania własnych działań komunikacyjnych oraz stałego dostosowywania do treści komunikatów do bieżącej analizy środowiska informacyjnego.

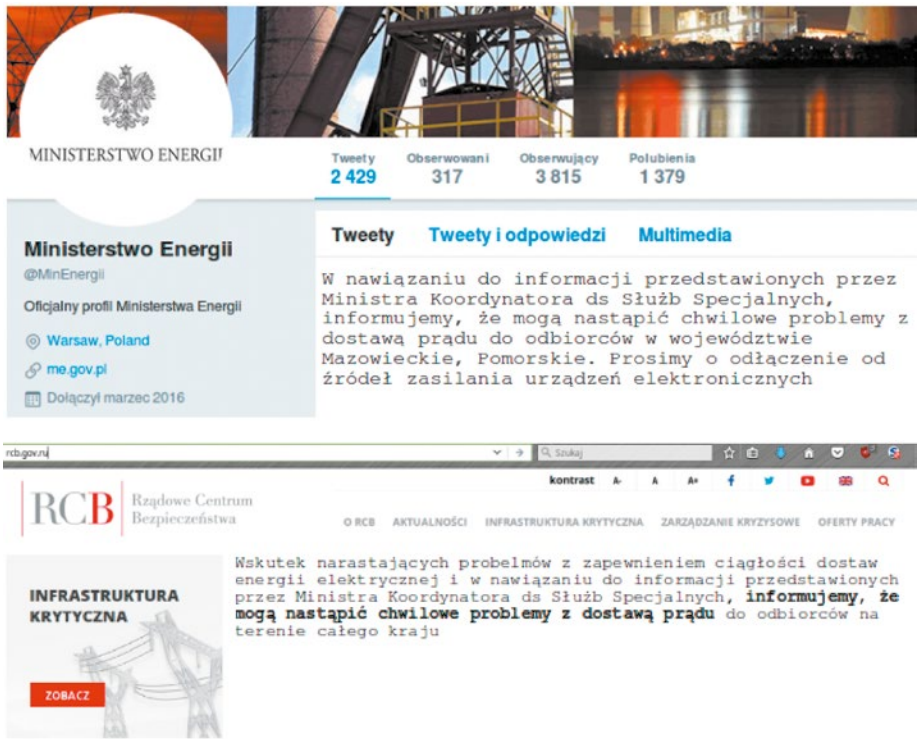
3. Zaleca się opracowanie procesu rozpoznania pochodzenia materiału informacyjnego oraz weryfikacji jego wiarygodności.

4. Podniesienie zdolności ochrony własnych kanałów komunikacji przed efektami dezinformacji.

5. Wypracowanie procesu ochrony środowiska informacyjnego, z uwzględnieniem działań aktywnych w celu uniknięcia uzyskania przez podmiot obcy, atakujący supremacji informacyjnej.

6. Opracowanie i wdrożenie metodyki rozpoznania operacji informacyjnej, szumu informacyjnego, celu i oczekiwanego efektu procesu manipulacji wizerunkiem przedsiębiorstw.

Rysunek 6.
Przykładowe screenshoty komunikatów „fake news" warstwy medialnej



9 Podziękowania

Ćwiczenia CYBER-EXE™ Polska 2017 Energy Black Shield nie mogłyby się odbyć bez dobrej woli i wyjątkowego zaangażowania wszystkich uczestniczących w nim podmiotów, a zwłaszcza osób, które brały aktywny udział w jego organizacji i przeprowadzeniu. Fundacja Bezpieczna Cyberprzestrzeń, jako organizator ćwiczeń, dziękuje im wszystkim za odwagę w realizacji tego przedsięwzięcia, za wielkie zaangażowanie zarówno podczas kilkumiesięcznych przygotowań oraz samego dnia ćwiczeń, a także pracy włożonej w ocenę przedsięwzięcia i ostatecznie przygotowanie wniosków i rekomendacji.

Dziękujemy współorganizatorom z Polskich Sieci Elektroenergetycznych za wszelkiego rodzaju wsparcie logistyczne przy organizacji ćwiczeń oraz aktywny udział w jego przygotowaniu i przeprowadzeniu. Merytoryczne i organizacyjne doświadczenia obydwu współorganizatorów były wielkim wkładem w końcowy sukces przedsięwzięcia.

Pragniemy podziękować za patronat, obserwacje ćwiczeń i wsparcie techniczne Rządowemu Centrum Bezpieczeństwa, oraz pozostałym obserwatorom ćwiczeń z Ministerstwa Cyfryzacji, Agencji Bezpieczeństwa Wewnętrznego i ENEA S.A.

Dziękujemy także wszystkim uczestnikom, czyli firmom działającym w sektorze energetycznym, które zdecydowały się na udział w ćwiczeniu. Podjęcie wyzwania, współdziałanie i otwartość reprezentantów tych organizacji pozwoliła na przygotowanie i przeprowadzenie niebanalnego scenariusza, sprawnych ćwiczeń i wyciągnięcie z nich pożytecznych wniosków.

FUNDACJA
bezpieczna
cyberprzestrzeń

FUNDACJA BEZPIECZNA CYBERPRZESTRZEŃ
Pozarządowa organizacja non-profit, której celem, jest działanie na rzecz bezpieczeństwa cyberprzestrzeni, w tym na rzecz poprawy bezpieczeństwa w sieci Internet. Osiągnięcie tych celów fundacja realizuje poprzez działalność w trzech głównych obszarach: UŚWIADAMIANIA o zagrożeniach teleinformatycznych, REAGOWANIA na przypadki naruszania bezpieczeństwa w cyberprzestrzeni, prowadzenia DZIAŁALNOŚCI BADAWCZO-ROZWOJOWEJ w dziedzinie bezpieczeństwa teleinformatycznego.

FUNDACJA BEZPIECZNA CYBERPRZESTRZEŃ
ul. Solec 22, 00-410 Warszawa
tel: +48 22 112 0 800
e-mail: kontakt@cybsecurity.org

www. cybsecurity.org

www.cyberexepolska.pl