Deloitte.

FUNDACJA bezpieczna cyberprzestrzeń

RCB Rządowe Centrum Bezpieczeństwa

# CYBER-EXE POLSKA 2015

# RAPORT

# CYBER-EXE™ POLSKA 2015

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

## PRZYGOTOWANIE, PRZEBIEG, ANALIZA, WNIOSKI I REKOMENDACJE.

# Spis treści

# 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 ćwiczenia, oraz wnioski i rekomendacje, sformułowane na podstawie zaobserwowanych reakcji ćwiczących na zdarzenia zaplanowane w scenariuszu.

Zagrożenia z cyberprzestrzeni nie są dla sektora finansowego nowością. Od wielu lat sektor ten jest liderem we wprowadzaniu w życie nowoczesnych rozwiązań technologicznych. Doświadczenie to (także z rzeczywistych incydentów) pozwoliło na wypracowanie szeregu procedur oraz technicznych systemów zabezpieczeń.

# 2 Podsumowanie menedżerskie

Cyber–EXE™ Polska 2015 ponownie dowiodło, że posiadanie wdrożonych procedur oraz wyposażenie w odpowiednie systemy są warunkiem koniecznym, ale niewystarczającym, by nawet duża organizacja mogła sprostać zaawansowanemu atakowi teleinformatycznemu. Podczas reakcji na cyberatak, który odbiega od przewidzianych procedurami i standardowo realizowanych schematów, istotną rolę odgrywa doświadczenie pracowników, ich kreatywność i osobiste zaangażowanie, a także zdolność do koordynacji działań wielu zaangażowanych wewnętrznie komórek organizacyjnych. W związku z tym kompetencje pracowników odpowiedzialnych za reagowanie na zdarzenia związane z cyberatakiem powinny iść w parze z poziomem wiedzy potencjalnych atakujących.

Kolejna edycja ćwiczeń potwierdziła konieczność zacieśnienia operacyjnej współpracy między organizacjami sektora na wypadek zajścia cyberataków. W sytuacji występowania konkurencji pomiędzy częścią organizacji niezbędne jest uregulowanie zasad takiej współpracy. 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.

Wydaje się, że ze względu na zasięg swojego działania, podmiotem predestynowanym do opracowania takich rekomendacji jest Związek Banków Polskich i Polska Izba Ubezpieczeniowa, natomiast wdrożenie rekomendacji powinno nastąpić w drodze wprowadzenia przez wszystkie organizacje odpowiednich przepisów i regulacji wewnętrznych. Warto również, aby zarówno ZBP jak i PIU aktywnie wspierały działania prowadzące do organizacji okresowych, branżowych ćwiczeń z zakresu zarządzania kryzysowego oraz zachęcania podmiotów skupionych w ZBP i PIU do udziału w tych ćwiczeniach.

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

Wszyscy uczestnicy ćwiczeń wskazali na korzyści wyniesione z udziału w tym przedsięwzięciu. Cyber–EXE™ Polska 2015 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.

# 3 Ćwiczenia

## 3.1 Idea ćwiczeń ochrony w cyberprzestrzeni

Ćwiczenia Cyber-EXE™ Polska 2015 są 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 się 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], a następnie miały kontynuację w roku 2012[2] i 2014[3]. Wśród tych 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, również podmiotów reprezentujących sektor prywatny. Dodatkową motywacją okazały się udane ćwiczenia Cyber-EXE™ Polska 2012 w sektorze energetycznym[4], Cyber-EXE™ Polska 2013 w sektorze bankowym[5] oraz Cyber-EXE™ Polska 2014 w sektorze telekomunikacyjnym[6].

## 3.2 Geneza ćwiczeń Cyber-EXE™ Polska 2015

Po pozytywnych doświadczeniach związanych z ćwiczeniami w latach 2012 – 2015, w sposób oczywisty istniała chęć kontynuacji tej inicjatywy. Duże zainteresowanie powtórzeniem ćwiczeń ze strony uczestników edycji z roku 2013, w połączeniu ze szczególną rolą sektora finansowego dla indywidualnych odbiorców sprawiły, że decyzja o tym, by „celem" tegorocznych ćwiczeń był ten sektor była naturalna. Edycja 2015 dodatkowo została rozszerzona o sektor ubezpieczeniowy, dzięki czemu można było przeprowadzić ćwiczenie w dwóch najistotniejszych typach organizacji dla sektora finansowego – bankach i firmach ubezpieczeniowych[7]. Nie bez znaczenia była również chęć sprawdzenia w jaki sposób organizacje ćwiczące w roku 2013 zaimplementowały wnioski i rekomendacje z poprzednich ćwiczeń.

Przychylne wsparcie organizatora ćwiczeń przez podmioty publiczne oraz prywatne, tj. Rządowe Centrum Bezpieczeństwa i firmę doradczą Deloitte, przy jednoczesnym zainteresowaniu organizacji uczestnictwem w tym przedsięwzięciu sprawiło, że pomysł organizacji ćwiczeń mógł być zrealizowany.

## 3.3 Organizatorzy

Organizatorem ćwiczeń Cyber-EXE™ Polska 2015 była Fundacja Bezpieczna Cyberprzestrzeń. Współorganizatorami byli Rządowe Centrum Bezpieczeństwa oraz firma doradcza Deloitte.

1. „Cyber Europe 2010 – Evaluation Report" - http://www.enisa.europa.eu/activities/Resilience-and-CIIP/cyber-crisis-cooperation/cyber-europe/ce2010/ce2010report
2. „Cyber Europe 2012 – Główne ustalenia i zalecenia" - https://www.enisa.europa.eu/activities/Resilience-and-CIIP/cyber-crisis-cooperation/cce/cyber-europe/cyber-europe-2012/ENISA_2012_00490000_PL_TRA.pdf
3. „ENISA Cyber Europe 2014 – After Action Report" - https://www.enisa.europa.eu/activities/Resilience-and-CIIP/cyber-crisis-cooperation/cce/cyber-europe/ce2014/ce2014-after-action-report

## 3.4 Uczestnicy ćwiczeń

Do ćwiczeń przystąpiło 7 organizacji. 5 organizacji reprezentowało sektor bankowy, 2 organizacje sektor ubezpieczeniowy. Liczba uczestników nie upoważnia nas do uznania całości wniosków za reprezentatywne dla wszystkich organizacji z tych sektorów. Niemniej jednak w opinii organizatorów, wypracowane wnioski i rekomendacje w bardzo istotnym stopniu oddają podstawowe zjawiska dotyczące poziomu gotowości organizacji z sektora finansowego, na skuteczne odparcie ataków w cyberprzestrzeni. Zdaniem organizatorów ustalone wnioski i wynikające z nich rekomendacje z powodzeniem mogą być wykorzystane do działań zmierzających do poprawy poziomu zdolności walki polskiego sektora finansowego z atakami w cyberprzestrzeni.

## 3.5 Patroni ćwiczeń

Ćwiczenia uzyskały poparcie instytucji związanych z sektorem finansowym. Patronami ćwiczeń Cyber-EXE™ Polska 2015 zostały:

- Komisja Nadzoru Finansowego,
- Związek Banków Polskich.

## 3.6 Zespół projektowy

Kilkunastoosobowy zespół projektowy stanowili przedstawiciele wszystkich podmiotów zaangażowanych w organizację ćwiczeń oraz uczestniczących organizacji. W ramach prowadzonych przygotowań zespół projektowy realizował zadania w kilku obszarach tematycznych. Najważniejsze z nich to:

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

4. więcej o ćwiczeńch Cyber-EXE™ Polska 2012 można znaleźć w raporcie z ćwiczeń: http://cybsecurity.org/raport-cyber-exe-polska-2012/

5. więcej o ćwiczeńch Cyber-EXE™ Polska 2013 można znaleźć w raporcie z ćwiczeń: https://www.cyberexepolska.pl/?page_id=123

6. więcej o ćwiczeniach Cyber-EXE™ Polska 2014 można znaleźć w raporcie z ćwiczeń: https://www.cyberexepolska.pl/?page_id=1276

7. zasadnicze różnice dotyczyły obsługi (lub nie) klientów detalicznych

# 4 Cele ćwiczeń Cyber-EXE™ Polska 2015

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

A. **Sprawdzenie zdolności reakcji organizacji na atak teleinformatyczny:**
- sprawdzenie istniejących planów i procedur zarządzania, identyfikacja potrzeb ich uzupełnienia, aktualizacji lub stworzenia nowych,
- sprawdzenie współpracy i komunikacji wewnątrz i na zewnątrz organizacji.

B. **Zidentyfikowanie zależności i współzależności pomiędzy podmiotami rynku finansowego, regulatorem tego rynku, a także innymi organizacjami mającymi wpływ na jego działanie, takimi jak izby gospodarcze.**

C. **Sprawdzenie komunikacji między przedsiębiorcami oraz regulatorem i innymi podmiotami rynku finansowego:**
- sprawdzenie czy występuje wymiana informacji o zagrożeniach i czy ma ona realny wpływ na zarządzanie nimi,
- sprawdzenie jakości i przydatności wymienianych informacji w reakcji na zagrożenie.

# 5 Proces organizacji ćwiczeń

## 5.1 Faza Identyfikacji

W tej fazie zostały ustalone podstawowe cele ćwiczeń oraz lista jego uczestników. W sformułowaniu celów ćwiczeń bardzo pomocne okazały się wcześniejsze doświadczenia z edycji z roku 2013, Rekomendacja D Komisji Nadzoru Finansowego dotycząca zarządzania obszarami technologii informacyjnej i bezpieczeństwa środowiska teleinformatycznego w organizacjach, oraz szczegółowe cele, które stawiały sobie na celu poszczególne organizacje przystępujące do ćwiczeń. Wszystko to w naturalny sposób pomogło wyznaczyć ramy i zakres tematyczny Cyber-EXE™ Polska 2015. Faza ta obejmowała również określenie przybliżonego obszaru tematycznego ćwiczeń, czyli omówienie wstępnych założeń scenariusza.

## 5.2 Faza Planowania

W trakcie fazy planowania dokładnie określono obszar tematyczny ćwiczeń, który następnie został opisany szczegółowo w postaci scenariusza. W tej fazie został wybrany przez uczestników ostateczny model przeprowadzenia ćwiczeń i lista uczestniczących wewnętrznie komórek organizacyjnych i stanowisk. Bardzo ważnym elementem fazy planowania było ustalenie organizacyjnych i technicznych zasad przeprowadzenia ćwiczeń, w tym przydzielenia ról związanych z zarządzaniem ćwiczeniami oraz opracowanie instrukcji ćwiczeń.

W trakcie fazy planowania w każdej z organizacji przeprowadzono wewnętrzne szkolenia oparte na instrukcjach ćwiczeń przygotowanych przez organizatorów. W praktyce cały proces przygotowania do ćwiczeń był koordynowany przez moderatora organizacyjnego.

Fot. 1: Centrum Koordynacji Ćwiczeń CEP15.

## 5.3 Faza Przeprowadzenia

W trakcie tej fazy przeprowadzono zasadnicze ćwiczenia. Było one poprzedzone próbami generalnymi ćwiczeń (tzw. dry run), podczas których zespół planistyczny „przeszedł" przez scenariusz, dokonując ostatnich korekt. Przetestowano również rozwiązania techniczne, które posłużyły do przeprowadzenia ćwiczeń – przede wszystkim system zarządzania zdarzeniami (ang. injects) – EXITO (the EXercise event Injection TOolkit)[8].

Wspomniane próby generalne miały bardzo istotny wpływ na końcowy kształt ćwiczeń i sprawność ich przeprowadzenia.

Przeprowadzono dwie próby typu dry run. Pierwsza odbyła się w dniu 23 października 2015. W jej trakcie wszystkie osoby zaangażowane w przygotowanie ćwiczeń zasymulowały jego przebieg, odgrywając według swojej najlepszej wiedzy potencjalne zachowania poszczególnych osób i komórek organizacyjnych, których uczestnictwo było przewidziane w ćwiczeniu. Dodatkowo, ta próba miała istotny wpływ na ostateczne decyzje dotyczące scenariusza ćwiczeń, gdyż pokazała jego braki i pozwoliła na wprowadzenie korekt.

Druga próba typu dry run odbyła się w 27 października, na dwa dni przed planowaną datą ćwiczeń. Celem tej próby było przede wszystkim przećwiczenie wszystkich aspektów organizacyjnych ćwiczeń. Ćwiczono komunikację pomiędzy moderatorami organizacyjnymi i moderatorem głównym, sposób wypracowywania decyzji dotyczących przebiegu ćwiczeń, udziału zespołu technicznego i jego realizację zadań związanych z obsługą systemu EXITO, obowiązkiem dokumentacji przebiegu ćwiczeń i jego wizualizacji.

## 5.4 Faza Oceny

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

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

# 6 Scenariusz ćwiczeń

Scenariusz ćwiczeń został opracowany przez zespół projektowy, w skład którego wchodzili przedstawicieli banków, firm ubezpieczeniowych oraz eksperci zewnętrzni specjalizujący się w bezpieczeństwie teleinformatycznym sektora finansowego.

Założono, że charakter zdarzeń powinien dotyczyć całego sektora oraz doprowadzić do poważnej sytuacji kryzysowej w organizacjach, na którą nie ma gotowych, szczegółowych planów postępowania. Założono także, że organizacje mają cząstkowe plany reakcji, które łącznie mogą składać się na plan postępowania w sytuacji kryzysowej. Podobnie do ćwiczeń realizowanych w latach ubiegłych czwarta edycja ćwiczeń Cyber-EXE™ Polska składała się z dwóch realizowanych równolegle strumieni ataku: zagrożenia dla klientów uczestników ćwiczeń oraz dla samych uczestników – podmiotu sektora finansowego.

Wykreowana sytuacja wymagała od uczestników podejmowania szybkich decyzji oraz umiejętności trafnej diagnozy zdarzenia - tak by nie doprowadzić do jego eskalacji.

W praktyce scenariusz zakładał, że każda z organizacji stanie się obiektem dwóch ataków. Pierwszy, główny atak, przewidywał dokonanie nieautoryzowanej zmiany w kodzie aplikacji odpowiadającej za logikę jednej z głównych funkcji biznesowych organizacji. Zmiany tej miał dokonać szantażysta żądający w dalszej części ćwiczeń okupu.

Drugą fazą ćwiczeń był atak typu phishing nakierowany na personel organizacji, którego skutkiem było zaszyfrowanie znaczącej części stacji roboczych, w tym komputerów administratorów.

Scenariusz ćwiczeń został oparty na aktualnych i przewidywanych trendach dotyczących złożonych ataków teleinformatycznych, gdzie widoczny jest coraz większy poziom wyrafinowania ataków. W związku z powyższym, każde wprowadzenie scenariusza było sprawdzone i dostosowywane dla poszczególnych organizacji.

Niezależnie od wprowadzonych modyfikacji o charakterze technicznym, scenariusz uwzględniał wszystkie istotne punkty kontrolne i zdarzenia opisane poniżej.

Równolegle do części organizacyjnej ćwiczeń, rozgrywana była również warstwa medialna, w której uczestnicy musieli w odpowiedzi na zdarzenia ze scenariusza przygotować politykę informacyjną i odpowiadać na zapytania dziennikarzy[9].

## 6.1 Atak nr 1 - zmiana kodu aplikacji służącej jednej z głównych funkcji biznesowych organizacji - szantażysta

Atak zaimplementowany w pierwszej części scenariusza zakładał, że w kodzie aplikacji, która jest wykorzystywana do realizacji jednego z głównych procesów biznesowych, realizowanych na rzecz klientów organizacji, dokonano nieautoryzowanej zmiany.

Każdy moderator organizacyjny ćwiczących banków i firm ubezpieczeniowych przewidział indywidualne dla swojego zespołu rozwinięcie techniczne tego zdarzenia, wskazując główne systemy i usługi będące celem ataku (transakcje, weryfikacja ubezpieczeń itp.).

Scenariusz był rozwijany w kolejnych fazach omówionych poniżej, choć należy wziąć pod uwagę, że poszczególne fazy nachodziły na siebie. Przedstawiona kolejność pokazuje ich sekwencję z punktu widzenia ich największego nasilenia.

Faza „Klienci" – ćwiczenia rozpoczęły się od skarg klientów na infolinii organizacji, którzy nie mogli wykonać podstawowych operacji świadczonych przez banki i firmy ubezpieczeniowe. Uwagi dotyczyły braku otrzymywania odpowiednich potwierdzeń dla swoich zleceń. Inna część klientów informowała o wiadomościach dotyczących transakcji, o które nie prosili. W związku z faktem, że klientami ćwiczących byli również dziennikarze, zwrócili się oni do poszczególnych organizacji z prośbą o udzielenie wyczerpujących informacji na temat tego zdarzenia.

Faza „Szantażysta" – kolejnym etapem scenariusza był kontakt szantażysty. Złożył on propozycję okupu finansowego. Ostrzegł jednocześnie o możliwości przeprowadzenia jeszcze groźniejszego ataku, jeśli jego żądania nie zostaną spełnione. Szantażysta, jeśli okup byłby przekazany, obiecał wskazać złośliwy fragment kodu, co pozwoliłoby na przyspieszenie procesu przywrócenia poprawnej obsługi klientów.

Faza „Media" – z upływem czasu o kłopotach sektora finansowego dowiadywało się coraz szersze grono przedstawicieli mediów. Skutkowało to podaniem do publicznej wiadomości przez serwisy internetowe zajmujące się tematyką cyberbezpieczeństwa informacji o ataku teleinformatycznym na poszczególne organizacje.

Faza „Atak zasadniczy" – scenariusz zakładał, że żądania szantażysty nie zostaną spełnione i dojdzie do eskalacji zdarzenia związanego z działaniem złośliwego kodu, a tym samym nasilą się wielokrotnie zgłoszenia klientów na infolinię i organizacje będą miały do czynienia z całkowitym paraliżem kluczowych usług. Coraz częściej pojawiające się informacje w mediach utrudniały sprawne zarządzanie sytuacją kryzysową.

9. Dziennikarzy odgrywali przedstawiciele organizatorów ćwiczeń, działający w ramach specjalnie wydzielonego zespołu medialnego. Wszyscy członkowie zespołu mieli odpowiednie przygotowanie i doświadczenie zawodowe pozwalające na wykonanie tego zadania.

## 6.2 Atak nr 2 – phishing – zaszyfrowanie dysków

Drugim atakiem zaplanowanym w czasie ćwiczeń była akcja phishingowa, wymierzona w wielu pracowników ćwiczących organizacji. Scenariusz przewidywał, że personel otrzyma wiadomości z adresu przypominającego oficjalne konto prezesa lub jego sekretariatu z informacją o nowym regulaminie premiowania pracowników. Wiadomość zawierała odnośnik do pliku zawierającego złośliwy kod, znajdującego się na zewnętrznym serwerze, po otwarciu którego dochodziło do zaszyfrowania zasobów zgromadzonych na stacji roboczej.

Na zainfekowanych komputerach pojawiała się informacja o konieczności wpłacenia odpowiedniej kwoty celem odszyfrowania danych. Założono, że atak powiódł się również w stosunku do pojedynczych stacji administratorów.

Scenariusz ćwiczeń skończył się wyciekiem danych[10]. W jednym z portali pojawiły się oferty sprzedaży pełnej listy kontaktowej pracowników organizacji, wraz z próbką kilkudziesięciu rekordów.

Fot. 2: Organizatorem ćwiczenia CEP15 była FBC, partnerami Deloitte i RCB.


10. Nie zawierały one danych klientów.

# 7 Przebieg ćwiczeń

## 7.1 Informacje podstawowe

Ćwiczenia CYBER-EXE™ Polska 2015 zostały przeprowadzone w dniu 29 października 2015 r. w godzinach 10:00 – 16:00. Cyber-EXE™ Polska 2015 i były rozproszonymi ćwiczeniami sztabowymi. Uczestnicy ćwiczeń podzieleni byli na dwie grupy. Pierwsza grupa znajdowała się w Centrum Kontroli Ćwiczeń (CKC). Druga pozostawała we własnych lokalizacjach.

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

- moderator główny,
- wspierający moderatora głównego, odpowiedzialny za zarządzanie zdarzeniami,
- wspierający moderatora głównego, odpowiedzialny za aspekty techniczne ćwiczeń,
- wspierający moderatora głównego, odpowiedzialny za podgrywanie niećwiczących organizacji,
- koordynator oceny,
- moderatorzy organizacyjni,
- zespół techniczny (2 osoby),
- zespół medialny (5 osób).

W tej grupie pracowało 20 osób.

**Druga grupa obejmowała:**

- ćwiczących,
- służby prasowe,
- inne podmioty.

Po stronie ćwiczących organizacji w ćwiczeniu wzięło udział około 80 pracowników.

## 7.2 Modele przeprowadzenia ćwiczeń

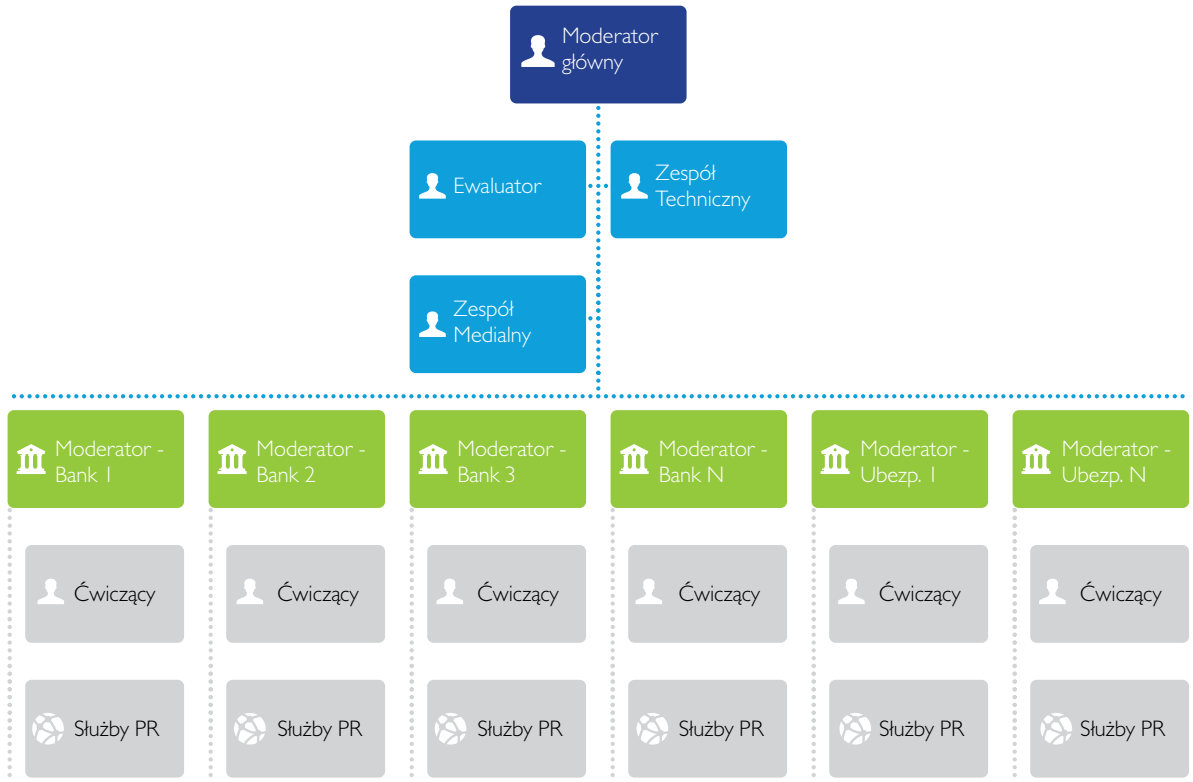
W fazie planowania ćwiczeń Cyber-EXE™ Polska 2015 uczestnicy zdecydowali się na przeprowadzenie go wg trzech modeli:

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

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

## 7.3 Struktura organizacyjna ćwiczeń

Rysunek 1.
**Struktura organizacyjna ćwiczeń Cyber-EXE™ Polska 2015**



### 7.3.1 Moderator główny

Moderatorem głównym CEP15 był przedstawiciel FBC. Osobie moderatora przypisane zostały następujące zadania:

- koordynacja całości przebiegu CEP15,
- podejmowanie decyzji o uruchamianiu kolejnych zdarzeń scenariusza,
- współpraca z moderatorami organizacyjnymi poszczególnych uczestników w celu przekazywania informacji o przebiegu zdarzeń oraz reakcjach na nie w oparciu o ustalony zakres informacji,
- rozstrzyganie wątpliwości dotyczących przebiegu CEP15,
- odbieranie raportów z przebiegu CEP15 od moderatorów organizacyjnych,
- podgrywanie działań podmiotów nieuczestniczących w ćwiczeniu oraz zewnętrznych systemów teleinformatycznych.

Moderatorowi głównemu w jego zadaniach pomagali moderatorzy wspierający, którzy byli przedstawicielami FBC, RCB i Citi.

### 7.3.2 Ewaluator

Ewaluatorem CEP15 był przedstawiciel RCB. Osobie ewaluatora przypisane zostały następujące zadania:

- stała obserwacja przebiegu ćwiczeń,
- rejestracja przebiegu zdarzeń służących przyszłej ocenie ćwiczeń,
- współpraca z moderatorami organizacyjnymi w celu zebrania obserwacji związanych z oceną przebiegu CEP15.

### 7.3.3 Moderatorzy organizacyjni

Moderatorzy organizacyjni byli wyznaczeni przez poszczególnych uczestników biorących udział w ćwiczeniu CEP14.
Osobie moderatora organizacyjnego przypisane zostały następujące zadania:

- koordynacja ćwiczeń CEP15 w danej organizacji, a w szczególności:
  - organizacji i przeszkolenia zespołu uczestniczącego w ćwiczeniu ze strony organizacji, w tym przygotowania wewnętrznych instrukcji dla uczestników ćwiczeń w przypadku jeśli przygotowanie takowych uznano za celowe,
  - koordynacji ćwiczeń z kierownictwem,
  - przekazywania zdarzeń ze scenariusza ćwiczeń uruchamianych przez moderatora głównego,
  - symulowania działań wewnętrznych systemów teleinformatycznych danej organizacji,
  - monitorowania przebiegu ćwiczeń w danej organizacji oraz reakcji na ewentualne zakłócenia jego przebiegu,
  - przekazywania informacji o przebiegu ćwiczeń w danej organizacji w oparciu o ustalony zakres informacji,
- współpracy z moderatorem głównym oraz ewaluatorem ćwiczeń CEP15,
- opcjonalnie – współpracy z ewaluatorem organizacyjnym, w sytuacji jego wyznaczenia.

### 7.3.4 Zespół techniczny

Zespół techniczny składał się z przedstawicieli FBC, RCB i Deloitte. Zadaniem zespołu technicznego było przygotowanie techniczne i logistyczne ćwiczeń. W szczególności zespół techniczny był odpowiedzialny za:

- organizację logistyczną ćwiczeń (przygotowanie sali i urządzeń koniecznych do przeprowadzenia ćwiczeń),
- przygotowanie i obsługę systemu wizualizacji CEP15,
- przygotowanie i obsługę systemu zarządzania zdarzeniami EXITO,
- stałą współpracę z moderatorem głównym i ewaluatorem CEP15, w celu prezentowania w systemie wizualizacji CEP15 bieżącego przebiegu CEP15 dla poszczególnych organizacji,
- wsparcie dla zespołu medialnego przy technicznym utrzymaniu systemu CISKOM[11].

### 7.3.5 Zespół medialny

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

- przygotowanie artykułów symulujących materiały medialne na podstawie informacji przekazywanych przez moderatora ćwiczeń, komunikatów wydawanych przez organizacje ćwiczące oraz na podstawie rozmów telefonicznych i informacji mailowych od rzeczników prasowych ćwiczących organizacji,
- współpracę z moderatorem głównym w celu publikowania komunikatów medialnych w systemie CISKOM, zgodnie z przebiegiem zdarzeń,
- reagowanie na komunikaty publikowane przez służby PR organizacji biorących udział w ćwiczeniu.

### 7.3.6 Ćwiczący

W zależności od przyjętego modelu przeprowadzenia ćwiczeń, ćwiczącymi byli przedstawiciele wyznaczonych komórek organizacyjnych wchodzący w skład zespołu ćwiczeniowego lub pracownicy poszczególnych organizacji, którzy byli zaangażowani w realizację działań przewidzianych w scenariuszu CEP15.

### 7.3.7 Zespoły prasowe

Zespoły prasowe (zespoły PR) stanowiły szczególny typ uczestników ćwiczeń CEP15. W realizacji swoich zadań korzystały z dostępu do systemu CISKOM, przez co informacje o zdarzeniach przewidzianych w scenariuszu i ich konsekwencjach, docierały do nich za pomocą symulowanych materiałów medialnych, niezależnie od informacji, które przekazywać im mogli uczestnicy ćwiczeń oraz moderatorzy organizacyjni w ich organizacjach. Jednocześnie służby PR mogły publikować w systemie CISKOM komunikaty, odpowiedzi, zaproszenia na konferencje prasowe, a także przekazywać informacje o swoich decyzjach do innych uczestników ćwiczeń oraz własnych moderatorów organizacyjnych.

11. CISKOM to system zarządzania informacjami symulującymi media elektroniczne. System został wypracowany i jest wykorzystywany przez Rządowe Centrum Bezpieczeństwa.

### 7.3.8 Inne podmioty

Innymi podmiotami były organizacje niebiorące aktywnego udziału w ćwiczeniach, a które zdaniem danej organizacji, mogły wziąć udział w rozwiązaniu problemu zarysowanego w scenariuszu ćwiczeń. Komunikacja z tymi organizacjami była realizowana z udziałem moderatora głównego ćwiczeń, którego zadaniem było podgrywanie działań innych podmiotów. Podmiotami podgrywanymi byli m.in. rządowy zespół CERT.GOV.PL, operator telekomunikacyjny, szantażyści.

## 7.4 Zarządzanie zdarzeniami i komunikacja w trakcie ćwiczeń

Ćwiczenia przebiegały zgodnie z wcześniej przygotowanym scenariuszem. Zaplanowane w scenariuszu zdarzenia wraz z rozwojem ćwiczeń były systematycznie uruchamiane przez osobę wspierającą moderatora głównego, odpowiedzialnego za obsługę systemu zarządzania incydentami, z wykorzystaniem narzędzia EXITO.

Zdarzenia przewidziane w scenariuszu podzielone były na dwie grupy:

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

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

Fot. 3: Centrum Koordynacji Ćwiczeń CEP15. Od lewej: Konrad Pszenny (Deloitte), Adam Politowski (RCB), Maciej Pyznar (RCB), Mirosław Maj (FBC), Paweł Chwiećko (Citi).

### 7.4.1 Komunikacja pomiędzy moderatorem głównym a moderatorami organizacyjnymi

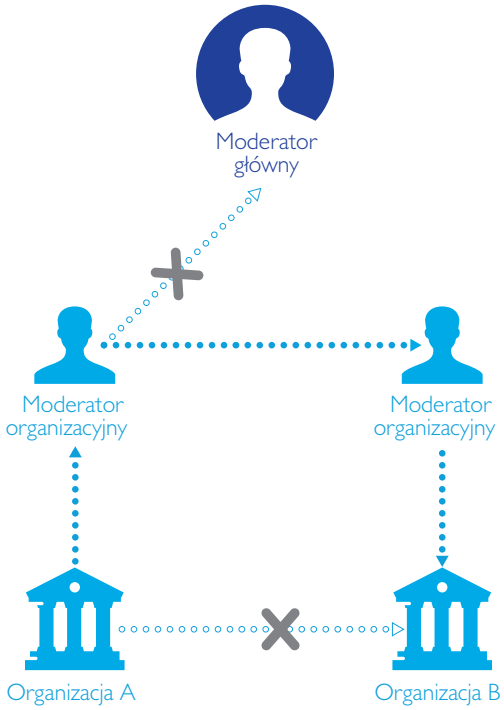
Komunikacja pomiędzy moderatorem głównym a moderatorami organizacyjnymi prowadzona była dla każdej z organizacji oddzielnie. Przybierała ona następujące formy:

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

### 7.4.2 Komunikacja pomiędzy ćwiczącymi organizacjami

W trakcie ćwiczeń dopuszczona była komunikacja bezpośrednia pomiędzy ćwiczącymi. Odbywała się ona poprzez moderatorów organizacyjnych. W sytuacji kiedy uczestnik ćwiczeń z organizacji A chciał skontaktować się z uczestnikiem ćwiczeń z organizacji B to informację tę przekazywał do swojego moderatora organizacyjnego (moderator organizacyjny organizacji A). W informacji wskazywał dane dotyczące konkretnego adresata (organizacja, stanowisko lub podmiot wewnątrz struktury organizacyjnej) oraz treść komunikatu. Moderator organizacyjny organizacji A przekazywał tę informację do moderatora organizacyjnego organizacji B, a ten z kolei do uczestnika ćwiczeń w swojej organizacji (moderator główny był informowany o wystąpieniu takiej komunikacji poprzez obserwacje faktu korespondencji pomiędzy moderatorami organizacyjnymi). Przyjęcie takiej zasady komunikacji, choć odbiegające od zwyczajowo przyjętej, było niezbędne ze względu na konieczność jej dokumentacji na potrzeby ćwiczeń. W sytuacji, kiedy wskazana do komunikacji organizacja nie był uczestnikiem ćwiczeń CEP15, moderator organizacyjny organizacji A postępował zgodnie z zasadami komunikacji przewidzianymi dla komunikacji z podmiotami nieuczestniczącymi w ćwiczeniach.

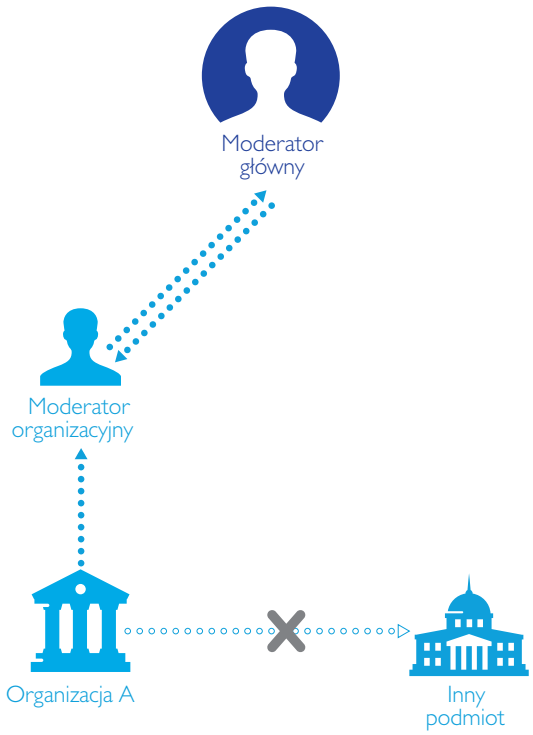
Rysunek 2.
**Zasady komunikacji pomiędzy organizacjami.**



### 7.4.3 Komunikacja z innymi podmiotami

W trakcie ćwiczeń dopuszczona była komunikacja pomiędzy organizacjami a innymi podmiotami zewnętrznymi, które nie były uczestnikami ćwiczeń CEP15. Podmioty te były podgrywane przez moderatora głównego. Komunikacja odbywała się za pośrednictwem moderatorów organizacyjnych. W sytuacji kiedy uczestnik ćwiczeń z organizacji A chciał skomunikować się z innym podmiotem, informację tę przekazywał do swojego moderatora organizacyjnego (moderator organizacyjny organizacji A). W informacji zawierał dane dotyczące konkretnego adresata (nazwa podmiotu X, stanowisko lub podmiot wewnątrz struktury organizacyjnej) oraz treść komunikatu. Moderator organizacyjny organizacji A przekazywał tę informację do moderatora głównego. Moderator główny przekazywał informację zwrotną, która następnie trafiała do nadawcy informacji pierwotnej.

Rysunek 3.
**Zasady komunikacji pomiędzy uczestnikiem ćwiczeń a podmiotem niebiorącym udziału w ćwiczeniach.**



### 7.4.4 Wykorzystanie wewnętrznych i zewnętrznych systemów teleinformatycznych

W związku z tym, że CEP15 nie odbywały się w warstwie technicznej, interakcja z wewnętrznymi i zewnętrznymi systemami teleinformatycznymi była symulowana przez moderatora – odpowiednio – organizacyjnego lub głównego. Interakcja z systemem była inicjowana przez jego użytkownika wysłaniem emaila na adres moderatora organizacyjnego. 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 organizacyjnego 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.

Fot. 4: Centrum Koordynacji Ćwiczeń CEP15. Od lewej: Krystian Kochanowski (FBC), Dawid Osojca (FBC), Michał Grzybowski (FBC).

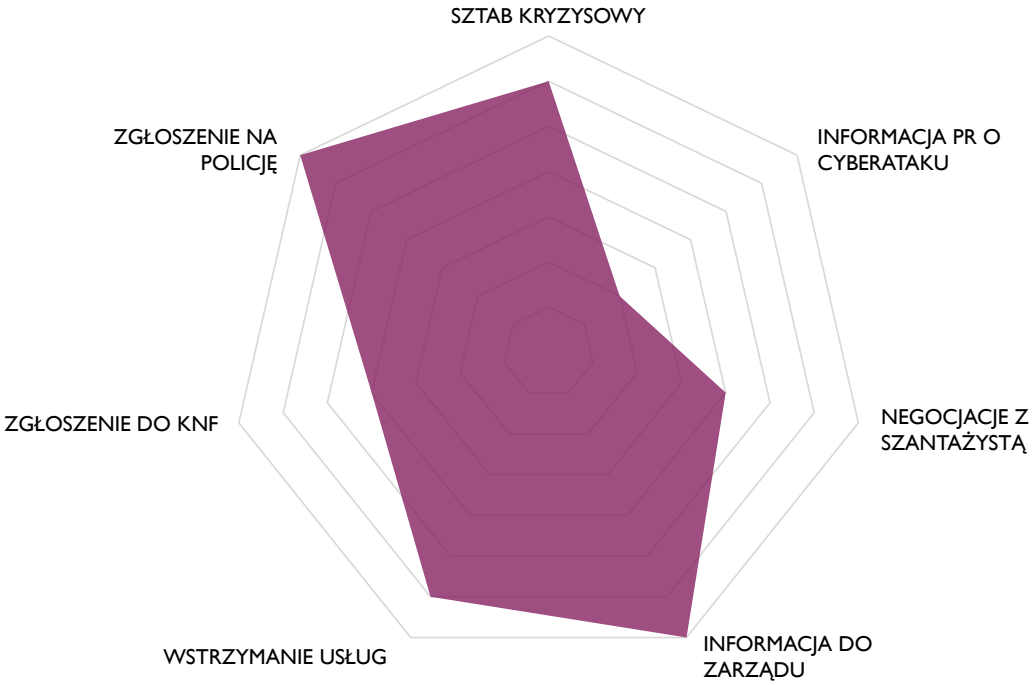
## 7.4.5 Kluczowe decyzje podejmowane w trakcie ćwiczeń

Organizatorzy w trakcie ćwiczeń monitorowali wystąpienie kilku ważnych zdarzeń, które w ich opinii mogły świadczyć o przebiegu ćwiczeń w poszczególnych organizacjach. Poniższy wykres przedstawia dane pokazujące w ilu z ćwiczących organizacji zaszły poszczególne zdarzenia. Monitorowano następujące zdarzenia:

- powołanie sztabu kryzysowego,
- poinformowanie przez służby PR organizacji o wystąpieniu cyberataku[12],
- podjęcie negocjacji z szantażystą[13],
- przekazanie informacji o cyberataku do zarządu organizacji,
- wstrzymanie (częściowe lub całkowite) świadczenia usługi,
- zgłoszenie przypadku cyberataku do KNF,
- zgłoszenie przypadku cyberataku na Policję.

Rysunek 4.

**Kluczowe zdarzenia w trakcie ćwiczeń. Liczba wystąpień w ćwiczących organizacjach.**




12. Mowa o informacji przekazywanej do wiadomości publicznej.

13. Kontakt z szantażystą nie jest oceniany jako działanie błędne. Umiejętnie prowadzony, w porozumieniu z organami ścigania, w oparciu o dobre praktyki, może być istotnym elementem strategii zarządzania kryzysowego.

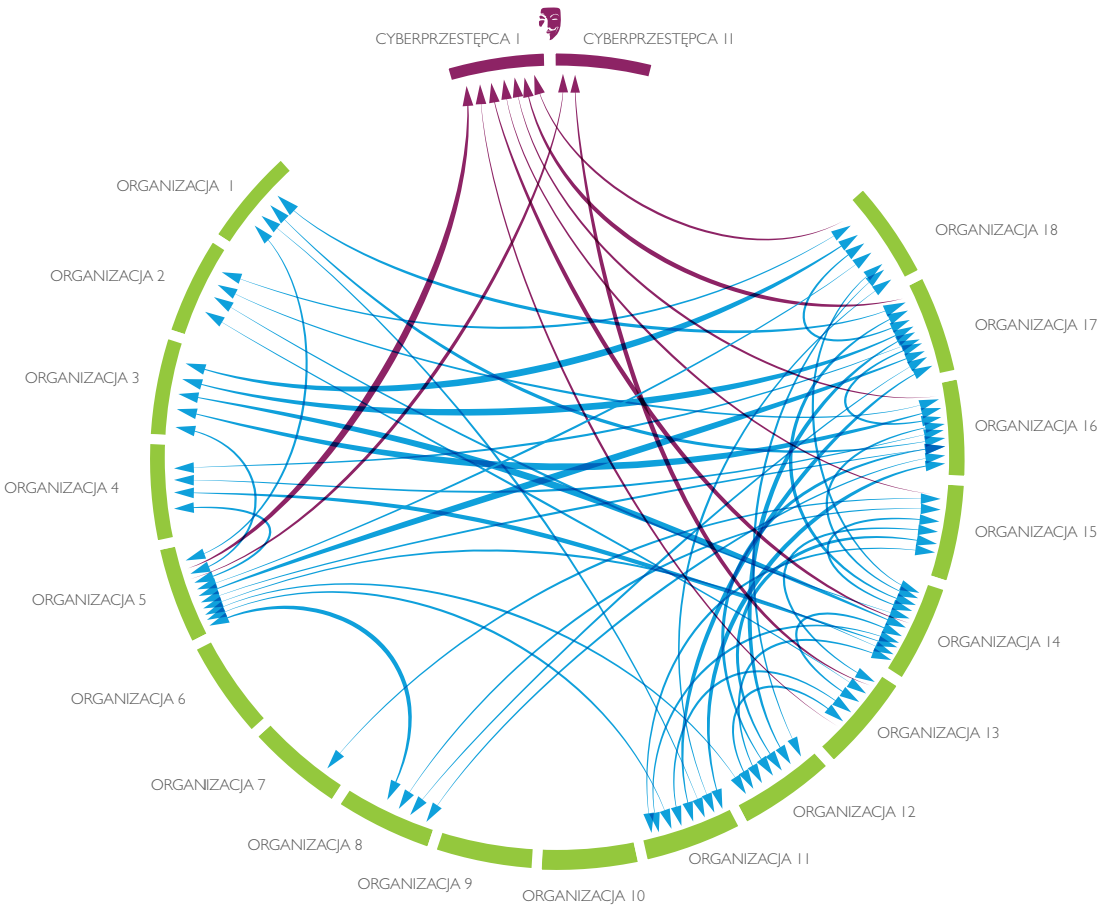
## 7.5 Dokumentacja i monitoring przebiegu ćwiczeń

Podstawową formę dokumentacji i monitoringu przebiegu ćwiczeń stanowiły raporty sytuacyjne oraz monitoring kontaktów pomiędzy poszczególnymi podmiotami. Począwszy od godziny 11:00 wszyscy moderatorzy organizacyjni co godzinę przekazywali swoje raporty sytuacyjne do moderatora głównego. Zawierały one między innymi:

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

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

Rysunek 5.
**Mapa relacji zachodzących pomiędzy podmiotami uczestniczącymi (i podgrywanymi) w czasie CEP15**



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

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

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

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

## 7.6 Przebieg ćwiczeń w warstwie komunikacji medialnej

Ćwiczenia Cyber-EXE™ Polska 2015 miały również za zadanie sprawdzić reakcje zespołów prasowych (zespołów PR) organizacji ćwiczących w zakresie działań komunikacyjnych rzeczników z klientami i mediami.

Ćwiczenia w warstwie medialnej są niezwykle istotne, zazwyczaj bowiem w dużym stopniu odbiór sytuacji kryzysowej poprzez klientów kształtowany jest właśnie w warstwie medialnej, która w największym stopniu wpływa na ich reakcje.

Warstwa komunikacji medialnej ćwiczenia Cyber-EXE™ Polska 2015 przeprowadzona została za pomocą internetowej strony komunikacji medialnej (CISKOM), do której dostęp w postaci loginu i hasła miały służby prasowe/PR ćwiczących.

Strona składała się z dwóch części. Na pierwszej ukazywały się komunikaty, które były symulacją komunikatów medialnych (TV, radio, prasa, agencje informacyjne, portale internetowe i portale społecznościowe, itp.) - takie komunikaty były tworzone przez grupę symulującą pracę mediów - grupa ta (osoby, które w trakcie ćwiczeń odgrywały rolę dziennikarzy) ściśle współpracowała z moderatorem głównym.

Druga część strony CISKOM zarządzana była przez zespoły prasowe (zespoły PR) ćwiczących. Mogły one prezentować tam swoje komunikaty oraz wszelką inną aktywność medialną, na którą decydowały się w związku z sytuacją kryzysową. Strona była tak skonstruowana, że organizacje ćwiczące mogły rozróżniać komunikaty, tzn. zaznaczać czy dany komunikat jest symulacją oświadczenia, komunikatu prasowego czy też np. odpowiedzią na skargi klientów na portalu społecznościowym firmy.

Dodatkowo grupa symulująca pracę mediów telefonicznie lub za pomocą poczty e-mail mogła zadawać pytania rzecznikom poszczególnych firm i prosić ich o uzupełnienie komunikatów lub dodatkowy komentarz:

# 8 Wnioski i rekomendacje

## 8.1 Wnioski podstawowe

Uczestnicy ćwiczeń zgodnie stwierdzili, że ich cele zostały przez ich organizacje w pełni osiągnięte. Zdaniem ćwiczących było ono jak najbardziej przydatne. 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 pracowników,
- sprawdzenie zachowań w sytuacjach kryzysowych,
- weryfikacja relacji z podmiotami trzecimi,
- zdobycie doświadczenia w sytuacji kryzysowej,
- test współdziałania ze służbami prasowymi organizacji.

Uczestnicy wskazywali na fakt, że ćwiczenia mogłyby przynieść jeszcze więcej pozytywnych efektów, jeśli na uczestnictwo w nim zdecydowałoby się więcej podmiotów i innych istotnych podmiotów sektora finansowego, wśród których wymienili: Krajową Izbę Rozliczeniową, Narodowy Bank Polski, Komisję Nadzoru Finansowego, operatorów telekomunikacyjnych, zespół CERT.GOV.PL, podmioty świadczące usługi reagowania na incydenty. Zaangażowanie tych ostatnich jest szczególnie ważne w sytuacji decyzji o realizacji ćwiczeń w warstwie technicznej.

Uczestnicy ćwiczeń zwrócili również uwagę, że warto byłoby, aby kolejne potencjalne edycje Cyber-EXE™ Polska zawierały elementy ćwiczeń technicznych, przygotowanych w oparciu o dedykowaną infrastrukturę teleinformatyczną. Tego typu podejście nadałoby jeszcze większej realności ćwiczeniom i w większym stopniu zaangażowałoby wewnętrzne służby techniczne, a także pozwoliłoby sprawdzić faktyczny poziom odporności organizacji na zagrożenia z cyberprzestrzeni.

## 8.2 Tabela wniosków i rekomendacji

| Wnioski | Rekomendacje |
|---|---|
| 1. Organizacje osiągnęły wewnętrzne cele związane z udziałem w ćwiczeniach CEP15. Udało się im realne przetestowanie istniejących procedur reagowania na zdarzenia oraz identyfikacja niepokrytych nimi obszarów. | Należy systematycznie organizować dalsze edycje ćwiczeń dla sektora finansowego. Warto również organizować ćwiczenia wewnętrzne w organizacjach dla przetestowania poszczególnych elementów systemu reagowania na incydenty. |
| 2. Nie udało się zidentyfikować zależności i współzależności pomiędzy podmiotami rynku finansowego, regulatorem tego rynku, a także innymi organizacjami mającymi wpływ na jego działanie takimi jak izby gospodarcze. Wynikało to przede wszystkim z braku reprezentacji innych podmiotów niż banki i ubezpieczyciele. | Kolejne edycje ćwiczeń powinny zgromadzić możliwie jak najwięcej podmiotów, które odgrywają istotną rolę w systemie reagowania na incydenty w całym środowisku finansowym. |
| 3. Informacja odnośnie możliwości wystąpienia ataku została w szybkim czasie przekazana do wszystkich komórek organizacyjnych, które powinny zostać zaangażowane w zarządzanie incydentem. | |
| 4. O sytuacji kryzysowej przewidzianej scenariuszem ćwiczeń szybko zostało poinformowane kierownictwo organizacji (przynajmniej członek zarządu odpowiedzialny za bezpieczeństwo IT), który koordynował reakcją organizacji lub wskazywał odpowiedzialnego za koordynację. | Warto określić „single point of contact"[14] na wypadek wystąpienia zdarzeń podobnych do przewidzianych scenariuszem ćwiczeń. Określenie osoby lub komórki organizacyjnej, która koordynowałyby komunikacje i działania podejmowane przez poszczególne komórki organizacyjne do momentu zaangażowania zarządu lub powołania zespołu (sztabu) kryzysowego znacznie zmniejsza „chaos informacyjny", a także przyspiesza znalezienie rozwiązania problemu. Takim SPoC mogłaby być osoba o wysokich kompetencjach, podejmująca na co dzień decyzje operacyjne. |

14. Kontaktem może być zespół, np. zespół odpowiedzialny za obsługę incydentów bezpieczeństwa, uzupełniony o wyznaczonych koordynatorów działań (SPoC) dla poszczególnych obszarów (PR, obsługa klienta itp.) lub np. zespół, składający się z SPoC dla poszczególnych obszarów..

| Wnioski | Rekomendacje |
|---|---|
| 5. Tylko w jednej organizacji nie powołano sztabu kryzysowego. Zespoły były powoływane w różnych fazach ćwiczeń i w różnym składzie. | Należy rozwijać (doskonalić) prace nad regułami współpracy w rozwiązaniu problemu pomiędzy działem IT, Security Oficerem oraz PR, tworzącymi kluczowy zespół zarządzania kryzysowego w organizacji. Rekomendowany skład zespołu kryzysowego: BCM Oficer, COO, CIO, ABI, ISO przedstawiciele zespołów odpowiedzialnych za utrzymanie systemów, rzecznik prasowy. |
| 6. W organizacjach gdzie funkcjonują zespoły odpowiedzialne za bezpieczeństwo IT, zostały one szybko poinformowane przez komórki PR i obsługi klienta o zaistniałej sytuacji. Możliwe to było dzięki obecności procedur zgłaszania anomalii oraz właściwego poziomu wyszkolenia pracowników tych komórek. | |
| 7. We wszystkich ćwiczących organizacjach, w których funkcjonował adekwatny do scenariusza system bankowości elektronicznej, wstrzymano transakcje za pomocą platform internetowych do czasu wyjaśnienia (naprawienia) sytuacji. | Nieoczywiste jest na ile łatwość podjęcia tak znaczącej decyzji była podyktowana symulacyjnym charakterem ćwiczeń i czy podobne rozwiązanie przyjęto by w przypadku realnego ataku. W ramach oceny wewnętrznej ćwiczeń warto przeanalizować i usystematyzować tryb w jakim podjęto tę decyzję. |
| 8. Nie wszystkie ćwiczące organizacje poinformowały o występujących trudnościach Komisję Nadzoru Finansowego. Zaznaczyć należy jednak, że zasady współpracy pomiędzy organizacjami a KNF nie wymagają natychmiastowego informowania o zdarzeniach objętych scenariuszem ćwiczeń[15]. | Komisja Nadzoru Finansowego we współpracy z bankami i firmami ubezpieczeniowymi oraz Związkiem Banków Polskich i Polskiej Izby Ubezpieczeniowej, mogłaby określić jasne kryteria informowania o przypadkach naruszenia bezpieczeństwa teleinformatycznego. Kryteria te mogą być bardzo pomocne przy implementacji Dyrektywy NIS w polskim systemie prawnym. |

15. Pismo KNF z 26 kwietnia 2013 zawiera tylko ogólny zapis o potrzebie informowania UKNF o wystąpieniu DDoS (lub innych działań o podobnym charakterze) skutkujących istotnymi zakłóceniami w funkcjonowaniu banku, bez podania formy zawiadomienia, oczekiwanych szczegółów, itp. Dodatkowo znane są rekomendacje dotyczące bezpieczeństwa płatności internetowych: „Dostawcy usług płatniczych i systemy płatności powinni posiadać procedurę niezwłocznego informowania właściwych organów (tj. organów nadzoru oraz organów ds. ochrony danych), tam gdzie one istnieją, w przypadku wystąpienia istotnych incydentów bezpieczeństwa w zakresie świadczonych usług płatniczych."

| Wnioski | Rekomendacje |
|---|---|
| 9. Dwie z ćwiczących organizacji poinformowały się nawzajem o zdarzeniach – nie odbyło się to jednak na podstawie sformalizowanej procedury, a wynikało z relacji zawodowych osób odpowiedzialnych za bezpieczeństwo. Komunikacja prowadzona była drogą oficjalną. | Banki i firmy ubezpieczeniowe, we współpracy z ZBP i PIU, powinny określić zasady wymiany informacji pomiędzy sobą. Dotyczy to szczególnie sytuacji związanych z zarządzaniem kryzysowym. |
| 10. Występująca znaczna rozbieżność w charakterze działalności tegorocznych uczestników ćwiczeń spowodowała duże trudności w opracowaniu scenariusza odpowiadającego wszystkim. Z konieczności zatem scenariusz zawierał uproszczenia, które w trakcie ćwiczeń były przyczyną samodzielnej jego modyfikacji przez uczestników. | Należy dostosować grono podmiotów uczestniczących, kierując się podobnym profilem działalności. Takie działanie pozwoli na lepsze dostosowanie scenariusza ćwiczeń. To dopasowanie powinno iść w parze ze zwiększeniem liczby uczestników reprezentujących ćwiczące sektory. |
| 11. W przypadku naruszenia danych osobowych organizacje powiadomiły GIODO, mimo iż obecna sytuacja prawna nie określa takiego obowiązku. | GIODO we współpracy z bankami i firmami ubezpieczeniowymi oraz Związkiem Banków Polskich i Polskiej Izby Ubezpieczeniowej, mogłaby określić jasne kryteria informowania o przypadkach naruszenia bezpieczeństwa danych osobowych. Kryteria te mogą być bardzo pomocne przy implementacji nowego europejskiego rozporządzenia dotyczącego ochrony danych osobowych w polskim systemie prawnym. |
| 12. W większości przypadków wystąpił kontakt do zewnętrznego, komercyjnego zespołu CERT, świadczącego usługi wsparcia w reagowaniu na incydenty. | Uzasadnione jest powołanie CERT-u i ISAC-a (Information Sharing and Analysis Center) dla sektora finansowego. Istotną rolę mogłyby w tym odegrać PIU i ZBP[16]. Powinny być określone zasady funkcjonowania takich podmiotów. Umożliwi to działania w imieniu i na rzecz instytucji finansowych w przypadku wystąpienia sytuacji związanej z cyberatakiem. Uzasadnione jest również powołanie stosownych zespołów w strukturach każdej organizacji. |

16. W 2015 r. Związek Banków Polskich ogłosił powstanie Bankowego Centrum Cyberbezpieczeństwa, które w opinii przedstawicieli ZBP spełniać będzie wiele funkcji charakterystycznych dla działania CERT-u sektorowego.

| Wnioski | Rekomendacje |
|---|---|
| 13. Podejmowanie decyzji przez osoby z kierownictwa organizacji, szczególnie w obliczu presji czasowej, było czynnikiem kluczowym. | Podejmowanie decyzji na wyższym szczeblu, szczególnie w obliczu presji czasowej jest czynnikiem decydującym w dalszym postepowaniu i ograniczeniu skutków działania cybeprzestępców. W związku z tym konieczne jest uświadomienie kadry kierowniczej (w drodze szkoleń lub ćwiczeń) w takim stopniu, aby mogła ona sprawnie podejmować ważne decyzje. Do dyspozycji decydentów powinien pozostawać maksymalnie kompetentny i obiektywny zespół ekspercki, wspierający podejmowanie decyzji. Tę rolę może odgrywać sztab kryzysowy, przy jednoczesnym uczestnictwie zespołu, o którym mowa w rekomendacji nr 4. |
| 14. Jako niewystarczające oraz mało realistyczne zostało ocenione odgrywanie przez organizatorów roli służb oraz organów administracji. Zbyt duże opóźnienia oraz ogólnikowe odpowiedzi prowadziły do opóźnień w podejmowaniu decyzji po stronie ćwiczących. Należy przy tym zauważyć, że rzeczywista reakcja ze strony odpowiedzialnych służb jest, wobec braku miarodajnych przykładów, nieznana. | Konieczne jest zapewnienie w przyszłych edycjach ćwiczeń odpowiedniego zestawu ćwiczących organizacji, eliminujących konieczność podgrywania części ich uczestników. |
| 15. Większość działań podejmowanych przez pracowników ćwiczących organizacji była poprawna. Nie zawsze był możliwy udział w ćwiczeniu wszystkich komórek organizacyjnych odpowiedzialnych za zrządzenie incydentami. Dotyczyło to na przykład komórek grup kapitałowych, działających zagranicą. | Pracownicy dedykowani, uczestniczący w obsłudze typów zdarzeń przewidzianych w scenariuszu ćwiczeń, powinni brać udział w organizowanych przez poszczególne jednostki operacyjne, wewnętrznych szkoleniach, które dałyby im wiedzę i pewność działania w sytuacjach kryzysowych. Jest to szczególnie przydatne w przypadku nieszablonowych ataków, które podobnie jak w rzeczywistych zdarzeniach tego typu, niejednokrotnie wymagają indywidualnego podejścia i „wyjścia" poza obowiązujące według określonej procedury schematy podstępowań. |
| | W przypadku organizacji z kapitałem zagranicznym lub posiadających zagraniczne aktywa rekomendowane jest zaangażowanie w przyszłości oddziałów zagranicznych celem weryfikacji znajomości procedur i postępowania w podobnych sytuacjach krytycznych. Działania tego typu powinny być przeprowadzane ze szczególną starannością związaną z zachowaniem prawa i zaleceń KNF. |

| Wnioski | Rekomendacje |
|---|---|
| 16. Scenariusz dotknął istotnego aspektu korzystania z usług podmiotów trzecich, na przykład dostawców rozwiązań programistycznych. | Należy zapewnić sobie zdolność (ludzie i ich kompetencje oraz wyposażenie) do przeglądu i regularnie przeglądać kod źródłowy krytycznych aplikacji pod kątem jego integralności. Można to osiągnąć na przykład poprzez zapewnienie sobie prawa do dostępu do kodu źródłowego w celu przeprowadzenia niezależnego audytu kodu przez pracowników organizacji (jeśli organizacja zdecyduje się na utrzymywanie odpowiednich kompetencji po swojej stronie) lub firmy trzecie. |
| 17. Niektóre z organizacji w komunikacji z szantażystą korzystały z wewnętrznych regulacji (procedur) z tego zakresu. | Konieczne jest opracowanie podręcznika dobrych praktyk w zakresie negocjacji z szantażystami dla sektora finansowego. Razem z praktycznym szkoleniem dla osób decyzyjnych oraz osób biorących udział w rozmowach z szantażystą jak postępować w przypadku szantażu podniosłoby to skuteczność negocjacji. Zadanie to mogłoby być zrealizowane we współpracy z Policją. |

## 8.3 Wnioski dotyczące warstwy komunikacji medialnej CEP 2015

1. Pozytywnie należy ocenić fakt, że szczególnie w drugiej fazie ćwiczeń, służby PR-owe aktywnie komunikowały się z klientami i dziennikarzami. W większości organizacje 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. Reagowali na kontakt ze strony dziennikarzy, zarówno telefoniczny jak i za pośrednictwem poczty elektronicznej. W przypadku braku możliwości odebrania połączenia, oddzwaniali. Odpisywali także na zadawane pytania przez dziennikarzy. Wyjątkiem były dwie organizacje – jedna z nich nie kontaktowała się z mediami za pomocą platformy CISKOM w ogóle. Druga zaś podjęła komunikację tylko raz. W realnej sytuacji takie postępowanie – nie odpowiadanie na liczne oznaki niezadowolenia klientów na portalach społecznościowych – może być wykorzystane przez dziennikarzy do przedstawienia organizacji jako instytucji, która nie jest w stanie skutecznie zarządzać zaistniałą sytuacją.

2. Rzecznicy uczestniczących w ćwiczeniach podmiotów odpowiadając na pytania dziennikarzy, zarówno telefonicznie jak i za pomocą poczty elektronicznej, starali się utrzymać zakres informacji przedstawiony w ustalonych i opublikowanych wcześniej przez te organizacje komunikatach na platformie CISKOM.

3. Służby PR-owe prawie przy każdym komunikacie lub kontakcie telefonicznym z dziennikarzami powtarzały zapewnienie, że pieniądze oraz dane klientów są bezpieczne. Taki przekaz należy ocenić pozytywnie – bezpieczeństwo powierzonych bankom i ubezpieczycielom środków finansowych oraz informacji to najistotniejsza kwestia dla klientów.

Fot. 5: Zespół medialny ćwiczeń CEP15. Od lewej: Izabella Laskowska ( MF) i Adrianna Maj (FBC), Paweł Majcher (RCB), Anna Gosławska – Hrychorczuk (RCB), Beata Kałowska (FBC), Anna Bracik (Deloitte)

4. Żadna z ćwiczących organizacji nie podała w swoich komunikatach prawdziwej przyczyny problemów, które zakłócają funkcjonowanie systemów informatycznych, a co za tym idzie normalne świadczenie usług. Organizacje odsyłały zainteresowanych klientów do biur obsługi klientów, infolinii lub przekazywały komunikaty informujące o tymczasowych problemach technicznych, które w żaden sposób nie zagrażają klientom. Rzecznicy zapewniali, że „specjaliści pracują nad tematem i trwają starania, by jak najszybciej przywrócić normalne funkcjonowanie systemów informatycznych". Taka strategia jest zrozumiała w początkach kryzysu, jednak w miarę jego rozwoju klienci mają prawo do bardziej szczegółowej informacji. Należy zwrócić uwagę na to, że strategia zaprzeczania faktom, może spowodować poważny kryzys wizerunkowy. Potwierdzeniem tej tezy jest przykład rzeczywistego ataku na polski bank w 2015 roku, kiedy rzecznicy tego banku przez wiele dni negowali prawdziwą przyczynę problemu.

5. Tylko dwie organizacje wysłały oświadczenie na stronie www (symulacja za pomocą platformy CISKOM), w którym potwierdziła, że miał miejsce kontakt szantażysty z firmą, od razu dodając, że sprawca został zatrzymany. Informacji towarzyszył komentarz, że dane klientów są bezpieczne.

6. Pozytywnie należy ocenić fakt, że komunikaty zawierały przeprosiny za utrudnienia i wspomniane „problemy techniczne".

7. Ćwiczące organizacje nie reagowały na ogólne informacje pojawiające się w mediach społecznościowych, dotyczące symulowanych problemów, które dotknęły ćwiczących. Większość reagowała dopiero, gdy byli wymienieni z nazwy lub w odpowiedzi na telefony dziennikarzy do konkretnych firm oraz pytań dziennikarzy drogą e-mail. Należy uznać, że było to prawidłowe działanie – organizacje nie odnosiły się do zarzutów, jeśli nie były one kierowane bezpośrednio do nich. W pojedynczych organizacjach zdarzały się jednak sytuacje, gdy brakowało reakcji biura prasowego, mimo że zarzuty były kierowane do konkretnej organizacji, wymienianych z nazwy - takie działanie należy ocenić negatywnie, gdyż pozwalały na formułowanie dowolnych wniosków i stwierdzeń autorom tych publikacji, co bez reakcji zainteresowanej organizacji mogło doprowadzić do przedstawienia rzeczywistej sytuacji w niekorzystny sposób.

8. W pojedynczym przypadku zaobserwowano niespójność komunikatów – pisemnego na portalu społecznościowym, w którym jest mowa o tym, że klienci mogą już bezpiecznie korzystać z serwisów a nieprawidłowości związane z autoryzacją przelewów są zlikwidowane, z komunikatem przekazanym telefonicznie dziennikarzowi, w którym podana została informacja, że problem wciąż istnieje i dotyczy niewielkiej grupy klientów. W realnej sytuacji taka niespójność może być wykorzystana przez dziennikarzy do przedstawienia organizacji jako instytucji, która nie jest w stanie zapanować nad kryzysem i pogrąża się w chaosie.

9. Każda z organizacji prowadziła zupełnie niezależne działania komunikacyjne, mimo iż wiadomości w mediach wyraźnie mówiły o problemach wielu firm z sektora finansowego (atakach na wiele firm). Informacja od szantażysty, jaka pojawiła się w mediach, również mówiła o tym, że kontaktował się on z kilkoma organizacjami. W komunikatach trzech podmiotów, pojawiły się wzmianki, które wskazują na to, że ćwiczące zespoły prasowe podjęły próbę współpracy ze sobą oraz instytucjami zewnętrznymi. Dziennikarze usłyszeli od trzech różnych organizacji informację o tym, że organy zewnętrzne wydadzą raport na temat ostatnio zaistniałych problemów w instytucjach finansowych, w tym jedna z firm

w komunikacji za pośrednictwem poczty e-mail wspomina o tym, że: „we współpracy ze Związkiem Banków Polskich oraz innym Bankami przygotowywane jest wspólne oświadczenie dotyczące ataków hakerskich na Banki". Pozytywnie należy ocenić fakt, że po raz pierwszy w ćwiczeniach Cyber-EXE™ Polska zaobserwowaliśmy próbę współpracy firm ćwiczących oraz firm zewnętrznych. W związku z narzuconymi ograniczeniami czasowymi ćwiczeń[17] niemożliwe jest zweryfikowanie czy współpraca okazałaby się skuteczna. Banki i firmy ubezpieczeniowe, we współpracy z ZBP i PIU, powinny określić warunki konieczne do spełnienia, które pozwolą na wydanie wspólnego komunikatu w sytuacji kryzysowej.

10. Dwie z ćwiczących organizacji oprócz zapewnień, że pieniądze klientów są bezpieczne i zaleceniu kasowania błędnych smsów oraz zapewnieniu, że firma pracuje nad rozwiązaniem problemu, poinformowały o tym jakie usługi nie są zagrożone i które są bezpieczne: „występują utrudnienia w dostępie do bankowości elektronicznej, natomiast korzystanie z kart płatniczych oraz bankomatów i wpłatomatów przebiega bez utrudnień". Ponadto podane zostało zalecenie zlecania przelewów bezpośrednio w placówkach Banku. Tego typu informacja byłaby wskazana także w komunikatach pozostałych instytucji.

11. Komunikaty podmiotów ćwiczących często nie były dostosowane do rodzaju kanału komunikacyjnego. Informacje przekazywane przez twitter.com zawierały najczęściej więcej niż dopuszczalne 140 znaków. Można jednak założyć, że ten problem nie wystąpiłby w czasie realnej sytuacji – po prostu nie da się opublikować na Twitterze dłuższej wiadomości.

17. Tego typu ograniczenie dotyczy również innych elementów ćwiczeń, jak na przykład „dokończenia" interakcji z szantażystą.

# 9 Podziękowania

Ćwiczenia Cyber-EXE™ Polska 2015 nie mogłyby się odbyć bez dobrej woli i wyjątkowego zaangażowania wszystkich uczestniczących w nim organizacji, a zwłaszcza osób, które brały aktywny udział w jego organizacji. Fundacja Bezpieczna Cyberprzestrzeń, jako organizator ćwiczeń, dziękuje im wszystkim za odwagę w realizacji bardzo ważnego przedsięwzięcia dla sektora finansowego w Polsce, za wielkie zaangażowanie w czasie wielomiesięcznych przygotowań, samego dnia ćwiczeń oraz pracy włożonej w ocenę przedsięwzięcia, przygotowanie wniosków i rekomendacji.

Dziękujemy współorganizatorom – Rządowemu Centrum Bezpieczeństwa i firmie doradczej Deloitte za wszelkiego rodzaju wsparcie przy organizacji ćwiczeń oraz aktywny merytoryczny udział w jego przygotowaniu i przeprowadzeniu. Merytoryczne i organizacyjne doświadczenia obydwu współorganizatorów były wielkim wkładem w końcowy sukces przedsięwzięcia.

Dziękujemy wszystkim uczestnikom ćwiczeń, tj. organizacjom, które zdecydowały się na udział w ćwiczeniu. Odwaga, współdziałanie i otwartość reprezentantów organizacji pozwoliła na przygotowanie ciekawych scenariuszy, sprawnych ćwiczeń i wyciągnięcie pożytecznych wniosków.

Dziękujemy również Ministerstwu Finansów, Komisji Nadzoru Finansowego oraz Związkowi Banków Polskich za objęcie patronatem tegorocznej edycji ćwiczeń

# 10 Słowniczek skrótów

| | |
|---|---|
| **CEP15** | Cyber-EXE™ Polska 2015 |
| **CERT** | Computer Emergency Response Team |
| **CISKOM** | Internetowy System Komunikacji Medialnej |
| **CKC** | Centrum Koordynacji Ćwiczeń |
| **ENISA** | European Network and Information Security Agency |
| **FBC** | Fundacja Bezpieczna Cyberprzestrzeń |
| **KNF** | Komisja Nadzoru Finansowego |
| **PIU** | Polska Izba Ubezpieczeniowa |
| **PR** | Public Relations |
| **RCB** | Rządowe Centrum Bezpieczeństwa |
| **SPoC** | Pojedynczy Punkt Kontaktu |
| **ZBP** | Związek Banków Polskich |

# Notatki


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