CYBER-EXE POLSKA 2012

RAPORT

CYBER-EXE POLSKA 2012

ĆWICZENIA
Z OCHRONY
W CYBERPRZESTRZENI
PRZYGOTOWANIE
PRZEBIEG
ANALIZA
WNIOSKI
I REKOMENDACJE
RAPORT

Spis Treści

Bakcyl dżumy nigdy nie umiera i nie znika (...) nadejdzie być może dzień, kiedy na nieszczęście ludzi i dla ich nauki dżuma obudzi swe szczury i pośle je, by umierały w szczęśliwym mieście.

Albert Camus

1 Wstęp

Organizacja ćwiczeń, które mają podnosić zdolność organizacji i struktur państwowych do skutecznej ochrony przed atakiem z cyberprzestrzeni jest jednym z wyraźnych trendów w dziedzinie działań na rzecz poprawy bezpieczeństwa w cyberprzestrzeni. Organizatorzy ćwiczenia Cyber-EXE Polska 2012 zdecydowali się w aktywny sposób włączyć się w ten nurt. Bezpośrednią zachętą i inspiracją do podjęcia się tego przedsięwzięcia były rekomendacje Europejskiej Agencji Bezpieczeństwa Sieci i Informacji (ENISA), które zostały przygotowane po przeprowadzeniu ćwiczeń Cyber Europe 2010[1]. Wśród 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 do rozpoczęcia pracy nad organizacją Cyber-EXE Polska 2012 był udział przedstawiciela Fundacji Bezpieczna Cyberprzestrzeń w spotkaniu przygotowanym przez Organisation of American States (w listopadzie 2011 r.), na którym przedstawiane były doświadczenia z podobnych ćwiczeń w Stanach Zjednoczonych, Kanadzie, Europie i krajach Ameryki Południowej. Praktyczna wiedza nabyta w trakcie spotkania była pomocna zarówno w fazie przygotowania jak i przeprowadzenia ćwiczeń.

Bezpośrednią decyzję o organizacji ćwiczenia Cyber-EXE Polska 2012 podjęto w gronie podmiotów: Computerworld Magazyn Menedżerów i Informatyków, Fundacja „Instytut Mikromakro", Fundacja Bezpieczna Cyberprzestrzeń. Zdecydowano, że ćwiczenia odbędą się przy okazji IX Konferencji Wolność i Bezpieczeństwo.

2 Ćwiczenie

2.1 Idea ćwiczeń ochrony w cyberprzestrzeni

Ćwiczenia ochrony w cyberprzestrzeni są jedną z najskuteczniejszych form przygotowania organizacji do reagowania 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 wszystkich szczebli. Ponadto stwarzają warunki do trafnego wyboru skutecznych form i metod działania w różnorodnych sytuacjach, głównie przy podejmowaniu i realizacji określonych decyzji oraz kierowaniu podległymi ogniwami.

[1] *„Cyber Europe 2010 – Evaluation Report" - http://www.enisa.europa.eu/activities/Resilience-and-CIIP/cyber-crisis-cooperation/cyber-europe/ce2010/ce2010report*

Ćwiczenia mają na celu:

- praktyczne sprawdzenie poprawności działania systemu ochrony organizacji przed zagrożeniami;
- identyfikację słabości procedur i zachowań osób w sytuacjach kryzysowych oraz odkrycie nowych metod działania;
- przygotowanie osób, którym powierzono wykonywanie zadań w ramach ochrony organizacji przed zagrożeniami, do prawidłowego działania w sytuacji wystąpienia zagrożenia z cyberprzestrzeni;
- kształtowanie umiejętności współdziałania komórek organizacyjnych wewnątrz organizacji, a także między odpowiednimi służbami, instytucjami i organami administracji państwowej;
- kształtowanie u osób biorących udział w ćwiczeniach świadomości na temat zagrożeń z cyberprzestrzeni i adekwatnych sposobów reagowania.

Ćwiczenia z zakresu ochrony organizacji przed zagrożeniami mogą przyjąć formę:

- testów gotowości (sprawdzenie czasu reakcji);
- testów standardowych procedur operacyjnych (np. procedur wymiany informacji);
- ćwiczeń sztabowych (table-top);
- ćwiczeń praktycznych;
- gier decyzyjnych.

2.2 Cele ćwiczenia Cyber-EXE Polska 2012

CYBER-EXE Polska 2012 było pierwszym tego typu ćwiczeniem w Polsce i miało pionierski charakter. Oto jego trzy priorytetowe cele:

I Sprawdzić zdolność do reakcji na atak pochodzący z cyberprzestrzeni, w tym powstrzymania tego ataku oraz minimalizacji jego skutków.

II Sprawdzić skuteczność informowania właściwych organów o ataku (identyfikacja właściwych organów, kanały łączności, jakość informacji).

III Sprawdzić zdolność do współpracy pomiędzy właściwymi organami administracji publicznej oraz innymi podmiotami uczestniczącymi w ćwiczeniach, w tym podmiotami sektora prywatnego.

Dodatkowymi celami było zbadanie zdolności do organizacji ćwiczeń w ramach współpracy publiczno--prywatnej oraz budowa zaufania między jego uczestnikami, jak również wypracowanie dobrych praktyk w zakresie technicznych aspektów organizacji cwiczeń.

3 Uczestnicy ćwiczenia Cyber-EXE Polska 2012

W ćwiczenie Cyber-EXE Polska 2012 zaangażowanych było 13 instytucji i około 80 osób (14 osób w Centrum Kontroli Ćwiczenia oraz około 65 osób w lokalizacjach należących do ćwiczących). Instytucje biorące udział w Cyber-EXE Polska 2012 odegrały różne role: ćwiczących, oceniających, obserwatorów, wspierających organizację i przeprowadzenie ćwiczenia.

Instytucje uczestniczące w ćwiczeniach (w kolejności alfabetycznej):

- Computerworld - Magazyn Menedżerów i Informatyków
- Fundacja Bezpieczna Cyberprzestrzeń
- Fundacja „Instytut Mikromakro"
- Operator Gazociągów Przesyłowych GAZ-SYSTEM SA
- Komenda Główna Policji
- Ministerstwo Obrony Narodowej – Resortowe Centrum Zarządzania Bezpieczeństwem Sieci i Usług
- Orange Polska – TP CERT Orange
- Politechnika Wrocławska
- Polskie Sieci Elektroenergetyczne Operator SA
- RWE Polska SA
- Rządowe Centrum Bezpieczeństwa
- Wojskowa Akademia Techniczna – Wydział Cybernetyki

4 Przygotowanie i przeprowadzenie ćwiczenia

Do organizacji ćwiczenia wykorzystana została metodyka zaproponowana przez ENISA w dokumencie metodycznym na temat organizacji ćwiczeń[2]. Metodyka zakłada organizację w ramach czterech głównych faz:

- Identyfikacji

W tej fazie zostały ustalone podstawowe cele ćwiczenia i lista jego uczestników. Wystosowano zaproszenia do udziału w ćwiczeniu do wszystkich istotnych podmiotów administracji publicznej, które zdaniem organizatorów powinny w nich partycypować. Uczestnicy ćwiczenia wywodzący się z sektora prywatnego przystąpili do niego w związku ze swoim bezpośrednim zainteresowaniem i rozmowami z organizatorami na temat zakresu ich uczestnictwa. Faza ta obejmowała również określenie przybliżonego obszaru tematycznego ćwiczenia.

- Planowania

W trakcie fazy planowania określono obszar tematyczny ćwiczenia, który następnie został opisany szczegółowo w postaci scenariusza. Praca nad nim toczyła się równolegle w dwóch sektorowych ścieżkach, w których przewidywany był rozwój sytuacji: w sektorze przesyłu energii elektrycznej oraz w sektorze przesyłu gazu. W tej fazie określono również szczegółowo listę uczestników w postaci komórek organizacyjnych i stanowisk, które brały udział w ćwiczeniu. Ważnym elementem fazy planowania było ustalenie organizacyjnych i technicznych zasad jego przeprowadzenia, w tym przydzielenie ról związanych z zarządzaniem ćwiczeniem oraz opracowaniem instrukcji. Ta część przygotowań uwzględniała również sposób prezentacji dla uczestników konferencji ,,Wolność i Bezpieczeństwo", podczas której przeprowadzono Cyber-EXE Polska 2012.

- Przeprowadzenia

W tej fazie przeprowadzono zasadnicze ćwiczenie. Zostało ono poprzedzone jednodniowym treningiem w przeddzień ćwiczenia, podczas którego dokonano próby generalnej (tzw. dry run). Przed rozpoczęciem ćwiczenia przekazano uczestnikom również szczegółowe instrukcje postępowania pozwalające na sprawne technicznie działania.

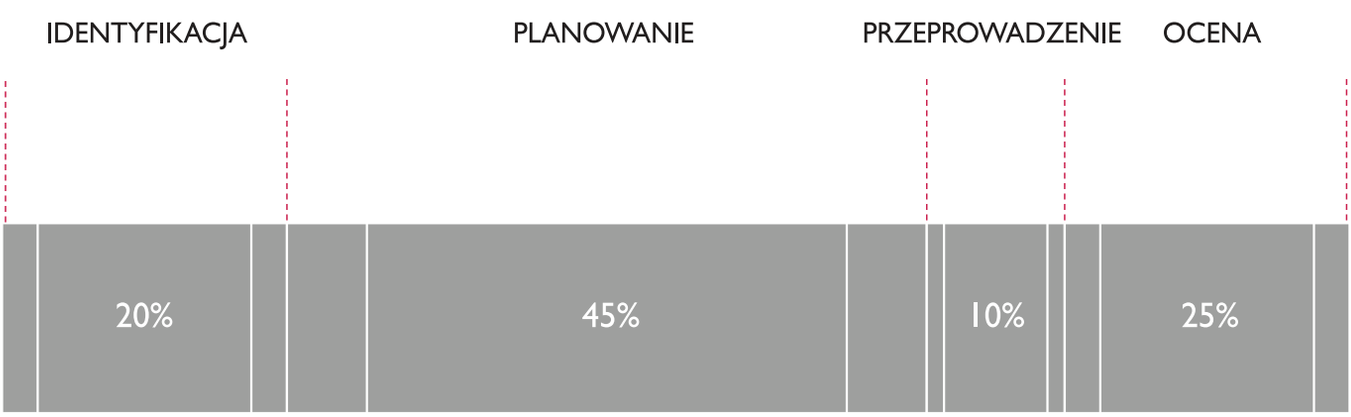
[2] *„Good Practice Guide on National Exercises – Enhencing the Resillience of Public Communications Networks" - http://www.enisa.europa.eu/activities/Resilience-and-CIIP/cyber-crisis-cooperation/exercises/national-exercise-good-practice-guide*

- Oceny

W trakcie tej fazy dokonano podsumowania ćwiczenia i przygotowano końcowy raport. Istotnym elementem pracy było przygotowanie wniosków i wynikających z nich rekomendacji. Raport końcowy został przygotowany przez wszystkich uczestników, którzy mieli prawo zgłaszać swoje oceny i zatwierdzać całość dokumentacji końcowej.

4.1 Modelowy harmonogram organizacji ćwiczeń

Opierając się na doświadczeniach Cyber-EXE Polska 2012, można przedstawić modelowy harmonogram organizacji ćwiczeń. Harmonogram powinien zawierać wszystkie wymienione w rozdziale 4 fazy oraz uwzględniać kluczowe punkty kończące każdą z nich. Czas organizacji ćwiczenia powinno się powiększyć o przyjętą długość fazy przeprowadzenia. Na fazę identyfikacji powinno się przeznaczyć około 20% czasu zaplanowanego na organizację ćwiczenia i zakończyć ją z chwilą ostatecznego ustalenia listy uczestników.
Faza planowania powinna wynosić około 45% czasu przeznaczonego na organizację ćwiczenia i zakończyć się przyjęciem ostatecznej wersji scenariusza.
Faza przeprowadzenia zależna jest od przyjętego czasu trwania ćwiczenia. Kończy się wraz z zakończeniem ćwiczenia. Powinno się na tę fazę przeznaczyć około 10% czasu. Faza oceny powinna wynosić około 25% czasu przeznaczonego na ćwiczenie. Kończy się ona, podobnie jak cała organizacja ćwiczeń, opracowaniem ostatecznej wersji raportu końcowego.
Przyjęty przez organizatorów harmonogram powinien cechować się również elastycznością,
dlatego podane przykładowe proporcje mogą odbiegać od propozycji o około 10 – 20% czasu ich trwania.



Rysunek 1 Propozycja modelowego harmonogramu organizacji ćwiczeń.

4.2 Zespół projektowy

Dla realizacji ćwiczenia zgodnie z przedstawioną metodyką powołano zespół projektowy składający się z przedstawicieli organizatorów i uczestników ćwiczenia. Zespół ten pracował od marca do listopada 2012 r., organizując w tym czasie kilkanaście spotkań o różnym charakterze w tym:

- wspólne spotkania zespołu projektowego,
- pojedyncze spotkania przedstawicieli zespołu projektowego z uczestnikami ćwiczenia po stronie organizacji biorących udział w ćwiczeniach,
- szkolenie w zakresie metodyki organizacji ćwiczeń przeprowadzone przez ENISA.

Dodatkowo w celu sprawniejszej realizacji przygotowań do ćwiczenia zespół projektowy podzielony został na podzespoły odpowiedzialne za poszczególne elementy ćwiczenia, takie jak:

- opracowanie scenariusza,
- przygotowanie środowiska testowego,
- atak na przygotowane środowisko testowe,
- szkolenia,
- infrastrukturę ćwiczenia,
- wizualizację.

4.3 Rola poszczególnych organizacji

Poniżej przedstawiona jest rola poszczególnych organizacji (wymienionych w kolejności alfabetycznej) w ćwiczeniu. Wskazane zostały najważniejsze zadania i odpowiedzialności tych organizacji, jak również ich udział w poszczególnych fazach organizacji ćwiczenia.

Computerworld Magazyn Menedżerów i Informatyków – inicjator i jeden ze współorganizatorów Cyber-EXE Polska 2012. Przedstawiciele Computerworld uczestniczyli we wszystkich fazach organizacji ćwiczenia. Szczególną rolę odegrał w fazie inicjacji oraz zaplecza organizacyjnego i medialnego. Computerworld odpowiedzialny był również za przygotowanie materiału wizualizacyjnego ćwiczenia, który był prezentowany uczestnikom konferencji „Wolność i Bezpieczeństwo".

Fundacja Bezpieczna Cyberprzestrzeń – inicjator i jeden ze współorganizatorów Cyber-EXE Polska 2012. Przedstawiciel FBC uczestniczył we wszystkich fazach organizacji ćwiczenia. Przedstawiciel fundacji odegrał kluczową rolę, podejmując się zadania koordynacji organizacji ćwiczenia oraz funkcji głównego moderatora.

Fundacja Instytut Mikromakro – inicjator i jeden ze współorganizatorów Cyber-EXE Polska 2012. Przedstawiciel IMM uczestniczył we wszystkich fazach organizacji ćwiczenia. Szczególną rolę odegrał w fazie inicjacji oraz zabezpieczenia logistycznego.

Operator Gazociągów Przesyłowych Gaz-System SA – jeden z dwóch głównych aktywnie ćwiczących. Przedstawiciele Gaz-System SA uczestniczyli w wszystkich fazach organizacji Cyber-EXE Polska 2012. Szczególną rolę odegrali w fazie planowania, budując scenariusz dla sektorowej ścieżki rozwoju sytuacji oraz w fazie przeprowadzenia ćwiczenia. Na potrzeby przeprowadzenia kontrolowanego ataku z cyberprzestrzeni Gaz-System SA zbudował środowisko testowe (patrz rozdz. 5.4 Środowisko testowe).

Komenda Główna Policji – aktywnie ćwiczący. Przedstawiciele KGP uczestniczyli we wszystkich fazach organizacji Cyber-EXE Polska 2012. Szczególny wkład wnieśli w fazę planowania, budując część scenariusza dotyczącą działania i współpracy służb odpowiedzialnych za bezpieczeństwo państwa.

Ministerstwo Obrony Narodowej – Resortowe Centrum Zarządzania Bezpieczeństwem Sieci i Usług – aktywnie ćwiczący. Przedstawiciele MON uczestniczyli we wszystkich fazach organizacji Cyber-EXE Polska 2012. Szczególny wkład wnieśli w fazę planowania budując część scenariusza dotyczącą działania i współpracy służb odpowiedzialnych za bezpieczeństwo państwa. Dodatkowo, opierając się na doświadczeniach z ćwiczeń przeprowadzanych w resorcie Obrony Narodowej, wnieśli istotny wkład metodyczny.

Orange Polska – TP CERT Orange – aktywnie ćwiczący. Przedstawiciel TP CERT Orange uczestniczył we wszystkich fazach organizacji Cyber-EXE Polska 2012. Szczególny wkład wniósł w fazie planowania, opiniując scenariusze oraz oceniając na bazie kilkunastoletniego doświadczenia faktyczne prawdopodobieństwo wystąpienia opisanych w nich sytuacji.

Politechnika Wrocławska – nie uczestniczyła aktywnie w ćwiczeniu. Przedstawiciele Politechniki Wrocławskiej uczestniczyli w fazie planowania oraz przeprowadzenia Cyber-EXE Polska 2012 udzielając wsparcia pozostałym uczestnikom, zwłaszcza przy tworzeniu dokumentacji przebiegu ćwiczenia.

Polskie Sieci Elektroenergetyczne Operator SA – jeden z dwóch głównych aktywnie ćwiczących. Przedstawiciel PSE Operator SA uczestniczył w wszystkich fazach organizacji Cyber-EXE Polska 2012. Szczególną rolę odegrał w fazie planowania budując scenariusz dla sektorowej ścieżki rozwoju sytuacji, oraz w fazie przeprowadzenia ćwiczenia.

RWE Polska SA – nie uczestniczyła aktywnie w ćwiczeniu. Przedstawiciel RWE uczestniczył we wszystkich fazach Cyber-EXE Polska 2012, udzielając wsparcia pozostałym uczestnikom. Szczególną rolę przedstawiciel spółki odegrał w fazie przeprowadzania wspierając głównego moderatora.

FOT. 1 UCZESTNICY ĆWICZENIA W CENTRUM KOORDYNACJI ĆWICZENIA WE WROCŁAWIU

Od lewej: Rafał Kasprzyk (WAT), Grzegorz Kołaczek (PWr), Mirosław Maj (FBC), Maciej Pyznar (RCB)

FOT. 2 UCZESTNICY ĆWICZENIA W CENTRUM KOORDYNACJI ĆWICZENIA WE WROCŁAWIU

Od prawej: Tomasz Zachmacz (KGP), Aneta Trojanowska (KGP), Artur Barankiewicz (Orange)

Rządowe Centrum Bezpieczeństwa – nie uczestniczyło aktywnie w ćwiczeniu. Przedstawiciele RCB uczestniczyli we wszystkich fazach Cyber-EXE Polska 2012. Byli odpowiedzialni za przeprowadzenie instruktaży u głównych ćwiczących i koordynację oceny ćwiczenia. RCB umożliwiło formalne kontakty z ENISA i podmiotami z sektora administracji państwowej.

Wojskowa Akademia Techniczna – **Wydział Cybernetyki** – przedstawiciele WAT uczestniczyli we wszystkich fazach organizacji Cyber-EXE Polska 2012. Szczególną rolę odegrali w fazie planowania oraz przeprowadzenia ćwiczenia. Wykładowcy i studenci podjęli się roli zespołu atakującego. Ponadto przedstawiciel WAT pełnił rolę koordynatora metodycznego, odpowiedzialnego również za dokumentację egu ćwiczeń.

5 Przebieg ćwiczenia

5.1 Informacje podstawowe

Ćwiczenie CYBER-EXE Polska 2012 zostało przeprowadzone w dniu 19 września 2012 r. w godzinach 09.00–17.00. Cyber-EXE Polska 2012 było rozproszonym ćwiczeniem sztabowym połączonym z częścią praktyczną, w postaci ataku z cyberprzestrzeni na wyodrębnioną w środowisku testowym infrastrukturę jednego z ćwiczących (patrz rozdz. 5.4). Symulowany atak miał dowieść, że zdarzenia ujęte w scenariuszu ćwiczenia są prawdopodobne. Podawane do wiadomości uczestników konferencji relacje z kolejnych etapów ataku były ściśle powiązane z wprowadzanymi zdarzeniami ze scenariusza sztabowego, uwiarygadniając w ten sposób cały przebieg zdarzeń.

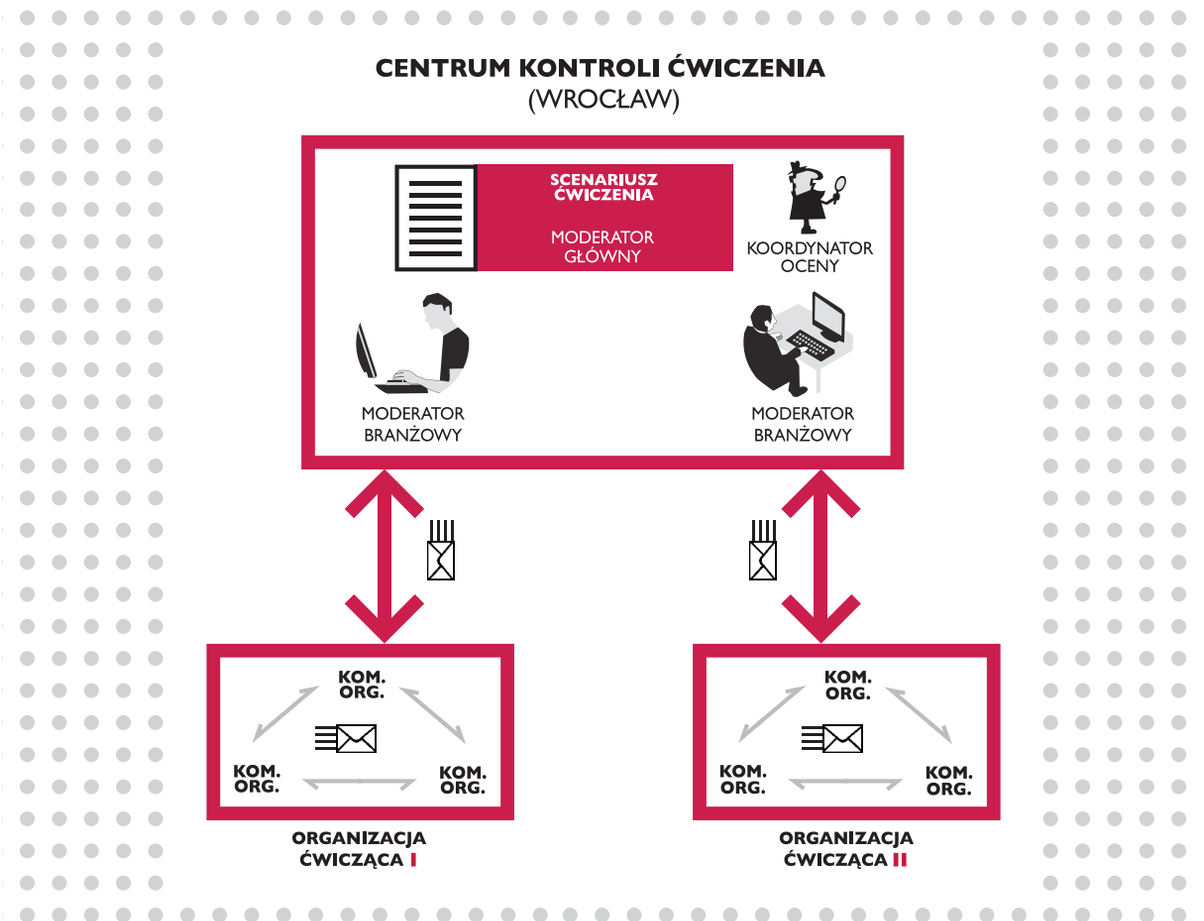
5.2 Struktura organizacyjna ćwiczenia

Uczestnicy ćwiczenia podzieleni byli na dwie grupy. Pierwsza grupa znajdowała się w Centrum Kontroli Ćwiczenia (CKC) w Centrum Kongresowym Hali Stulecia we Wrocławiu. Druga pozostawała we własnych lokalizacjach.
W grupie pierwszej znalazły się osoby, które odgrywały następujące role:

- Moderator główny – odpowiedzialny za koordynację całości przebiegu ćwiczenia, w tym w szczególności za poprawność przebiegu scenariusza.
- Moderatorzy branżowi – odpowiedzialni za koordynację ćwiczenia w ramach poszczególnych sektorów, w tym przebieg scenariusza w ramach tych sektorów.

- Uczestnicy ćwiczenia – niektórzy ćwiczący odpowiedzialni za reakcję na te fragmenty scenariusza, które dotyczyły ich organizacji.
- Koordynator metodyczny – odpowiedzialny za kontrolę fazy przebiegu ćwiczenia i dokumentację jego przebiegu.
- Koordynator oceny ćwiczenia – odpowiedzialny za obserwację przebiegu ćwiczenia i wstępne przygotowanie jego oceny.

Druga grupa obejmowała głównych ćwiczących oraz oceniających ćwiczenie lokalnie. Osoby należące do drugiej grupy pozostawały we własnych lokalizacjach, przede wszystkim w lokalizacjach należących do Gaz System SA oraz PSE Operator SA. Zespół atakujący działał w laboratorium Wydziału Cybernetyki WAT.



Rysunek 2 Schemat organizacji ćwiczenia Cyber-EXE Polska 2012

5.3 Atak na infrastrukturę teleinformatyczną w środowisku testowym

Fot. 3 PREZENTACJA PRZEBIEGU ĆWICZENIA
Zbigniew Świerczyński (WAT) omawia przebieg ataków w środowisku testowym.

W celu wykazania, że zdarzenia ujęte w scenariuszu ćwiczenia mogą wystąpić w rzeczywistości, równolegle do ćwiczenia sztabowego przeprowadzono kontrolowany atak teleinformatyczny na wyodrębnioną wirtualnie infrastrukturę jednego z ćwiczących (patrz rozdział 5.4 Środowisko testowe).

Atak został poprzedzony rozpoznaniem udostępnionego środowiska oraz konsultacjami z osobami, które to środowisko przygotowywały. Należy również dodać, że systemy znajdujące się w wirtualnym środowisku celowo nie zostały poddane skrupulatnej aktualizacji i tzw. utwardzaniu (ang. hardening), co znacznie utrudniłoby lub w niektórych przypadkach nawet uniemożliwiło działania zespołu atakującego. Rozpoznanie środowiska pozwoliło na zidentyfikowanie potencjalnych podatności działających tam systemów i kanałów transmisyjnych. Zdobyta wiedza została wykorzystana przy układaniu scenariusza ataku oraz gromadzeniu potrzebnych do jego przeprowadzenia narzędzi.

Celem głównym ataku było przejęcie sterowania zaworem gazowym na stacji redukcyjno-pomiarowej i w konsekwencji przerwanie dostaw gazu do systemu.

Scenariusz zakładał, że punktem wyjścia będzie zainstalowanie przez napastników, przynajmniej na jednej stacji roboczej w sieci wewnętrznej, oprogramowania które może być później wykorzystane do przygotowania i przeprowadzenia ataku. Przyjęto, że zainstalowanie oprogramowania nastąpi na skutek uruchomienia przez pracownika szkodliwego załącznika wiadomości poczty elektronicznej lub wejścia na stronę z programem wykorzystującym np. podatność przeglądarki internetowej. Opierając się na takich założeniach, we współpracy z administratorami przygotowanej infrastruktury teleinformatycznej, umieszczono w atakowanym środowisku oprogramowanie, które umożliwiło wykorzystanie wykrytych wcześniej podatności i tym samym skuteczne przeprowadzenie ataku[3].

[3] *Szczegółowy opis zdarzeń związanych z atakiem na infrastrukturę teleinformatyczną znajduje się w załączniku „Opis najważniejszych zdarzeń scenariusza ataku przeprowadzonego przez zespół atakujący".*

5.4 Środowisko testowe

Na potrzeby przeprowadzenia kontrolowanego ataku teleinformatycznego, jeden z ćwiczących zbudował w swoim Centrum Przetwarzania Danych środowisko testowe. Składało się z serwerów i urządzeń sieciowych, których podatności bezpieczeństwa miały być celem identyfikacji oraz wykorzystania przy ataku na infrastrukturę teleinformatyczną.

W skład wydzielonej infrastruktury wchodziły typowe systemy i aplikacje, niezbędne do działania systemu telemetrycznego, a także systemy sterowania przemysłowego (z ang. Supervisory Control And Data Acquisition, w skrócie SCADA). W środowisku zainstalowanych zostało kilkadziesiąt serwerów, między innymi:

- serwer poczty elektronicznej,
- kontroler domeny Active Directory,
- system zobrazowania i raportowania zdarzeń w systemach sterowania przemysłowego,
- oddziałowe serwery telemetrii,
- centralny serwer telemetrii,
- serwery symulujące pracę urządzeń APN (z ang. *Access Point Name*),
- serwery symulujące działanie sterowników PLC (z ang. *Programmable Logic Controller)* umieszczonych na obiektach np. stacjach redukcyjno-pomiarowych,
- serwery przygotowane przez zespół atakujący; w ramach tych serwerów znajdowały się środowiska programistyczne, usługi i narzędzia wykorzystywane do przeprowadzenia ataku.

Całość środowiska wykonana została z wykorzystaniem tzw. wirtualnych maszyn. Połączenia pomiędzy poszczególnymi modułami lub serwerami stanowiły przełączniki wykonane również w technologii zwirtualizowanej.

5.5 Scenariusz ćwiczenia

Wykorzystany w trakcie ćwiczenia scenariusz (dla obydwu ścieżek sektorowych) nie zakładał odniesienia do rzeczywistego poziomu bezpieczeństwa teleinformatycznego ćwiczących. Skuteczność przeprowadzonych ataków teleinformatycznych możliwa była tylko i wyłącznie dzięki zamierzonemu, sztucznemu obniżeniu poziomu bezpieczeństwa użytych w scenariuszu systemów teleinformatycznych. Miało to na celu realizację pełnego scenariusza ćwiczenia.

5.5.1 Scenariusz dla sektora gazowego

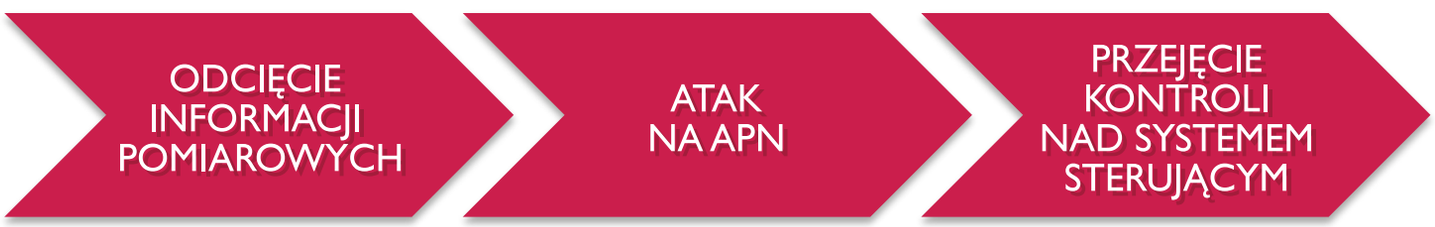
Scenariusz dla sektora gazowego zakładał wystąpienie zakłóceń w systemie przesyłu gazu, wynikających z kolejnych faz ataku z cyberprzestrzeni, przeprowadzanego na infrastrukturę telemetryczną obsługującą infrastrukturę przesyłową gazu w Polsce.

Początkowo skutki ataku ograniczyły się do odcięcia informacji pomiarowych z jednego punktu dystrybucyjnego. Brak danych pomiarowych z jednego punktu dystrybucyjnego w krótkim czasie nie wywołał jeszcze poważnych zakłóceń. W rzeczywistości tego typu sytuacje są zazwyczaj wynikiem awarii łącza GPRS bądź modemu.

Kolejnym etapem był atak na APN. Spowodował on odcięcie wszystkich informacji o parametrach urządzeń przesyłowych z obszaru odpowiedzialności całego oddziału. Problemem stały się rozliczenia pomiędzy dostawcą a odbiorcami gazu, a w dłuższym czasie zbilansowanie sieci przesyłowej. Kaskadowe pojawianie się problemów sugerowało nieprawidłowości, które nie mogły zostać uznane za przypadkowe.

Trzecim etapem, który zdecydowanie wskazywał na atak z cyberprzestrzeni, było przejęcie kontroli nad systemem sterującym urządzeniem przesyłowym. Jeden z systemów telemetrycznych zasygnalizował zamknięcie śluzy na gazociągu bez ingerencji dyspozytora.

Eskalacja problemów doprowadziła do podjęcia decyzji o powołaniu Sztabu Kryzysowego oraz uruchomieniu wszystkich służb dyspozytorskich w celu zapewnienia w pełni manualnego sterowania przepływem gazu.



Rysunek 3 Schemat scenariusza dla sektora gazowego.

5.5.2 Scenariusz dla sektora elektroenergetycznego

Scenariusz dla sektora elektroenergetyczna rozpoczął się od ataku dedykowanego typu APT (z ang. *Advanced Persistant Threat*). Atak polegał na identyfikacji podmiotów realizujących usługi wsparcia operatora, następnie infekcji systemów teleinformatycznych tego podmiotu, a w konsekwencji na zainfekowaniu obiektów stacji elektroenergetycznych najwyższych napięć. Infekcja nastąpiła poprzez przeniesienie złośliwego oprogramowania z nośnika pamięci należącego do pracownika wykonawcy prac serwisowych. Dodatkowo na jednym z obiektów stacyjnych znajdował się, niezarządzany przez Dział Teleinformatyki, aktywny modem GSM (pozostawiony przez pomyłke lub specjalnie przez jeden z podmiotów serwisujących obiekt), udostępniający łączność do sieci publicznej Internet za pomocą kanału GPRS.

Informacja na temat infrastruktury operatora oraz o wykonawcach usług serwisowych pozyskana została w wyniku przeglądu stron internetowych operatora, zawierających informacje o przeprowadzonych postępowaniach przetargowych.

Po zainfekowaniu pierwszego komputera na stacji elektroenergetycznej wirus rozpoczął dalszą propagację generując przy tym ruch sieciowy nieznanego typu. Działanie wirusa nakierowane było na znalezienie systemu teleinformatycznego podłączonego do sieci publicznej Internet, co umożliwiło infekcję kolejnych stacji elektroenergetycznych.

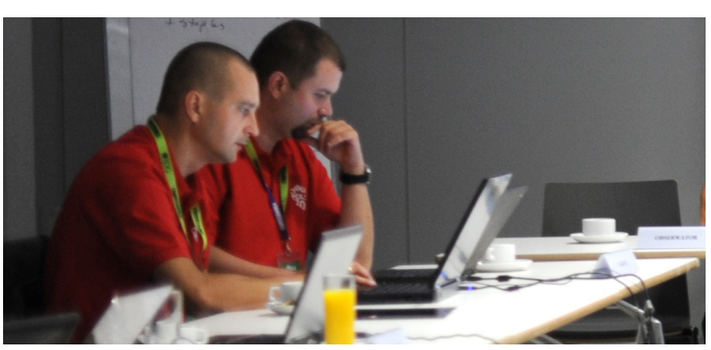
Głównym celem ataku było uszkodzenie autotransformatorów stacyjnych. Zostało to osiągnięte dzięki wyłączeniu urządzeń chłodzących poprzez podstawienie błędnych wyników pomiarów temperatury przez model cieplny systemu zdalnego sterowania i nadzoru nad pracą sieci przesyłowej. Złośliwe oprogramowanie miało możliwość blokowania komend wysyłanych z centrum nadzoru.

Likwidacja zagrożenia dla obiektów teleinformatycznych wymagała między innymi:

- współpracy kilku działów operatora (działy planujące i zarządzające systemem przesyłowym oraz stacjami z działem informatyki),
- prawidłowego powiadomienia służb ochrony państwa,
- stałej wymiany informacji pomiędzy wszystkimi zainteresowanymi stronami.

Rysunek 4 Schemat scenariusza dla sektora elektroenergetycznego.

Fot. 3-5 UCZESTNICY ĆWICZENIA W CKC
Od lewej:
Fot. 3 Maciej Pyznar (RCB), Mirosław Maj (FBC), Artur Ślubowski (RWE), Grzegorz Kołaczek (PWr), Piotr Choiński (IDG).
Fot. 4 Grzegorz Kołaczek (PWr), Rafał Kasprzyk (WAT).
Fot. 5 Michał Pawlak (GAZ–SYSTEM SA), Kamil Kowalczuk (GAZ–SYSTEM SA)



5.6 Zarządzanie zdarzeniami

Ćwiczenia przebiegały zgodnie z wcześniej przygotowanymi fikcyjnymi zdarzeniami, które wraz z rozwojem ćwiczenia były systematycznie uruchamiane przez moderatora.

Zdarzenia przewidziane scenariuszem podzielone były na dwie grupy:

- inicjujące – zdarzenia techniczne związane z przeprowadzanym atakiem, mające wywołać określoną reakcję ćwiczących;
- warunkowe – zdarzenia proceduralne uruchamiane w sytuacji kiedy ćwiczący nie podejmowali sami akcji, które były przewidziane.

Zdecydowaną większość zaplanowanych zdarzeń stanowiły zdarzenia warunkowe. Miało to na celu doprowadzenie do zaistnienia wszystkich zdarzeń, gdyż tylko to powodowało możliwość przećwiczenia wszystkich zakładanych sytuacji. W trakcie ćwiczenia zdarzenia warunkowe użyte zostały sporadycznie.

Całość komunikacji pomiędzy wszystkimi uczestnikami ćwiczenia odbywała się z wykorzystaniem systemu poczty elektronicznej, który na potrzeby ćwiczenia zastąpił i symulował użycie standardowych środków łączności. Nie były dopuszczone do użycia inne środki komunikacji (np. telefon). Jeśli ćwiczący, zgodnie ze swoim zamierzeniem, na przykład wynikającym z obowiązujących procedur, powinien użyć innego środka łączności niż poczta elektroniczna, to zaznaczał ten fakt w korespondencji elektronicznej. Przed przystąpieniem do ćwiczenia wszyscy uczestnicy otrzymali instrukcję korzystania z przygotowanych skrzynek pocztowych. Instrukcja zawierała również książkę adresową. Wszelka korespondencja mogła się odbywać tylko w ramach podmiotów wskazanych książce adresowej.

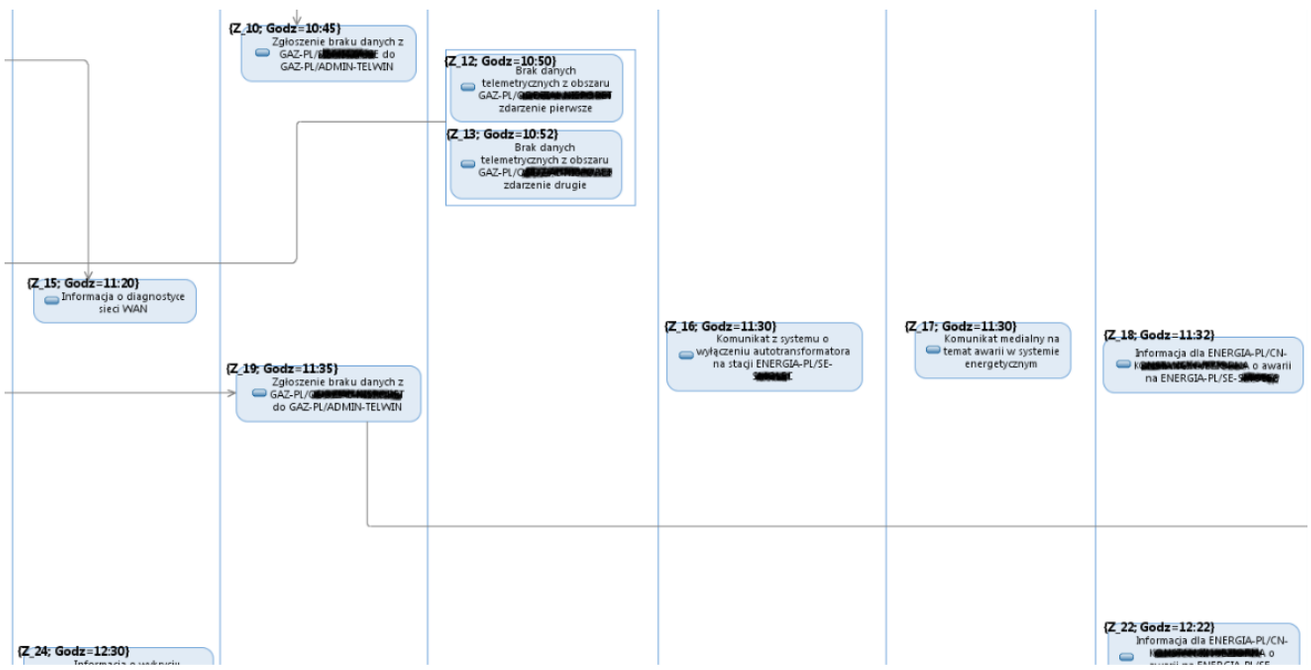
Całość korespondencji była dostępna dla takich osób jak:

- moderator główny
- moderatorzy branżowi
- koordynator metodyczny
- koordynator oceny ćwiczenia

5.7 Dokumentacja i monitoring przebiegu ćwiczenia

Scenariusz ćwiczenia został przygotowany z wykorzystaniem arkusza kalkulacyjnego, a następnie na potrzeby jego czytelnego zobrazowania i uszczegółowienia (w tym weryfikacji) wykorzystano jeden z diagramów UML (ang. *Unified Modeling Language*) nazywany diagramem czynności lub aktywności (ang. *activity diagram*). Posłużył on do modelowania dynamiki na poziomie procesów zachodzących w trakcie ćwiczenia. W ten sposób

powstały schematy blokowe, które przedstawiają przepływ sterowania z czynności do czynności. Obrazowały one sekwencyjne bądź równoległe lub współbieżne kroki procesu, a ich podstawowym zadaniem było modelowanie przetwarzania (przepływu zadań).

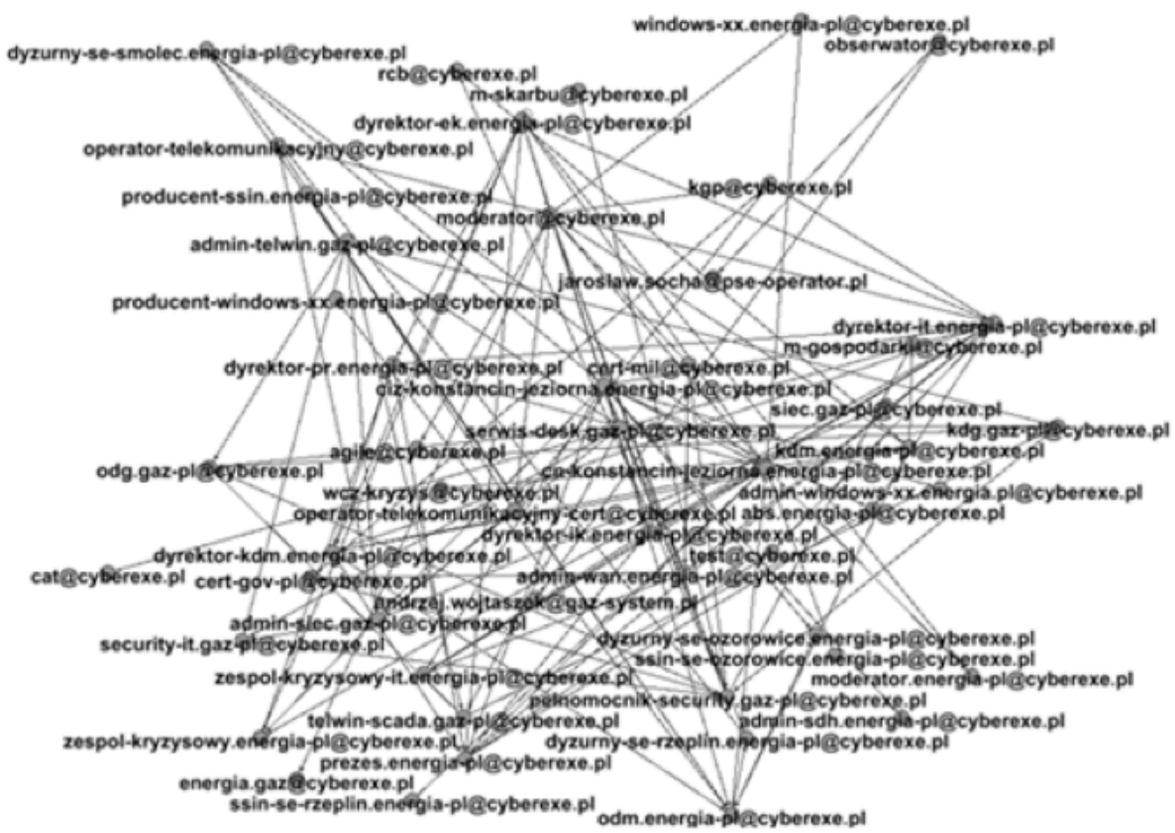


Rysunek 5 Fragment scenariusza Cyber-EXE Polska 2012 w postaci diagramu UML.

Monitoring stanu ćwiczenia i kontrola jego przebiegu zostały zapewnione poprzez możliwość obserwacji całości korespondencji wymienianej pomiędzy uczestnikami ćwiczenia przez moderatora głównego i koordynatora oceny. Zostało to osiągnięte poprzez automatyczne przesyłanie kopii każdej wiadomości poczty elektronicznej.

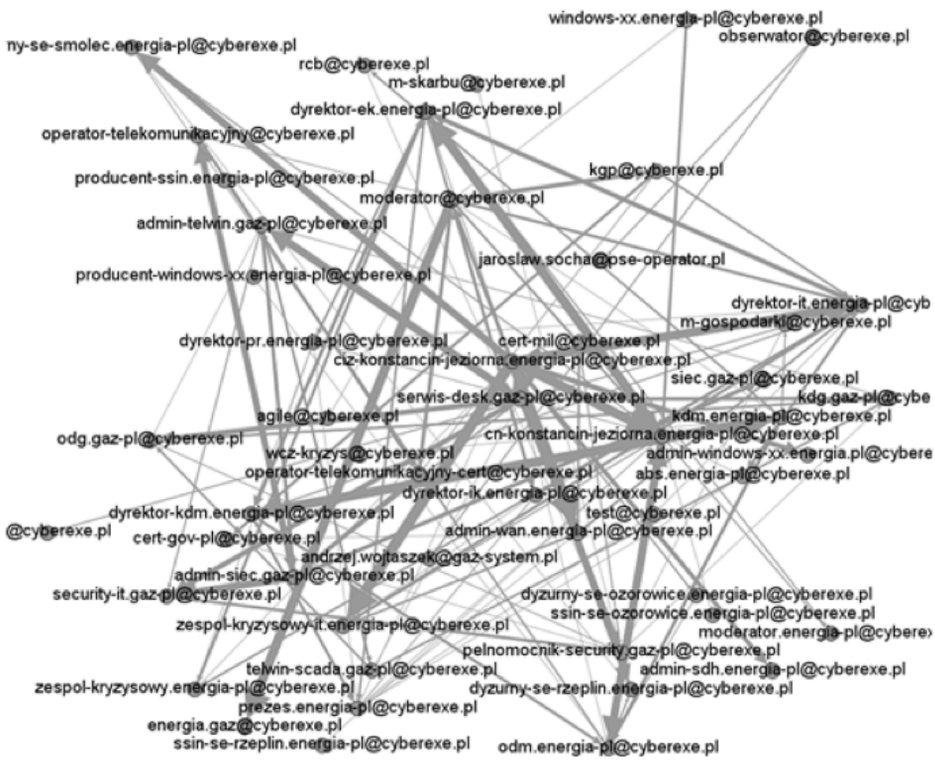
Dla zobrazowania przebiegu ćwiczenia w trakcie jego trwania wykorzystano diagramy czynności, podobnie jak w przypadku dokumentowania scenariusza ćwiczenia. Jednak ze względu na liczbę zdarzeń, która generowana była w ćwiczeniu (pomiędzy ćwiczącymi wymienionych zostało 604 przesłanych komunikatów, co dawało średnio od 2 do 3 komunikatów w ciągu minuty) ręczne wprowadzanie zdarzeń było niemożliwe.

W zwiazku z tym zdecydowano się na automatyzację procesu monitorowania przebiegu ćwiczenia poprzez wizualizację stanu zaangażowania poszczególnych ćwiczących i przepływu informacji. Zbudowana sieć kontaktów składa się z węzłów (każdy węzeł to inny ćwiczący) oraz łuków (każdy łuk oznacza wymianę informacji– wysłanie poczty elektronicznej pomiędzy parą węzłów).



Rysunek 6 Przykład sieci komunikacji pomiędzy uczestnikami Cyber-EXE Polska 2012 (19.09.2012 godz. 16.00).

Sieć kontaktów, która powstała w trakcie ćwiczenia zawiera 51 węzłów. W wyniku wymiany 604 emaili powstało 178 łuków (kanałów komunikacyjnych) pomiędzy ćwiczącymi. Grubość łuku, nazywana często jego wagą, jest proporcjonalna do liczby emaili przesłanych pomiędzy daną parą węzłów.



Rysunek 7 Sieć kontaktów Cyber-Exe-Polska 2012.

5.8 Wizualizacja ćwiczeń

Podczas przygotowań do ćwiczeń Cyber-EXE Polska 2012 przygotowano cztery filmy obrazujące skutki ataków. Filmy były wyświetlane w trakcie konferencji Wolność i Bezpieczeństwo, towarzyszącej ćwiczeniom, jak również były elementem scenariusza w sektorze energetycznym. W ten sposób ćwiczenie obserwowało około 200 osób.

Przygotowane filmy miały uzmysłowić uczestnikom konferencji, że atak z cyberprzestrzeni na infrastrukturę wpływa bezpośrednio na powstanie poważnych zagrożeń w realnym świecie, a jego efekty w zależności od skali i przygotowania ataku są bardzo podobne do skutków wielkich katastrof czy klęsk żywiołowych.

Materiały filmowe informowały między innymi o:

- przerwie w dostawach energii elektrycznej;
- paraliżu komunikacji miejskiej na skutek unieruchomienia tramwajów i wyłączenia sygnalizacji świetlnej;
- utrudnieniach w pracy szpitali;
- niedostępności usług telefonii komórkowej;
- przerwach w pracy sklepów na skutek braku zasilania kas fiskalnych i terminali płatniczych,
- kłopotach z dostępem do części usług bankowych;
- przerwach w dostawach gazu, wstrzymaniu produkcji w niektórych zakładach przemysłowych,
- konsekwencjach tych wydarzeń dla rynków finansowych.

Nie wszystkie prezentowane zdarzenia miały swoje bezpośrednie odpowiedniki w scenariuszu ćwiczeń. W wielu przypadkach miały one jedynie za zadanie uświadomić skalę i realność problemów mogących wyniknąć w przypadku wystąpienia ataków podobnych do tych, które uwzględniał scenariusz.

Dodatkowo wizualizacja ćwiczeń odbywała się również w odniesieniu do przebiegu konkretnych zdarzeń ujętych w scenariuszu. Dotyczyła ona przebiegu zdarzeń w środowisku testowym, wymiany informacji pomiędzy uczestnikami ćwiczenia i sukcesywnego pojawiania się kolejnych elementów scenariusza. Ta część wizualizacji odbywała się z wykorzystaniem oprogramowania przygotowanego specjalnie w tym celu.

Fot. 6 WIZUALIZACJA ĆWICZENIA Cyber-EXE Polska 2012.
Przebieg ataków w środowisku testowym prezentuje Kamil Wiśniewski (HP)

6 Wnioski i rekomendacje

Zebrane w trakcie ćwiczenia Cyber-EXE Polska 2012 dane są doskonałym materiałem do przeprowadzenia analiz pozwalających na wyciągnięcie wniosków w kilku istotnych obszarach:

- reagowania ćwiczących zgodnie z istniejącymi procedurami obowiązującymi w ich macierzystych organizacjach;
- efektywności istniejących procedur w poszczególnych organizacjach;
- identyfikacji kluczowych podmiotów występujących w procedurach (w przypadku ćwiczenia reprezentowani oni byli przez grających, a na schematach przebiegu ćwiczeń przez tzw. „węzły"), mających wpływ na skuteczność podjętych działań.

Analizy tego typu pozwolą na przeprowadzenie modyfikacji istniejących procedur w celu ich optymalizacji, zwłaszcza poprawy efektywności.

Wnioski i rekomendacje z ćwiczenia Cyber-EXE Polska 2012 mogą być przydatne zarówno dla sektora publicznego jak i podmiotów prywatnych. Służyć mają poprawie naszego przygotowania na sytuacje kryzysowe związane z atakiem z cyberprzestrzeni oraz sprawniejszej organizacji ewentualnych przyszłych ćwiczeń. Porównując ćwiczenie Cyber-EXE Polska 2012 z innymi ćwiczeniami przeprowadzonymi w ostatnich latach innych krajach można stwierdzić, że w obliczu zagrożeń z cyberprzestrzeni wszyscy dzielimy podobne doświadczenia, a proponowane rozwiązania, które możemy zastosować, również są podobne. W związku z tym **wnioski i rekomendacje z ćwiczeń można wykorzystać, wdrażając je w Politykę Ochrony Cyberprzestrzeni RP.**

Wnioski i rekomendacje z ćwiczenia Cyber-EXE Polska 2012 zostały podane w odniesieniu do jego celów, sformułowanych w fazie identyfikacji. Ich znaczenie zostało odzwierciedlone w kolejności wymieniania. Oddzielnie zawarto wnioski i rekomendacje dla organizacji samego ćwiczenia.

6.1 Wnioski z ćwiczenia Cyber-EXE Polska 2012

Wnioski odnoszące się do celu ćwiczenia

*Sprawdzić **zdolność do reakcji** na atak pochodzący z cyberprzestrzeni, w tym powstrzymania tego ataku oraz minimalizacji jego skutków.*

- Znajomość zagadnień związanych z zagrożeniami z cyberprzestrzeni i świadomość ich potencjalnych skutków posiadane przez pracowników organizacji są najważniejszym czynnikiem skutecznej reakcji na te zagrożenia.
- Organizacje okazały się być bardzo dobrze przygotowane w kontekście radzenia sobie z sytuacją kryzysową. Warto jednak wciąż pogłębiać wiedzę na temat specyfiki zagrożeń płynących z cyberprzestrzeni, gdzie znalezienie przyczyn ataku jest często nie mniej ważne niż usunięcie ich skutków. Wymaga to od osób na stanowiskach decyzyjnych znajomości tej specyfiki. Szczególnie ważny jest wysoki poziom świadomości wśród osób decydujących osposobie reakcji na zagrożenie.
- Reakcja ćwiczących na sytuację ataków z cyberprzestrzeni na systemy typu SCADA, które to sytuacje zawierał scenariusz ćwiczeń, potwierdziła konieczność rozpoznawania potencjalnych podatności tych systemów oraz procedur reagowania na tego typu zagrożenia.
- Komunikacja wewnątrz poszczególnych organizacji były skuteczna i przebiegała sprawnie.

Wnioski odnoszące się do celu ćwiczenia

*Sprawdzić **skuteczność informowania** właściwych organów o ataku (identyfikacja właściwych organów, kanały łączności, jakość informacji).*

- Komunikacja z podmiotami istniejącymi na zewnątrz organizacji miała głównie charakter informacyjny i nie uwzględniała zapotrzebowania na wsparcie zewnętrzne w rozwiązaniu problemu.
- Wystąpiły trudności w identyfikacji właściwego zespołu CERT, wynikające z braku upublicznionej informacji o obszarach działania takich zespołów pracujących w kraju.

Wnioski odnoszące się do celu ćwiczenia:

*Sprawdzić **zdolność do współpracy** pomiędzy właściwymi organami administracji publicznej oraz innymi podmiotami uczestniczącymi w ćwiczeniach, w tym podmiotami sektora prywatnego.*

- Brak istotnych podmiotów sektora publicznego oraz prywatnego nie pozwolił na pełne sprawdzenie istniejących powiązań i wzajemnych relacji pomiędzy nimi.
- Wystąpiły trudności w identyfikacji podmiotu (organu) koordynującego obsługę incydentu.
- Zaobserwowano jednoczesną komunikację do szerokiej grupy organów administracji państwowej. Wynikała ona najprawdopodobniej z braku informacji o właściwości organów w zakresie zagrożeń z cyberprzestrzeni.

Wnioski dotyczące organizacji i przeprowadzenie ćwiczenia

- Sprawdził się przjęty model organizacji ćwiczenia, polegający na współpracy pomiędzy organizacjami pozarządowymi, środowiskiem akademickim, administracją publiczną i sektorem prywatnym sprawdził się. Osiągnięto efekt synergii i udowodniono możliwość skutecznej współpracy między wymienionymi grupami podmiotów.
- Działanie (reakcja) zbyt wielu komórek organizacyjnych (w tym również podmiotów z administracji publicznej), które nie uczestniczyły aktywnie w ćwiczeniach musiała być symulowana (podgrywana).
- Świadomość ćwiczących (zwłaszcza kierownictwa) w zakresie celów ćwiczeń i korzyści wynikających z udziału w takim przedsięwzięciu jest decydująca dla skuteczności ćwiczenia oraz ma wpływ na decyzję o ilości i poziomie zaangażowania komórek organizacyjnych ćwiczącego.
- Opracowanie realistycznego scenariusza jest kluczowym elementem procesu planowania ćwiczeń. Ma decydujący wpływ na sprawne przeprowadzenie ćwiczeń.
- Organizacja części związanej z przeprowadzeniem technicznych ataków na przygotowaną infrastrukturę jest istotnym i pożytecznym przedsięwzięciem, które uwiarygodnia i lepiej uświadamia istotę zagrożeń.
- Przyjęty sposób dystrybucji wprowadzeń i komunikacji został odpowiednio przygotowany na potrzeby ćwiczeń. Ułatwiło to zarządzanie zdarzeniami oraz kontrolę nad przebiegiem ćwiczenia, ale zmniejszyło realność działań podejmowanych przez ćwiczących.
- W organizacji ćwiczeń duże znaczenie ma wsparcie udzielone ze strony istotnych podmiotów sektora administracji publicznej.
- Przygotowanie logistyczne CKC ma istotny wpływ na sprawne przeprowadzenie ćwiczenia i komfort pracy ćwiczących.
- Ćwiczenia i ich przebieg były mało nagłośnienie w mediach.

6.2 Rekomendacje z ćwiczenia Cyber-EXE Polska 2012

Rekomendacje odnoszące się do celu ćwiczenia:

*Sprawdzić **zdolność do reakcji** na atak pochodzący z cyberprzestrzeni, w tym powstrzymania tego ataku oraz minimalizacji jego skutków.*

- Biorąc pod uwagę fakt, że ćwiczenia są najskuteczniejszą formą przygotowania do reakcji organizacji na zagrożenia, należy regularnie przeprowadzać ćwiczenia obejmujące w swoich

scenariuszach ataki z cyberprzestrzeni. Ćwiczenia tego typu powinny odbywać się we wszystkich organizacjach wykorzystujących sieci i systemy teleinformatyczne, w tym również w administracji publicznej.

- Doświadczenia z ćwiczenia mogą i powinny być wykorzystane w ćwiczeniach innych sektorów gospodarki (np. w sektorze finansowym).
- Świadomość i kompetencje kierowników jednostek organizacyjnych w zakresie funkcjonowania użytkowanych systemów teleinformatycznych oraz zagrożeń dla nich i ich bezpieczeństwapowinny być systematycznie poszerzane i stać się przedmiotem wewnętrznych szkoleń. Systematyczne podnoszenie kwalifikacji w obszarze zagrożeń z cyberprzestrzeni i ich potencjalnych skutków jest niezbędnym elementem zwiększenia odporności organizacji na te zagrożenia.
- Należy wypracować najlepsze praktyki reakcji na zagrożenia systemów teleinformatycznych obsługujących elementy infrastruktury strategicznej dla bezpieczeństwa państwa.
- Należy powołać do życia forum wymiany doświadczeń dla operatorów infrastruktury krytycznej w obszarze ochrony teleinformatycznej. Forum mogłoby funkcjonować jako podgrupa forów wymiany informacji przewidzianych w projekcie Narodowego Programu Ochrony Infrastruktury Krytycznej.
- Wnioski i rekomendacje z przebiegu ćwiczeń oraz metodyka ich organizacji powinny stać się przedmiotem szkoleń w wewnętrznych w organizacjach.

Rekomendacje odnoszące się do celu ćwiczenia

*Sprawdzić **skuteczność informowania** właściwych organów o ataku (identyfikacja właściwych organów, kanały łączności, jakość informacji).*

- Istnieje potrzeba stworzenia standardowej procedury operacyjnej (SOP) dotyczącej współpracy w obsłudze ataku z cyberprzestrzeni. SOP powinna zawierać elementy opisane w rozdziale 7 odnoszące się do zasad informowania właściwych organów o ataku.
- Konieczne jest rozpowszechnienie i upowszechnienie wiedzy o obszarach działania (z ang. *Constituency*) zespołów CERT funkcjonujących w Polsce.
- Nadmiarowa komunikacja (lub jej brak) na zewnętrz (a także wewnątrz) organizacji powinna być punktem wyjścia do przeglądu procedur funkcjonujących w organizacji i ich korekty lub stworzenia nowych.

Rekomendacje odnoszące się do celu ćwiczenia

*Sprawdzić **zdolność do współpracy** pomiędzy właściwymi organami administracji publicznej oraz innymi podmiotami uczestniczącymi w ćwiczeniach, w tym podmiotami sektora prywatnego.*

- Istnieje potrzeba stworzenia standardowej procedury operacyjnej (SOP) dotyczącej współpracy w obsłudze ataku z cyberprzestrzeni. SOP powinna zawierać elementy opisane w rozdziale 7 odnoszące się do współpracy pomiędzy podmiotami administracji publicznej i podmiotami sektora prywatnego.
- Procedury zarządzania kryzysowego należy uzupełnić o procedury na wypadek ataku z cyberprzestrzeni.

Rekomendacje dotyczące organizacji i przeprowadzenie przyszłych ćwiczeń

- Potencjał tkwiący w modelu organizacji ćwiczenia, polegający na współpracy pomiędzy organizacjami pozarządowymi, środowiskiem akademickim, administracją publiczną i sektorem prywatnym powinien być wykorzystywany w organizacji przyszłych ćwiczeń Cyber-EXE Polska.
- W celu podniesienia realizmu ćwiczeń i osiągnięcia zakładanych celów konieczne jest zaangażowanie większej liczby rzeczywistych uczestników. Dotyczy to:
  - wewnętrznych komórek organizacyjnych;
  - organów administracji rządowej, zwłaszcza tych, w których właściwości znajduje się bezpieczeństwo cyberprzestrzeni, łączność, informatyzacja oraz zarządzanie kryzysowe;
  - organów administracji samorządowej;
  - służb, inspekcji i straży odpowiedzialnych za zapewnienie bezpieczeństwa obywateli,
  - organizacji pozarządowych zajmujących się tematyką bezpieczeństwa cyberprzestrzeni.
- W opracowanie szczegółowego scenariusza dla uczestniczących w ćwiczeniu branż powinny być zaangażowane także inne osoby niż specjaliści działów ICT. Pozwoli to na uwzględnienienie w scenariuszu wszystkich elementów procedur reagowania na zagrożenia i procedur minimalizacji skutków zagrożeń.
- W celu zachowania swobody komunikacji oraz dotrzymania obowiązujących regulacji wewnętrznych podmioty angażujące się w przeprowadzenie ćwiczeń powinny w początkowej fazie określić zasady zachowania poufności przekazywanych informacji.
- Praca nad scenariuszem jest kluczowa pod względem przygotowania ćwiczenia zgodnie z harmonogramem, dlatego powinna zakończyć się w ściśle określonym punkcie tego harmonogramu. Harmonogram powinien uwzględniać również inne kluczowe punkty, m.in.: ustalenie listy uczestników, przygotowanie scenariusza i ćwiczących, przeprowadzenie ćwiczeń, opracowanie raportu końcowego (patrz rozdz. 4.1).
- Podnoszenie świadomości ćwiczących oraz praktyczna strona przeprowadzenia ćwiczenia

powinny stać się celem szkoleń przed jego rozpoczęciem. Szkolenia powinny zostać zaplanowane w harmonogramie organizacji ćwiczeń.

- Szkolenia i instruktaże do ćwiczenia warto przeprowadzać w lokalizacji ćwiczących organizacji.
- Przy organizacji tego rodzaju ćwiczeń rekomenduje się włączenie w działania uświadamiające przedstawicieli wielu niezależnych mediów oraz staranne zaplanowanie akcji informacyjnej o ćwiczeniach.

7 Standardowa Procedura Operacyjna (SOP) jako kluczowa rekomendacja

Doświadczeniem ćwiczeń Cyber Euro 2010[4] był brak procedur współpracy międzynarodowej podczas kryzysów wywołanych atakami z cyberprzestrzeni. Najważniejszym wnioskiem z ćwiczeń była konieczność stworzenia standardowej procedury operacyjnej w tym zakresie.

Przebieg ćwiczenia Cyber-EXE Polska 2012 pozwala stwierdzić, że podobna konieczność występuje na szczeblu krajowym.

Każdy potencjalny atak z cyberprzestrzeni jest inny, może mieć różne skutki i dotyczyć różnych podmiotów. SOP w zakresie współpracy podczas ataku z cyberprzestrzeni może pomóc w przejmowaniu kontroli nad potencjalną sytuacją kryzysową w drodze zaplanowanych działań, reagowaniu w przypadku wystąpienia ataków z cyberprzestrzeni oraz usuwaniu ich skutków.

SOP powinna zawierać elementy dotyczące:

I. Przekazywania informacji o ataku (alarmowania), w tym m.in.:
   - formularze zgłoszenia incydentu (uproszczony i pełny – w zależności od poziomu kompetencji zgłaszającego),
   - obszary działania zespołów typu CERT pracujących w kraju;

II. Ustalenia obszarów współpracy, w tym m.in.:
   - sposobu ustanowienia koordynatora działań (w zależności od sytuacji np. pierwszy zaatakowany
     najbardziej dotknięty, mający najlepsze warunki do działania),
   - określenia głównych zadań koordynatora i uczestników grupy reagowania,
   - określenia ramowych zasad współpracy z zaatakowanymi podmiotami.

III. Sposobów i kanałów wymiany informacji, w tym m.in.:

[4] *Ćwiczenie CYBER EURO 2010 było pierwszym ogólnoeuropejskim ćwiczeniem z zakresu ochrony przed atakiem z cyberprzestrzeni. Zostało zorganizowane przez państwa członkowskie EU oraz Europejską Agencję ds. Bezpieczeństwa Sieci i Informacji (ENISA) i Wsólne Centrum Badawcze (JRC). Uczestniczyło w nim 30 krajów (22 aktywnie ćwiczących i 8 obserwujących).*

- książkę kontaktową, która byłaby centralnym elementem systemu powiadamiania,
- zasady wymiany informacji wrażliwych,
- zasady przekazywania raportów sytuacyjnych i ich wzór.

Fot. 7 UCZESTNICY Cyber-EXE POLSKA 2012.
Od lewej: Tadeusz Włodarczyk (PSE OPERATOR SA), Grzegorz Kołaczek (PWr), Rafał Kasprzyk (WAT), Mirosław Maj (FBC), Kamil Kowalczuk (GAZ–SYSTEM SA), Maciej Pyznar (RCB), Tomasz Zachmacz (KGP), Krzysztof Tomkiel (MON), Michał Pawlak (GAZ–SYSTEM SA), Marcin Brzeziński (MON), Aneta Trojanowska (KGP), Artur Barankiewicz (ORANGE), Artur Ślubowski (RWE).

8 Podziękowania

Ćwiczenie nie mogłoby się odbyć bez dobrej woli i wyjątkowego zaangażowania wszystkich uczestniczących w nim organizacji, a zwłaszcza osób, które brały aktywny udział w jego organizacji. Bez nich ta szczytna i pożyteczna idea nie byłaby możliwa do zrealizowania. Organizatorzy dziękują im za odwagę w realizacji tego pionierskiego w Polsce przedsięwzięcia, za rzadko spotykaną sprawność działania, otwartość w komunikacji i aktywność w podejmowaniu zadań. Jesteśmy przekonani, że ćwiczenie Cyber-EXE Polska 2012 było doskonałym przykładem dobrze rozumianej i przeprowadzonej współpracy w ramach partnerstwa publiczno-prywatnego.

Dziękujemy podmiotom sektora prywatnego za udział w ćwiczeniu. Szczególne podziękowania pragniemy skierować na ręce kierownictwa OGP Gaz-System SA i PSE Operator SA. Ich reprezentanci swoim udziałem w ćwiczeniach podnieśli rangę wydarzenia i sprawili, że wnioski i rekomendacje oparte są na doświadczeniach pochodzących z niezwykle ważnych sektorów polskiej gospodarki. Podziękowania kierujemy również do operatora telekomunikacyjnego Orange Polska.

Dziękujemy podmiotom z sektora akademickiego, a zwłaszcza Wojskowej Akademii Technicznej, która w istotny sposób przyczyniła się do przeprowadzenia ćwiczenia.

Organizatorzy dziękują również wszystkim podmiotom administracji publicznej – Komendzie Głównej Policji, Ministerstwu Obrony Narodowej, a w szczególności Rządowemu Centrum Bezpieczeństwa, które wsparło inicjatywę ćwiczenia i wyjątkowo aktywnie uczestniczyło w jej realizacji.

Należy też wspomnieć o przychylności dla organizacji ćwiczenia Cyber-EXE Polska 2012 Biura Bezpieczeństwa Narodowego. W początkowej fazie organizacji był to ważny element mający wpływ na ostateczną decyzję o realizacji idei ćwiczenia.

Swój wkład w Cyber-EXE Polska 2012 wniosła również Europejska Agencja Bezpieczeństwa Sieci i Informacji (ENISA). Agencja wyraziła gotowość do wsparcia ćwiczenia i w ramach tego przeprowadziła szkolenie z metodyki przeprowadzania ćwiczeń. Pozwoliło ono zespołowi projektowemu i pozostałym uczestnikom szkolenia lepiej zrozumieć kompleksowy charakter organizacji ćwiczenia i potencjalne trudności w każdym z etapów jego realizacji.

9 Załączniki

Załącznik nr 1 Opis najważniejszych zdarzeń scenariusza ataku przeprowadzonego przez zespół atakujący

Lp.	Opis
1.	**Uzyskanie dostępu do sieci wewnętrznej ofiary** Uzyskanie dostępu do sieci wewnętrznej ofiary (sieć LAN) stanowiło punkt wyjścia do dalszych działań. W scenariuszu założono uzyskanie takiego dostępu poprzez realizację jednej lub obydwu z poniżej wymienionych metod: **Metoda I**: Wiadomość poczty elektronicznej zawierająca złośliwe oprogramowanie typu koń trojański (niewykluczone, że jest to zagrożenie o charakterze ,,zero-day'', czyli nieznane jeszcze producentowi) przedostaje się przez system zabezpieczeń i trafia do skrzynek pracowników. Otwarcie załącznika powoduje zainstalowanie złośliwego oprogramowania. To pozwala na uzyskanie przez intruzów zdalnego dostępu do zasobów zaatakowanego komputera i przejęcia do niego praw administracyjnych. **Metoda II**: Odnośnik do szkodliwej strony www jest przesłany w treści wiadomości poczty elektronicznej. Połączenie ze stroną powoduje infekcję komputera osoby odwiedzającej serwis.
2.	**Przygotowanie ataku prowadzącego do przejęcia danych autoryzacyjnych administratora domeny i administratora systemów SCADA** Przygotowanie ataku składało się z wymienionych poniżej etapów: a) Z ,,zarażonego'' komputera przeprowadzone zostało skanowanie sieci biznesowej. Zostały rozpoznane główne serwery systemu teleinformatycznego oraz nazwy DNS-owe. Uszczegóławiając, wykonano: • Wyszukiwanie aktywnych systemów i usług. Wykryto między innymi: serwer poczty elektronicznej, kontroler domeny Acive Directory oraz serwery z oprogramowaniem przemysłowym, tj. system bilansujący przepływ gazu oraz system sterowania i nadzoru. • Po zidentyfikowaniu serwerów istotnych dla działania atakowanego środowiska przeprowadzono wyszukiwanie potencjalnych podatności. Między innymi zidentyfikowano podatność związaną z protokołem RDP wykorzystywanym na serwerze systemu bilansującego przepływ gazu oraz możliwość przeprowadzenia ataku ARP

	poisoning/spoofing[1] na przełączniku obsługującym sieć biznesową. Informacja o wykrytej podatności RDP była dostępna publicznie. W Internecie dostępny był również exploit wykorzystujący tę podatność. Umożliwiał on „jedynie" wykonanie restartu zdalnego serwera. Dlatego też atak polegał na przekierowaniu użytkowników na podstawione serwery w celu przechwycenia ich danych autoryzacyjnych. Podatność RDP i wykonany dzięki niej restart serwera systemu bilansującego przepływ gazu zostały wykorzystane do sprowokowania zalogowania się osób odpowiedzialnych za działanie systemu teleinformatycznego. Przechwycenie tych danych poprzez klasyczny atak MiTM[2] był trudny do wykonania z powodu szyfrowania transmisji. • Następnie ze skutecznie przejętego komputera wykonywany został atak na przełącznik w podsieci. Był to ponownie ataku typu ARP poisoning/spoofing. To spowodowało przekierowanie transmisji na uruchomiony przez cyberprzestępców serwer DNS, a w konsekwencji użytkownicy chcący połączyć się z systemem poczty elektronicznej oraz dowolnym serwerem systemu sterowania i nadzoru zostali faktycznie skierowani na serwery www, zainstalowane i kontrolowane przez atakujących. Podstawione serwisy posiadały taki sam interfejs graficzny i przedstawiały się certyfikatami wygenerowanymi przez atakujących. W przypadku certyfikatów było to zadanie ułatwione, gdyż podobnie jak w przypadku oryginalnych certyfikatów nie było konieczności autoryzowania ich przez tzw. trzecią, zaufaną stronę. Następnie w sieci przeprowadzono atak DoS (patrz punkt następny), co sprowokowało administratorów do logowania się w serwisie i w rezultacie przejęcie ich danych autoryzacyjnych.
4.	**Atak DoS na serwer systemu bilansującego przepływ gazu.** Wykorzystana została podatność RDP i exploit opisany w poprzednim punkcie. Uruchomienie exploita spowodowało wyłączenie serwera systemu bilansującego przepływ gazu. Założono, że takie zdarzenie w sieci zostanie zauważone przez osoby odpowiedzialne za działanie firmowej sieci i systemów i spowoduje to ich zalogowanie do systemów oraz Active Directory, które jak wiadomo były podstawione przez atakujących. Przejęte dane autoryzacyjne zostały natychmiast wykorzystane i atakujący zmienili hasła dostępowe w serwisach co uniemożliwiło konieczną reakcję ze strony uprawnionych administratorów.
5.	Z wykorzystaniem przejętych danych autoryzacyjnych wyłączony został serwer systemu sterowania i nadzoru w jednym z oddziałów. Spowodowało to zakładany w scenariusz zanik transmisji danych telemetrycznych z jednej ze stacji. Oprócz oczywistych problemów z tym związanych, pozwoliło to na odwrócenie uwagi administratorów od działań przygotowujących dalsze etapy ataku, którego głównym celem było zamknięcie zaworu na jednej ze stacji.

6.	Dalsze rozpoznanie zaatakowanego środowiska pozwoliło na znalezienie serwera systemu sterowania i nadzoru, sterującego zaworami. Aby atak był udany konieczne było znalezienie odpowiedniego oprogramowania, służącego do dostępu zdalnego. Obserwacja połączeń sieciowych wykryto jeden z komputerów, które zdalnie łączyły się na z serwerem systemu sterowania i nadzoru. Komputer ten należał do operatora systemu. Został on skutecznie zaatakowany z wykorzystaniem protokołu RDP. Równocześnie prowadzone były kolejne działania odwracające uwagę od czynności mających na celu przejęcie serwera systemu sterowania i nadzoru w kluczowym z oddziałów. Między innymi przeprowadzony był atak, w wyniku którego przesłano sfałszowaną nominację (w tym wypadku zawierającą informacje i prognozę zużycia gazu. Było to możliwe w wyniku przejęcia danych dostępowych do skrzynki pocztowej jednego z pracowników.
7.	Na przejętym komputerze operatora systemu sterowania i nadzoru odnaleziono aplikację Telview (aplikacja zdalnego zarządzania serwerem systemu sterowania i nadzoru), która umożliwiła sterowanie zaworami krytycznej dla międzynarodowego przesyłu gazu. Aby tego dokonać wcześniej zmieniono odpowiednie uprawnienia atakującego w przejętym systemie Active Directory.
8.	Mając dostęp do systemu sterowania i nadzoru, w krytycznym oddziale został zamknięty zawór gazowy, co odpowiadało zdarzeniu co było ścisłą realizacją zakładanego scenariusza.

[1] http://pl.wikipedia.org/wiki/ARP_Spoofing
[2] http://pl.wikipedia.org/wiki/MITM