Deloitte.

FUNDACJA bezpieczna cyberprzestrzeń

RCB Rządowe Centrum Bezpieczeństwa

CYBER-EXE POLSKA 2013

RAPORT

CYBER-EXE POLSKA 2013

RAPORT Z ĆWICZENIA W ZAKRESIE OCHRONY PRZED ZAGROŻENIAMI Z CYBERPRZESTRZENI DLA POLSKIEGO SEKTORA BANKOWEGO

PRZYGOTOWANIE, PRZEBIEG, ANALIZA, WNIOSKI I REKOMENDACJE.

Celem ćwiczenia Cyber-EXE Polska 2013 było zbadanie zdolności i przygotowanie organizacji do identyfikacji zagrożeń w obszarze bezpieczeństwa teleinformatycznego oraz współpracy w ramach sektora bankowego w odniesieniu do zaleceń Rekomendacji Komisji Nadzoru Finansowego ze stycznia 2013 r., dotyczącej zarządzania obszarami technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego w bankach.

Spis treści

Cyber-Exe Polska 2013 dowiodło, że procedury i wyposażenie są warunkiem koniecznym, ale niewystarczającym, by nawet duża organizacja mogła sprostać zaawansowanemu atakowi teleinformatycznemu. Podczas reakcji na cyberatak istotną rolę odgrywa także doświadczenie pracowników, ich kreatywność i osobiste zaangażowanie oraz zdolność do koordynacji działań w sytuacjach kryzysowych.

1 Wstęp

Ćwiczenia są jedną z najskuteczniejszych form przygotowania do reakcji organizacji 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, głównie przy podejmowaniu i realizacji określonych decyzji oraz kierowaniu podległymi ogniwami.

W raporcie znajdą Państwo odpowiedź na pytanie, w jaki sposób praktycznie przygotowano i przeprowadzono ćwiczenie oraz, co najważniejsze, wnioski i rekomendacje sformułowane na podstawie zaobserwowanych reakcji uczestników na zdarzenia zaplanowane w scenariuszu ćwiczenia.

Mimo, iż do tej pory nie odnotowano przypadków skomasowanych, równolegle przeprowadzanych w tym samym czasie ataków na kilka instytucji finansowych, zagrożenia z cyberprzestrzeni nie są dla sektora bankowego nowością. Od wielu lat sektor ten jest liderem we wprowadzaniu w życie nowoczesnych rozwiązań technologicznych. Doświadczenie (także z rzeczywistych incydentów) umożliwiło wypracowanie szeregu procedur oraz technicznych systemów zabezpieczeń.

Ćwiczenia Cyber-Exe Polska 2013 dowiodły, że procedury i wyposażenie są warunkiem koniecznym, ale nie wystarczającym, by nawet duża organizacja mogła sprostać zaawansowanemu atakowi teleinformatycznemu. Podczas reakcji na cyberatak istotną rolę odgrywa także doświadczenie pracowników, ich kreatywność i osobiste zaangażowanie oraz zdolność do koordynacji działań w sytuacjach kryzysowych. W związku z tym kompetencje pracowników odpowiedzialnych za reagowanie na zdarzenia związane z cyberatakiem powinny iść w parze z poziomem wiedzy potencjalnych adwersarzy.

Ćwiczenie pokazało, że korzyści dla całego sektora bankowego może przynieść zacieśnienie operacyjnej współpracy między bankami na wypadek zajścia cyberataków. W sytuacji występowania konkurencji pomiędzy bankami niezbędne jest uregulowanie zasad takiej współpracy. Regulacja powinna obejmować w szczególności:

- zasady wymiany danych operacyjnych, w tym warunki, sposoby i zakres dzielenia się informacją oraz ochronę tej informacji,
- zasady udzielania wsparcia w odpieraniu ataku, w tym warunki jego udzielenia, role i odpowiedzialność współpracujących.

Wydaje się, że ze względu na zasięg swojego działania, podmiotem predestynowanym do opracowania takich rekomendacji jest Związek Banków Polskich, natomiast wdrożenie rekomendacji powinno nastąpić w drodze wprowadzenia przez wszystkie banki odpowiednich przepisów i regulacji wewnętrznych.

Wyzwaniem dla sektora jest zmapowanie zależności od dostawców zewnętrznych. W kontekście cyberprzestrzeni trzeba pamiętać, że korzystanie z usług oferowanych przez podmioty zewnętrzne, poza oczywistymi korzyściami, stanowi także potencjalne źródło zagrożeń trudnych do wykrycia, mogących mieć poważne konsekwencje dla sektora bankowego.

Wszyscy uczestniczy ćwiczenia wskazali na korzyści wyniesione z udziału w przedsięwzięciu. Cyber-Exe Polska 2013 zademonstrowało, że regularnie przeprowadzane ćwiczenia są szansą na osiągnięcie większej dojrzałości organizacji oraz zapewnienie sobie i innym bezpieczniejszego środowiska pracy, zaś wyciągnięte wewnętrznie wnioski mogą przyczynić się do natychmiastowej poprawy zidentyfikowanych luk.

Fot. 1. Ostatnie przygotowania do rozpoczęcia ćwiczenia CEP13.

2 Ćwiczenie

2.1 Idea ćwiczenia ochrony w cyberprzestrzeni

Ćwiczenie Cyber-EXE Polska 2013 jest kontynuacją inicjatywy organizacji polskich ćwiczeń z ochrony w cyberprzestrzeni, które po raz pierwszy zorganizowane zostały w Polsce w 2012 roku.

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. Organizatorzy cyklu ćwiczeń Cyber-EXE Polska zdecydowali się w sposób aktywny włączyć w ten nurt. 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[1]. Niektóre rekomendacje zachęcały do organizacji podobnych ćwiczeń na poziomie krajowym, jak również do działań na rzecz udziału w ćwiczeniach nie tylko przedstawicieli sektora publicznego, ale także podmiotów reprezentujących sektor prywatny. Dodatkową motywacją były udane ćwiczenia Cyber-EXE Polska 2012[2].

2.2 Geneza ćwiczenia Cyber-EXE Polska 2013

Po pozytywnych doświadczeniach związanych z ćwiczeniem Cyber-EXE Polska 2012 uczestnicy zgłosili chęć kontynuacji tej inicjatywy. Krytyczne znaczenie systemów teleinformatycznych w sektorze bankowym i szczególna rola tego sektora dla indywidualnych odbiorców sprawiły, że był on naturalnym kandydatem do roli pola doświadczalnego następnego ćwiczenia.

Dzięki przychylnemu wsparciu organizatora ćwiczenia przez podmioty publiczno-prywatne, tj. Rządowe Centrum Bezpieczeństwa i firmę doradczą Deloitte i duże zainteresowanie banków uczestnictwem w przedsięwzięciu pomysł organizacji ćwiczenia mógł być zrealizowany.

2.3 Organizatorzy i partnerzy ćwiczenia

Organizatorem ćwiczenia Cyber-EXE Polska 2013 była Fundacja Bezpieczna Cyberprzestrzeń. Partnerami organizacyjnymi było Rządowe Centrum Bezpieczeństwa oraz firma doradcza Deloitte.

2.4 Uczestnicy ćwiczenia

Do ćwiczenia przystąpiło sześć banków, które stanowiły reprezentatywną dla sektora grupę, tak pod względem ich typów, formy własności, jak i udziału w świadczeniu usług drogą elektroniczną.

1. „Cyber Europe 2010 – Evaluation Report" - http://www.enisa.europa.eu/activities/Resilience-and-CIIP/cyber-crisis-cooperation/cyber-europe/ce2010/ce2010report
2. Więcej informacji o ćwiczeniu Cyber-EXE Polska 2012 w raporcie: http://cybsecurity.org/raport-cyber-exe-polska-2012/

2.5 Patroni ćwiczenia

Wydarzenie uzyskało poparcie instytucji związanych z sektorem finansowym. Patronami ćwiczenia zostały następujące podmioty:

- Ministerstwo Finansów,
- Narodowy Bank Polski,
- Komisja Nadzoru Finansowego,
- Związek Banków Polskich.

Przedstawiciele powyższych instytucji jednocześnie zostali bezpośrednimi obserwatorami ćwiczenia.

2.6 Zespół projektowy

Zespół projektowy stanowili przedstawiciele wszystkich podmiotów zaangażowanych w organizację ćwiczenia oraz uczestniczących banków. W ramach prowadzonych przygotowań zespół projektowy podzielony został na grupy zadaniowe odpowiedzialne za wydzielone aktywności. Utworzono następujące grupy zadaniowe:

- Grupa SCENARIUSZ – odpowiedzialna za przygotowanie szczegółowego scenariusza ćwiczenia,
- Grupa MEDIALNA – odpowiedzialna za koordynację informowania o ćwiczeniu na zewnątrz zespołu projektowego oraz przygotowanie warstwy medialnej ćwiczenia,
- Grupa TECHNICZNA – odpowiedzialna za przygotowanie warstwy technicznej ćwiczenia, w tym systemu raportowania oraz wizualizacji przebiegu ćwiczenia,
- Grupa LOGISTYKA – odpowiedzialna za przygotowanie zaplecza logistycznego do przeprowadzenia ćwiczenia.

Fot. 2. Maciej Pyznar (RCB) przedstawia przebieg ćwiczenia obserwatorom. Są wśród nich przedstawiciele MF, NBP, KNF i ZBP.

3 Cele ćwiczenia Cyber-EXE Polska 2013

Celem głównym ćwiczenia było zbadanie zdolności i przygotowanie organizacji do identyfikacji zagrożeń w obszarze bezpieczeństwa teleinformatycznego, odpowiedzi na nie oraz współpracy w ramach sektora bankowego w odniesieniu do zaleceń Rekomendacji D Komisji Nadzoru Finansowego ze stycznia 2013 r. Poza celem ogólnym konieczne stało się sformułowanie celów szczegółowych. Rekomendacja D zawiera listę 22 rekomendacji, zatem ćwiczenie nie mogło uwzględnić wszystkich. Dlatego cele szczegółowe obejmowały:

A. **Sprawdzenie zdolności reakcji organizacji na atak teleinformatyczny:**
- sprawdzenie istniejących planów i procedur zarządzania,
- identyfikację potrzeb uzupełnienia planów i procedur zarządzania, ich aktualizacji lub stworzenia nowych,
- sprawdzenie współpracy i komunikacji wewnątrz organizacji,
- sprawdzenie poziomu świadomości oraz skuteczności działania pracowników banków w zakresie reagowania na nietypowe zdarzenia, w szczególności zagrożenia z cyberprzestrzeni.

B. **Zidentyfikowanie zależności i współzależności pomiędzy bankami oraz regulatorami i innymi podmiotami rynku finansowego.**

C. **Sprawdzenie komunikacji między bankami i regulatorami oraz innymi podmiotami rynku finansowego:**
- sprawdzenie, czy występuje wymiana informacji o zagrożeniach,
- sprawdzenie jakości i przydatności wymienianych informacji.

4 Proces organizacji ćwiczenia

4.1 Faza identyfikacji

W tej fazie zostały ustalone podstawowe cele ćwiczenia oraz lista jego uczestników. W sformułowaniu celów ćwiczenia pomocna okazała się Rekomendacja D Komisji Nadzoru Finansowego dotycząca zarządzania obszarami technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego w bankach, wydana w styczniu 2013 r. Pomogła ona wyznaczyć ramy i zakres tematyczny Cyber-EXE Polska 2013, a także, w związku z tym, że realizacja zaleceń Komisji Nadzoru Finansowego jest jednym z głównych zadań dla środowiska bankowców w roku 2014, stała się ona również katalizatorem decyzji banków o uczestnictwie w ćwiczeniu. Faza ta obejmowała także określenie przybliżonego obszaru tematycznego ćwiczenia.

4.2 Faza planowania

W trakcie fazy planowania precyzyjnie określono obszar tematyczny ćwiczenia, który następnie został opisany szczegółowo w postaci scenariusza. Praca nad scenariuszem toczyła się równolegle w dwóch wątkach, w których przewidywany był rozwój sytuacji. W tej fazie został wybrany przez uczestników ostateczny model przeprowadzenia ćwiczenia oraz lista uczestniczących wewnętrznie komórek organizacyjnych i stanowisk. Ważnym elementem fazy planowania było ustalenie organizacyjnych i technicznych zasad przeprowadzenia ćwiczenia, w tym przydzielenia ról związanych z zarządzaniem ćwiczeniem oraz opracowanie instrukcji.

W trakcie fazy planowania w każdym z banków przeprowadzono wewnętrzne szkolenia oparte na instrukcji ćwiczenia przygotowanej przez organizatora i partnerów. W praktyce cały proces przygotowania do ćwiczenia był koordynowany przez moderatora bankowego.

Fot. 3. Widok ze stanowiska zespołu technicznego ćwiczenia CEP13.

4.3 Faza przeprowadzenia

W trakcie tej fazy przeprowadzono zasadnicze ćwiczenie. Było one poprzedzone próbą generalną ćwiczenia (tzw. dry run), podczas której zespół planistyczny „przeszedł" przez scenariusz, dokonując ostatnich korekt. Na tydzień przed rozpoczęciem ćwiczenia przekazano jego uczestnikom instrukcję.

Próby generalne miały istotny wpływ na końcowy kształt ćwiczenia i sprawność jego przeprowadzenia. Odbyły się dwie takie próby:

Pierwszą próbę typu dry run przeprowadzono w dniu 18 września 2013 roku. W jej trakcie wszystkie osoby zaangażowane w przygotowanie ćwiczenia zasymulowały jego przebieg, odgrywając potencjalne zachowania poszczególnych osób i komórek organizacyjnych, których uczestnictwo było przewidziane w ćwiczeniu. Dodatkowo ćwiczenie miało istotny wpływ na ostateczne decyzje dotyczące scenariusza ćwiczenia, gdyż pokazało jego braki i pozwoliło na przygotowanie korekt.

Druga próba typu dry run odbyła się w przeddzień ćwiczenia. Jej celem było przede wszystkim przećwiczenie wszystkich aspektów organizacyjnych zdarzenia. Ćwiczono komunikację pomiędzy moderatorami bankowymi i moderatorem głównym, sposób wypracowywania decyzji dotyczących przebiegu ćwiczenia, udziału zespołu technicznego, ze szczególnym obowiązkiem dokumentacji przebiegu ćwiczenia i jego wizualizacji.

4.4 Faza oceny

W trakcie tej fazy dokonano podsumowania ćwiczenia i przygotowano końcowy raport. Istotnym elementem pracy było przygotowanie i przekazanie uczestnikom ćwiczenia ankiety ewaluacyjnej. Stała się ona podstawą do opracowania wniosków i wynikających z nich rekomendacji. Materiał dotyczący sporządzenia raportu końcowego został przygotowany przez wszystkich uczestników, którzy mogli zarówno zgłaszać swoje uwagi, jak i zatwierdzać całość dokumentacji końcowej.

Fot. 4. Centrum Koordynacji Ćwiczenia CEP13. Na sali moderatorzy bankowi, ewaluator, moderatorzy główny i pomocniczy oraz zespół techniczny.

5 Scenariusz ćwiczenia

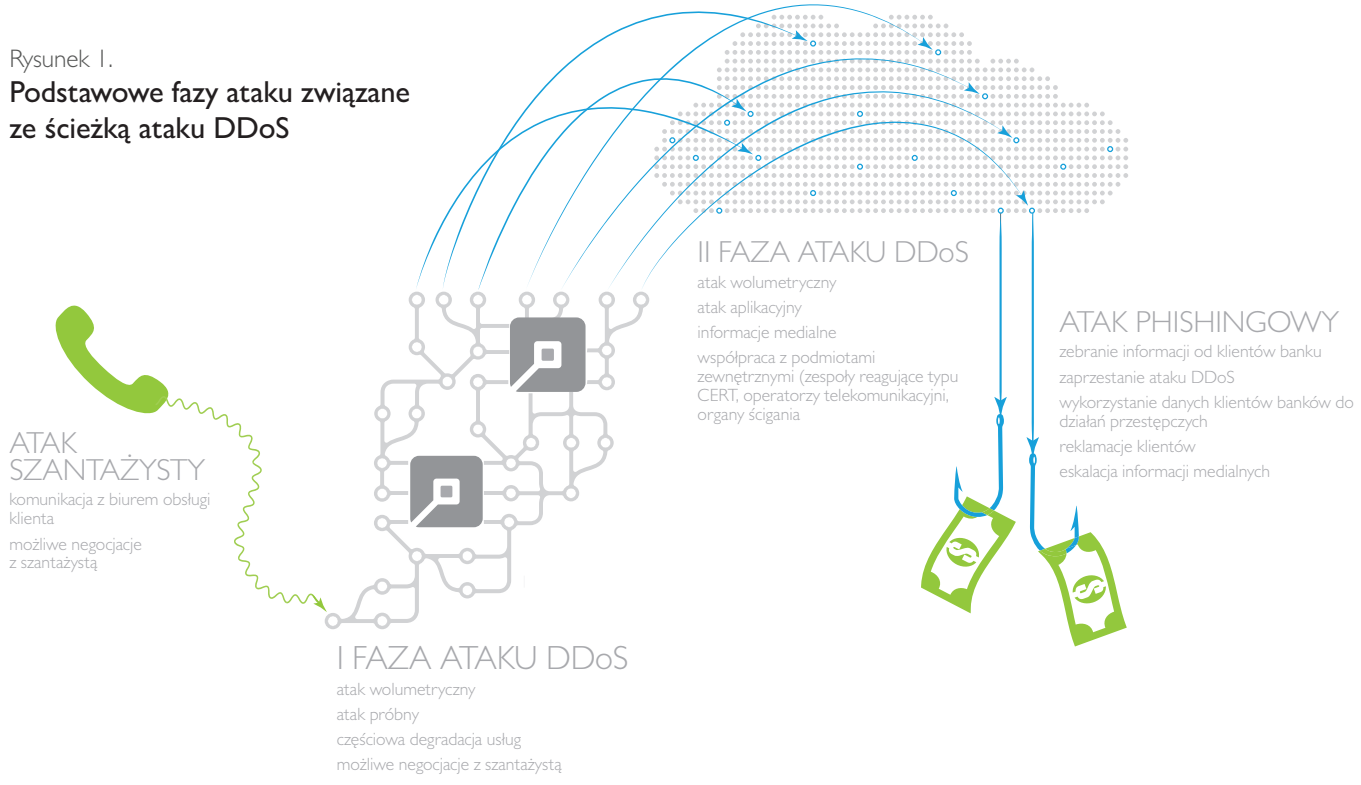
Scenariusz ćwiczenia powstał na podstawie najbardziej istotnych dla sektora bankowego typów zagrożeń. Przy jego tworzeniu uwzględniono również możliwości zrealizowania celów ćwiczenia. Scenariusz, zdaniem uczestników, był bardzo ambitny. Symulowana sytuacja wymagała od uczestników dużego zaangażowania i szybkich reakcji, powodując w założeniu bardzo duże obciążenie pracą i stres.

Scenariusz ćwiczenia w praktyce składał się z dwóch ścieżek tematycznych. Związane one były z rozproszonymi atakami prowadzącymi do blokady serwisów bankowych (ścieżka ataku DDoS) oraz atakami dedykowanymi prowadzącymi do wycieku poufnych informacji z infrastruktury bankowej (ścieżka ataku APT). Warto dodać, że ścieżka ataku DDoS zawierała w sobie również atak typu phishing na klientów banku.

5.1 Ścieżka ataku DDoS (Distributed Denial of Service)

Ścieżka ataku DDoS składała się z kilku faz przedstawionych na poniższym rysunku.

Rysunek 1.
Podstawowe fazy ataku związane ze ścieżką ataku DDoS



Faza „Atak szantażysty" – w początkowej fazie doszło do kontaktu szantażysty z komórką bankową odpowiedzialną z kontakt z klientem. Tym kanałem szantażysta przekazał swoje żądania wobec banku, będące próbą wymuszenia okupu finansowego w zamian za odstąpienie od planów ataku typu DDoS, który miał prowadzić do blokady serwisu bankowości elektronicznej.

Faza „I faza ataku DDoS" – atakujący przystępował do uruchomienia ataku wolumetrycznego (tj. prowadzącego do wysycenia łącza dostępowego) na serwis bankowości elektronicznej. W praktyce oznaczało to atak próbny, który doprowadził tylko do częściowej degradacji usług, a jego celem miało być przekonanie banku do pozytywnej, z punktu widzenia atakującego, reakcji na próbę szantażu.

Faza „II faza ataku DDoS" – w tej fazie do ataku wolumetrycznego został dołączony atak aplikacyjny, który doprowadził do całkowitej blokady usług bankowości elektronicznej. Nastąpiła też eskalacja problemów związanych z pojawieniem się serii informacji medialnych oraz informacji przekazywanych przez klientów banków, mówiących o problemach w sektorze bankowym. W tej fazie istotną rolę odgrywała komunikacja pomiędzy bankami a podmiotami zewnętrznymi, takimi jak operatorzy telekomunikacyjni, zewnętrzne zespoły typu CERT czy organy ścigania.

Faza „Atak phishingowy" – atakujący wykorzystał niedostępność prawdziwego serwisu bankowego do „reklamowania" oszukanego serwisu, który udawał rzeczywisty. W ten sposób, po logowaniu się klientów banku w podstawionym serwisie, atakujący zbierał dane autoryzacyjne do serwisów bankowych, a następnie zaczął je wykorzystywać w dalszej działalności przestępczej. Rezultatem działalności była kradzież środków finansowych z kont klientów banków. Taki przebieg sytuacji prowadził do dalszej eskalacji problemów, na co składało się również pojawianie się reklamacji klientów, informacji o problemach publikowanych w serwisach internetowych i informacji medialnych.

Fot. 5. Organizatorem ćwiczenia CEP13 była FBC, partnerami Deloitte i RCB.

5.2 Ścieżka ataku APT (Advanced Persistant Threat)

Ścieżka ataku APT składała się z kilku faz przedstawionych na poniższym rysunku.

Rysunek 2.
Podstawowe fazy ataku związane ze ścieżką APT

Faza „Publikacja informacji poufnej" – w tej fazie doszło do publikacji dziennikarskiej informacji dotyczącej wycieku danych z jednego z banków. Informacja stanowiła część całościowej informacji o poufnych zasobach banków, które dostały się w ręce szantażysty. Zgodnie z informacją od szantażysty zatrzymanie zapowiedzianych dalszych publikacji było możliwe tylko w przypadku zapłacenia okupu.

Faza „Analiza ataku" – główne czynności skupiały się wokół analizy ataku, który wystąpił. Analiza odbywała się na bazie zebranych informacji technicznych, z wykorzystaniem wsparcia podmiotów zewnętrznych (np. zewnętrznych zespołów typu CERT czy operatorów telekomunikacyjnych). Wysiłkom towarzyszyły pojawiające się seryjnie informacje medialne, które dodatkowo utrudniały zarządzanie sytuacją kryzysową.

Faza „Współpraca z podmiotami zewnętrznymi" – w tej fazie, zgodnie z nazwą, najistotniejsze było nawiązanie współpracy z podmiotami zewnętrznymi. Oprócz wspomnianych w opisie fazy „Analiza ataku" najistotniejszą rolę odgrywały same banki. Celem współpracy było pozyskanie i wymiana informacji, co miało zwiększać prawdopodobieństwo identyfikacji źródła ataku oraz skuteczną politykę informacyjną wobec klientów banków.

6 Przebieg ćwiczenia

6.1 Informacje podstawowe

Ćwiczenie CYBER-EXE Polska 2013 zostało przeprowadzone w dniu 29 października 2013 r. w godzinach 09.00–17.00. Cyber-EXE Polska 2013 było rozproszonym ćwiczeniem sztabowym. Uczestnicy ćwiczenia podzieleni byli na dwie grupy. Pierwsza grupa znajdowała się w Centrum Kontroli Ćwiczenia (CKC). Druga pozostawała we własnych lokalizacjach.

W grupie pierwszej znalazły się osoby, które odgrywały następujące role:

- moderator główny,
- koordynator oceny,
- moderatorzy bankowi,
- zespół techniczny,
- zespół medialny.

Druga grupa obejmowała:

- ćwiczących,
- służby prasowe (patrz: 6.7 Przebieg ćwiczenia w warstwie medialnej),
- inne podmioty.

6.2 Modele przeprowadzenia ćwiczenia

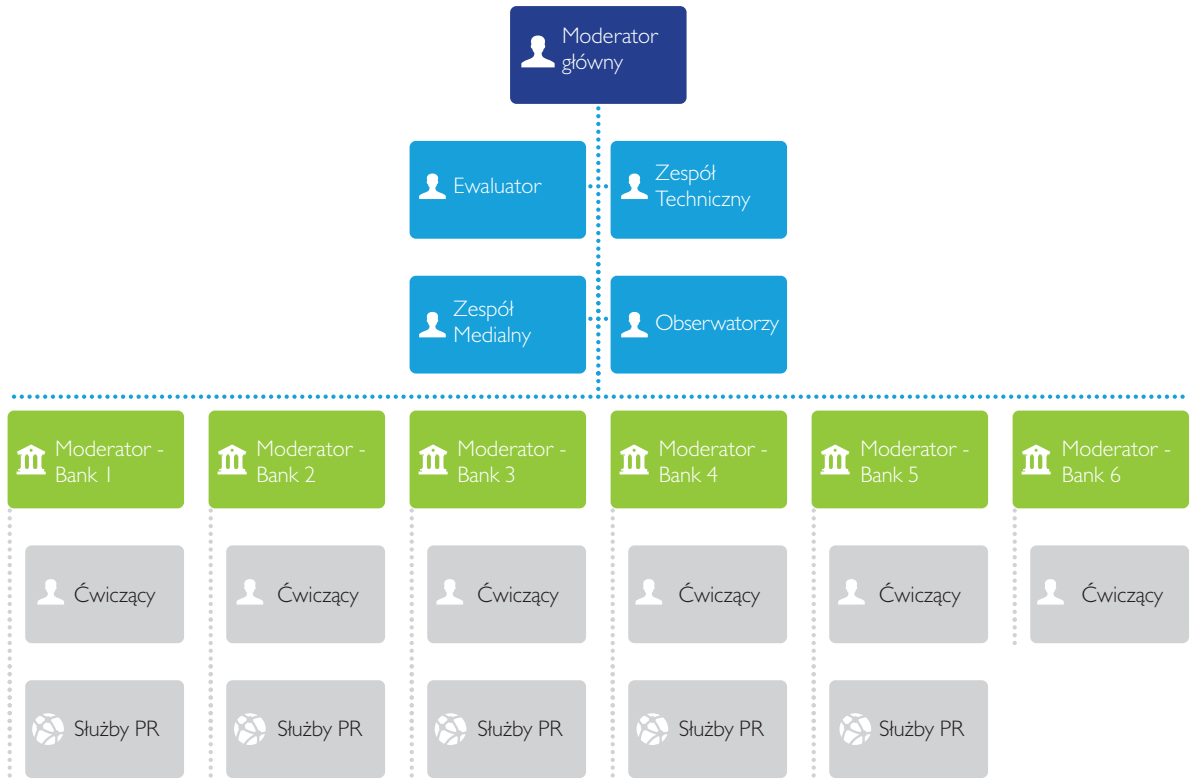
W fazie planowania ćwiczenia Cyber-EXE Polska 2013 uczestnicy zdecydowali się na przeprowadzenie go wg trzech modeli:

1. Zespołowe ćwiczenie sztabowe – uczestnicy byli zorganizowani w zespół uprzednio powiadomiony o terminie, ogólnym zakresie oraz planowanym czasie trwania ćwiczenia. Zespół przebywał w jednym pomieszczeniu, a komunikacja między członkami zespołu miała charakter otwarty,
2. Model częściowej symulacji – uczestnicy otrzymali informacje o zbliżającym się ćwiczeniu, swoim udziale w nim, ale nie otrzymali dodatkowych danych o samym scenariuszu, przedmiocie ćwiczenia czy oczekiwanej roli. Ćwiczący przebywali przy swoich stanowiskach pracy, realizując również inne codziennie obowiązki służbowe,
3. Model pełnej symulacji – uczestnicy otrzymali informacją o ćwiczeniach już w trakcie wydarzenia (np. w formie informacji dołączonych do zdarzeń – „UWAGA! TO TYLKO ĆWICZENIE"). Grupa uczestników nie była zdefiniowana i mogła się dynamicznie rozszerzać zależnie od przebiegu ćwiczenia w danej organizacji.

Wybór modelu był zależny od wewnętrznych oczekiwań uczestników ćwiczenia. Wpływał również na zasady postępowania oraz przygotowania i przeprowadzenia ćwiczenia w organizacji.

6.3 Struktura organizacyjna ćwiczenia

Rysunek 3.
Struktura organizacyjna ćwiczenia



6.3.1 Moderator główny

Moderatorem głównym CEP13 był przedstawiciel FBC. Moderatorowi przypisane zostały następujące zadania:

- koordynacja całości przebiegu CEP13,
- podejmowanie decyzji o uruchamianiu kolejnych zdarzeń scenariusza; w przypadku zdarzeń warunkowych decyzja jest podejmowana w porozumieniu z moderatorem bankowym,
- współpraca z moderatorami bankowymi poszczególnych banków w celu przekazywania informacji o przebiegu zdarzeń oraz reakcjach na nie, opierając się na ustalonym zakresie informacji,
- rozstrzyganie wątpliwości dotyczących przebiegu CEP13,
- odbieranie raportów z przebiegu CEP13 od moderatorów bankowych,
- przekazywanie informacji obserwatorom ćwiczenia CEP13,
- odgrywanie działań podmiotów nieuczestniczących w ćwiczeniu oraz zewnętrznych systemów teleinformatycznych.

6.3.2 Ewaluator

Ewaluatorem CEP13 był przedstawiciel RCB. Ewaluatorowi przypisane zostały następujące zadania:

- stała obserwacja przebiegu ćwiczenia,
- rejestracja przebiegu zdarzeń służących przyszłej ocenie ćwiczenia,
- wsparcie moderatora głównego w realizacji jego zadań,
- współpraca z moderatorami bankowymi w celu zebrania obserwacji związanych z oceną przebiegu CEP13[3],
- przekazywanie informacji obserwatorom ćwiczenia CEP13 (patrz: 6.8 Obserwatorzy ćwiczenia).

6.3.3 Moderatorzy bankowi

Moderatorzy bankowi są wyznaczeni przez poszczególne banki biorące udział w ćwiczeniu CEP13. Osobie moderatora bankowego przypisane zostały następujące zadania:

- koordynacja ćwiczenia CEP13 w danym banku, a w szczególności:
  - organizacja i przeszkolenie zespołu uczestniczącego w ćwiczeniu ze strony banku, w tym przygotowanie wewnętrznych instrukcji dla uczestników ćwiczenia,
  - koordynacja ćwiczenia z kierownictwem,
  - przekazywanie wprowadzeń ze scenariusza ćwiczenia uruchamianych przez moderatora głównego,
  - symulowanie działania wewnętrznych systemów teleinformatycznych danego banku,
  - monitorowanie przebiegu ćwiczenia w wybranym banku oraz reakcja na ewentualne zakłócenia jego przebiegu,
  - przekazywanie informacji o przebiegu ćwiczenia w banku na podstawie ustalonego zakresu informacji,
- współpraca z moderatorem głównym oraz ewaluatorem ćwiczenia CEP13,
- opcjonalnie – wyznaczenie i współpraca z ewaluatorem bankowym, w sytuacji jego wyznaczenia.

3. Moderator bankowy mógł wskazać dodatkową osobę na stanowisko ewaluatora bankowego, któremu byłyby przypisane zadania związane z obserwacją przebiegu CEP13 w danym banku.

6.3.4 Zespół techniczny

Zespół techniczny składał się z przedstawicieli firmy Deloitte oraz FBC. Jego zadaniem było przygotowanie techniczne i logistyczne ćwiczenia. Przede wszystkim zespół techniczny był odpowiedzialny za:

- organizację logistyczną ćwiczenia (przygotowanie sali i urządzeń koniecznych do przeprowadzenia ćwiczenia),
- przygotowanie i obsługę systemu wizualizacji CEP13,
- stałą współpracę z moderatorem głównym i ewaluatorem CEP13, w celu prezentowania w systemie wizualizacji CEP13 bieżącego przebiegu CEP13 dla poszczególnych banków,
- odnotowanie szczegółów dotyczących przebiegu ćwiczenia, tj. czasów wystąpienia poszczególnych zdarzeń reprezentowanych w systemie wizualizacji CEP13,
- wsparcie moderatora w przygotowaniu technicznych szczegółów wprowadzeń scenariusza i ewentualnie odpowiedzi zewnętrznych systemów teleinformatycznych,
- wsparcie dla zespołu medialnego przy technicznym utrzymaniu systemu CISKOM (patrz: 6.7 Przebieg ćwiczenia w warstwie medialnej).

6.3.5 Zespół medialny

Zespół medialny składał się z przedstawicieli Deloitte, FBC i RCB. Był on odpowiedzialny za:

- przygotowanie komunikatów medialnych związanych ze scenariuszem ćwiczenia CEP13,
- współpracę z moderatorem głównym w celu publikowania komunikatów medialnych w systemie CISKOM, zgodnie z przebiegiem zdarzeń,
- reagowanie na komunikaty publikowane przez służby PR banków biorących udział w ćwiczeniu.

6.3.6 Ćwiczący

W zależności od przyjętego modelu przeprowadzenia ćwiczenia brali w nim udział przedstawiciele wyznaczonych komórek organizacyjnych wchodzący w skład zespołu ćwiczeniowego lub pracownicy poszczególnych banków, którzy byli zaangażowani w realizację działań przewidzianych w scenariuszu CEP13.

6.3.7 Służby public relations

Służby public relations (dalej: PR) stanowiły szczególny typ uczestników ćwiczenia CEP13 reprezentujących zaangażowane w wydarzenie banki. Służby korzystały z dostępu do systemu CISKOM, przez co informacja o konsekwencjach zdarzeń, jakie wystąpiły podczas ćwiczenia, docierały do nich niezależnie od informacji, które przekazywać im mogli uczestnicy oraz moderatorzy bankowi w ich organizacjach. Dzięki temu służby PR banków mogły przekazywać swoje decyzje poprzez publikacje własne w systemie CISKOM, będące symulacją ich zachowań na zewnątrz organizacji, jak również informować o swoich decyzjach innych uczestników ćwiczenia i własnych moderatorów bankowych.

6.3.8 Inne podmioty

Innymi podmiotami były organizacje nie biorące aktywnego udziału w ćwiczeniu, a które, zdaniem danego banku, mogły uczestniczyć w rozwiązaniu problemu zawartego w scenariuszu ćwiczenia. Komunikacja z tymi organizacjami była realizowana z udziałem moderatora głównego ćwiczenia, którego zadaniem było odgrywanie roli innych podmiotów.

6.4 Zarządzanie zdarzeniami i komunikacja w trakcie ćwiczenia

Ćwiczenia przebiegały zgodnie z wcześniej przygotowanym fikcyjnym scenariuszem. Zaplanowane w scenariuszu zdarzenia wraz z rozwojem ćwiczenia były systematycznie uruchamiane przez moderatora głównego.

Zdarzenia przewidziane scenariuszem podzielone były na dwie grupy:

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

W trakcie ćwiczenia założono, że banki będą wykorzystywać standardowe i na co dzień stosowane w tego typu organizacjach środki komunikacji.

Fot. 6. Stanowisko zarządzania ćwiczeniem. Od lewej - Maciej Pyznar (RCB), Mirosław Maj (FBC), Paweł Chwiećko (Citi).

6.4.1 Komunikacja pomiędzy moderatorem głównym a moderatorami bankowymi

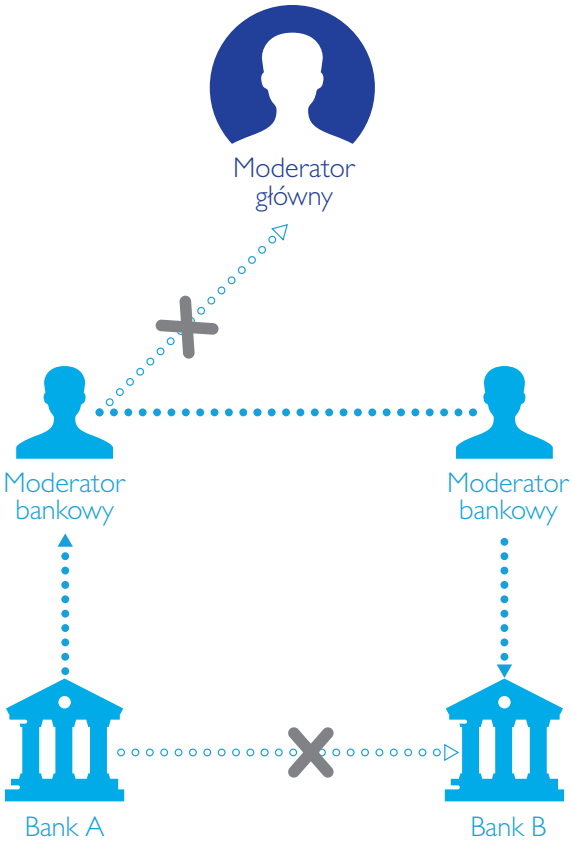
Komunikacja pomiędzy moderatorem głównym a moderatorami bankowymi prowadzona była dla każdego z banków oddzielnie. Przybierała ona następujące formy:

Forma komunikacji	Kierunek komunikacji	Opis
Wprowadzenie (z ang. inject)	Moderator główny ↓ Moderator bankowy	Podstawowa informacja dotycząca zdarzeń przewidzianych w scenariuszu. Stanowiła podstawę do dalszego postępowania moderatora bankowego wobec innych uczestników ćwiczenia z banku, który reprezentował. Dalszy sposób procedowania zdarzenia realizowany był metodami przyjętymi przez każdy z ćwiczących banków.
Konsultacja	Moderator główny ↕ Moderator bankowy	Komunikacja mająca na celu rozwiewanie wątpliwości dotyczących przebiegu ćwiczenia i udzielanie odpowiedzi na szczegółowe pytania na ten temat.
Komunikat	Moderator bankowy ↓ Moderator główny	Komunikat przekazywany w sytuacji, kiedy moderator bankowy uzna, że informacja dotycząca ćwiczenia w danym banku może mieć istotny wpływ na jego dalszy przebieg, a przekazanie wiadomości w postaci raportu może negatywnie wpłynąć na wydarzenie (głównie ze względu na opóźnienie przekazania tej informacji).
Raport	Moderator bankowy ↓ Moderator główny	Podstawowy sposób komunikacji pomiędzy moderatorem głównym i moderatorem bankowym. Wzór raportu stanowił załącznik do instrukcji ćwiczenia.

6.4.2 Komunikacja pomiędzy ćwiczącymi bankami

W trakcie ćwiczenia dopuszczona była komunikacja bezpośrednia pomiędzy uczestnikami. Odbywała się ona poprzez moderatorów bankowych. Kiedy uczestnik ćwiczenia z Banku A chciał skontaktować się z uczestnikiem ćwiczenia z Banku B, przekazywał informację do swojego moderatora bankowego (moderator bankowy Banku A). W informacji wskazywał dane dotyczące adresata (bank, stanowisko lub podmiot wewnątrz struktury organizacyjnej) oraz treść komunikatu. Moderator bankowy Banku A przekazywał tę informację do moderatora bankowego Banku B, a ten z kolei do uczestnika ćwiczenia w swoim banku (moderator główny był informowany o wystąpieniu komunikacji poprzez raport sytuacyjny). Przyjęcie takiej zasady komunikacji, choć odbiegające od zwyczajowo przyjętej, było niezbędne ze względu na konieczność jej dokumentacji na potrzeby ćwiczenia. W sytuacji, kiedy wskazany do komunikacji bank nie był uczestnikiem ćwiczenia CEP13, moderator bankowy Banku A postępował zgodnie z zasadami komunikacji przewidzianymi dla komunikacji z podmiotami nieuczestniczącymi w ćwiczeniu.

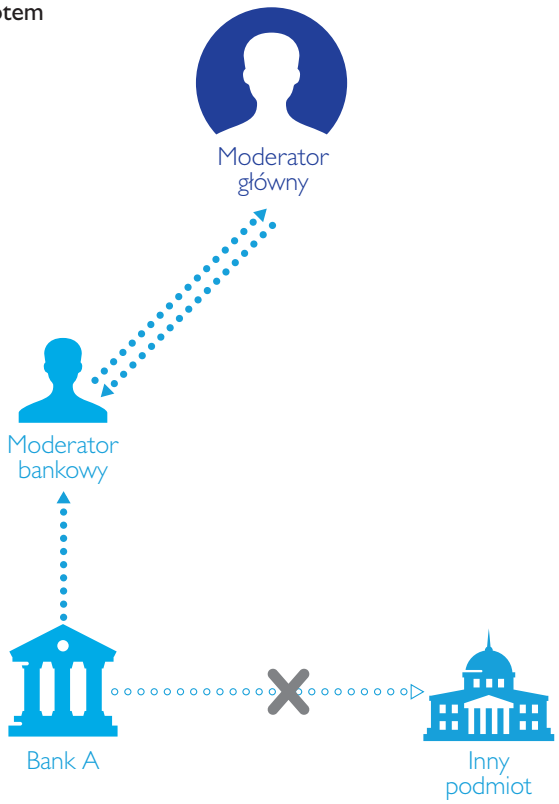
Rysunek 4.
Zasady komunikacji pomiędzy bankami



6.4.3 Komunikacja z innymi podmiotami

W trakcie ćwiczenia dopuszczona była komunikacja pomiędzy bankami a innymi podmiotami zewnętrznymi, które nie były uczestnikami CEP13. Role tych podmiotów były odgrywane przez moderatora głównego. Komunikacja odbywała się za pośrednictwem moderatorów bankowych. Kiedy uczestnik ćwiczenia z Banku A chciał skomunikować się z podmiotem X, to informację tę przekazywał do swojego moderatora bankowego (moderator bankowy Banku A). W informacji zawierał dane dotyczące adresata (nazwa podmiotu X, stanowisko lub podmiot wewnątrz struktury organizacyjnej) oraz treść komunikatu. Moderator bankowy Banku A przekazywał tę informację do moderatora głównego. Moderator główny przekazywał informację zwrotną, która następnie trafiała do nadawcy informacji pierwotnej.

Rysunek 5.
Zasady komunikacji pomiędzy bankiem a innym podmiotem



6.4.4 Wykorzystanie wewnętrznych i zewnętrznych systemów teleinformatycznych

CEP2013 nie odbywało się w warstwie technicznej, dlatego interakcja z wewnętrznymi i zewnętrznymi systemami teleinformatycznymi była symulowana przez moderatora – w zależności od sytuacji, bankowego lub głównego. Interakcja z systemem była inicjowana przez jego użytkownika wysłaniem e-maila na adres moderatora bankowego. W treści wiadomości użytkownik wpisywał nazwę systemu oraz zakres czynności, które chciałby wykonać. Jeśli operatorem systemu była organizacja ćwicząca, odpowiedź systemu była symulowana przez moderatora bankowego w wiadomości zwrotnej. Należało ją traktować jako komunikat z systemu, który w normalnych warunkach mógłby pojawić się na ekranie monitora. W przypadku, gdy operatorem systemu teleinformatycznego była organizacja zewnętrzna, komunikacja z tym systemem odbywała się zgodnie z zasadami komunikacji przewidzianymi dla komunikacji z podmiotami nieuczestniczącymi w ćwiczeniu (patrz: rozdział 6.4.2).

W swoich działaniach związanych z detekcją, analizą i ograniczeniem skutków cyberataku przedstawiciele banków korzystali z następujących klas produktów związanych z bezpieczeństwem teleinformatycznym:

- wewnętrzne systemy monitoringu zagrożeń,
- zewnętrzne systemy monitoringu zagrożeń,
- systemy wspomagające analizę ruchu sieciowego,
- systemy agregacji zdarzeń związanych z bezpieczeństwem teleinformatycznym,
- systemy typu firewall (w tym systemy dedykowane dla serwisów webowych),
- systemy obsługi incydentów naruszających bezpieczeństwo teleinformatyczne,
- systemy kontroli wycieku danych wrażliwych (tzw. Data Leakage Protecion/Prevention),
- własne systemy ochrony przed atakami DDoS,
- systemy ochrony przed atakami DDoS podmiotów trzecich (dostępne na zasadzie świadczenia usługi),
- systemy rejestracji zdarzeń (w tym rejestracji komunikacji głosowej z infolinią banku),
- systemy monitoringu realizowanych transakcji finansowych,
- systemy wspomagające analizę złośliwego oprogramowania,
- systemy archiwizacji danych,
- systemy ochrony przed propagacją złośliwego oprogramowania (w tym systemy antywirusowe).

6.5 Dokumentacja i monitoring przebiegu ćwiczenia

Podstawową formę dokumentacji i monitoringu przebiegu ćwiczenia stanowiły raporty sytuacyjne. Podzielono je na dwie grupy:

A. Raport sytuacyjny dla moderatora bankowego, zawierający m.in.:

- wewnętrzne komórki organizacyjne uczestniczące w reagowaniu na dane zdarzenie i dystrybucję informacji o zdarzeniu,
- podjęte działania,
- przewidywany rozwój wydarzeń,
- wykorzystanie wewnętrznych systemów teleinformatycznych.

Raport sporządzany był, w przypadku wyboru modelu z zespołem ćwiczeniowym, przez koordynatora tego zespołu, w odstępach czasu ustalonych przez moderatora bankowego.

B. Raport sytuacyjny dla moderatora głównego, zawierający m.in.:

- wewnętrzne komórki organizacyjne uczestniczące w reagowaniu na dane zdarzenie i dystrybucję informacji o zdarzeniu,
- informacje ogólne o podjętych działaniach,
- przewidywany rozwój wydarzeń,
- wykorzystanie zewnętrznych klas rozwiązań systemów teleinformatycznych,
- opis komunikacji na zewnątrz organizacji.

Raport sporządzany był przez moderatora bankowego w godzinnych odstępach czasu.

W przypadku wyboru modelu symulacji moderatorzy bankowi mieli zapewnioną kontrolę nad przebiegiem ćwiczenia poprzez możliwość obserwacji całości korespondencji wymienianej pomiędzy uczestnikami. Zostało to osiągnięte poprzez automatyczne przesyłanie kopii każdej wiadomości poczty elektronicznej. Ponadto, w związku z możliwością użycia w komunikacji wewnętrznej komunikacji telefonicznej, szczególne znaczenie miało informowanie moderatora bankowego o jej wykorzystaniu. Rozmowa telefoniczna pomiędzy uczestnikami ćwiczenia wewnątrz organizacji była udokumentowana poprzez wiadomość przesłaną pocztą elektroniczną do moderatora bankowego. W e-mailu uczestnik podawał następujące informacje:

1. Do kogo został wykonany telefon.
2. W jakiej sprawie (np. przekazanie polecenia, informacja, pytanie, prośba o wsparcie).
3. Dodatkowo dla zobrazowania przebiegu ćwiczenia w trakcie jego trwania przygotowano wizualizację, na której były prezentowane w uproszczonej formie raporty sytuacyjne, przekazywane moderatorowi głównemu ćwiczenia.

6.6 Przebieg ćwiczenia w warstwie komunikacji medialnej

Reakcja służb prasowych banków w przypadku ataków teleinformatycznych uwzględnionych w scenariuszu jest niezwykle istotna i czasami ma krytyczne znaczenie, gdyż w dużym stopniu kształtuje odbiór sytuacji przez klientów banku, a tym samym ich reakcje.

Warstwa komunikacji medialnej ćwiczenia Cyber-EXE Polska 2013 przeprowadzona została za pomocą internetowej strony komunikacji medialnej (CISKOM). Dostęp do tej strony (w postaci loginu i hasła) miały służby prasowe/PR banków. Strona internetowa składała się z dwóch części. W pierwszej ukazywały się informacje, które w sytuacji realnej byłyby przekazywane przez media (TV, radio, prasa, agencje informacyjne, portale internetowe i portale społecznościowe, itp.). Za informacje na tej części platformy odpowiadała występująca przy moderatorze głównym ćwiczenia grupa symulująca pracę mediów (osoby, które w trakcie ćwiczenia „udawały" dziennikarzy). W drugieja części strony internetowej służby prasowe/PR banków prezentowały swoje komunikaty i informacje oraz wszelką aktywność medialną w związku z sytuacją kryzysową. Ponadto grupa ds. mediów telefonicznie zadawala pytania i prosiła rzeczników banków o dodatkowe komentarze.

6.7 Obserwatorzy ćwiczenia

Obserwatorami ćwiczenia CEP13 byli przedstawiciele podmiotów, które objęły nad nim patronat honorowy, tj.:

- Ministerstwo Finansów,
- Narodowy Bank Polski,
- Komisja Nadzoru Finansowego,
- Związek Banków Polskich.

Obserwatorzy mieli wyznaczone pomieszczenie, w sali obok CKC, w którym udostępniony dla nich został obraz z sytemu wizualizacji ćwiczenia CEP13 oraz systemu CISKOM. Obserwatorzy w trakcie ćwiczenia otrzymywali informacje o najważniejszych faktach dotyczących jego przebiegu. Obserwatorzy nie byli obecni na całym CEP13. Godziny ich przebywania zostały ustalone pomiędzy nimi oraz organizatorem i partnerami ćwiczenia.

Fot. 7, Zespół medialny ćwiczenia CEP13. Od lewej - Anna Adamkiewicz (RCB), Katarzyna Madej (RCB), Joanna Makowska (Deloitte), Adrianna Maj (FBC).

Spotkaniu obserwatorów towarzyszyła żywa dyskusja, która toczyła się w kilku polemicznych nurtach:

- Bezpieczeństwo teleinformatyczne uważane było przez część dyskutantów jako element konkurencyjności, przez innych jako pole, na którym banki ze sobą nie konkurują, a wręcz współpracują. Poruszono konieczność edukacji banków w zakresie korzyści płynących z bardziej otwartej polityki informacyjnej na polu cyberbezpieczeństwa oraz konieczności prawnego uregulowania procesowych aspektów takiej współpracy.

- Zdaniem obserwatorów kluczowym elementem jest czynna i długoterminowa edukacja klientów w zakresie zagrożeń cyberbezpieczeństwa – rolę tę powinny przejąć wszystkie podmioty powiązane z sektorem finansowym.

- Rola Związku Banków Polskich w systemie ochrony cyberprzestrzeni, od edukacji klientów po aktywne przejmowanie funkcji związanych z reagowaniem na incydenty. Tym rozważaniom towarzyszyła ponownie dyskusja na temat braku regulacji prawnych i rozwiązań systemowych.

- Obserwatorzy byli zgodni co do potrzeby przeprowadzania cyklicznych ćwiczeń, które weryfikują poziom jakościowy systemu reagowania na występujące zagrożenia, co prowadzi do uszczelnienia systemów i procesów w poszczególnych bankach, a w konsekwencji do wzmocnienia całego systemu finansowego. Zdaniem obserwatorów niezwykle ważna jest regularność ćwiczeń, gdyż środowisko cyberprzestępczości jest zmienne i dynamicznie ewoluuje.

Fot. 8. Paweł Chwiećko (Citi) i Mirosław Maj (FBC) - moderator pomocniczy i moderator główny ćwiczenia EP13 (FBC).

7 Wnioski

7.1 Wnioski podstawowe

Uczestnicy ćwiczenia zgodnie stwierdzili, że jego cele zostały przez ich organizacje w pełni osiągnięte. Zdaniem ćwiczących było ono jak najbardziej przydatne, a scenariusz został określony jako realistyczny i dobrze odzwierciedlający założone cele. Najczęściej wskazywano na następujące korzyści wynikające z jego organizacji:

- przetestowanie istniejących procedur i identyfikacja niepokrytych nimi obszarów,
- sprawdzenie istniejących kanałów komunikacji wewnętrznej i zewnętrznej,
- sprawdzenie wiedzy i świadomości pracowników na temat zagrożeń,
- sprawdzenie zachowań w sytuacjach kryzysowych,
- weryfikacja relacji z podmiotami trzecimi,
- zdobycie doświadczenia w sytuacji kryzysowej,
- test współdziałania ze służbami prasowymi banków.

Uczestnicy wskazywali na fakt, że ćwiczenie mogłoby przynieść jeszcze więcej pozytywnych efektów, jeśli na uczestnictwo w nim zdecydowałoby się więcej podmiotów, zarówno banków, jak i innych istotnych podmiotów sektora finansowego, wśród których wymienili: Krajową Izbę Rozliczeniową, Narodowy Bank Polski, Komisję Nadzoru Finansowego, operatorów telekomunikacyjnych. Zaangażowanie tych ostatnich jest szczególnie ważne w sytuacji decyzji o realizacji ćwiczenia w warstwie technicznej.

Uczestnicy ćwiczenia zwrócili również uwagę, że dobrze byłoby, aby kolejne potencjalne edycje Cyber-EXE Polska zawierały elementy ćwiczenia przygotowanego na podstawie dedykowanej infrastruktury teleinformatycznej. Tego typu podejście nadałoby jeszcze większej realności ćwiczeniu, w większym stopniu zaangażowałoby bankowe służby techniczne i pozwoliłoby sprawdzić poziom odporności organizacji na zagrożenia z cyberprzestrzeni.

7.2 Wnioski dotyczące działań wewnętrznych banków

- Po stronie banków w ćwiczeniu brało udział średnio po około 10 osób reprezentujących komórki organizacyjne. W banku, który zastosował model pełnej symulacji, w ćwiczenie zaangażowanych było niemal dwukrotnie więcej komórek organizacyjnych.

- Zdecydowana większość uczestników wybrała model przeprowadzenia zajęć przez zespół ćwiczeniowy. Taki wybór ograniczał „nieprzewidziane" sytuacje, które podczas ćwiczenia mogłyby wpłynąć niekorzystnie na bieżące funkcjonowanie banków, oraz był łatwiejszy do zorganizowania. W przypadku wyboru modelu pełnej symulacji główną motywacją była chęć najbardziej realnego odzwierciedlenia sytuacji kryzysowej i działań podejmowanych przez pracowników.

- Znajomość procedur związanych z cyberatakiem i wynikającą z niego sytuacją kryzysową jest konieczna do sprawnego działania w czasie zdarzenia. Nie jest jednak warunkiem wystarczającym dla pełnego rozwiązania problemów, ponieważ nie wszystkie zdarzenia zawarte w scenariuszu były objęte procedurami. Istotną rolę odgrywa w tej sytuacji doświadczenie osób uczestniczących w reagowaniu, ich kreatywność i osobiste zaangażowanie oraz zdolność do koordynacji działań w sytuacjach kryzysowych.

- U wszystkich ćwiczących można było zaobserwować szybkie eskalowanie problemu wewnątrz organizacji, objawiające się dużą liczbą zaangażowanych wewnętrznych komórek organizacyjnych oraz podjęciem bez zbędnej zwłoki współpracy z zespołami prasowymi.

- Wraz z rozwojem sytuacji równie szybko podejmowane były decyzje o zwołaniu zespołów kryzysowych lub ciał podejmujących kluczowe decyzje.

- Można było zaobserwować szybkie zgłoszenia problemów do zespołów typu CERT i Policji.

- Procedury banków w praktyce angażowały wszystkie osoby niezbędne do działania w przypadku wystąpienia cyberataku.

- Kompetencje osób zaangażowanych w sytuację kryzysową oraz ich decyzyjność zostały wysoko ocenione. Osoby te wyczerpywały możliwości działania w ramach zakresu swoich kompetencji, a w przypadku takiej konieczności dokonywały eskalacji problemu lub sięgały po wsparcie zewnętrzne.

- Poza ISP do mitygacji ataków wykorzystane zostały firmy zewnętrzne specjalizujące się w usługach typu antyDDoS. Zewnętrzne podmioty wykorzystywane zostały również do analizy zagrożeń związanych z malware.

- Pomimo wsparcia się podmiotami zewnętrznymi w rozwiązywaniu szczegółowych technicznych problemów, banki posiadają w swojej strukturze własne zespoły techniczne. W skład tych zespołów wchodzi wysoce wykwalifikowany personel, który korzystając z przeznaczonych do tego systemów teleinformatycznych jest w stanie podjąć działania zmierzające do mitygacji ataków DDoS, analizę powłamaniową oraz monitoring zagrożeń teleinformatycznych, na co najmniej podstawowym poziomie.

- Jako przykłady dobrej praktyki i ciekawego podejścia do minimalizacji negatywnych skutków ataków zaobserwowanych podczas ćwiczenia Cyber-EXE Polska 2013 można wskazać:
  - wykorzystanie kanału SMS do wysłania ostrzeżeń do klientów banku o próbach wyłudzenia loginów i haseł,
  - informowanie oddziałów banków, spółek zależnych, agentów zewnętrznych pośredniczących w kontakcie z klientem o problemach z systemami teleinformatycznymi.

- Moderatorzy bankowi podkreślali duże zaangażowanie ćwiczących. Ich motywacją była chęć sprawdzenia się w grze symulacyjnej, ciekawość scenariusza i w pewnym stopniu elementy wewnętrznej rywalizacji.

7.3 Wnioski dotyczące całości sektora bankowego

- Współpraca pomiędzy bankami w sytuacjach kryzysowych jest prowadzona w podstawowym zakresie. Polega ona przede wszystkim na przekazywaniu ostrzeżeń i informacji.

- Zaobserwowano ograniczoną koordynację wspólnych działań ćwiczących (np. w celu przygotowania wspólnego komunikatu medialnego dla całego sektora konieczna była ingerencja zewnętrzna moderatora ćwiczenia; banki pozytywnie zareagowały tylko na taką propozycję).

- 75% ankietowanych wskazało niski (wartości od 1 do 3 w sześciostopniowej skali) wpływ współpracy z innymi uczestnikami ćwiczenia na „neutralizację" zagrożenia i jego skutków. Oznacza to, że rzeczywisty wpływ współpracy na końcowy sukces był niewielki. Nie jest jasne, czy zacieśnienie współpracy mogłoby podnieść te oceny, zwłaszcza w przypadku ataku typu DDoS, w którego mitygacji banki zazwyczaj działają samodzielnie.

- Rzadko występuje komunikacja jednoczesna z całym sektorem. Współpraca miedzy bankami zwykle odbywa się na zasadach kontaktów dwustronnych.

- Głównym kanałem wymiany informacji pomiędzy bankami była platforma SWOZ, udostępniana przez Związek Banków Polskich. Nie wszystkie banki korzystały z tego kanału komunikacji.

- Nie nastąpiła komunikacja na temat występujących zakłóceń w dostępie do usług e-bankingu z podmiotem nadzorującym sektor finansowy, tj. KNF, natomiast niektóre banki rozpoczęły przygotowywanie stosownego komunikatu lecz nie został on wysłany do regulatora w czasie trwania ćwiczenia.

- Nie wszystkie podmioty ćwiczące mają formalne zasady komunikacji z innymi podmiotami. Połowa uczestników wskazała brak formalnych zasad wymiany informacji z podmiotami zewnętrznymi, takimi jak: inne banki, operatorzy telekomunikacyjni, CERT-y zewnętrzne.

- Dostępność działania usług e-bankingu jest w dużej mierze zależna od usług świadczonych przez operatora telekomunikacyjnego.

7.4 Wnioski dotyczące warstwy komunikacji medialnej

- Ze sposobu, w jaki rzecznicy prowadzili działania komunikacyjne, można wnioskować, że w bankach istnieją procedury komunikacji społecznej na wypadek sytuacji kryzysowej.

- Wydawano komunikaty przedstawiające stanowiska banków. Odpowiadając na pytania dziennikarzy, rzecznicy starali się trzymać zakresu informacji przedstawionego w komunikacie. Jeśli pytania wykraczały poza treść komunikatu, większość rzeczników prosiła o przesłanie pytań e-mailem. W realnej sytuacji takie prośby mogą spowodować, że stanowisko banku nie zostanie uwzględnione w przygotowywanym przez dziennikarza materiale, zwłaszcza gdy jest on przedstawicielem mediów elektronicznych, w których szybkość otrzymania odpowiedzi odgrywa kluczową rolę.

- Unikanie odpowiedzi na pytania i zmuszanie dziennikarzy do wysyłania pytań drogą mailową w realnej sytuacji jest bezpieczne dla rzecznika, jednak z drugiej strony w odbiorze dziennikarza może sprawiać wrażenie, że rzecznicy są niezorientowani w sytuacji.

- Pozytywnie należy ocenić fakt, że rzecznicy banków reagowali na kontakt telefoniczny ze strony dziennikarzy. W przypadku braku możliwości odebrania połączenia oddzwaniali.

- Banki bardzo szybko reagowały na komentarze pojawiające się w mediach i na portalach społecznościowych. Rzecznicy publikowali komunikaty na stronie internetowej i rozsyłali je do mediów. Publikowali także informacje w serwisach społecznościowych imitujących działanie Facebooka i Twittera oraz odpowiadali na bezpośrednie pytania mediów. Jeden z banków uruchomił też infolinię dla klientów.

- W sytuacji, gdy uruchomione zostały fałszywe strony internetowe banków (związane z phishingiem), co miało umożliwić kradzieże loginów i haseł użytkowników, większość ćwiczących zareagowała natychmiast, ostrzegając klientów. Brak odpowiednio szybkiej reakcji ze strony niektórych uczestników w realnej sytuacji może skutkować utratą zaufania klientów.

- Każdy bank prowadził zupełnie niezależne działania komunikacyjne. Nie ma wyraźnych dowodów na to, że ćwiczący rzecznicy współpracowali ze sobą.

- W czasie ćwiczenia służby prasowe kontaktowały się (otrzymywały informacje o rozwoju sytuacji) przede wszystkim z komórkami organizacyjnymi odpowiedzialnymi merytorycznie za reakcję w sytuacji przewidzianej scenariuszem ćwiczenia.

- Jakość informacji, niezbędnych do prowadzenia skutecznej komunikacji społecznej, przekazywanych przez merytoryczne komórki organizacyjne została w ankietach pozytywnie oceniona.

- Przebieg ćwiczenia potwierdził zasadność decyzji o rozszerzeniu go o warstwę komunikacji medialnej. Prace grupy symulującej działania mediów urealniają sytuację ćwiczebną i wywierając presję, stymulują ćwiczących do działania.

7.5 Wnioski dotyczące organizacji ćwiczenia

- W większości opinii uczestników Cyber-EXE Polska 2013 tego typu ćwiczenie powinno się odbywać co roku.

- Istotne jest wsparcie idei ćwiczenia poprzez kierownictwa podmiotów biorących w nim udział. Takie wsparcie jasno sformułowane ułatwia przygotowanie i przeprowadzenie ćwiczenia, w szczególności jest ono pomocne dla moderatora bankowego.

- Organizacja ćwiczenia w modelu pełnej symulacji wymaga bardzo intensywnej pracy moderatora bankowego. Zastosowanie tego modelu zdecydowanie zwiększa liczbę uczestniczących po stronie banku komórek organizacyjnych. Wydaje się jednak, że takie podejście do ćwiczeń daje organizacji możliwość bardziej realnego zasymulowania rzeczywistych zagrożeń i reakcji na nie.

- Pełnienie roli moderatora głównego, w tym odgrywanie roli podmiotów zewnętrznych bezpośrednio nieuczestniczących w ćwiczeniu, nie wymaga znajomości szczegółów organizacji i procesów bankowych. Konieczne jest jednak ogólne rozeznanie w tych procesach i działaniach. Można je nabyć w fazie planowania ćwiczenia.

- Wizualizacja i dokumentacja ćwiczenia są szczególnie istotne dla zebrania wartościowego materiału do późniejszej oceny ćwiczenia. Odgrywają one wtórną rolę w trakcie przeprowadzenia incydentu. Zdecydowana większość uczestników nie korzystała z przygotowanej wizualizacji ćwiczenia, choć jej projekt został oceniony pozytywnie. Na niskie wykorzystanie wizualizacji wpłynęło znaczne obciążenie pracą moderatorów bankowych.

- Niejednoznaczne jest określenie, komu powinna być przypisana rola moderatora bankowego. 50% uczestników jest zdania, że moderatorem bankowym powinna być osoba bezpośrednio zaangażowana w reakcję na zdarzenia przewidziane w scenariuszu w ramach codziennych obowiązków. Pozostałe 50%, że powinna to być osoba nie zaangażowana, ale doskonale znająca specyfikę działania organizacji w zakresie scenariusza, oraz osoba niezależna pośrednicząca jedynie w kontaktach pomiędzy moderatorem głównym a uczestnikami ćwiczenia.

- Ważne jest, aby instrukcja dla uczestników ćwiczenia powstała odpowiednio wcześnie, żeby było możliwe jej użycie w każdym z przyjętych modeli przeprowadzenia incydentu, zwłaszcza w tych, które wymagają dłuższych przygotowań po stronie banku.

- Obsługa wielu podmiotów ćwiczących przez moderatora głównego, przy jednoczesnej konieczności odgrywania przez niego ról podmiotów nieuczestniczących, jest dużym wyzwaniem i powinna być wsparta działaniami pomocniczymi. Spiętrzenie zadań operatora głównego wywołuje zachwianie płynności w przeprowadzaniu ćwiczenia.

- Z oceny uczestników ćwiczenia wynika, że zespół projektowy został prawidłowo dobrany i powołany, a także odbył on odpowiednią liczbę spotkań przygotowawczych, pozwalających na przygotowanie scenariusza oraz organizację techniczną i logistyczną ćwiczenia.

Fot. 9. Przerwa w ćwiczeniu była okazją do wymiany opinii na gorąco.

8 Rekomendacje

8.1 Rekomendacje dotyczące działań wewnętrznych banków

- Pracownicy odpowiedzialni za reagowanie na zdarzenia związane z cyberatakiem powinni regularnie dokonywać przeglądu procedur i przypominać je sobie. Warto, aby w przeglądzie wykorzystywano wyniki przeprowadzonych testów technicznych, analizy umów i kontraktów z podmiotami zewnętrznymi (np. z operatorem telekomunikacyjnym).

- Ćwiczenie reagowania na sytuacje kryzysowe jest jednym z kluczowych rozwiązań wzmacniających zdolności obronne banku, zwłaszcza gdy stosowanie procedur nie jest warunkiem wystarczającym do opanowania sytuacji kryzysowej.

- Zdobywanie aktualnej wiedzy na temat wszelkich aspektów specyfiki cyberataków może mieć kluczowe znaczenie dla skutecznej obrony przed nimi, dlatego personel odpowiedzialny za te zadania powinien mieć pełen dostęp do wiedzy (np. subskrypcja na branżowych portalach internetowych) oraz szkoleń w tym zakresie. Szkolenia powinny dotyczyć nie tylko osób bezpośrednio odpowiedzialnych za bezpieczeństwo teleinformatyczne, ale również wszystkich pracowników, których nieprawidłowe działanie może istotnie wpłynąć na poziom bezpieczeństwa w banku.

- Warto wyznaczyć osobę (osoby) odpowiedzialną za prowadzenie negocjacji z potencjalnymi szantażystami. Osoba (osoby) ta powinna posiadać kompetencje w tym zakresie. Można zaprosić do współpracy Policję.

8.2 Rekomendacje dotyczące całości sektora bankowego

- Współpraca operacyjna pomiędzy bankami, na wypadek zajścia cyberataków dotyczących całego sektora, wymaga zacieśnienia . Niezbędne jest uregulowanie zasad współpracy pomiędzy zaatakowanymi bankami, mimo konkurowania ze sobą w świadczeniu usług bankowych. Regulacja powinna obejmować w szczególności:
  - zasady wymiany danych operacyjnych, w tym warunki, sposoby oraz zakres dzielenia się informacją oraz ochronę tej informacji,
  - zasady udzielania wsparcia w odpieraniu ataku, w tym warunki jego udzielenia, role i odpowiedzialność współpracujących.

- Przed przygotowaniem powyższych regulacji potrzebne jest sprawdzenie regulacji i rekomendacji w tej dziedzinie, np.: wydanych przez ZBP. Podmiotem, który mógłby opracować takie rekomendacje jest właśnie Związek Banków Polskich. Wdrożenie takich rekomendacji powinno nastąpić w drodze wprowadzenia przez wszystkie banki odpowiednich przepisów i regulacji wewnętrznych.

- Banki powinny bardziej efektywnie wykorzystywać przestrzeń stworzoną przez ZBP do przeciwdziałania atakom na bankowość elektroniczną oraz w celu minimalizacji skutków tych ataków – wspólna polityka informacyjna i koordynacja działań.

- Należy określić zakres koniecznej i rekomendowanej informacji, które powinny być przekazywane przez banki do innych podmiotów sektora bankowego, zwłaszcza do podmiotu nadzorującego rynek finansowy – KNF.

- Banki powinny realizować zalecenia w przedmiotowym zakresie wynikające z Rekomendacji D KNF dotyczącej zarządzania obszarem technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego w bankach – rek. 18.9. Zaleca się nawiązanie stałej współpracy z innymi bankami (w szczególności z wykorzystaniem międzybankowych systemów wymiany informacji) w zakresie wymiany informacji o zidentyfikowanych zagrożeniach oraz wniosków i doświadczeń wynikających z analizy zidentyfikowanych przypadków naruszeń bezpieczeństwa środowiska teleinformatycznego. Sposób oraz zakres wymienianych informacji powinny zapewniać ich poufność, zwłaszcza dochowanie tajemnicy bankowej.

- Budowę mechanizmów obrony i rozwój możliwości odparcia ewentualnego cyberataku oraz minimalizacji jego skutków należy oprzeć na współpracy pomiędzy bankami a innymi podmiotami mającymi istotny wpływ na przeprowadzanie transakcji za pośrednictwem zdalnych kanałów.

8.3 Rekomendacje dotyczące warstwy komunikacji medialnej

- Służby prasowe banków powinny przygotować się na wypadek wystąpienia zdarzeń opisanych w scenariuszu i przedstawionych w ćwiczeniu lub na podobne incydenty. Oznacza to opracowanie materiału zawierającego potencjalne pytania i sugerowane odpowiedzi, kluczowe przesłania, „talking points" i projekty komunikatów prasowych. Usprawni to działanie rzeczników prasowych, skróci czas reakcji banku i pozwoli na sprawniejsze zarządzanie sytuacją kryzysową.

- Banki powinny dokonać przeglądu procedur obiegu informacji pod kątem dostosowania ich do prowadzenia skutecznej polityki informacyjnej. W rzeczywistej sytuacji kryzysowej, w warunkach stresu, dynamicznie zmieniającej się sytuacji i pod presją czasu potrzebne są ustalone wcześniej szybkie ścieżki kontaktu z wybranymi komórkami organizacyjnymi lub podmiotami zewnętrznymi.

- Rzecznik prasowy powinien mieć stały kontakt z kierownictwem instytucji lub wchodzić w skład sztabu kryzysowego.

- Warto zorganizować spotkania rzeczników banków biorących udział w ćwiczeniu w celu omówienia prowadzonej polityki informacyjnej i wymiany wniosków z wydarzenia. Reagowanie w sytuacji kryzysowej powinno stanowić również przedmiot szkoleń i doskonalenia kompetencji zawodowych pracowników służb prasowych.

8.4 Rekomendacje dotyczące organizacji ćwiczenia

- Warto organizować kolejne edycje ćwiczenia ochrony w cyberprzestrzeni z rekomendowaną częstotliwością raz na rok. W wersji minimum ćwiczenie powinno być organizowane nie rzadziej niż raz na dwa lata. W przypadku organizacji ćwiczenia w modelu pełnej symulacji zaleca się, aby moderator bankowy otrzymał dodatkowe wsparcie osób, z którymi będzie mógł koordynować przebieg ćwiczenia we własnej organizacji.

- Zespół planistyczny odpowiedzialny za przygotowanie ćwiczenia po stronie banku powinien składać się co najmniej z dwóch osób – jednej dobrze przygotowanej merytorycznie do pracy nad scenariuszem oraz drugiej mającej możliwości podejmowania samodzielnych decyzji dotyczących udziału organizacji w ćwiczeniu.

- W przypadku organizacji ćwiczenia w modelu pełnej symulacji zaleca się ograniczenie liczby zdarzeń powodujących reakcje uczestników ćwiczenia.

- Warto przeanalizować możliwość stworzenia wspólnej platformy technicznej do przeprowadzenia ćwiczenia. Powinna ona odpowiadać metodyce przyjętej do organizacji ćwiczenia Cyber-EXE Polska. Platforma taka powinna mieć także możliwość wizualizacji przebiegu ćwiczenia, w tym przedstawiać przepływ informacji pomiędzy uczestnikami. Możliwe jest w tym celu wykorzystanie innych, istniejących narzędzi wspomagających przeprowadzenie ćwiczenia.

- W przypadku uczestnictwa w ćwiczeniu więcej niż pięciu banków oraz konieczności odgrywania ról innych podmiotów (np. organów ścigania, operatorów telekomunikacyjnych, CERT-ów zewnętrznych itp.) należy zapewnić wsparcie operacyjne dla moderatora głównego.

- Warto rozważyć realizację kolejnego ćwiczenia w warstwie technicznej. W takim przypadku konieczne jest zaangażowanie operatorów telekomunikacyjnych do wspólnego ćwiczenia.

- Warto doprowadzić do uczestnictwa w kolejnych wydarzeniach większej liczby podmiotów ćwiczących ze strony banków oraz innych podmiotów istotnych dla zapewnienia bezpieczeństwa funkcjonowania usług sektora bankowego, np. ZBP, KNF, NBP, MF, organów ścigania, zewnętrznych zespołów typu CERT czy operatorów telekomunikacyjnych.

9 Podziękowania

Ćwiczenie Cyber-EXE Polska 2013 nie mogłoby się odbyć bez dobrej woli i wyjątkowego zaangażowania uczestniczących w nim organizacji, a zwłaszcza osób, które brały aktywny udział w jego organizacji. Fundacja Bezpieczna Cyberprzestrzeń, jako organizator ćwiczenia, dziękuje wszystkim za odwagę w realizacji pionierskiego przedsięwzięcia dla sektora bankowego w Polsce, za wielkie zaangażowanie w czasie wielomiesięcznych przygotowań, podczas samego ćwiczenia oraz pracy włożonej w ocenę wydarzenia, opracowanie wniosków i rekomendacji.

Dziękujemy partnerom ćwiczenia – Rządowemu Centrum Bezpieczeństwa i firmie doradczej Deloitte – za duże wsparcie przy organizacji ćwiczenia oraz aktywny merytoryczny udział w jego przygotowaniu i przeprowadzeniu. Merytoryczne i organizacyjne doświadczenia obydwu partnerów były wielkim wkładem w końcowy sukces przedsięwzięcia.

Dziękujemy wszystkim uczestnikom ćwiczenia, tj. bankom, które zdecydowały się na udział w wydarzeniu. Odwaga, współdziałanie i otwartość reprezentantów banków przyczyniły się do przygotowania ciekawych scenariuszy, sprawnego przeprowadzenia ćwiczeń i wyciągnięcia pożytecznych wniosków.

Dziękujemy również obserwatorom ćwiczenia: Ministerstwu Finansów, Narodowemu Bankowi Polskiemu, Komisji Nadzoru Finansowego oraz Związkowi Banków Polskich. Niezwykle istotna rola, jaką wszystkie te podmioty odgrywają w polskim sektorze bankowym, połączona z decyzją o obserwacji i wsparciu ćwiczenia, była ważnym czynnikiem motywującym do realizacji przedsięwzięcia oraz oceny jego rezultatów.

10 Słowniczek skrótów

APT	Advanced Persistant Threat
CEP13	Cyber-EXE Polska 2013
CERT	Computer Emergency Response Team
CISKOM	Internetowy System Komunikacji Medialnej
CKC	Centrum Koordynacji Ćwiczenia
DDoS	Distributed Denial of Service
ENISA	European Network and Information Security Agency
FBC	Fundacja Bezpieczna Cyberprzestrzeń
KNF	Komisja Nadzoru Finansowego
MF	Ministerstwo Finansów
NBP	Narodowy Bank Polski
PR	Public Relations
RCB	Rządowe Centrum Bezpieczeństwa
SWOZ	System Wymiany Ostrzeżeń o Zagrożeniach
ZBP	Związek Banków Polskich

Opinie obserwatorów

Banki są jednym z najistotniejszych elementów infrastruktury krytycznej Polski i dlatego tego typu ćwiczenia dają praktyczną możliwość skonfrontowania regulacji prawnych (prawa powszechnie obowiązującego oraz regulacji wewnętrznych w bankach) i faktycznych możliwości podejmowania działań prewencyjnych oraz post factum przez banki w obliczu ataku na bankowość elektroniczną. Wyniki tych ćwiczeń powinny pokazać na ile banki są odporne na zagrożenia ze strony cyberprzestępców. Rola podmiotów zaproszonych przez organizatorów ćwiczeń: Ministerstwo Finansów, Komisję Nadzoru Finansowego, Narodowy Bank Polski i Związek Banków Polskich powinna być bardziej aktywna, gdyż instytucje te mają istotny wpływ na bezpieczeństwo banków w tym obszarze. Brakowało w ćwiczeniach udziału instytucji takich jak Policja oraz wspierających banki w zakresie bezpieczeństwa elektronicznego.

Ćwiczenia te pokazały, że banki potrafią pojedynczo i przy współpracy z innymi bankami oraz Związkiem Banków Polskich skutecznie minimalizować skutki tego typu incydentów. Jednak działania podejmowane przez sektor bankowy wymagają wsparcia ze strony instytucji państwowych w obszarach gdzie kompetencje banków są niewystarczające, w tym przypadku negocjacje z szantażystą oraz ściganie przestępców przez organy ścigania.

Ćwiczenia te pokazały, że banki skutecznie potrafią przeciwdziałać przestępczości elektronicznej nakierowanej na banki oraz ich klientów.

Piotr Balcerzak, Związek Banków Polskich

Segment bankowy jest istotnym elementem systemu finansowego Narodowego Programu Ochrony Infrastruktury Krytycznej (NPOIK), a potencjalne powstanie w nim zakłóceń może mieć katastrofalny wpływ na funkcjonowanie całego systemu. Kluczowe staje się odpowiednie zabezpieczenie zarówno instytucji finansowych jak również administracji publicznej przed wszelkim formami ataków skierowanych na ten obszar działalności.

Organizacja i przeprowadzanie ćwiczeń sprawdzających mechanizmy ochrony przed atakami z cyberprzestrzeni były i są najlepszym sposobem sprawdzenia mechanizmów zarządzania kryzysowego jak również przygotowania się do tej formy zagrożeń. W związku z powyższym organizowanie tego typu przedsięwzięć powinno odbywać się przynajmniej raz do roku.

Hubert Krztoń, Ministerstwo Finansów

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. Tytoniowa 20, 04-228 Warszawa
tel: +48 22 112 0 800
e-mail: kontakt@cybsecurity.org

www. cybsecurity.org

www.cyberexepolska.pl