CYBER-EXE POLSKA 2024

Raport z ćwiczeń

Cyber-EXE Polska 2024

FUNDACJA bezpieczna cyberprzestrzeń

EY
Shape the future with confidence

SIMSPACE

splunk>

mastercard

CROWDSTRIKE

Spis treści

Szanowni Państwo,

Z wielką satysfakcją oddajemy w Państwa ręce raport z ćwiczeń Cyber-EXE Polska 2024. Fundacja Bezpieczna Cyberprzestrzeń, organizator tego przedsięwzięcia, miała zaszczyt współpracować z szerokim gronem partnerów, których wsparcie i zaangażowanie były kluczowe dla powodzenia projektu. Wspólnie stworzyliśmy platformę, która nie tylko umożliwiła praktyczne przetestowanie procesów dostosowania do nadchodzących regulacji DORA, ale także dała okazję do wzmacniania współpracy w sektorze finansowym.

Ćwiczenia Cyber-EXE Polska odbywają się już od 2012 roku i są dowodem na to, jak wielką wartość ma współpraca różnych podmiotów w obliczu dynamicznie zmieniających się cyberzagrożeń. Sektor finansowy, który jest najczęściej ćwiczącym, miał dzięki wspólnemu wysiłkowi okazję nie tylko sprawdzić swoje przygotowanie, ale także wymienić doświadczenia i najlepsze praktyki z zakresu reagowania na incydenty. Jesteśmy też przekonani, że kilka edycji ćwiczeń znacząco przyczyniło się do zacieśnienia operacyjnej współpracy sektorowej.

Dziękujemy wszystkim partnerom, którzy wspierali Fundację w organizacji tego wydarzenia, w szczególności firmie doradczej EY Polska oraz CSIRT KNF, a także CSIRT-om poziomu krajowego, firmom Simspace, Splunk, Mastercard i CrowdStrike. Zaangażowanie wszystkich Partnerów przyczyniło się do sukcesu tego przedsięwzięcia. Wierzymy, że wyniki tych ćwiczeń oraz wyciągnięte z nich wnioski przyczynią się do podniesienia poziomu cyberbezpieczeństwa całego sektora finansowego w Polsce, a doświadczenia tego sektora będą również wykorzystane przez innych.

Zapraszam do lektury raportu i korzystania z przedstawionych w nim rekomendacji, które mogą stać się fundamentem dalszych działań na rzecz budowy bezpiecznej cyberprzestrzeni w Polsce.

Mirosław Maj
Prezes Fundacji
Bezpieczna Cyberprzestrzeń

Jakub Teska
Partner, Zespół Technology Consulting
EY Polska

Wprowadzenie

Ćwiczenia Cyber-EXE Polska 2024 (dalej CEP24) to kontynuacja serii ćwiczeń z tego cyklu realizowanych dla sektora bankowego w latach 2013, 2015 i 2018. Bezpośrednią inspiracją i punktem wyjścia zorganizowania ich po raz kolejny było zbliżające się wejście w życie rozporządzenia DORA.

DORA oraz nowelizacja ustawy o krajowym systemie cyberbezpieczeństwa (UoKSC) to istotne wyzwanie dla sektora finansowego, ponieważ wymuszają dostosowanie procesów i procedur w obszarze cyberbezpieczeństwa. Kluczową rolę w tych przepisach odgrywają regulacyjne standardy techniczne (RTS) opracowane przez organy nadzorcze, mające na celu ujednolicenie sposobu realizacji wymogów i zapewnienie wysokiego, zharmonizowanego poziomu bezpieczeństwa.

RTS dotyczący klasyfikacji incydentów jako poważne nakłada na podmioty finansowe obowiązek precyzyjnej ich oceny. Z kolei RTS dotyczący treści zgłoszeń incydentów poważnych oraz terminów ich raportowania określa wymogi co do struktury i zawartości raportów oraz ramy czasowe zgłaszania incydentów.

Ćwiczenia CEP24 były odpowiedzią na te wyzwania umożliwiając podmiotom sektora finansowego przetestowanie gotowości do spełnienia wymagań nowych regulacji, przy czym weryfikacji zostały poddane nie tylko warstwa procesowa (procedury), ale również zdolności techniczne zespołów zaangażowanych w reakcję na cyberzagrożenia. Ich zakres w dużym stopniu wychodzi naprzeciw rekomendacjom, które pojawiały się w poprzednich edycjach ćwiczeń. W niniejszym raporcie przedstawiono opis ćwiczeń, metodykę, przebieg oraz analizę wyników, która umożliwiła przygotowanie wniosków i nowych rekomendacji.

Organizatorzy i partnerzy ćwiczeń

Organizatorem ćwiczeń Cyber-EXE Polska 2024 była Fundacja Bezpieczna Cyberprzestrzeń (dalej FBC).

Partnerem głównym była firma doradcza EY.

Organizację ćwiczeń wsparli również pozostali partnerzy: SimSpace, Splunk, Mastercard oraz CrowdStrike.

Uczestnicy ćwiczeń

W ćwiczenia zaangażowanych było 18 podmiotów, a aktywnie ćwiczącymi byli:

- Santander SA
- mBank SA
- Alior Bank SA
- Pekao SA
- Bank Ochrony Środowiska SA
- ING Bank Śląski SA
- BNP Paribas Bank Polska SA
- Bank Gospodarstwa Krajowego
- CSIRT sektorowy – CSIRT KNF działający w strukturach Komisji Nadzoru Finansowego
- CSIRT-y poziomu krajowego:
  - CSIRT NASK – działający w strukturach Naukowej i Akademickiej Sieci Komputerowej – Państwowego Instytutu Badawczego,
  - CSIRT GOV – działający w strukturach Agencji Bezpieczeństwa Wewnętrznego,
  - CSIRT MON – działający w strukturach Ministerstwa Obrony Narodowej.

Zespół projektowy

Zespół projektowy składał się z przedstawicieli FBC, EY, SimSpace oraz CSIRT KNF. Celem jego prac było opracowanie szczegółowych scenariuszy ćwiczeń, integracja warstw, w których się odbywały oraz zaprojektowanie systemu punktacji, który umożliwiał uczestnikom bieżący wgląd w wyniki ich działań. Zespół projektowy pracował od czerwca 2024 roku. W trakcie kilkunastu spotkań opracowano spójny plan ćwiczeń, przygotowano infrastrukturę techniczną umożliwiającą symulację incydentów i zdalne monitorowanie działań uczestników. Prace zespołu obejmowały także analizę wymagań regulacyjnych i bieżące dostosowywanie elementów ćwiczeń umożliwiających osiągniecie ich celów.

Cele ćwiczeń

Celem głównym CEP24 było przygotowanie podmiotów sektora finansowego do wdrożenia i działania zgodnie z nowymi regulacjami z zakresu cyberbezpieczeństwa (rozporządzenie DORA, nowelizacja UoKSC).

Celami szczegółowymi były:

1. Weryfikacja procesu klasyfikacji incydentu jako poważny zgodnie z wytycznymi właściwych regulacyjnych standardów technicznych (RTS).
2. Weryfikacja kompetencji zespołów technicznych cyberbezpieczeństwa do analizy artefaktów i zbierania informacji niezbędnych do zgłoszenia incydentu poważnego.
3. Weryfikacja współpracy zespołów technicznych i pozostałych komórek organizacyjnych w wypełnianiu formularza zgłoszenia incydentu poważnego.
4. Ocena przydatności formularza zgłoszenia incydentu poważnego, opracowanego przez KNF na podstawie RTS.
5. Weryfikacja procesu współpracy banków z CSIRT KNF.

Celem dodatkowym, biorąc pod uwagę udział w ćwiczeniu CSIRT KNF oraz CSIRT-ów krajowych, była weryfikacja współpracy pomiędzy CSIRT-em poziomu krajowego, sektorowym a CSIRT-ami poziomu krajowego.

Metodyka przeprowadzenia ćwiczeń

Warstwy ćwiczeń

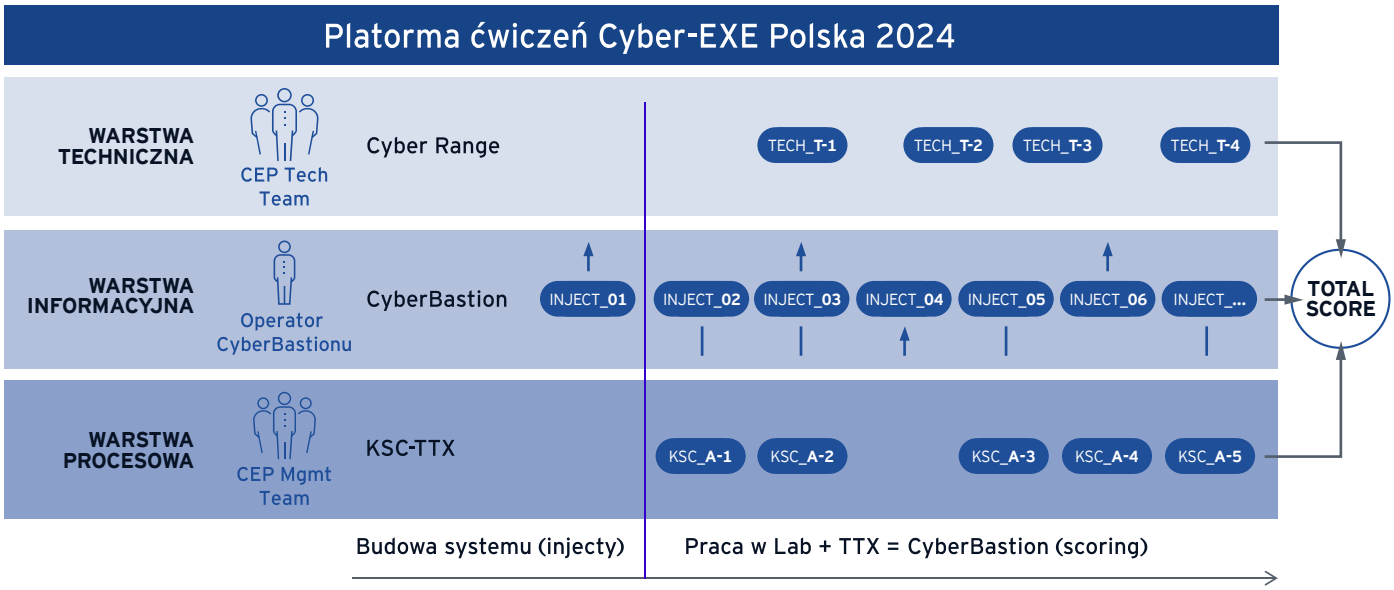
Ćwiczenia były zrealizowane w trzech wzajemnie powiązanych warstwach, by umożliwić osiągnięcie wszystkich celów. Każda warstwa miała na celu sprawdzenie różnych zdolności w zakresie cyberbezpieczeństwa w organizacji i umożliwiała kompleksową symulację działań obronnych oraz reagowanie na symulowane incydenty.

Warstwa informacyjna była realizowana w aplikacji CyberBastion. Pozwalała na symulację podejmowania decyzji związanych z inwestowaniem w zabezpieczenia i reagowaniem na dynamicznie rozwijający się incydent. Dla każdego ćwiczonego scenariusza podczas CEP24 w CyberBastion pojawiały się wprowadzenia (tzw. injecty) o charakterze informacyjnym oraz przedstawiające kolejne kroki atakującego. W tej warstwie uczestnicy mogli zweryfikować skuteczność swoich działań, ponieważ poza przekazywaniem injectów w CyberBastionie prezentowana była również ogólna punktacja sumująca dane wynikowe z pozostałych warstw.

Warstwa techniczna była realizowana w środowisku klasy cyber range, w którym symulowano fragment środowiska IT organizacji. Było to środowisko fikcyjne, nieodzwierciedlające konkretne środowisko uczestników. Zadaniem ćwiczących była identyfikacja wskaźników kompromitacji *(Indicators of Compromise*, IoC) związanych z incydentem bezpieczeństwa odtwarzanym w danym scenariuszu. IoC możliwe do odnalezienia w cyber range były skorelowane z injectami scenariusza prezentowanymi w CyberBastionie. Celem w tej warstwie było sprawdzenie własnych zdolności technicznych uczestników (kompetencji technicznych zespołów reagowania). Zgłaszanie odnalezionych w cyber range IoC było punktowane.

Warstwa procesowa skupiała się na procedurach i miała na celu sprawdzenie efektywności komunikacji oraz współpracy pomiędzy różnymi podmiotami uczestniczącymi w ćwiczeniach. W tej warstwie były weryfikowane zdolności organizacji do skutecznego zgłoszenia incydentu CSIRT sektorowemu. Zgłoszenia były przekazywane za pośrednictwem poczty elektronicznej. Działanie było punktowane.

Rysunek 1 – schemat ideowy warstw ćwiczeń CEP24



Tryby działania

Ćwiczenia CEP24 zostały zrealizowane w dwóch trybach determinujących interakcje pomiędzy uczestnikami ćwiczeń:

Tryb samodzielnego działania w pierwszym scenariuszu

Banki ćwiczyły indywidualnie i nie mogły komunikować się z pozostałymi pozostałymi ćwiczącymi organizacjami, oprócz komunikacji wymaganej regulacjami. Każdy z banków podejmował samodzielne decyzje oraz realizował zadania w oparciu o dostępne informacje i własne zasoby. Uczestnicy musieli polegać wyłącznie na swojej wiedzy, doświadczeniu i udostępnionych narzędziach. Komunikacja wewnętrzna odbywała się na ogólnych zasadach przyjętych w danej organizacji (maile, telefony, wiadomości tekstowe w komunikatorach, spotkania online). Natomiast komunikacja zewnętrzna została ograniczona do zespołów CSIRT uczestniczących w ćwiczeniu i dozwolona wyłącznie w ramach zgłaszanego incydentu, zgodnie z ustalonymi procedurami, bez udziału pozostałych organizacji ćwiczących.

Tryb samodzielnego działania służył identyfikacji potencjalnych luk we własnych zdolnościach do reakcji na incydent.

Tryb pełnej współpracy w drugim scenariuszu

W trybie pełnej współpracy uczestnicy mieli możliwość swobodnego kontaktu i wymiany informacji z innymi organizacjami. Możliwa była wymiana doświadczeń, wsparcie techniczne oraz konsultacje, by znaleźć najlepsze rozwiązania pojawiających się zagrożeń. Dzielono się konkretnymi informacjami powiązanymi z przebiegiem incydentu oraz ustaleniami poszczególnych uczestników (np. będącymi wynikami analiz w środowisku cyber range). W komunikacji zewnętrznej możliwe było użycie różnych form (maile, telefony, wiadomości tekstowe w komunikatorach, spotkania online). W tym trybie zespoły CSIRT uczestniczące w ćwiczeniach mogły aktywnie wspierać banki.

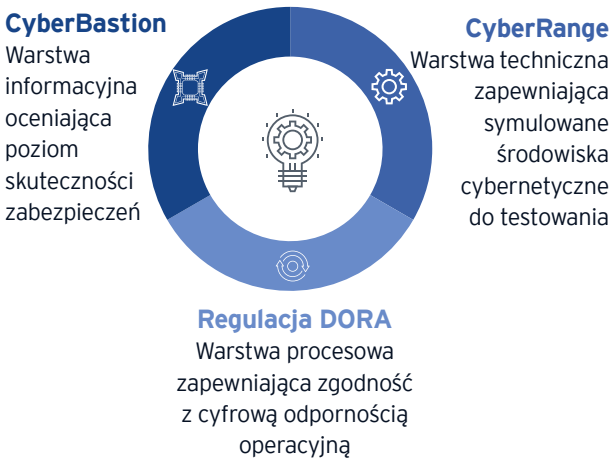
Tryb pełnej współpracy służył ocenie efektywności uczestników w dzieleniu się informacjami, koordynowaniu działań i wspólnego rozwiązywania problemów. Jak również sprawdzeniu, czy współpraca pozwala na skuteczniejsze i szybsze zażegnanie kryzysu.

Metody oceny i weryfikacji

Punktacja i ocena wyników w ćwiczeniach CEP24 zostały opracowane jako narzędzie bieżącego monitorowania postępów uczestników oraz skuteczności w realizacji zadań zgodnych z DORA, RTS oraz wytycznymi KNF. Pozwalały także sprawdzić umiejętności budowania systemu zabezpieczeń odpowiedniego dla ćwiczonego wektora ataku. W ćwiczeniach do rozdysponowania było 500 punktów, podzielonych na trzy główne składniki:

- cyber range,
- procedura zgłaszania incydentów zgodnie z DORA, przy użyciu formularza,
- CyberBastion.

Rysunek 2. Ocena Cyber-EXE Polska 2024



Taki system umożliwiał kompleksowe podejście do oceny działań uczestników.

W cyber range do zdobycia było 200 punktów. Ocenie poddano zdolność uczestników do odnajdywania i raportowania wskaźników kompromitacji (IoC) pozostawionych przez symulowanego atakującego. W trakcie ćwiczeń systematycznie analizowano raportowane IoC, a ocena była dokonywana automatycznie. Proces zbierania danych odbywał się w systemie zapewniając obiektywizm i dokładność wyników.

Zgłoszenie incydentu zgodnie z procedurami i poprawne wypełnienie formularza umożliwiało zdobycie 200 punktów. Oceniane były kompetencje uczestników w zakresie formalnej klasyfikacji incydentu jako poważnego oraz umiejętność kompletnego i zgodnego z wytycznymi jego zgłaszania. Ocenie podlegały:

- poprawność klasyfikacji incydentu jako poważnego,
- kompletność zgłoszenia,
- dokładność informacji,
- zgodność z procedurami,
- jasność komunikacji.

Dane zebrane w tej warstwie opierały się na formularzach zgłoszeniowych przekazanych przez uczestników, które następnie były analizowane przez CSIRT KNF. Taka forma oceny pozwalała na dogłębną weryfikację zgodności z wytycznymi RTS oraz wymogami KNF, a przyjęte kryteria oceny umożliwiały identyfikację ewentualnych obszarów do ulepszenia.

W CyberBastionie, w którym można było zdobyć pozostałe 100 punktów, oceniane było przygotowanie uczestników do ochrony systemu bezpieczeństwa banku przed zagrożeniami bezpośrednio wynikającymi ze scenariusza. W ramach tej warstwy uczestnicy musieli ocenić potencjalne ryzyko i podejmować decyzje dotyczące priorytetów inwestycji w hipotetyczne środki bezpieczeństwa banku. Kluczowym elementem oceny była zdolność zespołów do wyboru zabezpieczeń, które bezpośrednio wpływały na szybkość spadku odporności organizacji (Health Points - HP).

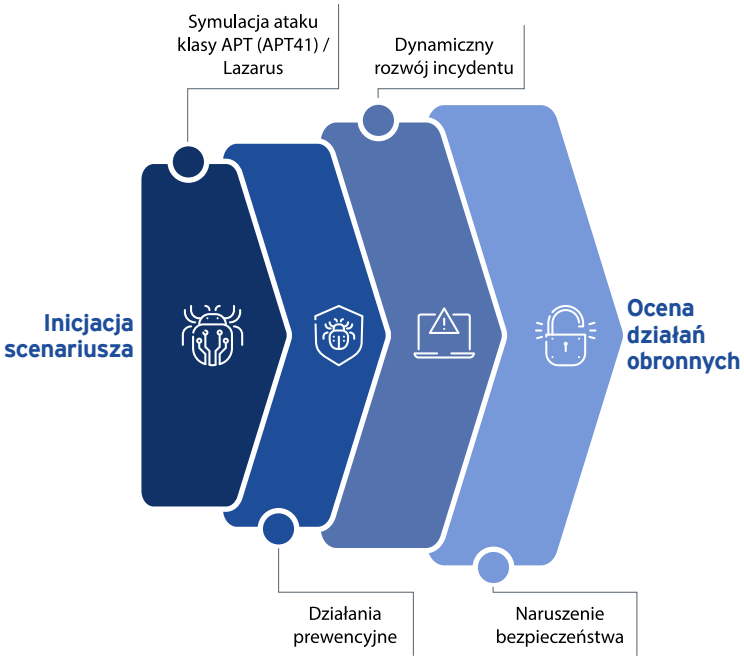
W każdym scenariuszu zabezpieczenia były inaczej punktowane. Zależało to od ich skuteczności w zakresie prewencji (identyfikacji i ochrony) oraz reakcji (odpowiedzi, wykrywania i odzyskiwania) w konkretnym, ćwiczonego w danym momencie scenariuszu. Ocena była dokonywana automatycznie, a narzędzie przyznawało punkty na podstawie decyzji zespołów dotyczących zakupu i wdrożenia zabezpieczeń.

Końcowa punktacja była sumą działań i decyzji podejmowanych przez uczestników we wszystkich trzech warstwach i pełniła rolę porównawczą pomiędzy ćwiczeniami. Należy jednak podkreślić, że celem punktacji nie była ocena działań, lecz umożliwienie uczestnikom śledzenie postępów oraz identyfikację efektywności. Ostateczne wnioski i rekomendacje dla sektora oraz refleksje uczestników dotyczące ich gotowości do spełnienia wymagań DORA zostały opracowane niezależnie od wyników punktacji.

Scenariusze ćwiczeń

W ramach CEP24 rozegrano dwa scenariusze symulujące ataki na sektor finansowy, wzorowane na rzeczywistych działaniach grup APT (*Advanced Persistent Threat*).

Rysunek 3. Proces symulacji incydentów w cyberbezpieczeństwie



W pierwszym scenariuszu odtworzono działania grupy APT41[1], a w drugim grupy Lazarus[2]. Każdy ze scenariuszy zakładał dynamiczną symulację rozwoju incydentu, w której kolejne injecty przedstawiały dalsze kroki atakującego, prowadzące do krytycznego naruszenia bezpieczeństwa, zgodnie z wymogami rozporządzenia DORA (szczegóły dotyczące scenariuszy znajdują się w załącznikach nr 2 i 3). Na realizację każdego scenariusza przeznaczono 165 minut. Scenariusze były realizowane w odmiennych trybach, co determinowało sposób interakcji i współpracy pomiędzy uczestnikami.

Projektując scenariusze przyjęto dwa kluczowe założenia:

1. Nieuchronność działań atakującego: w scenariuszach (symulacji) przewidziano, że działania atakującego nie mogą być zatrzymane. Rzeczywiste systemy bezpieczeństwa wdrożone w środowisku ćwiczącej organizacji lub wybrane w CyberBastion nie miały wpływu na przebieg symulacji ataku. Celem było stworzenie sytuacji, w której uczestnicy muszą zarządzać narastającym incydentem, gdy wszystkie mechanizmy obronne zostaną przełamane, co odpowiada obserwowanym w rzeczywistości atakom na sieci i systemy teleinformatyczne.

2. Incydent poważny: scenariusze zostały zaprojektowane tak, aby doprowadzić do wystąpienia incydentu poważnego, zgodnie z definicją rozporządzenia DORA. Uczestnicy musieli nie tylko reagować na zagrożenia, ale także koordynować działania naprawcze, współpracować z odpowiednimi organami oraz minimalizować skutki incydentu.

1 https://attack.mitre.org/groups/G0096/

2 https://attack.mitre.org/groups/G0032/

Fazy scenariusza

Każdy ze scenariuszy został podzielony na dwie fazy: budowy systemu bezpieczeństwa (prewencja) oraz reagowanie (reakcja). Każda z tych faz odzwierciedlała kluczowe elementy strategii obrony przed cyberzagrożeniami i miała na celu weryfikację różnych aspektów zdolności organizacji do zarządzania incydentami.

Faza Budowy Systemu Bezpieczeństwa

Uczestnicy byli odpowiedzialni za budowę wirtualnego systemu bezpieczeństwa na platformie CyberBastionu. Jej celem było zaplanowanie i wdrożenie odpowiednich mechanizmów ochrony przed zagrożeniami, zanim się zmaterializują. Każdy zespół dysponował z góry określonym, wirtualnym budżetem przeznaczonym na zakup różnych środków ochrony. Uczestnicy mieli do wyboru środki bezpieczeństwa podzielone na osiem kategorii:

Organizacja

Infrastruktura fizyczna

Cała sieć / Brzeg sieci

Sieć wewnętrzna

Urządzenia końcowe

Aplikacje

Dane

Źródła danych

Możliwość zakupu zabezpieczeń była dostępna aż do pojawienia się ostatniego injectu odwzorowującego wystąpienie negatywnego skutku incydentu, np. transferu poufnych danych poza organizację czy szyfrowania zasobów. Ostatni inject oznaczał wystąpienie incydentu poważnego i kończył możliwość dalszego kupowania zabezpieczeń.

Faza Reagowania na incydent

Wraz z pierwszym injectem odwzorowującym działania atakującego uczestnicy mogli przejść do fazy reagowania na zagrożenia. Została podzielona na dwie główne aktywności: pracę zespołu technicznego w cyber range[3] oraz współpracę zespołu zarządzania z odpowiednimi organami.

Praca w cyber range obejmowała:

- Monitorowanie zaimplementowanych systemów ITSec pod kątem podejrzanych aktywności,
- Identyfikację i analizę IoC, które wskazują na potencjalne incydenty bezpieczeństwa,
- Zgłoszenie zidentyfikowanych IoC.

W tej fazie zadaniem zespołów zarządzających była koordynacja reakcji organizacji na incydent oraz współpraca z odpowiednimi organami, takimi jak zespoły CSIRT (Computer Security Incident Response Team). Kluczowe znaczenie miało odpowiednie raportowanie incydentów do właściwych organów zgodnie z przyjętymi procedurami. Praca zespołów zarządzających obejmowała:

- Analizę wpływu incydentu na organizację, jego klasyfikację i podjęcie decyzji o eskalacji,
- Współpracę z zespołem technicznym, by otrzymać jak najwięcej technicznych informacji niezbędnych do zgłoszenia incydentu,
- Komunikację z zespołami CSIRT oraz innymi zewnętrznymi organami w celu zgłoszenia incydentu.

3 Praca w cyber range była możliwa od chwili zalogowania, przy czym obecność IoC była ściśle skorelowana z injectami w warstwie Cyber Bastionu

Rodzaje injectów

W scenariuszach ćwiczeń przewidziano dwa rodzaje wprowadzeń (injectów):

Injecty informacyjne

Przekazywane w fazie budowy systemu cyberbezpieczeństwa. Stanowiły podpowiedzi dotyczące charakteru ataku i zawierały wskazówki związane z nietypowymi działaniami w sieci, anomaliami w systemach, wykryciem złośliwego oprogramowania lub informacjami od podmiotów zewnętrznych wskazującymi na aktywność grupy APT. Ich celem była pomoc uczestnikom w identyfikacji zagrożenia i dostosowaniu strategii obrony. Injecty informacyjne pojawiały się również w fazie reakcji jako forma przypomnienia o konieczności realizacji niektórych obowiązków.

Injecty odwzorowujące działania atakującego

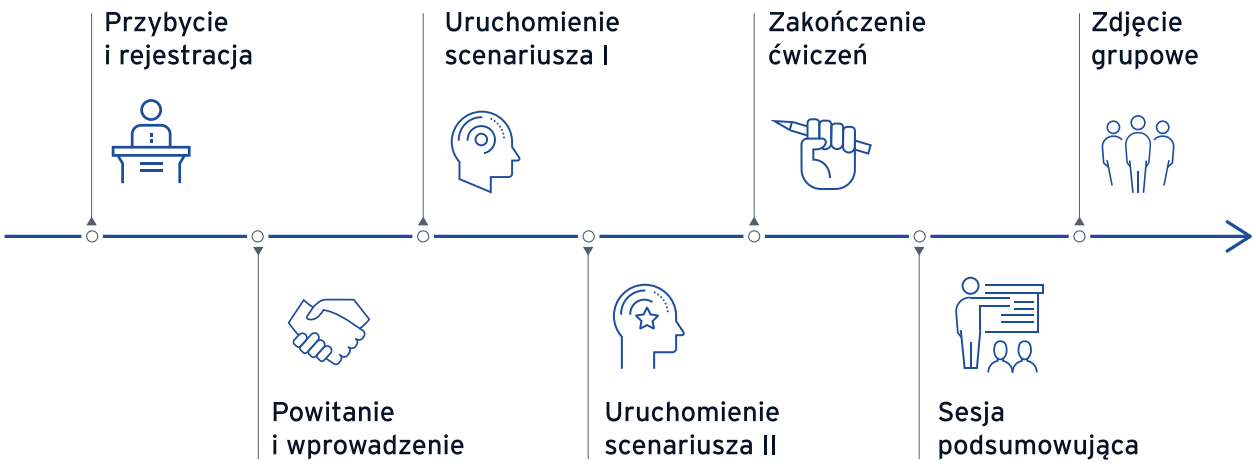
Przekazywane w fazie reagowania. Ilustrowały kolejne etapy działań atakującego koncentrując się na efektach uzyskanych w wyniku zastosowania określonych technik ataku. Każdy inject opisywał zdobyte przez atakującego informacje lub osiągnięte rezultaty, które przybliżały go do celu ataku. Działania te mogły obejmować np. eskalację uprawnień, przemieszczanie się wewnątrz sieci, kradzież danych, instalację złośliwego oprogramowania czy próby wyłączenia mechanizmów zabezpieczeń.

Przebieg ćwiczeń

Informacje podstawowe

Ćwiczenia Cyber-EXE Polska 2024 zostało przeprowadzone 26 września 2024 r. w godzinach 8:00–18:00. Centrum Koordynacji Ćwiczeń znajdowało się w siedzibie firmy EY Polska w Warszawie, Rondo ONZ 1.

Rysunek 4. Harmonogram ćwiczeń

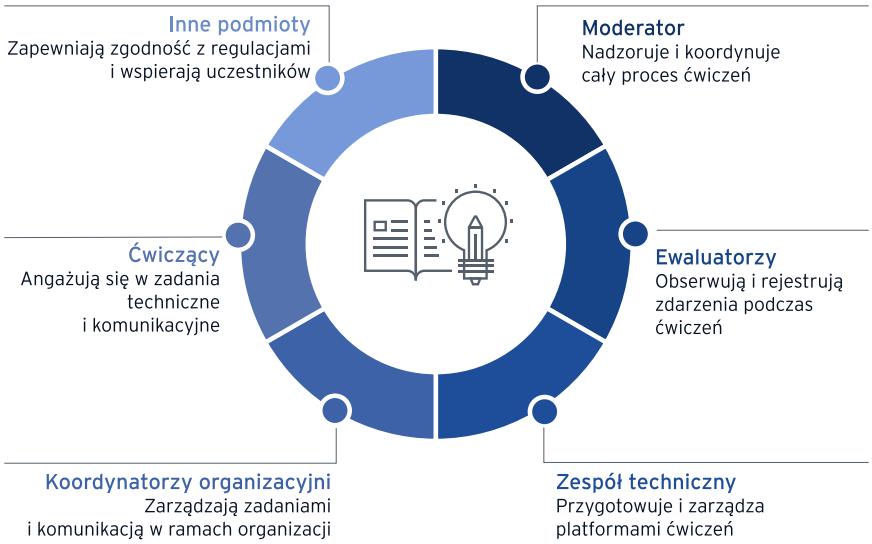


Ćwiczenia zaczęły się pierwszym scenariuszem. Aktywna faza ćwiczeń rozpoczęła się o godz. 10:00, a zakończyła się o godz. 16:45. Podczas podsumowującej sesji uczestnicy mieli okazję podzielić się swoimi wrażeniami oraz kluczowymi wnioskami.

Struktura organizacyjna ćwiczeń

W strukturze organizacyjnej ćwiczeń wyodrębniono następujące role:

Rysunek 5. Funkcje uczestników Cyber-EXE Polska 2024



Główny moderator

był odpowiedzialny za koordynację całości ćwiczenia, w tym za podejmowanie decyzji o uruchamianiu scenariuszy i współpracę z organizacyjnymi koordynatorami.

Ewaluatorzy

odpowiadali za obserwację przebiegu ćwiczeń, rejestrację zdarzeń i wsparcie głównego moderatora w ocenie realizacji ćwiczeń.

Zespół techniczny

przygotował i obsługiwał platformę ćwiczeń (CyberBastion, cyber range), odpowiadał też za organizację logistyczną oraz zbieranie danych dotyczących przebiegu ćwiczeń.

Organizacyjni koordynatorzy

byli odpowiedzialni za koordynację przebiegu ćwiczeń w ramach swoich organizacji, monitorowanie realizacji zadań, przekazywanie komunikatów oraz współpracę z głównym moderatorem i ewaluatorami.

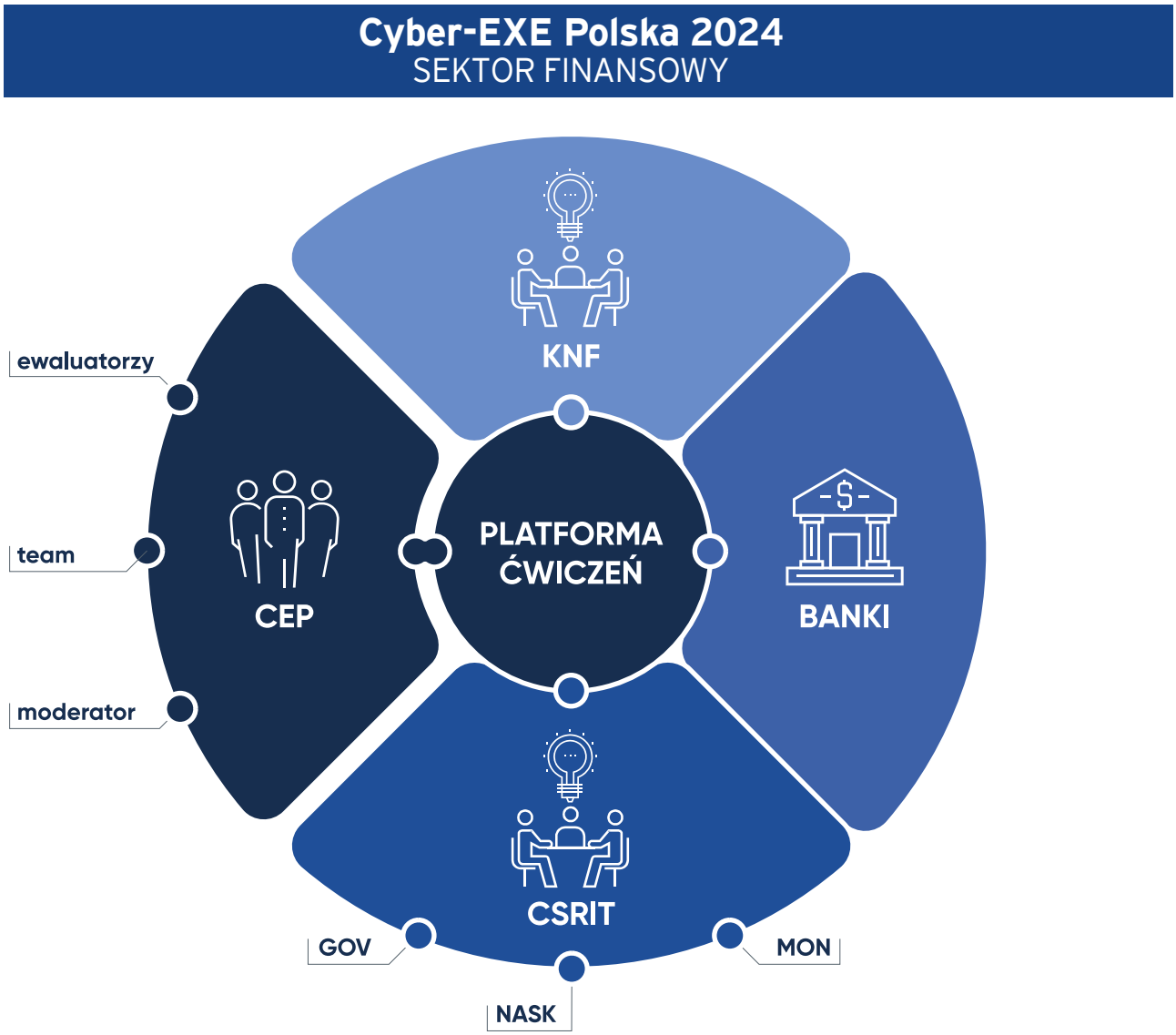
Ćwiczący

to przedstawiciele organizacji uczestniczących zaangażowani w realizację zadań technicznych i komunikacyjnych w odpowiedzi na symulowane incydenty.

Innymi podmiotami

byli przedstawiciele CSIRT KNF i CSIRTy krajowe (CSIRT NASK, CSIRT GOV, CSIRTy poziomu krajowego) zapewniający realizację przepisów DORA i UoKSC, w tym przyjmujący zgłoszenia o o incydentach poważnych i ewentualne wspierających uczestników ćwiczeń.

Rysunek 6. Struktura organizacyjna ćwiczeń Cyber-EXE Polska 2024



Ćwiczący byli podzieleni na dwie grupy. Pierwsza przebywała fizycznie w Centrum Kontroli Ćwiczenia (CKC). Pozostali członkowie zespołów uczestniczyli zdalnie z głównych lokalizacji swoich organizacji, a liczba uczestników nie była ograniczona. Taki podział umożliwiał efektywną współpracę na poziomie organizacji, przy jednoczesnym zachowaniu centralnego nadzoru w CKC.

Komunikacja w trakcie ćwiczeń CEP24

W trakcie ćwiczeń przewidziano różne formy komunikacji, których celem było zapewnienie skutecznego i uporządkowanego przepływu informacji między uczestnikami, koordynatorami oraz moderatorem.

Komunikacja w relacji Bank – CSIRT KNF (lub CSIRT poziomu krajowego)

W komunikacji pomiędzy uczestniczącymi bankami a zespołami CSIRT przewidziano wykorzystanie przeznaczonych do tego kanałów e-mailowych (skrzynek mailowych w domenie cyberexepolska.pl). Zapewniały bezpieczną, kontrolowaną i uporządkowaną wymianę informacji. Komunikacja z zespołami CSIRT odbywała się wyłącznie w sposób oficjalny, jako część symulowanego procesu reagowania na incydenty. Przesyłane wiadomości zawierały pełne informacje wymagane przez odpowiednie procedury i przepisy (np. formularz zgłaszania incydentu poważnego, przygotowany przez KNF), takie jak: szczegóły techniczne incydentu, podjęte działania oraz inne istotne dane.

Komunikacja w relacji organizacja ćwicząca A – organizacja ćwicząca B

Komunikacja między organizacjami biorącymi udział w ćwiczeniach odbywała się za pośrednictwem standardowych środków: e-mail, telefon i komunikatory. Umożliwiało to sprawną współpracę, wymianę informacji, koordynację działań oraz podejmowanie wspólnych decyzji w trakcie ćwiczeń. W celu minimalizacji ryzyka nieporozumień lub przypadkowego wywołania rzeczywistego incydentu, każda wiadomość lub komunikat związany z ćwiczeniami były oznaczane jako „CYBER-EXE POLSKA 2024" lub skrótem „CEP24" w tytule bądź treści, co jednoznacznie wskazywało, że dotyczą symulowanych działań.

Komunikacja między organizacjami była prowadzona wyłącznie przez koordynatorów, którzy nadzorowali przebieg ćwiczeń w swoich organizacjach. Udział innych osób, np. członków zespołów technicznych, był możliwy tylko za zgodą koordynatora. Wymagane było także unikanie nieoznaczonych komunikatów, które mogłyby zostać uznane za rzeczywiste zgłoszenia lub incydenty. Wszystkie działania komunikacyjne realizowano zgodnie z zasadami poufności i wewnętrznymi politykami bezpieczeństwa informacji.

Komunikacja wewnątrz organizacji ćwiczącej

W komunikacji wewnętrznej pomiędzy zespołami w ćwiczących organizacjach wykorzystywano standardowe narzędzia: e-mail, komunikatory firmowe i platformy do zarządzania incydentami. Wszystkie wiadomości i komunikaty związane z ćwiczeniami były jednoznacznie oznaczane jako „CYBER-EXE POLSKA 2024" lub skrótem „CEP24", co jasno wskazywało ich symulacyjny charakter oraz zapobiegało przypadkowemu potraktowaniu ich jako rzeczywistych incydentów.

Koordynatorzy mieli możliwość angażowania dowolnych osób z organizacji w wewnętrzną komunikację związaną z ćwiczeniami. Dla zwiększenia jasności przekazu zalecano dodanie w stopce e-maili informacji o ćwiczebnym charakterze wiadomości oraz danych kontaktowych koordynatora organizacyjnego, co mogło być pomocne zwłaszcza dla osób niezaznajomionych z udziałem organizacji w ćwiczeniach. Uczestnicy byli zobowiązani do przestrzegania zasad poufności i wewnętrznych polityk bezpieczeństwa informacji. Ostateczny wybór metod i środków komunikacji pozostawiono w gestii każdej organizacji, pozwalając im dostosować procesy komunikacyjne do wewnętrznych potrzeb.

Komunikacja w relacji koordynator organizacji ćwiczącej – moderator ćwiczeń

W celu zapewnienia skutecznej koordynacji i monitorowania postępów ćwiczeń przewidziano możliwość bezpośredniej komunikacji pomiędzy koordynatorami organizacji uczestniczących a moderatorem. Ponieważ w Centrum Koordynacji obecni byli zarówno koordynatorzy, jak i moderator, to komunikacja odbywała się bezpośrednio lub za

pomocą przeznaczonego do tego adresu e-mailowego. Komunikacja z moderatorem miała na celu rozwiązywanie bieżących problemów operacyjnych, wyjaśnianie zadań oraz otrzymywanie informacji zwrotnej na temat postępów ćwiczeń.

Komunikacja z innymi podmiotami niebiorącymi aktywnego udziału w CEP24

Podczas ćwiczeń przewidziano możliwość komunikacji między uczestniczącymi organizacjami a zewnętrznymi podmiotami, które formalnie nie brały udziału. W takich przypadkach koordynator danej organizacji przesyłał wiadomość e-mail na przeznaczony do tego adres moderatora, który symulował odpowiedź w imieniu wskazanego adresata. W temacie wiadomości koordynator określał podmiot, z którym organizacja chciała się skontaktować (np. „Mail do Departamentu Cyberbezpieczeństwa Ministerstwa Cyfryzacji"), natomiast w treści zamieszczano zasadniczy komunikat skierowany do tego podmiotu. Taki sposób komunikacji umożliwiał możliwie realistyczne odwzorowanie reakcji podmiotów zewnętrznych na potrzeby symulacji.

Wnioski i rekomendacje

Wnioski i rekomendacje przedstawione w tym raporcie zostały opracowane na podstawie spostrzeżeń zebranych przez osoby oceniające w trakcie ćwiczeń, wyników ankiet przeprowadzonych wśród uczestników oraz podsumowania sporządzonego przez CSIRT KNF. Uwzględniają one również ocenę efektywności użytych narzędzi oraz sposób organizacji samych ćwiczeń. Wnioski (oznaczone jako „W") i rekomendacje (oznaczone jako „R") obejmują zarówno główny cel CEP24, jak i poszczególne cele szczegółowe.

Cel główny: przygotowanie podmiotów sektora finansowego do wdrożenia i działania zgodnie z nowymi regulacjami z zakresu cyberbezpieczeństwa (rozporządzenie DORA, nowelizacji UoKSC).

W Udział w ćwiczeniach pomógł w ocenie przygotowań banków do wdrożenia i działania zgodnie DORA.

R1 Kontynuować organizację ćwiczeń wśród podmiotów finansowych objętych rozporządzeniem DORA, aby umożliwić im regularną ocenę zgodności i doskonalenie procedur. Przyszłe ćwiczenia mogą umożliwić weryfikację innych elementów regulacji DORA niż uwzględnione w CEP24, co pozwoli na podejmowanie działań ulepszających i dostosowanych do najnowszych wyzwań.

R2 W przyszłych ćwiczeniach warto zaangażować dostawców usług zewnętrznych, aby przetestować efektywność komunikacji oraz reakcję na incydenty powiązane z usługami ICT świadczonymi przez strony trzecie.

Cel główny: scenariusze

W Scenariusze odzwierciedlały realne incydenty, z jakimi banki mogą się zetknąć. Co prawda pozwoliły na weryfikację celów ćwiczeń, ale były zbyt uproszczone i za mało zróżnicowane.

R Należy zwiększać zaawansowanie scenariuszy ćwiczeń. Scenariusze powinny uwzględniać bardziej złożone sytuacje wymagające koordynacji między zespołami technicznymi, zarządzającymi incydentem, a także przedstawicielami biznesu i zarządu, co pomoże w lepszym odwzorowaniu rzeczywistych procesów reagowania na incydenty.

Cel główny: współpraca

W1 Dzięki dwóm trybom ćwiczeń udało się potwierdzić hipotezę, że współpraca przynosi korzyści, które widać w końcowych rezultatach samodzielnych działań. W trybie pełnej współpracy między ćwiczącymi zespołami zauważono szybsze zgłoszenia incydentów oraz wyższą jakość informacji dotyczących wskaźników kompromitacji (IoC)[4].

R1 W kolejnych ćwiczeniach należy nadal realizować scenariusze współpracy zespołów ćwiczących. Natomiast instytucje finansowe powinny organizować dodatkowe szkolenia i warsztaty dotyczące skutecznej komunikacji i wymiany danych w czasie rzeczywistym, aby jeszcze bardziej poprawić współpracę zespołów oraz rozwijać poszczególne elementy tej współpracy.

W2 Wykorzystanie platformy MISP[5] do wymiany informacji pozwoliło sprawniej weryfikować zgromadzone dane oraz je wzbogacać. W rezultacie zmniejszyła się liczba błędnych zgłoszeń (false positives), co ułatwiło zespołom CSIRT szybszą i dokładniejszą ocenę incydentów.

R2 Należy propagować wdrażanie narzędzi do wymiany informacji o zagrożeniach lub automatycznej komunikacji między systemami do obsługi incydentów za pośrednictwem API (Application Programming Interface). Dzięki temu możliwe będzie szybkie i bezbłędne przekazywanie danych o incydentach między zespołami reagowania w różnych organizacjach, co znacząco usprawniłoby ich współpracę.

W3 Obecne podejście do wymiany wskaźników kompromitacji (IoC) jest niejednolite. Brakuje standaryzacji zarówno na poziomie przekazywania informacji do regulatora (KNF), jak i wewnątrz zespołów bankowych. Nie ma ustalonych wytycznych czy jednolitego formatu zgłaszania IoC. To powoduje niepewność, jakie informacje powinny być przekazywane i w jaki sposób.

R3 Wprowadzić jednolite wytyczne dotyczące formatu zgłaszania IoC zarówno na potrzeby regulatora (KNF), jak i wymiany informacji między zespołami bankowymi. Regulator powinien określić szczegółowe zasady dotyczące zgłaszanych IoC, w tym typy i format danych oraz przeprowadzić szkolenia dla pracowników banków. Jeśli wybranym narzędziem do wymiany IoC byłby np. MISP, by usprawnić analizę i wymianę informacji, zaleca się standaryzację

4 Dane przygotowane przez CSIRT KNF.
Zgłoszenie formularza wstępnego:
- Scenariusz 1: Średni czas zgłoszenia: 38 minut
- Scenariusz 2: Średni czas zgłoszenia: 30 minut

Zgłoszenie formularza śródokresowego:
- Scenariusz 1: Średni czas zgłoszenia: 108 minut
- Scenariusz 2: Średni czas zgłoszenia: 70 minut

Jakość zgłaszanych IoC:
Scenariusz 1:
- Formularze bez informacji o IOC: 19%
- Formularze z pojedynczymi lub szczątkowymi danymi: 30%
- Formularze z pełnymi informacjami o IOC: 51%

Scenariusz 2:
- Formularze bez informacji o IOC: 7%
- Formularze z pojedynczymi lub szczątkowymi danymi: 22%
- Formularze z pełnymi informacjami o IOC: 71%

5 MISP – Malware Information Sharing platform. Więcej o platformie: https://www.misp-project.org/

sposobu ich wprowadzania z uwzględnieniem dobrych praktyk dotyczących doboru tagów i taksonomii.

Cel główny: punktacja

W1 Próba przedstawienia wyników ćwiczeń w oparciu punktację została oceniona niejednoznacznie. Zdaniem uczestników była pomocna w szacowaniu skuteczności ich działań w czasie ćwiczeń, ale jednocześnie nie była w pełni reprezentatywna dla końcowych ocen. Trzeba jednak pamiętać, że celem ćwiczeń nie było zebranie jak największej liczby punktów, które były tylko formą uatrakcyjniającą ćwiczenia.

R1 Należy utrzymać punktowanie, ale konieczna jest poprawa metodyki przyznawania punktów oraz jej przejrzystości. Trzeba także zadbać o lepsze wyjaśnienie zasad uczestnikom, by wiedzieli, za jakie działania otrzymują punkty i jaki jest sposób ich przyznawania. Poza tym muszą na bieżąco otrzymywać aktualne wyniki, gdyż będzie to elementem motywacji i poprawi skupienie na głównych celach ćwiczeń.

W2 Informacja o punktacji została wykorzystana do stworzenia benchmarku wobec innych uczestników i zwiększenie zaufania wewnątrz organizacji do zespołów cyberbezpieczeństwa.

R2 Zaleca się wykorzystanie systemu punktacji, opracowanego jako sposób oceny działań uczestników ćwiczeń, do stworzenia sektorowego benchmarku. Pozwoliłby podmiotom sektora śledzić postępy w czasie i identyfikować obszary wymagające poprawy, niezależnie od wyników uzyskanych w pojedynczym wydarzeniu, takim jak np. CEP24. Warto rozważyć udostępnianie wyników ćwiczeń w odniesieniu do benchmarków interesariuszom organizacji, aby wzmacniać kulturę bezpieczeństwa i promować wartość pracy zespołów cyberbezpieczeństwa.

Cel główny: warstwy ćwiczeń

W Realizacja ćwiczeń w warstwie technicznej oraz procesowo-organizacyjnej pozwoliła na jednoczesne zaangażowanie osób o różnym zakresie odpowiedzialności oraz różnych rolach w ramach obsługi incydentu.

R Zaleca się dalsze rozwijanie scenariuszy, które uwzględniają zarówno warstwę techniczną, jak i procesowo-organizacyjną, ale także symulujących dwukierunkową komunikację z mediami. Dzięki temu zostaną zaangażowane zespoły odpowiedzialne za Public Relations. Pozwoliłoby to sprawdzić ich gotowość do zarządzania kryzysem w komunikacji zewnętrznej organizacji. Dodatkowo należy tak zintegrować wszystkie warstwy, aby uczestnicy ćwiczeń mogli skorelować zależności między poszczególnymi zabezpieczeniami w warstwie

technicznej a działaniami w warstwie procesowo-organizacyjnej.

Cel szczegółowy 1: Weryfikacja procesu klasyfikacji incydentu jako poważny zgodnie z wytycznymi wskazanymi we właściwych, regulacyjnych standardach technicznych (RTS).

W1 W ramach CEP24 udało się zweryfikować lub zebrać dane do opracowania wewnętrznego procesu klasyfikacji incydentu.

W2 RTS w zakresie klasyfikacji incydentu był dla ćwiczących banków zrozumiały, ale w trakcie korzystania z formularzy zgłoszeń incydentów zauważono, że niektóre pola, zwłaszcza związane z klasyfikacją incydentów, powodowały trudności interpretacyjne. Problemy te mogą prowadzić do niepoprawnego wypełnienia formularza, co wpływa na dokładność i użyteczność zgłoszeń.

W3 Ćwiczące banki dysponowały narzędziami umożliwiającymi klasyfikację incydentu jako poważny wg RTS.

R1 Należy zidentyfikować, jakiego rodzaju narzędzia były stosowane przez ćwiczące banki i zapewnić dostępność podobnych funkcjonalności dla wielu instytucji finansowych. W szczególności powinno to obejmować funkcjonalność generowania danych statystycznych dotyczących liczby i wartości realizowanych transakcji, z podziałem na ich typy, w określonym przedziale czasu. Powinny zostać określone sektorowe wytyczne dla generowania takich statystyk, nawet w przypadku braku konkretnych narzędzi, aby umożliwić oszacowanie skali awarii lub ataku oraz jego wpływu na klientów i transakcje. Jest to kluczowe do klasyfikacji incydentu jako poważnego.

R2 Należy prowadzić wewnętrzne szkolenia w zakresie klasyfikacji incydentu jako poważny, a także rozważyć organizację wspólnych szkoleń pod przewodnictwem KNF.

Cel szczegółowy 2: Weryfikacja kompetencji zespołów technicznych cyberbezpieczeństwa do analizy artefaktów (śladów działania atakujących) i zbierania informacji niezbędnych do zgłoszenia incydentu poważnego.

W1 W ramach CEP24 udało się zweryfikować lub zebrać dane na temat kompetencji zespołów technicznych cyberbezpieczeństwa do analizy artefaktów i zbierania informacji niezbędnych do zgłoszenia incydentu poważnego.

W2 Zespoły techniczne dysponowały wystarczającymi kompetencjami do analizy artefaktów związanych z ćwiczonym incydentem oraz do zebrania wszystkich niezbędnych informacji technicznych do zgłoszenia incydentu poważnego.

R Zaleca się kontynuowanie szkoleń i ćwiczeń, które pozwolą na utrzymanie wysokiego poziomu kompetencji zespołów technicznych. Wskazane jest wprowadzenie do przyszłych ćwiczeń elementów "threat huntingu" oraz analizy powłamaniowej systemów (stacji roboczych oraz serwerów), aby dodatkowo rozwijać umiejętności.

Cel szczegółowy 3: Weryfikacja współpracy zespołów technicznych i pozostałych komórek organizacyjnych w wypełnianiu formularza zgłoszenia incydentu poważnego.

W1 W ramach CEP24 większości uczestników udało się zweryfikować lub zebrać dane na temat współpracy zespołów technicznych i pozostałych komórek organizacyjnych w wypełnianiu formularza zgłoszenia incydentu poważnego. Nieudane próby mogły być związane z przyjętym modelem udziału w ćwiczeniach (zaangażowanie jedynie zespołów technicznych). W takim przypadku weryfikacja współpracy z innymi komórkami organizacyjnymi nie mogła mieć miejsca.

W2 Większość banków nie angażowała w wypełnianie formularza zgłoszenia incydentu poważnego innych niż zespoły cyberbezpieczeństwa komórek organizacyjnych. Jednocześnie większości z nich udało się zidentyfikować komórki, które powinny być w ten proces zaangażowane, a wcześniej nie były brane pod uwagę. Dotyczy to w szczególności komórek prawnych oraz odpowiedzialnych za zewnętrzną komunikację organizacji.

R Należy dokonać przeglądu i aktualizacji wewnętrznych procedur i upewnić się, że uwzględniają (na zasadach *need-to-act*) i jasno określają rolę poszczególnych komórek organizacyjnych w procesie zgłaszania incydentu poważnego do organu nadzorczego (raportowania do CSIRT KNF). Pozwoli to uwzględnić w procesie wypełniania formularza wiedzy innych działów, która – biorąc pod uwagę kompleksowość zgłoszenia (duża ilość informacji na co dzień niedostępne dla zespołów cyberbezpieczeństwa) – mogłaby być istotna.

Cel szczegółowy 4: Ocena przydatności formularza zgłoszenia incydentu poważnego, opracowanego przez KNF na podstawie RTS (zgłoszenie wszelkich uwag).

W1 W ramach CEP24 udało się ocenić przydatność formularza zgłoszenia incydentu poważnego opracowanego przez KNF na podstawie RTS.

W2 Dla większości uczestników formularz był zrozumiały, ale zauważono, że niektóre pola, zwłaszcza związane z klasyfikacją incydentów, powodowały trudności interpretacyjne:

(1) *Classification criteria that triggered the incident report* – kryteria klasyfikacji incydentu.

(2) *Types of impact in the Member States* – wpływ na podmioty w innych krajach.

(3) *Information whether the numbers are actual or estimates, or whether there has not been any impact* – określenie sposobu wyliczeń lub szacowania danych niezbędnych do klasyfikacji incydentu.

(4) *Date and time when services, activities and/or operations have been restored* – terminy przywrócenia usług.

(5) *Service downtime* – czas niedostępności usług.

W3 W przypadku wystąpienia rzeczywistego incydentu formularz nie byłby łatwy do wypełniania. Należy pamiętać, że w trakcie rzeczywistego incydentu nakład pracy zaangażowanych w obsługę komórek organizacyjnych będzie znacznie większy niż w przypadku ćwiczeń, co w konsekwencji może doprowadzić do sytuacji, w której wypełnienie formularza będzie miało niższy priorytet i tym samym zasoby przypisane do tej czynności będą mocno ograniczone. W rzeczywistym wystąpieniu incydentu narzędzia/systemy mogą być po prostu niedostępne.

R Organy nadzorcze powinny udzielić instytucjom finansowym dodatkowe wsparcie w zdobywaniu niezbędnych kompetencji umożliwiających poprawne wypełnianie formularza zgłoszenia incydentu poważnego. Można to zrealizować poprzez:

- dodatkowe szkolenia,
- szczegółowe wytyczne dotyczące wypełniania formularza (dokument),
- tutorial filmowy,
- podpowiedzi/wskazówki do poszczególnych pól w formularzu online (pop-up),
- wspólne warsztaty, na których trzeba pokazać wzorcowo wypełniony formularz.

Cel szczegółowy 5: Weryfikacja procesu współpracy banków z CSIRT KNF

W1 W ramach CEP24 udało się zweryfikować proces współpracy banków z CSIRT KNF. Została oceniona bardzo dobrze, co świadczy o dużej dojrzałości CSIRT KNF. Warunkiem skutecznej współpracy są jej autentyczność, wzajemność i dążenie do wspólnej korzyści. Wydaje się, że te warunki współpracy z CSIRT KNF zostały spełnione.

W2 Ćwiczące banki są na tyle przygotowane do obsługi incydentu, że nie występowały o wsparcie CSIRT KNF. Należy pamiętać, że

w ćwiczeniach brały udział największe banki w Polsce. Nie wiadomo, z jakimi wyzwaniami w skali kraju trzeba będzie się mierzyć po wejściu w życie rozporządzenia DORA – w większości podmioty objęte wymaganiami rozporządzenia nie są aż tak dojrzałe w zakresie cyberbezpieczeństwa, jak podmioty biorące udział w CEP24.

R1 Należy rozpropagować model i sposoby współpracy z podmiotami sektora wdrożone przez CSIRT KNF w innych sektorach, które zgodnie z przepisami nowelizacji ustawy o krajowym systemie cyberbezpieczeństwa będą musiały powołać CSIRT sektorowy.

R2 Zorganizować ćwiczenia typu CEP24 dla innych instytucji finansowych wymienionych w art. 2 ust. 1 rozporządzenia DORA, np. banków spółdzielczych, lub przeprowadzić badanie dotyczące oczekiwań wobec CSIRT KNF w kwestiach wsparcia w zakresie cyberbezpieczeństwa. Do tego celu można wykorzystać katalog usług FIRST CSIRT Services Framework[5].

Cel dodatkowy: weryfikacja procesu współpracy pomiędzy CSIRT sektorowym a CSIRT-ami krajowymi

W1 Przeprowadzone ćwiczenia wykazały, że współpraca pomiędzy CSIRT-em sektorowym a CSIRT-ami krajowymi przebiega zgodnie z przyjętymi procedurami, umożliwia skuteczną wymianę informacji oraz reagowanie na incydenty w cyberprzestrzeni. Niestety w ramach ćwiczonego scenariusza pełne zweryfikowanie tej współpracy, z uwagi na konieczność zapewnienia szerszego grona ćwiczącego uwzględniającego również szczebel decyzyjny, nie było możliwe. Okoliczności te wpłynęły na zakres ćwiczenia, co ograniczyło przeprowadzenie bardziej realistycznej symulacji podejmowania strategicznych decyzji na poziomie krajowym.

W2 Ćwiczenia wykazały konieczność poprawy procedur przekazywania i aktualizacji informacji o incydentach pomiędzy CSIRT-em sektorowym a CSIRT-ami krajowymi. Obecnie używany kontakt emailowy ma ograniczoną skalowalność, co może utrudniać sprawną komunikację przy wystąpieniu wielu incydentów jednocześnie.

5 https://www.first.org/standards/frameworks/csirts/csirt_services_framework_v2.1

R1 Zaleca się organizację ćwiczeń z zakresu cyberbezpieczeństwa na poziomie krajowym, które uwzględnią incydenty na dużą skalę (incydent krytyczny) np. atak na łańcuch dostaw lub jednoczesne wystąpienie wielu zgłoszeń incydentów poważnych. Udział osób decyzyjnych oraz reprezentantów kluczowych podmiotów z CSIRT-ów krajowych i sektorowych jest niezbędny do efektywnego sprawdzenia procesów współpracy oraz możliwości skutecznego zarządzania incydentami na poziomie krajowym. Tego typu ćwiczenia pozwolą na ocenę zarówno operacyjnych zdolności zespołów/departamentów, jak i procedur decyzyjnych na poziomie strategiczno-politycznym.

R2 Zaleca się wypracowanie wspólnej platformy lub lepsze wykorzystanie istniejących narzędzi do wymiany najważniejszych informacji o incydentach, takich jak IoC. Powinny usprawnić i przyspieszyć przekazywanie informacji między CSIRT-em sektorowym a CSIRT-ami krajowymi. Dodatkowo rekomenduje się analizę i optymalizację kanałów dystrybucji informacji, aby efektywniej docierały do odpowiednich sektorów i podmiotów.

Narzędzia: CyberBastion

W Platforma CyberBastion jest istotnym narzędziem w ćwiczeniach z zakresu cyberbezpieczeństwa (jej wykorzystanie jako głównej warstwy informacyjnej ćwiczeń w większości zostało ocenione pozytywnie). Wymaga usprawnień w zakresie systemu proponowanej punktacji oraz oceny skuteczności reakcji na zagrożenia.

R Wykorzystanie CyberBastionu jako warstwy informacyjnej powinno mieć zastosowanie w przyszłych ćwiczeniach cyklu Cyber-EXE Polska. Należy jednak wprowadzić modyfikacje i usprawnienia zgłaszane przez uczestników ćwiczeń CEP24. Dotyczyły przede wszystkim systemów punktacji oraz większej integracji z innymi narzędziami wykorzystywanymi w czasie ćwiczeń, np.: cyber range.

Narzędzia: cyber range

W Platforma cyber range jest potrzebnym narzędziem w ćwiczeniach z zakresu cyberbezpieczeństwa, ale wymaga rozbudowy, integracji nowych funkcji oraz optymalizacji. Rekomendowane zmiany pozwolą lepiej odwzorować rzeczywiste środowisko pracy i zwiększyć efektywność szkoleń (realizację bardziej zaawansowanych scenariuszy).

R1 Uzupełnić platformę o inne funkcje cyberbezpieczenstwa używane przez banki, by odzwierciedlić rzeczywiste środowiska stosowane w firmach.

R2 Dodać narzędzia do zarządzania zagrożeniami: EDR (Endpoint Detection and Response) oraz NDR (Network Detection and Response), by poszerzyć zakres możliwości analizy.

R3 Zintegrować w ramach platformy narzędzia do komunikacji lub pracy grupowej umożliwiające bezpośrednią wymianę informacji przez członków zespołów ćwiczących w cyber range.

R4 Należy kontynuować dalszą optymalizację wydajności platformy, aby jednoczesna praca większej liczby uczestników przebiegała bezproblemowo. Zaawansowani uzytkownicy są w stanie zwiększyć obciążenie platformy rozbudowanymi czynnościami analitycznymi.

Organizacja: zabezpieczenie logistyczne

W Komfort i funkcjonalność pomieszczeń, dostępność i jakość środków łączności, wsparcia technicznego oraz wsparcia organizatorów w pełni odpowiadały potrzebom ćwiczenia.

R Zaleca się utrzymanie dotychczasowego wysokiego standardu zabezpieczenia logistycznego. Dodatkowo warto przeprowadzać regularne oceny potrzeb uczestników, aby stale dostosowywać infrastrukturę i wsparcie do zmieniających się wymagań ćwiczeń.

Komentarze uczestników

Komentarz CSIRT KNF

“

Ćwiczenia CYBER-EXE Polska 2024 były ważnym testem dla systemów i procesów komunikacji, zarówno pomiędzy podmiotami sektora finansowego, jak i zespołami CSIRT na poziomie krajowym. Praktyka pokazuje, że w sytuacjach kryzysowych sprawdzona i dobrze funkcjonująca komunikacja jest fundamentem skutecznej reakcji na incydenty i cyberzagrożenia.

Przeprowadzone ćwiczenia uwzględniały wymogi rozporządzenia DORA, które wprowadza nowe obowiązki dotyczące zgłaszania incydentów ICT, w tym konieczność przekazywania wskaźników IoC (Indicators of Compromise). Posiadanie takich informacji umożliwia lepsze rozpoznanie specyfiki incydentu oraz podjęcie skuteczniejszych działań mitygujących.

Istotnym elementem ćwiczeń była także wymiana informacji dotyczących cyberzagrożeń bezpośrednio pomiędzy podmiotami finansowymi. Współdzielenie informacji o technikach ataku oraz wskaźnikach IOC pozwala podmiotom lepiej przygotować się na potencjalne cyberataki.

Sprawna reakcja na incydenty i cyberzagrożenia to kluczowy element budowania odporności organizacji. Realizacja ćwiczeń wpływa na podniesienie cyberodporności sektora finansowego, zapewniając lepsze przygotowanie na nowe wyzwania technologiczne i regulacyjne. To istotny krok w kierunku zwiększenia bezpieczeństwa całego ekosystemu finansowego.

Komentarz Simspace

“

Cyber-EXE Polska 2024 dostarczyło uczestnikom cenne praktyczne doświadczenie w wykrywaniu i raportowaniu wskaźników ataków, zwiększając ich zaufanie do możliwości branży do obrony przed nowoczesnymi cyberzagrożeniami. Angażując się w środowisko współpracy, wzmocnili także kluczowe relacje, które umożliwiają terminową wymianę informacji, pomagając organizacjom partnerskim pozostać przygotowanymi i reagować na zdeterminowanych przeciwników. Rutynowe inicjatywy, takie jak Cyber-EXE, są niezbędne do rozwijania umiejętności i zdolności potrzebnych do stawienia czoła stale ewoluującym cyberzagrożeniom.

Komentarz Splunk

“

Jako partner tegorocznych ćwiczeń Cyber-EXE Polska, mieliśmy okazję wspierać sektor bankowy w przygotowaniach do wymagań rozporządzenia DORA i reagowania na realne zagrożenia w cyberprzestrzeni. Scenariusze zaprezentowane podczas wydarzenia uwidoczniły kluczową rolę monitorowania środowiska IT w czasie rzeczywistym oraz szybkiej analizy danych.

System Splunk umożliwił skuteczną agregację i korelację zdarzeń z różnych źródeł, co pozwoliło na błyskawiczne wykrywanie i priorytetyzację zagrożeń. Dzięki temu zespoły CSIRT mogły szybko reagować na symulowane ataki i minimalizować potencjalne skutki incydentów.

Jesteśmy dumni, że mogliśmy wspierać uczestników w doskonaleniu ich zdolności obronnych i pokazać, jak technologia Splunk wspiera bezpieczeństwo w kluczowych sektorach gospodarki. Gratulujemy wszystkim zaangażowanym!

Komentarz Crowdstrike

“

Jesteśmy dumni, że mogliśmy wspierać Cyber-EXE Polska 2024, inicjatywę umożliwiającą instytucjom finansowym testowanie ich gotowości do wykrywania i zatrzymywania cyberzagrożeń, która jest również zgodna z misją CrowdStrike. Mocno wierzymy, że ćwiczenia stanowiły znaczący krok w kierunku zwiększenia cyberbezpieczeństwa w polskim sektorze finansowym, który jest popularnym celem cyberprzestępców. Symulowane ataki ujawniły kluczowe obszary do poprawy i cieszymy się, że możemy wspierać firmy w dalszym pokonywaniu wyzwań związanych z cyberbezpieczeństwem i wzmacnianiu ich obrony.

Komentarz Mastercard

“

W Mastercard od wielu lat prowadzimy ciągłe działania mające na celu poprawę bezpieczeństwa ekosystemu płatności cyfrowych i nieustannie wprowadzamy kolejne rozwiązania wykorzystujące najnowsze zdobycze technologii, odpowiadające na pojawiające się zagrożenia. Wspieramy aktywnie różnych interesariuszy ekosystemu, począwszy od wydawców kart płatniczych, agentów rozliczeniowych, integratorów płatności, a także detalistów, sprzedawców czy sieci handlowe.

Nasza obecność na ćwiczeniach Cyber EXE 2024 wynika z jednej strony z zainteresowania stanem przygotowań polskiego sektora bankowego do zapewnienia zgodności z wymogami regulacji DORA, ale również z racji możliwości wsparcia sektora finansowego w realizacji poszczególnych wymogów regulacji, szczególnie w zakresie monitorowania ryzyka cyberbezpieczeństwa dostawców.

Z przygotowanego przez nas w połowie 2024 roku raportu na temat cyber zagrożeń w polskim sektorze finansowym wynika, że zmagał się on z największą liczbą ataków od stycznia 2023 do maja 2024, kiedy to 37% ataków było skierowanych na dane i usługi finansowe klientów, co stanowi wskaźnik istotnie wyższy średniej europejskiej (23%). Podmioty finansowe były celem 11% ataków, co czyni ją trzecią najczęściej atakowaną branżą w tym okresie. Jednocześnie nasze analizy wykonywane dzięki technologii RiskRecon wskazują, że średni poziom oceny cyberbezpieczeństwa polskich banków (8,6 w skali 1-10) jest wyższy niż średnia europejska (8,3), co niewątpliwie bardzo dobrze świadczy o Polskich bankach.

Podsumowanie

Ćwiczenia w zakresie ochrony w cyberprzestrzeni stanowią jedną z najbardziej efektywnych metod przygotowania organizacji do skutecznego reagowania na zagrożenia.

Pozwalają nie tylko na zdobycie i utrzymanie wysokiego poziomu wiedzy oraz praktycznych umiejętności, lecz także na identyfikację luk czy słabości, które mogą zmniejszyć zdolność organizacji do skutecznego zarządzania incydentami. Ćwiczenia wyrabiają nawyki oraz zwiększają kompetencje konieczne do sprawnego zarządzania kryzysowego, angażując zarówno osoby pełniące kluczowe funkcje, jak i zespoły na różnych poziomach organizacji. Dodatkowo dają możliwość optymalizacji sposobów działania w złożonych sytuacjach wspierając podejmowanie trafnych decyzji oraz efektywne zarządzanie podległymi strukturami.

Cele ćwiczeń Cyber-EXE Polska 2024 zostały osiągnięte. Uczestnicy ćwiczeń zgodnie stwierdzili, że dodatkowe, wewnętrzne cele postawione przez ich organizacje również zostały osiągnięte. Zdaniem ćwiczących było jak najbardziej przydatne.

Ćwiczenia mogłyby przynieść jeszcze więcej pozytywnych efektów, jeśli uczestniczyłoby więcej podmiotów objętych rozporządzeniem DORA. Przede wszystkim udział powinny wziąć organizacje mniej dojrzałe w zakresie cyberbezpieczeństwa, a także inne ważne podmioty sektora finansowego np. Związek Banków Polskich, który uczestniczy w koordynacji działań branży.

Podziękowania

Ćwiczenia Cyber-EXE Polska 2024 nie mogłyby się odbyć bez dobrej woli i wyjątkowego zaangażowania wszystkich uczestniczących w nim organizacji, a zwłaszcza osób, które brały aktywny udział w organizacji.

Fundacja Bezpieczna Cyberprzestrzeń jako organizator ćwiczeń dziękuje wszystkim za odwagę w realizacji bardzo ważnego w obliczu zbliżającego się wejścia w życie rozporządzenia DORA przedsięwzięcia dla sektora finansowego w Polsce. Składa podziękowania za wielkie zaangażowanie w czasie wielomiesięcznych przygotowań, za dzień ćwiczeń oraz pracę włożoną w ocenę przedsięwzięcia, przygotowanie wniosków i rekomendacji.

Dziękujemy partnerowi głównemu – firmie doradczej EY – za wsparcie przy organizacji ćwiczeń oraz aktywny, merytoryczny udział w jego przygotowaniu i przeprowadzeniu.

Dziękujemy wszystkim uczestnikom ćwiczeń, tj. organizacjom, które zdecydowały się na aktywny udział. Odwaga, współdziałanie i otwartość Państwa reprezentantów pozwoliła na sprawne przeprowadzenie ćwiczeń i wyciągnięcie pożytecznych wniosków.

Serdeczne podziękowania kierujemy do zespołów CSIRT, które po raz pierwszy tak licznie (w komplecie) wzięły udział w ćwiczeniach z cyklu Cyber-EXE Polska. Szczególne wyrazy wdzięczności składamy CSIRT KNF za wkład w określenie celów ćwiczeń, przygotowanie formularza zgłoszenia incydentu oraz aktywny udział na każdym etapie. Dzięki współpracy oraz zaangażowaniu w przygotowanie wniosków końcowych mogliśmy uzyskać pełniejszy obraz gotowości sektora do wejścia w życie rozporządzenia DORA oraz reagowania na incydenty poważne. Dziękujemy wszystkim zespołom CSIRT za ich nieocenioną pomoc i udział, który pozwolił zrealizować ćwiczenia na najwyższym poziomie.

Dziękujemy również pozostałym partnerom ćwiczeń CEP24: SimSpace, Splunk, Mastercard i CrowdStrike. SimSpace dziękujemy za udostępnienie platformy cyber range, która umożliwiła nam realizację postulatów uczestników poprzednich ćwiczeń cyklu CEP – przygotowanie w oparciu o przeznaczoną do tego infrastrukturę teleinformatyczną elementu ćwiczeń technicznych. Dzięki zaawansowanym możliwościom platformy udostępnionej przez SimSpace uczestnicy mogli sprawdzić swoje umiejętności techniczne w warunkach zbliżonych do rzeczywistych oraz doskonalić zdolność reagowania na zagrożenia. Profesjonalizm i wsparcie zespołu SimSpace w trakcie trwania ćwiczeń przyczyniły się do sukcesu całego przedsięwzięcia i pozwoliły na podniesienie ich jakości do najwyższego poziomu.

Organizatorzy i partnerzy Cyber-EXE Polska 2024

FBC – Fundacja Bezpieczna Cyberprzestrzeń

FBC to niezależna organizacja pozarządowa założona w czerwcu 2010 roku, której misją jest zwiększanie świadomości na temat zagrożeń cybernetycznych. Fundacja koncentruje się na edukacji, organizowaniu ćwiczeń i wydarzeń jednoczących społeczność zajmującą się bezpieczeństwem informacji. Ponadto wspiera badania przygotowując raporty, opinie eksperckie oraz specjalistyczne projekty, a także wspomaga rozwój systemów cyberbezpieczeństwa w Polsce i za granicą. Fundacja organizuje ćwiczenia z cyklu Cyber-EXE zarówno w Polsce, jak i za granicą, symulując incydenty cybernetyczne w celu wzmocnienia zdolności reakcji na zagrożenia.

EY

Działając na polskim rynku co roku EY doradza tysiącom firm, zarówno małym i średnim przedsiębiorstwom, jak i największym firmom. Zespoły audytorskie, consultingowe, prawne, strategiczne, podatkowe i transakcyjne zadają nieoczywiste pytania, by móc znaleźć nowe odpowiedzi na złożone wyzwania, przed którymi stoi dziś świat. EY w Polsce to ponad 5000 specjalistów pracujących w 8 miastach: w Warszawie, Gdańsku, Katowicach, Krakowie, Łodzi, Poznaniu, Wrocławiu i Rzeszowie oraz w Centrum Usług Wspólnych EY.

SimSpace

SimSpace jest wiodącym dostawcą zaawansowanych cyberpoligonów, oferującym dostosowane, immersyjne środowiska, które pomagają organizacjom wzmocnić ich cyberobronę. Naśladując rzeczywiste środowiska operacyjne i taktyki przeciwników, SimSpace umożliwia specjalistom ds. cyberbezpieczeństwa szkolenie, testowanie i doskonalenie umiejętności w scenariuszach wykorzystujących rzeczywiste zagrożenia. Dzięki zaawansowanym możliwościom replikacji specyficznych infrastruktur, w tym pełnego łańcucha działań przeciwnika, SimSpace umożliwia obrońcom ochronę swoich organizacji przed najbardziej zaawansowanymi zagrożeniami cybernetycznymi. Zaufany przez rządy, przedsiębiorstwa i organizacje wojskowe, SimSpace dostarcza praktyczne szkolenia i kompleksowe analizy, które zwiększają gotowość na cyberzagrożenia. Więcej informacji można znaleźć na stronie https://simspace.com/.

Splunk

Splunk został założony w 2003 roku, aby rozwiązywać problemy w złożonych infrastrukturach cyfrowych. Od samego początku pomagaliśmy organizacjom eksplorować ogromne zasoby ich danych niczym speleolodzy w jaskini (stąd nazwa „Splunk"). W 2024 roku Splunk został przejęty przez Cisco, aby pomóc klientom w dalszym budowaniu odporności w całym ich cyfrowym ekosystemie. Splunk przeszedł ogromną ewolucję w ciągu ostatnich 20 lat, gdy cyfryzacja stała się kluczowym elementem, a rodzaje i liczba zakłóceń jednocześnie wzrosły. Posiadając ponad 1,100 patentów i kulturę innowacji, zawsze byliśmy o krok przed potrzebami naszych klientów.

Obecnie wiele największych i najbardziej złożonych organizacji na świecie polega na Splunk, aby zapewnić bezpieczeństwo i niezawodność swoich krytycznych systemów. Naszym celem jest budowanie

bezpieczniejszego i bardziej odpornego cyfrowego świata. Każdego dnia realizujemy ten cel, pomagając zespołom ds. bezpieczeństwa, IT i DevOps utrzymywać organizacje w bezpiecznym działaniu. Gdy organizacje mają odporne systemy cyfrowe, mogą się adaptować, rozwijać i dostarczać wartość swoim klientom. Odporność to praca zespołowa. Budujmy ją razem.

Mastercard

Mastercard napędza gospodarki i wspiera rozwój społeczności w ponad 200 krajach i terytoriach na całym świecie. Wspólnie z naszymi klientami budujemy zrównoważoną gospodarkę, w której każdy może się rozwijać. Wspieramy szeroki wachlarz cyfrowych metod płatności, sprawiając, że transakcje są bezpieczne, proste, wygodne i szeroko dostępne. Dzięki połączeniu naszej technologii, innowacji, partnerstw oraz możliwości naszej sieci dostarczamy rozwiązania, które pomagają konsumentom, przedsiębiorstwom i sektorowi publicznemu w pełni realizować swój potencjał.

CrowdStrike

CrowdStrike (Nasdaq: CRWD), globalny lider w dziedzinie cyberbezpieczeństwa, redefiniuje nowoczesne bezpieczeństwo dzięki zaawansowanej platformie opartej na chmurze i sztucznej inteligencji, chroniącej kluczowe obszary ryzyka – punkty końcowe, środowiska chmurowe, tożsamości i dane. Platforma Falcon® zapewnia precyzyjną detekcję, skuteczną ochronę, uproszczenie procesów i natychmiastową wartość dzięki analizie w czasie rzeczywistym oraz zaawansowanej telemetrii.

Załączniki

Załącznik 1

Szablon zawartości raportu pośredniego zgłoszenia incydentu poważnego wykorzystywany w trakcie ćwiczeń

ID	Opis pola ENG	Opis Pola PL	Treść zgłoszenia
3.1	Incident reference code provided by the financial entity/ Kod referencyjny incydentu dostarczony przez podmiot finansowy	Unikalny kod referencyjny wydany przez podmiot finansowy jednoznacznie identyfikujący poważny incydent.	
3.2	Incident reference code provided by the competent authority/Kod referencyjny incydentu podany przez właściwy organ	Niepowtarzalny kod referencyjny przypisany przez właściwy organ w momencie otrzymania wstępnego zgłoszenia w celu jednoznacznej identyfikacji incydentu poważnego.	
3.3	Date and time of occurrence of the incident/Data i godzina wystąpienia incydentu	Data i godzina wystąpienia incydentu związanego z ICT, jeśli różni się od godziny wykrycia.	
3.4	Date and time of occurrence of recurring incidents/Data i godzina wystąpienia powtarzających się incydentów	W przypadku zgłaszania powtarzających się incydentów, data i godzina wystąpienia pierwszego incydentu związanego z ICT.	
3.5	Date and time when services, activities and/or operations have been restored/Data i godzina przywrócenia usług, działań i/lub operacji	Informacje o dacie i godzinie przywrócenia usług, działań i/lub operacji dotkniętych incydentem.	
3.6	Number of clients affected/Liczba klientów, których to dotyczy	Liczba klientów dotkniętych incydentem związanym z ICT, którymi mogą być osoby fizyczne lub prawne korzystające z usług świadczonych przez podmiot finansowy.	
3.7	Percentage of clients affected/ Odsetek klientów, których to dotyczy	Odsetek klientów dotkniętych incydentem związanym z ICT w stosunku do całkowitej liczby klientów korzystających z danej usługi świadczonej przez podmiot finansowy. W przypadku więcej niż jednej usługi, której dotyczy incydent, dane należy podać w sposób zagregowany.	

ID	Opis pola ENG	Opis Pola PL	Treść zgłoszenia
3.8	Number of financial counterparts affected/Liczba dotkniętych kontrahentów finansowych	Liczba kontrahentów finansowych dotkniętych incydentem związanym z ICT, którzy zawarli porozumienie umowne z podmiotem finansowym	
3.9	Percentage of financial counterparts affected/Odsetek dotkniętych kontrahentów finansowych	Odsetek kontrahentów finansowych dotkniętych incydentem związanym z ICT w stosunku do całkowitej liczby kontrahentów finansowych, którzy zawarli ustalenia umowne z podmiotem finansowym	
3.10	Impact on relevant clients or financial counterpart/Wpływ na istotnych klientów lub kontrahentów finansowych	Wszelki zidentyfikowany wpływ na odpowiednich klientów lub kontrahentów finansowych zgodnie z art. 1.3 9.1(f) RTS w sprawie klasyfikacji incydentów związanych z ICT.	
3.11	Number of affected transactions/ Liczba transakcji, których to dotyczy	Liczba transakcji dotkniętych incydentami związanymi z ICT.	
3.12	Percentage of affected transactions/Procent dotkniętych transakcji	Odsetek transakcji dotkniętych naruszeniem w stosunku do regularnego poziomu transakcji krajowych i transgranicznych przeprowadzanych przez podmiot finansowy związany z usługą dotkniętą naruszeniem	
3.13	Value of affected transactions/ Wartość transakcji, których to dotyczy	Całkowita wartość transakcji dotkniętych incydentem związanym z ICT zgodnie z art. 1.4 i art. 9.1 lit. e) RTS w sprawie klasyfikacji incydentów związanych z ICT.	
3.14	Information whether the numbers are actual or estimates/ Informacja, czy liczby są rzeczywiste czy szacunkowe	Informacja, czy wartości podane w polach danych od 3.5. do 3.12. są rzeczywiste czy szacunkowe.	
3.15	Reputational impact/Wpływ na reputację	Informacje o wpływie na reputację wynikającym z incydentu zgodnie z art. 2 i art. 10 RTS w sprawie klasyfikacji incydentów związanych z ICT.	
3.16	Contextual information about the reputational impact/Informacje kontekstowe na temat wpływu na reputację	Informacje opisujące, w jaki sposób incydent związany z ICT wpłynął lub mógłby wpłynąć na reputację podmiotu finansowego, takie jak naruszenia prawa, niespełnione wymogi regulacyjne, liczba skarg klientów i inne.	
3.17	Duration of the incident/Czas trwania incydentu	Czas trwania incydentu związanego z TIK mierzy się od momentu wystąpienia incydentu do momentu jego rozwiązania	

ID	Opis pola ENG	Opis Pola PL	Treść zgłoszenia
3.18	Service downtime/Czas przestoju usługi	Czas przestoju usługi mierzony od momentu, gdy usługa(i) jest(są) całkowicie lub częściowo niedostępna(e) dla klientów i/lub kontrahentów finansowych do momentu, gdy regularne działania/operacje zostały przywrócone do poziomu usług(i), który był świadczony przed incydentem. W przypadku wpływu na wiele usług, czas przestoju usługi powinien być mierzony do momentu przywrócenia wszystkich usług.	
3.19	Information whether the numbers for duration and service downtime are actual or estimates./Informacja, czy liczby dotyczące czasu trwania i przestojów serwisowych są rzeczywiste czy szacunkowe.	Informacja, czy wartości podane w polach danych 3.16 i 3.17 są rzeczywiste czy szacunkowe.	
3.20	Types of impact in the Member States/Rodzaje wpływu w państwach członkowskich	Rodzaj wpływu w poszczególnych państwach członkowskich EOG. Obowiązkowe do zgłoszenia w raporcie pośrednim i końcowym, jeśli osiągnięto próg "rozprzestrzenienia geograficznego".	
3.21	Description of how the incident has an impact in other Member States/Opis wpływu incydentu na inne państwa członkowskie	Opis wpływu i powagi incydentu w każdym dotkniętym państwie członkowskim	
3.22	Materiality thresholds for the classification criterion "Data losses"/Progi istotności dla kryterium klasyfikacji "Utrata danych"	Rodzaj utraty danych, które pociąga za sobą incydent związany z ICT w odniesieniu do dostępności, autentyczności, integralności i poufności danych.	
3.23	Description of the data losses/ Opis utraconych danych	Opis wpływu incydentu na dostępność, autentyczność, integralność i poufność krytycznych danych	
3.24	Materiality thresholds for the classification criterion "Critical services affected"/ Progi istotności dla kryterium klasyfikacji "Usługi krytyczne, na które ma wpływ"	Informacje związane z kryterium "Usługi krytyczne, na które ma to wpływ	
3.25	Comments to the classification criteria/Uwagi do kryteriów klasyfikacji	Wszelkie dalsze informacje związane z kryteriami klasyfikacji	

ID	Opis pola ENG	Opis Pola PL	Treść zgłoszenia
3.26	Type of the incident/Typ incydentu	Klasyfikacja incydentów według typu	
3.27	Threats and techniques used by the threat actor/Zagrożenia i techniki stosowane przez podmiot stanowiący zagrożenie	Wskaż zagrożenia i techniki stosowane przez podmiot stanowiący zagrożenie.	
3.28	Other types of incidents and techniques/Inne typy incydentów i technik	Inne typy incydentów i technik	
3.29	Information about affected functional areas and business processes/Informacje o dotkniętych obszarach funkcjonalnych i procesach biznesowych	Wskazanie obszarów funkcjonalnych i procesów biznesowych, na które incydent ma wpływ, w tym produktów i usług.	
3.30	Affected infrastructure components supporting business processes/Dotknięte komponenty infrastruktury wspierające procesy biznesowe	Informacje o tym, czy incydent miał wpływ na komponenty infrastruktury (serwery, systemy operacyjne, oprogramowanie, serwery aplikacji, oprogramowanie pośredniczące, komponenty sieciowe, inne) wspierające procesy biznesowe.	
3.31	Information about affected infrastructure components supporting business processes/ Informacje o dotkniętych komponentach infrastruktury wspierających procesy biznesowe	Opis wpływu incydentu na elementy infrastruktury wspierające procesy biznesowe, w tym sprzęt i oprogramowanie.	
3.32	Communication to clients/ financial counterparts/ Komunikacja z klientami / partnerami finansowymi	Informacje o tym, czy podmiot finansowy poinformował klientów i/lub kontrahentów finansowych o incydencie oraz o środkach, które zostały podjęte w celu złagodzenia negatywnych skutków.	
3.33	Information about communication to clients/ financial counterparts/ Informacje dotyczące komunikacji z klientami/partnerami finansowymi	Opis przekazywania informacji o incydencie klientom lub partnerom finansowym	
3.34	Reporting to other authorities/ Raportowanie do innych organów	Określenie władz, które zostały poinformowane o incydencie.	
3.35	Specification of "other" authorities/Wyszczególnienie "innych" organów	Wyszczególnienie "innych" rodzajów organów poinformowanych o incydencie	

ID	Opis pola ENG	Opis Pola PL	Treść zgłoszenia
3.36	Temporary actions/measures taken or planned to be taken to recover from the incident/ Tymczasowe działania/środki podjęte lub planowane do podjęcia w celu wyjścia z incydentu	Wskazanie, czy podmiot finansowy wdrożył (lub planuje wdrożyć) wszelkie tymczasowe działania, które zostały podjęte (lub planowane do podjęcia) w celu odzyskania sprawności po incydencie.	
3.37	Description of any temporary actions and measures taken or planned to be taken to recover from the incident/Opis wszelkich tymczasowych działań i środków podjętych lub planowanych do podjęcia w celu naprawy po incydencie	Opis takich działań tymczasowych	
3.38	Information on involvement of CSIRTs in dealing with the incident/Informacje na temat zaangażowania CSIRT w obsługę incydentu	Informacje na temat zaangażowania CSIRT w obsługę incydentu, jeśli dotyczy.	
3.39	Information on involvement of CSIRTs in dealing with the incident/Informacje na temat zaangażowania CSIRT w obsługę incydentu	Dodatkowe informacje na temat zakresu, w jakim CSIRT był zaangażowany w obsługę zgłoszonego incydentu i konkretnego obszaru, w przypadku wybrania kategorii "inne" w polu danych 28.1.	
3.40	Indicators of compromise/ Wskaźniki kompromitacji	Informacje związane z incydentem, które mogą pomóc w zidentyfikowaniu złośliwej aktywności w sieci lub systemie informatycznym (Indicators of Compromise, IoC), w stosownych przypadkach.	
3.41	Vulnerabilities exploited/ Wykorzystane podatności	Opis luk w zabezpieczeniach wykorzystanych podczas incydentu, w tym słabości, podatności lub wad produktów lub usług ICT.	

Załącznik 2

opis scenariusza nr 1 użytego w ćwiczeniach CEP24 (inspirowany działaniami grupy APT41)

Tło:

Medialne doniesienia ze Szwajcarii wskazują na trwającą kampanię cyberprzestępczą skierowaną przeciw instytucjom finansowym. Celem jest uzyskanie dostępu do wrażliwych danych płatniczych oraz manipulacja systemami bankowymi. Sektor finansowy w Europie znajduje się w stanie podwyższonego zagrożenia – CSIRT NASK oraz CSIRT KNF ostrzegają przed atakami, w których wykorzystywane są zaawansowane metody, w tym nieznane podatności przeglądarek. Ataki mają na celu kradzież środków oraz pozyskanie danych, które mogą być użyte do przyszłych działań cyberprzestępczych.

Opis zdarzeń:

1. Pracownik banku wchodzi na spreparowaną stronę internetową, na której – dzięki wykorzystaniu podatności przeglądarki – automatycznie pobrane zostaje złośliwe oprogramowanie.
2. Złośliwe oprogramowanie uruchamia się na komputerze ofiary inicjując połączenie z serwerem Command and Control (C2) napastników.
3. Atakujący uzyskują dostęp do szczegółowych informacji o systemie pracownika, w tym adresów MAC, GUID interfejsów sieciowych, konfiguracji sieciowej i użytkownika zalogowanego do systemu.
4. Kolejnym krokiem jest odkrycie przez atakujących zasobów sieciowych i usunięcie administracyjnych udziałów "ADMIN$", co znacząco utrudnia identyfikację nieautoryzowanych działań.
5. Następnie napastnicy kopiują wrażliwe dane z systemu pracownika i eksfiltrują je poza bankową infrastrukturę przy użyciu protokołów sieciowych.
6. Cyberprzestępcy tak modyfikują usługi systemowe, że złośliwe oprogramowanie uruchamia się automatycznie po restarcie. Ponadto wprowadzają nowe usługi z uprawnieniami administratora, co daje im zdalny dostęp do plików i zasobów sieciowych.
7. W dalszym etapie złośliwe oprogramowanie zostaje przesłane na inne maszyny w sieci, co pozwala atakującym na stopniowe przejmowanie kontroli nad całą infrastrukturą.
8. Atakujący przeprowadzają zaawansowane działania w celu ukrycia śladów, takie jak: czyszczenie dzienników zdarzeń i usuwanie plików.
9. Na końcowym etapie dodają nowego użytkownika do lokalnej grupy administratorów, co zabezpiecza im dostęp do systemu w przyszłości.

Załącznik 3

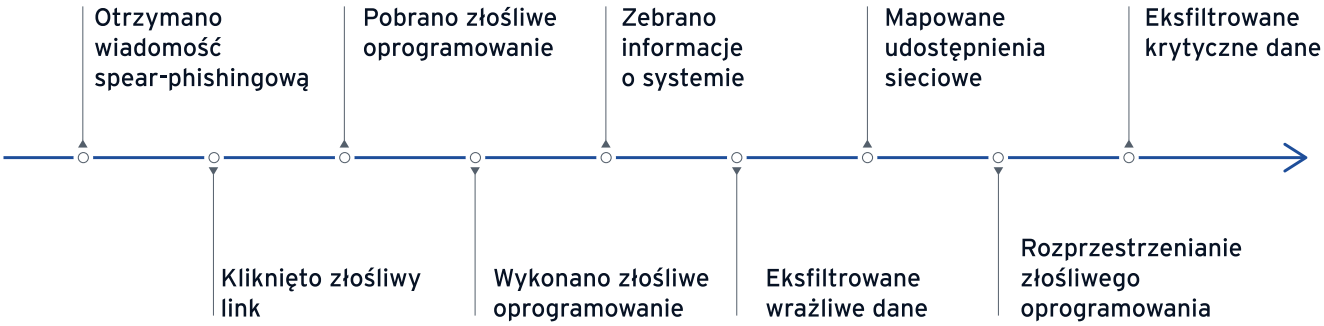
opis scenariusza nr 2 użytego w ćwiczeniach CEP24 (inspirowany działaniami grupy Lazarus)

Tło:

Medialne doniesienia z Niemiec wskazują na nową kampanię wymierzoną w sektor bankowy, a CSIRT NASK ostrzega przed atakami grupy Lazarus na instytucje finansowe w kilku krajach Europy. Kampania wykorzystuje zaawansowane techniki spear phishingowe w celu nakłonienia pracowników do otwierania zainfekowanych linków. CSIRT KNF podkreśla, że celem cyberprzestępców jest eksfiltracja wrażliwych danych, które mogą być później wykorzystane w kolejnych operacjach lub sprzedane na czarnym rynku.

Opis zdarzeń:

1. Pracownik banku otrzymuje specjalnie przygotowaną wiadomość spear phishingową zawierającą złośliwy link, który po kliknięciu przenosi go na stronę ze złośliwym oprogramowaniem.
2. Wykorzystując podatność przeglądarki internetowej zainfekowana strona automatycznie pobiera i zapisuje plik ze złośliwym oprogramowaniem na komputerze pracownika w ogólnodostępnej lokalizacji systemu.
3. Pracownik zmanipulowany technikami socjotechnicznymi otwiera złośliwy plik, co pozwala atakującym na ustanowienie komunikacji z serwerem Command and Control (C2).
4. Atakujący zbierają szczegółowe informacje o systemie, w tym o uruchomionych procesach, konfiguracji systemu operacyjnego, kontach użytkowników oraz aktywnych interfejsach sieciowych.
5. Dalsze działania atakujących obejmują przeszukiwanie folderów użytkownika w celu zebrania wrażliwych plików, które są następnie eksfiltrowane poza infrastrukturę banku przy użyciu nietypowych protokołów komunikacyjnych.
6. W następnej fazie atakujący mapują udziały sieciowe oraz kopiują złośliwy plik do udziału administracyjnego na zdalnej maszynie.
7. Cyberprzestępcy tworzą i uruchamiają zaplanowane zadanie na zdalnym komputerze, co umożliwia uruchomienie złośliwego oprogramowania i uzyskanie dostępu do systemów realizujących krytyczne funkcje bankowe.
8. Atakujący zbierają szczegółowe informacje o zainfekowanym, zdalnym systemie, analogicznie do poprzednich działań i ustanawiają połączenie z serwerem C2, by nadal kontrolować sieć.
9. W finalnym etapie atakujący wykradają dane z systemów realizujących funkcje krytyczne, wykorzystując nietypowe protokoły komunikacyjne, co pozwala na niezauważoną eksfiltrację informacji.



Raport z ćwiczeń Cyber-EXE Polska 2024