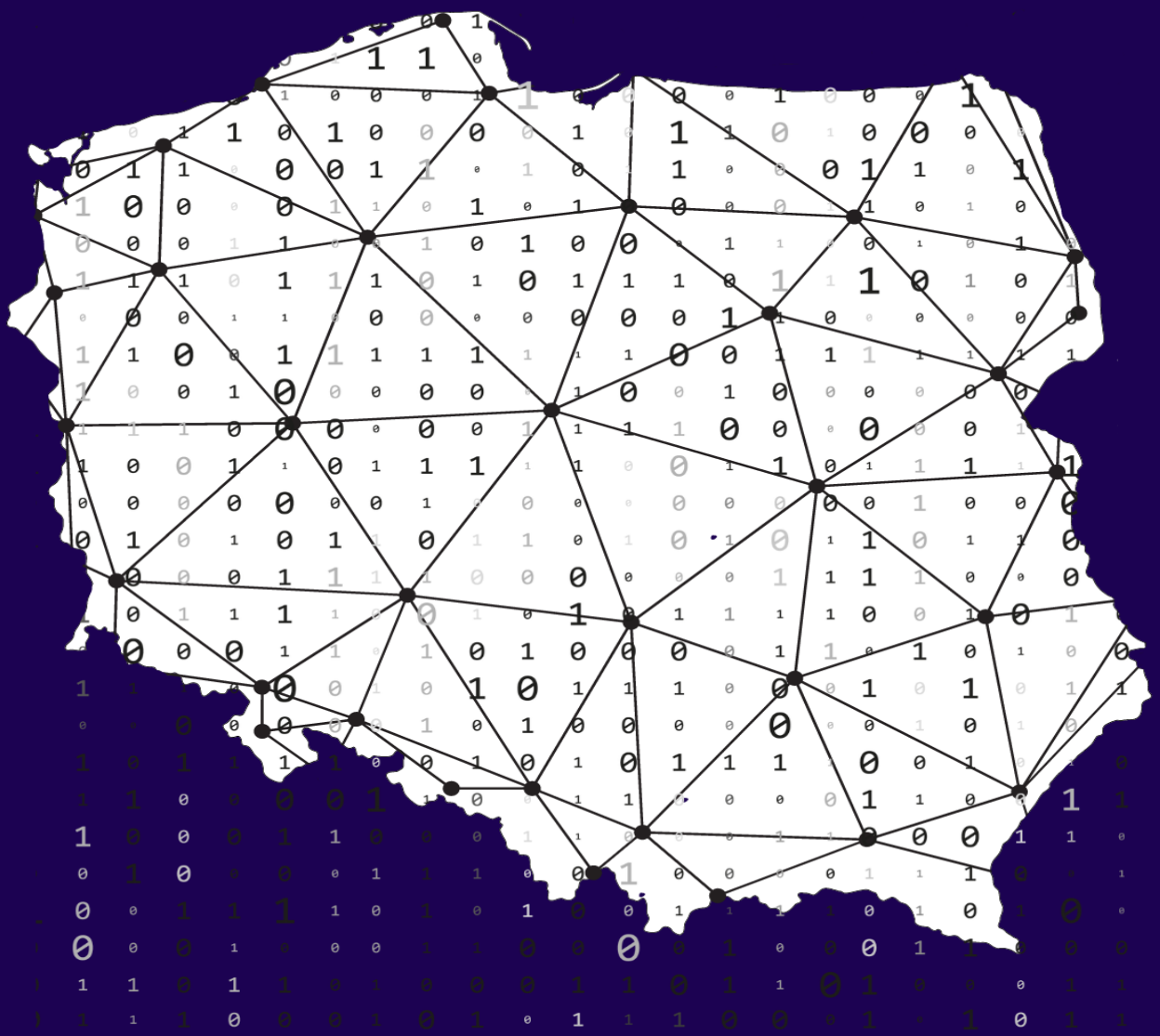
Ministerstwo Cyfryzacji

Departament Cyberbezpieczeństwa

TLP:CLEAR

SPRAWOZDANIE

PEŁNOMOCNIKA RZĄDU DO SPRAW CYBERBEZPIECZEŃSTWA ZA 2023 ROK



2024

Sprawozdanie Pełnomocnika Rządu do Spraw Cyberbezpieczeństwa za 2023 rok

Legenda TLP: https://cert.pl/tlp/

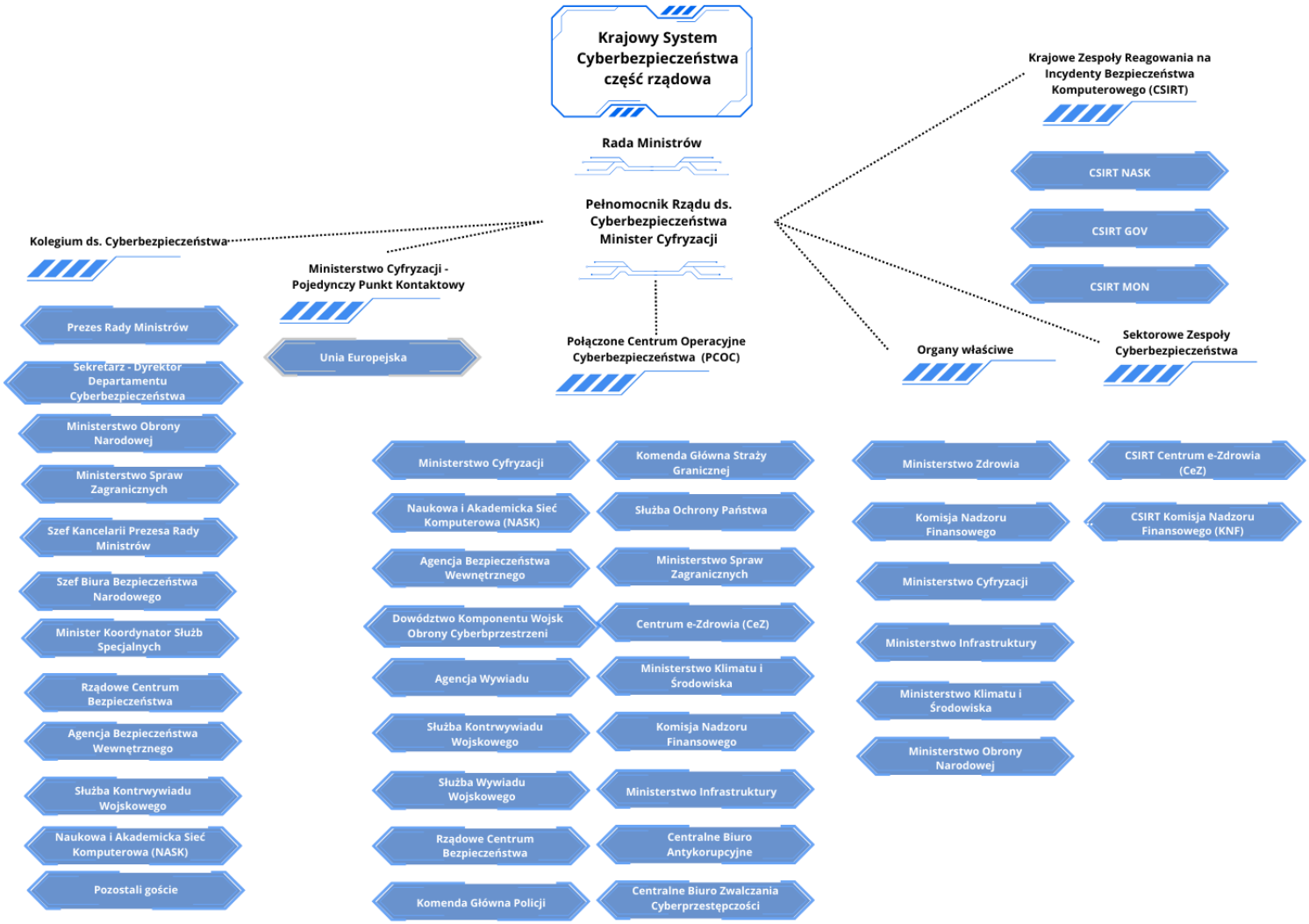
Spis treści

Wstęp

Zgodnie z art. 63 ust. 1 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (dalej: UKSC) Pełnomocnik Rządu do Spraw Cyberbezpieczeństwa (dalej: Pełnomocnik) opracowuje i przedkłada Radzie Ministrów w terminie do dnia 31 marca każdego roku sprawozdanie za poprzedni rok kalendarzowy zawierające informacje o prowadzonej działalności w zakresie zapewnienia cyberbezpieczeństwa na poziomie krajowym.

Sprawozdanie zostało opracowane przez Departament Cyberbezpieczeństwa Ministerstwa Cyfryzacji na podstawie własnych danych oraz przy wykorzystaniu informacji przedstawionych przez instytucje krajowe, w szczególności zespoły reagowania na incydenty bezpieczeństwa komputerowego (CSIRT) poziomu krajowego, organy właściwe ds. cyberbezpieczeństwa, służby specjalne, organy ścigania i wymiaru sprawiedliwości, inne instytucje publiczne, jak również podmioty uczestniczące w Programie Współpracy w Cyberbezpieczeństwie (PWCyber).

Informacje uzupełniające zostały zawarte w niejawnym[1] załączniku do Sprawozdania.

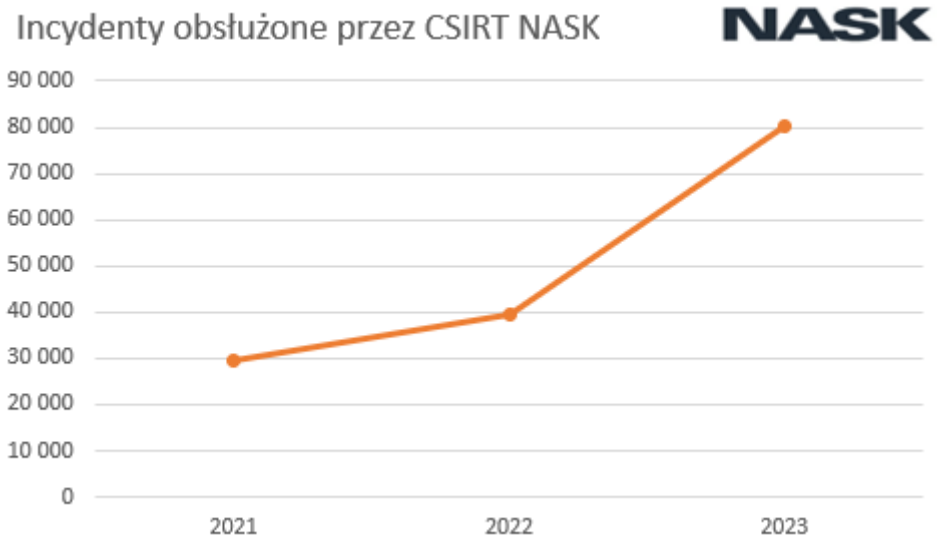


[1] W rozumieniu ustawy z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych.

Podsumowanie zarządcze

Rok 2023 był kolejnym rokiem krzepnięcia Krajowego Systemu Cyberbezpieczeństwa (KSC), formalnie ustanowionego poprzez UKSC w 2018 r., ale faktycznie istniejącego i ewoluującego od lat. Obecnie jest to stabilny system z rosnącym potencjałem tworzących go instytucji. W KSC centralną rolę pełni Ministerstwo Cyfryzacji, w którym umocowany jest Pełnomocnik, odpowiedzialne m.in. za kreowanie systemu. Pod względem operacyjnym, w tym w zakresie reagowania na zagrożenia, kluczowe są trzy zespoły CSIRT poziomu krajowego (CSIRT NASK, CSIRT GOV, CSIRT MON). Ponadto w swoich sektorach coraz aktywniej działają organy właściwe, z których część posiada już własne sektorowe zespoły cyberbezpieczeństwa, a cześć planuje ich powołanie. Projektowane zmiany prawne przewidują przekształcenie tych zespołów w sektorowe CSIRT-y. Poza tym, dla stabilności KSC istotne znaczenie ma organ doradczy, jakim jest Kolegium do Spraw Cyberbezpieczeństwa, w którego skład wchodzą przedstawiciele najważniejszych dla bezpieczeństwa narodowego instytucji. W 2023 r. coraz większe znaczenie dla bieżącej koordynacji działań i reagowania na incydenty miało, ustanowione przez Ministerstwo Cyfryzacji i Rządowe Centrum Bezpieczeństwa (RCB), Połączone Centrum Operacyjne Cyberbezpieczeństwa (PCOC), w którym uczestniczą kluczowe instytucje zapewniające bezpieczeństwo teleinformatyczne na poziomie krajowym. Nie można również zapomnieć jaką rolę dla bezpieczeństwa narodowego, także w cyberprzestrzeni, odgrywają służby wywiadowcze i kontrwywiadowcze, a w zakresie zwalczania cyberprzestępczości organy ścigania.

Ubiegły rok upłynął pod znakiem rosnącej skali cyberataków. Świadczy o tym wzrost obsłużonych incydentów przez CSIRT NASK, nie tylko w porównaniu z rokiem 2022, ale i wcześniejszych lat. W 2021 r. był to blisko 30 tys. incydentów, w kolejnym roku już prawie 40 tys. incydentów (wzrost o ok. 25% r/r), a w 2023 r. już ponad 80 tys. incydentów (wzrost o ponad 100% r/r). Jest to związane z rosnącym zjawiskiem cyberprzestępczości, jak również rosnącym zagrożeniem ze strony grup haktywistycznych oraz grup APT powiązanych ze służbami państw-adwersarzy. W szczególności to ostatnie zagrożenie ma szczególny wymiar wobec trwającej wojny Rosji z Ukrainą, w której Polska pełni rolę hubu wsparcia dla Ukrainy oraz sama udziela wielkoskalowej pomocy, jak również działań hybrydowych ze strony Rosji, Białorusi i innych aktorów wymierzonych w Zachód, w tym w Polskę.



Kolejnym zjawiskiem, coraz bardziej dostrzegalnym w minionym roku, był wpływ nowych technologii na cyberbezpieczeństwo, zarówno w kontekście generowanych zagrożeń, jak i zwiększenia możliwości cyberochrony. W szczególności coraz większe znaczenie będzie mieć wykorzystanie sztucznej inteligencji. Również inne technologie już dziś mają krytyczne

znaczenie dla bezpieczeństwa narodowego (np. rozwiązania chmurowe) lub będą je mieć w perspektywie kolejnych lat (np. informatyka kwantowa, m.in. w zakresie kryptografii i łączności).

Sprawozdanie opisuje najważniejsze realizowane działania na rzecz zwiększenia poziomu bezpieczeństwa polskiej cyberprzestrzeni. Z jednej strony kluczowe znaczenie miało rozwijanie narzędzi i systemów zapewniających cyberbezpieczeństwo od strony technicznej, czego przykładem, wobec rosnącej skali ataków DDoS, jest projekt AntyDDoS, który ustanowiło Ministerstwo Cyfryzacji, powierzając jego realizację NASK-PIB. Dzięki tym działaniom na chwilę obecną osłonę przed atakami DDoS Ministerstwo Cyfryzacji zapewnia centralnie dla 67 instytucji, w tym np. także dla Sił Zbrojnych RP, służb specjalnych oraz urzędów centralnych. Z drugiej strony równie ważnym aspektem było zapewnienie zasobu kadrowego o odpowiednich kompetencjach, dla którego fundamentalne znaczenie miało świadczenie teleinformatyczne, pozwalające zapewnić specjalistom ds. cyberbezpieczeństwa w sektorze publicznym wynagrodzenie porównywalne do sektora prywatnego. W wymiarze ogólnospołecznym należy kontynuować działalność edukacyjną i szkoleniową, zarówno w zakresie podstaw higieny cyfrowej, jak i specjalistyczną.

W 2024 r. Krajowy System Cyberbezpieczeństwa czeka znacząca ewolucja związana z wdrożeniem do polskiego porządku prawnego dyrektywy NIS2 i innego prawodawstwa UE, przyjęciem nowej Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej, jak również zmianami wynikającymi z doświadczeń z dotychczasowego funkcjonowania KSC oraz nowymi wyzwaniami związanymi z postępem technologicznym, zmianami społecznymi oraz przeobrażeniem się środowiska bezpieczeństwa.

Jednym z głównych wniosków dla usprawnienia KSC jest potrzeba powołania podmiotu koordynującego cyberbezpieczeństwo na poziomie ogólnokrajowym, co znacznie usprawniłoby zarządzenie bezpieczeństwem polskiej cyberprzestrzeni oraz pozwoliłoby skuteczniej i szybciej reagować na zagrożenia.

1. Krajobraz bezpieczeństwa cyberprzestrzeni

W 2023 roku poziom zagrożeń w cyberprzestrzeni w skali globalnej utrzymywał się na wysokim poziomie, co powodowało również wysoki poziom cyberzagrożeń dla Polski. Wzrastała aktywność różnego rodzaju grup prowadzących nielegalne działania w świecie cyfrowym, począwszy od haktywistów, przez grupy cyberprzestępcze o charakterze zarobkowym, po grupy powiązane z innymi państwami lub wręcz bezpośrednio działające w ramach instytucji państw-adwersarzy (APT). Proliferacja cyberataków wynikała także z nowych rodzajów zagrożeń, które pojawiały się dzięki rozwojowi nowych technologii i ich coraz większej dostępności. Rosnący poziom cyberzagrożeń w dzisiejszym dynamicznym środowisku cyfrowym ma wpływ na codzienne funkcjonowanie obywateli, przedsiębiorstw i instytucji państwa, co wymaga ciągłego doskonalenia funkcjonowania skutecznego Krajowego Systemu Cyberbezpieczeństwa.

W kolejnych latach trend stale zwiększającej się skali cyberataków zapewne ulegnie wzmocnieniu. Ataki APT sponsorowane przez wrogie państwa mogą charakteryzować się długotrwałym działaniem, wykorzystaniem zawansowanych narzędzi, technologii i wiedzy atakujących. Są one zaawansowane, trudne do wykrycia, a właściwa reakcja na nie wymaga wielowarstwowych środków bezpieczeństwa oraz fachowej wiedzy pracowników komórek odpowiedzialnych za cyberbezpieczeństwo i działów IT. Obserwowane dotychczas problemy w podmiotach publicznych związane z pozyskiwaniem wykwalifikowanej kadry na kluczowe dla bezpieczeństwa zasobów stanowiska, a także znaczące obciążenie licznymi obowiązkami dotychczasowej kadry, mogą doprowadzić do przełamania w pewnym momencie całego systemu zabezpieczeń. Pogorszenie się sytuacji bezpieczeństwa na świecie i w regionie, w szczególności związane z konfliktem za wschodnią granicą kraju, stale rosnąca liczba systemów (w sytuacji zmniejszającej się liczby administratorów systemów oraz często nieadekwatnych do potrzeb zasobów finansowych w niektórych instytucjach) mogą mieć poważne konsekwencje dla poszczególnych podmiotów oraz w wymiarze narodowym. Stale rosnące, niekiedy wyjątkowo dynamicznie, koszty zakupu, utrzymania i rozbudowy infrastruktury bezpieczeństwa są trudne do udźwignięcia przez poszczególne jednostki sektora finansów publicznych. Dlatego też konieczne są dalsze działania wzmacniające Krajowy System Cyberbezpieczeństwa, koordynowanie działań, zwiększanie potencjału instytucji w zakresie cyberbezpieczeństwa, tak na szczeblu centralnym, jak we wszystkich podmiotach systemu, oraz zapewnienie odpowiednich środków finansowych na rozwój osobowy i techniczny.

Trwający nieustannie konflikt w cyberprzestrzeni, wojna Rosji z Ukrainą, działania hybrydowe Rosji, Białorusi i innych państw wymierzone w Zachód, w tym Polskę, toczące się wojny handlowe i technologiczne, w tym tzw. wojna o chipy, dynamiczna digitalizacja dodatkowo przyspieszona przez pandemię COVID-19, rozwój nowych i przełomowych technologii mających wpływ na wszystkie obszary funkcjonowania społeczeństw, gospodarek i systemów bezpieczeństwa narodowego, to kluczowe czynniki wpływające na diametralne przeobrażanie się świata.

Coraz większe znaczenie dla bezpieczeństwa cyberprzestrzeni, zarówno w wymiarze defensywnym, jak i ofensywnym, mają nowe technologie, w tym sztuczna inteligencja, rozwiązania chmurowe, duże zbiory danych, informatyka kwantowa, środki łączności nowych generacji. Wprowadzenie systemów AI do infrastruktury cyberbezpieczeństwa umożliwia szybsze wykrywanie i reagowanie na potencjalne zagrożenia. Przede wszystkim, narzędzia oparte na AI mogą analizować duże ilości danych w czasie rzeczywistym, identyfikując wzorce i anomalie, które mogą wskazywać na ataki lub niebezpieczne zachowania. Dodatkowo, systemy oparte na sztucznej inteligencji mogą dostosowywać się do zmieniających się warunków i nowych rodzajów zagrożeń, co czyni je bardziej elastycznymi i efektywnymi w porównaniu do tradycyjnych metod. Mogą również automatycznie aktualizować strategie obronne w zależności od ewolucji zagrożeń. Inteligentne systemy są również zdolne

do szybkiego reagowania na incydenty, ograniczając szkody i minimalizując czas, w jakim złośliwe działania mogą wpływać na systemy informatyczne. Wykorzystanie algorytmów uczenia maszynowego pozwala na budowanie modeli predykcyjnych, które potrafią antycypować potencjalne ataki na podstawie wcześniejszych wzorców.

W 2023 r. Polska pozostawała celem licznych cyberataków, w tym operacji prowadzonej przez służby wrogich państw, obliczonych na pozyskanie kluczowych informacji, rozpoznanie systemów ICT na potrzeby potencjalnych przyszłych destrukcyjnych cyberataków, zakłócenie infrastruktury krytycznej i innych kluczowych zasobów, jak również szerzenie dezinformacji mającej na celu rozpropagowywanie nieprawdziwych informacji i własnych narracji oraz pogłębianie polaryzacji społecznej.

1.1 Pełnomocnik Rządu do Spraw Cyberbezpieczeństwa

Umocowanie instytucjonalne Pełnomocnika

Zgodnie z art. 60 UKSC Pełnomocnik odpowiada za koordynowanie działań i realizowanie polityki rządu w zakresie zapewnienia cyberbezpieczeństwa w Rzeczypospolitej Polskiej. W 2023 r. funkcję tę pełnił najpierw Sekretarz Stanu w Kancelarii Prezesa Rady Ministrów, następnie - po odtworzeniu Ministerstwa Cyfryzacji w maju ub.r. - Minister Cyfryzacji, a od końca roku Minister Cyfryzacji, będący jednocześnie Wiceprezesem Rady Ministrów. Odpowiednie umocowanie instytucjonalne Pełnomocnika, swoista unia personalna, pozwalało na zwiększenie efektywności wykonywanych zadań w obliczu rosnącej skali zagrożeń. Liczne zadania na poziomie krajowym realizowane przez resort cyfryzacji (ministra właściwego ds. informatyzacji) mogły być należycie skoordynowane z działaniami innych instytucji zapewniających cyberbezpieczeństwo.

Pełnomocnik i Ministerstwo Cyfryzacji stanowią centralny element kształtujący krajowy system cyberbezpieczeństwa (KSC) tworzony, zgodnie z art. 4 UKSC, przez szereg podmiotów: operatorów usług kluczowych, dostawców usług cyfrowych, CSIRT MON, CSIRT NASK, CSIRT GOV, sektorowe zespoły cyberbezpieczeństwa, liczne jednostki sektora finansów publicznych, instytuty badawcze, urzędy centralne, spółki prawa handlowego wykonujące zadania o charakterze użyteczności publicznej, podmioty świadczące usługi z zakresu cyberbezpieczeństwa, organy właściwe do spraw cyberbezpieczeństwa, oraz Pojedynczy Punkt Kontaktowy do spraw cyberbezpieczeństwa (w rozumieniu UKSC).

Kolegium do Spraw Cyberbezpieczeństwa

Zgodnie z art. 64 UKSC przy Radzie Ministrów działa Kolegium do Spraw Cyberbezpieczeństwa, jako organ opiniodawczo-doradczy w sprawach cyberbezpieczeństwa oraz działalności w tym zakresie CSIRT MON, CSIRT NASK, CSIRT GOV, sektorowych zespołów cyberbezpieczeństwa i organów właściwych do spraw cyberbezpieczeństwa. Do zadań Kolegium należy także opracowywanie rekomendacji dla Rady Ministrów dotyczących działań w zakresie zapewnienia cyberbezpieczeństwa na poziomie krajowym. Posiedzenia Kolegium są organizowane przez Ministerstwo Cyfryzacji, które obsługuje Pełnomocnika. Przebieg prac Kolegium oraz treść wyrażonych stanowisk, rekomendacji oraz opinii posiadają charakter niejawny w rozumieniu ustawy o ochronie informacji niejawnych.

W 2023 r. odbyło się 7 posiedzeń Kolegium. Tematyka poruszana w minionym roku dotyczyła opinii w sprawach:

- aktywności grup APT w cyberprzestrzeni;
- informacji Prezesa UKE o wymaganiach dotyczących bezpieczeństwa i integralności telekomunikacyjnej oraz usług w kontekście rezerwacji częstotliwości po przeprowadzeniu aukcji na rezerwację częstotliwości z pasma 3,6 Ghz;
- wniosku Prokuratury Okręgowej w Gdańsku o udzielenie wsparcia z Funduszu Cyberbezpieczeństwa;
- zaprezentowanie przez Microsoft praktycznych aspektów użycia rozwiązań sztucznej inteligencji na rzecz bezpieczeństwa państwa i bezpieczeństwa narodowego;
- omówienie krytycznych podatności w rozwiązaniach sektora transportu;
- aktualizacji wniosków o udzielenie wsparcia z Funduszu Cyberbezpieczeństwa dotyczących prognozowanych kosztów związanych z przyznaniem świadczenia teleinformatycznego.

Połączone Centrum Operacyjne Cyberbezpieczeństwa

W celu należytej koordynacji bieżącego zarządzania cyberbezpieczeństwem Ministerstwo Cyfryzacji i RCB organizują spotkania w formacie Połączonego Centrum Operacyjnego Cyberbezpieczeństwa. Funkcjonowanie PCOC umożliwia szybką wymianę informacji, co pozwala podnieść poziom cyberbezpieczeństwa w kraju, w szczególności w zakresie reagowania na pojawiające się incydenty cyberbezpieczeństwa. W spotkaniach PCOC uczestniczą CSIRT-y poziomu krajowego oraz inne podmioty kluczowe dla bezpieczeństwa państwa.

Aby zapewnić odpowiednie środki techniczne dla funkcjonowania PCOC resort cyfryzacji zlecił NASK-PIB zadanie pn. „Wyposażenie uczestników Projektu Połączonego Centrum Operacyjnego Cyberbezpieczeństwa (PCOC) w niezbędne urządzenia i sprzęt ICT". Zadanie obejmuje możliwie szybkie, efektywne i optymalne wyposażenie wybranych podmiotów krajowego systemu cyberbezpieczeństwa, biorących udział w realizacji projektu PCOC, w urządzenia i sprzęt ICT pozwalające na podłączenie do sieci MILNET-Z niezbędnej do wymiany pomiędzy różnymi podmiotami informacji nie tylko jawnych, ale również informacji niejawnych o klauzuli „zastrzeżone", w czasie umożliwiającym szybką reakcję na pojawiające się cyberzagrożenia. PCOC funkcjonuje od 2022 r., kiedy to w niezbędne urządzenia i sprzęt wyposażono 12-tu uczestników projektu. W 2023 r. wyposażono kolejne 4 podmioty.

Zespół Incydentów Krytycznych

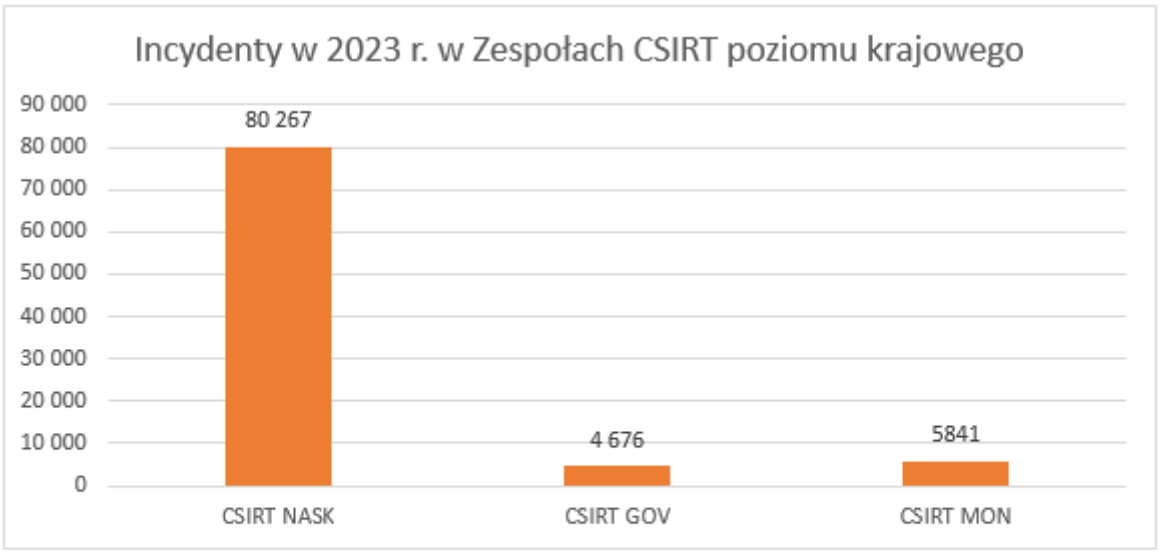
Zespół jest obsługiwany przez RCB. W celu konsolidacji zadań w zakresie cyberbezpieczeństwa w przygotowywanej nowelizacji UKSC przewiduje się przeniesienie obsługi Zespołu do urzędu obsługującego Pełnomocnika.

1.2 CSIRT-y poziomu krajowego

W ramach Krajowego Systemu Cyberbezpieczeństwa w zakresie operacyjnym kluczowe są trzy zespoły CSIRT:

1) **CSIRT GOV** – Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego działający na poziomie krajowym, prowadzony przez Szefa Agencji Bezpieczeństwa Wewnętrznego;
2) **CSIRT MON** – Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego działający na poziomie krajowym, prowadzony przez Ministra Obrony Narodowej;
3) **CSIRT NASK** – Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego działający na poziomie krajowym, prowadzony przez Naukową i Akademicką Sieć Komputerową – Państwowy Instytut Badawczy.

Zadania CSIRT-ów określa rozdział 6. UKSC. Każdy z nich cechuje się swoją specyfiką z uwagi na obszar odpowiedzialności (*constituency*). W pewnym uproszczeniu można stwierdzić, że CSIRT GOV odpowiada za administrację państwową i infrastrukturę krytyczną; CSIRT NASK za administrację samorządową, niektóre instytucje publiczne, operatorów usług kluczowych i dostawców usług cyfrowych (za wyjątkiem tych podległych pod MON), sektor przedsiębiorstw i „zwykłych obywateli"; a CSIRT MON za Siły Zbrojne RP, resort obrony narodowej (w tym jego jednostki i komórki organizacyjne), jak również niektóre inne podmioty realizujące zadania na rzecz Sił Zbrojnych RP, jak np. część przedsiębiorstw zbrojeniowych.



1.2.1 CSIRT NASK

Dane dotyczące liczby zgłoszeń i incydentów w 2023 r.

Zgłoszenia i incydenty cyberbezpieczeństwa zarejestrowane przez CSIRT NASK od 1 stycznia do 31 grudnia 2023 r.

Zagrożenia cyberbezpieczeństwa	Liczba
Zarejestrowane zgłoszenia	371 089
w tym zarejestrowane (obsłużone) incydenty	80 267

Incydenty zgłoszone ustawowo do CSIRT NASK od 1 stycznia do 31 grudnia 2023 r.

Zagrożenia cyberbezpieczeństwa	Liczba
Incydenty krytyczne	0
Incydenty poważne	40
Incydenty istotne	0
Incydenty w podmiotach publicznych	2184

Opis najważniejszych incydentów

Wśród 40 incydentów poważnych odnotowanych w 2023 r. 31 zdarzeń miało miejsce w sektorze bankowość i infrastruktura rynków finansowych. Pozostałe incydenty poważne dotyczyły sektora ochrony zdrowia (9). Wśród 2184 incydentów w podmiotach publicznych, zgłoszonych ustawowo do CSIRT NASK w 2023 r., ponad połowę (55%) stanowiły incydenty w administracji publicznej. W analizowanym okresie nie zarejestrowano żadnego incydentu krytycznego ani też żadnego incydentu istotnego.

Zgłoszenia nielegalnych treści

Oddzielną grupę zgłoszeń stanowią incydenty związane z publikacją potencjalnie nielegalnych treści w internecie, w szczególności materiałów przedstawiających seksualne wykorzystywanie dzieci lub innych szkodliwych treści skierowanych przeciwko bezpieczeństwu małoletnich. Tego typu zagrożenia obsługiwane są przez zespół Dyżurnet.pl.

Incydenty zarejestrowane przez zespół Dyżurnet.pl	Liczba
Zarejestrowane incydenty*, w tym:	**18 437**
treści przedstawiające seksualne wykorzystywanie dzieci (CSAM**)	**2 612**

*Incydent to zgłoszenie poddane analizie oraz odpowiednio zaklasyfikowane przez ekspertów Dyżurnet.pl.

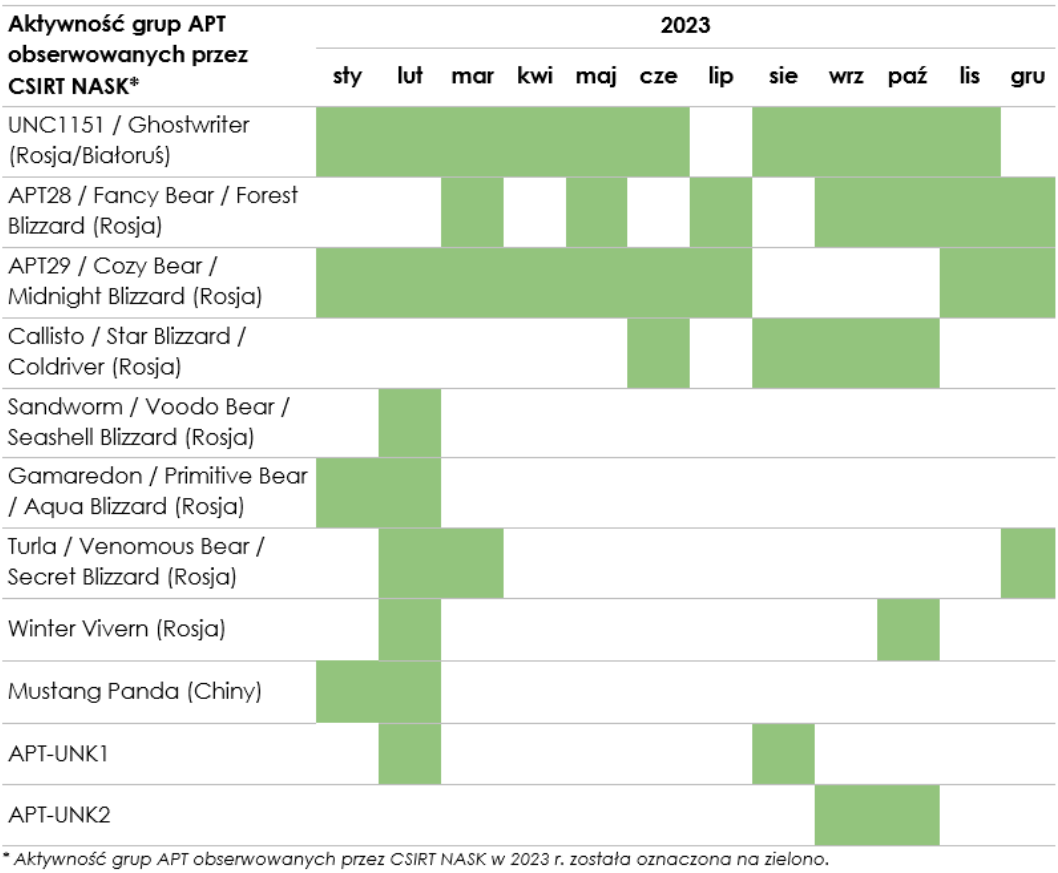
** CSAM (Child Sexual Abuse Materials), tj. materiały przedstawiające seksualne wykorzystywanie dziecka.

Incydenty zarejestrowane przez zespół Dyżurnet.pl od 1 stycznia do 31 grudnia 2023 r.

Działania grup APT obserwowane przez CSIRT NASK w 2023 r.

Od czasu rozpoczęcia wojny w Ukrainie CSIRT NASK obserwuje znaczne nasilenie aktywności grup APT, często wiązanych z obcymi państwami. Większość tych aktywności jest motywowana pozyskiwaniem informacji z zaatakowanych systemów, chociaż w 2023 r. zdarzały się również ataki, wymierzone w szczególności w sektor transportu i w logistykę, których celem było zakłócenie ciągłości działania. Większość grup jest wiązana z Federacją Rosyjską i część z nich przejawia stałą aktywność.

Przypadki opisywane poniżej są tylko fragmentem działalności grup APT, obserwowanym przez CSIRT NASK. Nie oddają one w pełni skali znanych ataków tych grup na polskie podmioty.

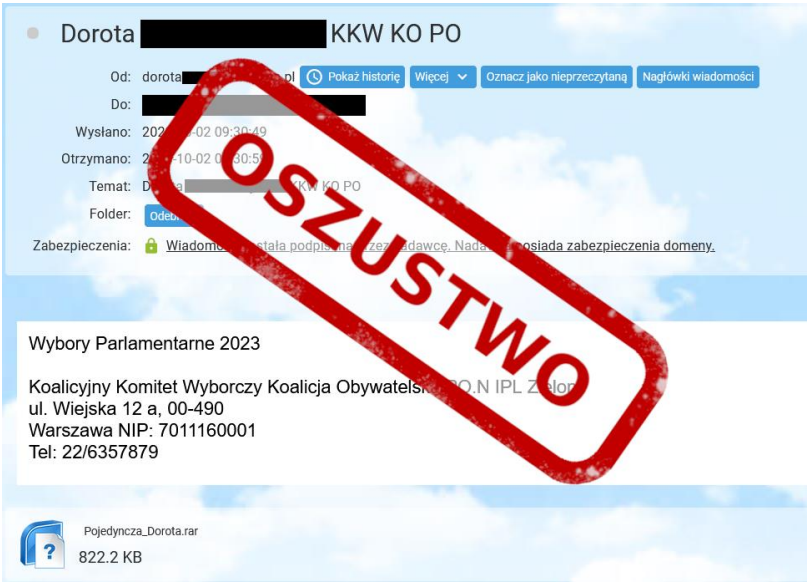


** Aktywność grup APT obserwowanych przez CSIRT NASK w 2023 r. została oznaczona na zielono.*

Wybrane kampanie UNC1151/Ghostwriter

W 2023 r. najbardziej aktywna była grupa UNC1151 powiązana z operacją Ghostwriter. Grupa ta z dużym prawdopodobieństwem jest powiązana z rządem Białorusi, ale według innych opracowań ma również związek z rosyjskimi służbami specjalnymi. Celami ataków są głównie osoby związane z polityką i wojskowością oraz mogące mieć pośredni związek z Rosją i Białorusią, np. tłumacze przysięgli języka rosyjskiego, prawnicy, pracownicy organizacji pozarządowych, księża prawosławni czy dziennikarze. Ataki obserwowano również w Ukrainie, Litwie, Łotwie czy w Niemczech. Motywacją była najczęściej kradzież informacji w celach wywiadowczych oraz prowadzenia kampanii dezinformacyjnych.

Większość obserwowanej aktywności była związana z kampaniami złośliwego oprogramowania oraz dezinformacją. W pierwszym kwartale 2023 r. CSIRT NASK rejestrował duże kampanie dezinformacyjne w Polsce, Litwie i Łotwie, związane z rzekomymi ćwiczeniami przy granicy z Ukrainą, rekrutacją do wojska, brakiem jodku potasu w aptekach czy zagrożeniem terrorystycznym na terenie Polski. W kolejnych kwartałach CSIRT NASK obserwował kampanie, w których przeważała tematyka związana z nadchodzącymi wyborami parlamentarnymi.



Wiadomość phishingowa zawierająca szkodliwy załącznik i podszywająca się pod jeden z komitetów wyborczych.

Działania dezinformacyjne, w tym także z wykorzystaniem wykradzionych materiałów, trwały do czasu wyborów. CSIRT NASK zaobserwował m.in. przykuwający uwagę atak na systemy informacji w wybranych centrach handlowych, gdzie wyświetlono plansze z fałszywymi informacjami. Następnie aktywność grupy UNC1151 znacznie zmalała.

Fałszywa informacja wyświetlona na przejętym systemie w centrum handlowym.

APT28 / Fancy Bear / Forest Blizzard

Główną informacją 2023 r. związaną z grupą APT28 było ujawnienie wykorzystywania przez nią, co najmniej od sierpnia 2022 r., nieznanej wcześniej podatności w Microsoft Outlook. Tuż po tym jak CSIRT NASK uzyskał informację o podatności, opublikowany został artykuł z rekomendacjami na stronie https://cert.pl. Ustalono, że celami ataków były polskie firmy z sektorów transportu, energetyki i zbrojeniowego.

W kolejnych miesiącach CSIRT NASK obserwował powtarzające się kampanie phishingowe (ukierunkowane na przejęcie haseł do kont pocztowych) oraz dystrybuujące złośliwe oprogramowanie. Większość tych kampanii była wysyłana do odbiorców z sektorów będących w obszarze zainteresowania grupy.

APT-UNK2

Oprócz grup, których działalność jest dobrze poznana i odpowiednio zakwalifikowana, CSIRT NASK w 2023 r. śledził również grupę, która przeprowadziła kampanię podszywającą się pod NASK. W załączniku do rozesłanego e-maila znajdowała się instrukcja, jak zainstalować rzekomy sieciowy program ochrony obywateli. Podczas uruchomienia pliku z linku podanego w instrukcji dochodziło do infekcji złośliwym oprogramowaniem Lumma Stealer. Mimo że jest ono wykorzystywane głównie w atakach motywowanych finansowo, w tym przypadku, na podstawie celów oraz powiązanych kampanii, eksperci CSIRT NASK ocenili, że motywacją aktora było pozyskiwanie informacji. Ta sama grupa korzystała wcześniej z domen podszywających się pod strony prezentujące informacje związane z cyberbezpieczeństwem w Polsce, szczytem NATO w Wilnie, czy organizacjami działającymi na rzecz wolności prasy.

Współpraca krajowa i międzynarodowa CSIRT NASK

W ramach codziennej pracy nad aktywnością grup APT CSIRT NASK blisko współpracuje z CSIRT-ami poziomu krajowego (CSIRT GOV i CSIRT MON) oraz z zespołami odpowiednich polskich służb specjalnych. Na uwagę zasługuje również współpraca międzynarodowa w ramach CSIRTs Network oraz z partnerami komercyjnymi.

W 2023 r. CSIRT NASK razem z partnerami dwukrotnie opisywał obserwowaną aktywność grupy APT29/Midnight Blizzard, powiązanej z Rosyjską Służbą Wywiadu Zagranicznego (SVR).

Pierwszy raport[2] w tej sprawie został przygotowany w kwietniu 2023 r. wspólnie ze Służbą Kontrwywiadu Wojskowego. Dotyczył on kampanii szpiegowskiej, której celem było pozyskiwanie informacji z ministerstw spraw zagranicznych oraz placówek dyplomatycznych, w większości znajdujących się w państwach należących do NATO i Unii Europejskiej. Udało się osiągnąć zakładany cel, którym było zakłócenie tej kampanii.

Drugi raport[3] został opublikowany w grudniu 2023 r. W operacji opisywanej w raporcie brały udział także FBI, CISA, NSA, UK NCSC oraz SKW. Prowadzone działania dotyczyły przeciwdziałania kampanii, w której wykorzystywana była podatność w oprogramowaniu JetBrains TeamCity. Oprogramowanie to jest używane do zarządzania i automatyzacji procesu kompilacji, budowania, testowania i wydawania oprogramowania. Dostęp do serwera TeamCity może prowadzić do dostępu do kodów źródłowych, certyfikatów kryptograficznych oraz może być wykorzystany do wpłynięcia na proces wytwarzania oprogramowania, co z kolei może umożliwić manipulowanie łańcuchem dostaw oprogramowania. Dzięki podjętym działaniom udało się zatrzymać tę kampanię i poinformować ofiary.

CSIRT NASK dostrzega w szczególności potrzebę podniesienia poziomu odporności i wzmocnienia jednostek samorządu terytorialnego (JST) w obszarze przeciwdziałania cyberzagrożeniom. W tym kontekście ważny jest udział NASK-PIB – jako partnera merytorycznego – w realizacji projektu grantowego pn. „Cyberbezpieczny Samorząd". W 2023 r. przygotowano publikację pt. „Cyberbezpieczny Samorząd – poradnik". Głównym celem opracowania jest ułatwienie JST identyfikacji aktualnego stanu cyberbezpieczeństwa oraz realnych możliwości podniesienia przez JST poziomu cyberbezpieczeństwa. Jednocześnie w poradniku przedstawiono podstawowe zagadnienia formalne, prawne, organizacyjne i techniczne, umożliwiające analizę stanu rozwoju JST w obszarze cyberbezpieczeństwa. Wskazano również przykłady przedsięwzięć, jakie mogą podjąć JST w celu zwiększenia bezpieczeństwa informacji przez wzmacnianie odporności oraz zdolności do skutecznego zapobiegania incydentom, wykrywania ich i reagowania na nie.

Ponadto w 2023 r. w ramach realizacji zadań związanych ze wzmacnianiem cyberbezpieczeństwa jednostek samorządu terytorialnego powołano Fundusz wsparcia JST, który funkcjonował do 31.12.2023 r.

W 2023 r. CSIRT NASK – w ramach monitorowania zmian w obszarze *constituency* CSIRT NASK związanych z nowelizacją ustawy o krajowym systemie cyberbezpieczeństwa, a także z rozwojem krajowego i europejskiego prawa w obszarze cyberbezpieczeństwa – opracowywał analizy:

- „Nowelizacja Ustawy o KSC – co przewiduje najnowsza wersja projektu?",
- „Dyrektywa NIS 2: wytyczne, akty delegowane i wykonawcze",

[2] https://cert.pl/posts/2023/04/kampania-szpiegowska-apt29
[3] https://cert.pl/posts/2023/12/apt29-teamcity

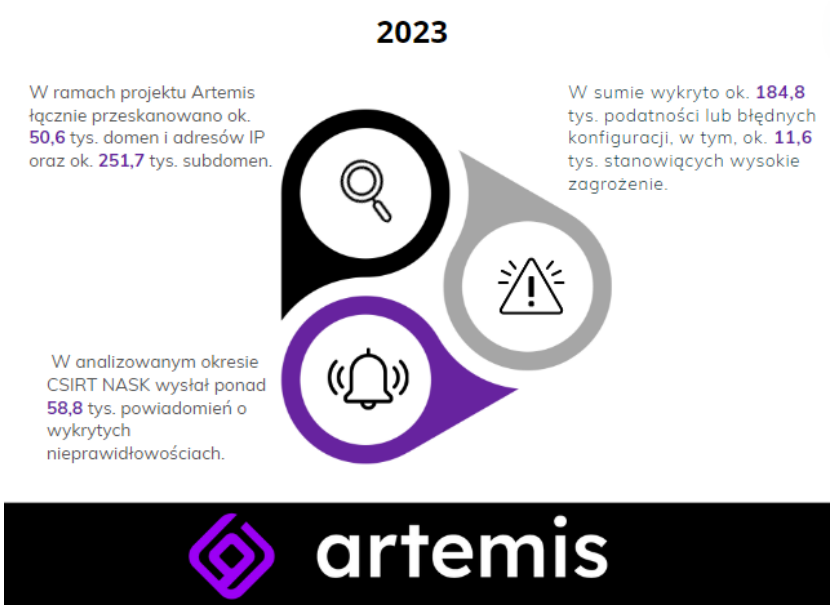
- „Dyrektywa CER – unijne wzmocnienie ochrony infrastruktury krytycznej",
- „Ustawa o zwalczaniu nadużyć w komunikacji elektronicznej",
- „Projekt przepisów w sprawie ograniczenia dostępu do pornografii osobom małoletnim".

W 2023 r. CSIRT NASK w celu wzmocnienia krajowego systemu cyberbezpieczeństwa wdrażał w życie zapisy ustawy o zwalczaniu nadużyć w komunikacji elektronicznej. Działania te obejmowały m.in.:

- Wprowadzenie bezpłatnego skróconego numeru 8080[4]. Od 1 stycznia do 31 grudnia 2023 r. CSIRT NASK otrzymał zgłoszenia 194,8 tys. podejrzanych SMS-ów.
- Stworzenie serwisu bezpiecznapoczta.cert.pl – serwis powstał, by chronić użytkowników poczty elektronicznej i ułatwić instytucjom sprawdzenie poprawności konfiguracji mechanizmów zapewniających jej bezpieczeństwo.
- Przygotowanie do uruchomienia systemu teleinformatycznego służącego do udostępniania i przekazywania informacji o wystąpieniu smishingu wraz z wzorcami wiadomości.
- Przygotowanie do utworzenia wykazu nazw i ich skrótów zastrzeżonych dla podmiotów publicznych jako tzw. nadpis wiadomości pochodzącej od tego podmiotu (zgodnie z ustawą dotyczy to podmiotów publicznych) oraz wariantów tych nazw i skrótów, mogących wprowadzać odbiorcę w błąd. Na stronie incydent.cert.pl/nadpis jest udostępniony formularz umożliwiający zgłaszanie nadpisów wiadomości SMS przez podmioty publiczne.

W związku z rosnącą liczbą cyberzagrożeń CSIRT NASK rozwijał narzędzie Artemis, służące do wykrywania najczęściej występujących podatności i błędów konfiguracyjnych obecnych w ramach usług sieciowych, a także przekazywał osobom odpowiedzialnym za dany system informacje o znalezionych podatnościach i błędnych konfiguracjach. W 2023 r. w ramach projektu Artemis łącznie przeskanowano ok. 50,6 tys. domen i adresów IP oraz ok. 251,7 tys. subdomen. W sumie wykryto ok. 184,8 tys. podatności lub błędnych konfiguracji, w tym ok. 11,6 tys. stanowiących wysokie zagrożenie. W analizowanym okresie CSIRT NASK wysłał ponad 58,8 tys. powiadomień o wykrytych nieprawidłowościach. Ostrzeżenia zostały przekazane m.in. do placówek oświatowych, uczelni, jednostek samorządu terytorialnego, placówek medycznych, producentów automatyki przemysłowej, mediów lokalnych, osób odpowiedzialnych za bezpieczeństwo systemów w domenie gov.pl, a także operatorów usług kluczowych. Dzięki temu, że znalezione podatności i błędne konfiguracje są zgłaszane osobom odpowiedzialnym za dany system, CSIRT NASK zwiększa bezpieczeństwo polskiego internetu.

[4] Do listopada 2023 r. CSIRT NASK przyjmował zgłoszenia SMS na numer 799 448 084.



Dane na temat projektu ARTEMIS za 2023 r.

W celu wzmocnienia międzysektorowej współpracy CSIRT NASK rozwijał Program Partnerstwo dla Cyberbezpieczeństwa (PdC). Jest to istotny kanał wymiany informacji pomiędzy podmiotami KSC. Celem PdC jest wymiana dobrych praktyk i zacieśnianie współpracy w ramach krajowego systemu cyberbezpieczeństwa. W 2023 r. w ramach PdC organizowano spotkania, warsztaty, w tym prowadzono prezentacje z udziałem ekspertów, a także przygotowywano i rozsyłano materiały informacyjno-edukacyjne dla uczestników programu PdC.

W ramach wzmacniania KSC CSIRT NASK rozwijał też platformę n6 (system przekazywania informacji o zagrożeniach zidentyfikowanych w sieci danego podmiotu), który jest udostępniany na licencji z otwartym kodem źródłowym.

W ramach wzmocnienia cyberbezpieczeństwa w sektorze ochrony zdrowia, CSIRT NASK wspierał utworzenie CSIRT CeZ, który pełni obecnie rolę Sektorowego Zespołu Cyberbezpieczeństwa dla sektora ochrony zdrowia. CSIRT CeZ został utworzony w strukturze NASK-PIB na podstawie zawartego w kwietniu 2023 r. porozumienia pomiędzy NASK-PIB a Centrum e-Zdrowia.

Rozpoczęto realizację projektu pn. Centrum Cyberbezpieczeństwa NASK (CCN), którego głównym celem jest wzmocnienie krajowego systemu cyberbezpieczeństwa poprzez utworzenie CCN. Realizacja projektu pozwoli na podniesienie poziomu bezpieczeństwa informacji poprzez wzmacnianie odporności oraz zdolności do skutecznego zapobiegania i reagowania na incydenty w systemach informacyjnych państwa oraz podmiotów mających kluczowe znaczenie dla gospodarki. Projekt stanowi odpowiedź na szereg zdefiniowanych wyzwań i potrzeb oraz szybko rosnącą liczbę coraz poważniejszych zagrożeń w cyberprzestrzeni i wynikających z nich strat gospodarczych.

W celu zapewnienia ochrony przed atakami DDoS – Distributed Denial of Service dla podmiotów realizujących zadania publiczne oraz podmiotów istotnych z punktu widzenia bezpieczeństwa RP uruchomiono usługę Anty DDoS.

Z uwagi na ustawowo określony zakres *constituency* analizy CSIRT NASK w zakresie funkcjonowania krajowego systemu cyberbezpieczeństwa obejmują w przeważającym zakresie ten obszar.

Zidentyfikowane najpoważniejsze zagrożenia

- Techniczne dla systemów teleinformatycznych:
  - ✓ Zbyt niski poziom wdrożenia oraz wykorzystania drugiego składnika uwierzytelnienia logowania przez użytkowników systemów.
  - ✓ Przeciągający się proces patchowania podatnych systemów dostępnych w sieci dla przypadku identyfikacji błędów z wysoką oceną punktową.
- Systemowe dla krajowego systemu cyberbezpieczeństwa:
  - ✓ Niska lub nieprecyzyjna jakość opisania własności administratorskiej sieci krajowych.
  - ✓ Brak sektorowych zespołów cyberbezpieczeństwa lub perspektyw ich powstania, które mogłyby stanowić rolę naturalnego kontynuatora zadań w momencie wdrożenia zapisów dyrektywy NIS 2.
  - ✓ Wątpliwości interpretacyjne dla potrzeb ustalania właściwego *constituency*.

Wnioski i rekomendacje

CSIRT NASK podkreśla wagę kontynuowania współpracy sektorowej w ramach KSC, prowadzenia konsultacji w zakresie rozwiązań prawnych na gruncie prawa unijnego, zwłaszcza implementacji dyrektywy NIS 2.

CSIRT NASK zwraca uwagę na konieczność monitorowania zmian w obszarze *constituency* CSIRT NASK związanych z nowelizacją ustawy o krajowym systemie cyberbezpieczeństwa i zaangażowania w proces konsultacji nowych przepisów związanych z rozwojem krajowego i europejskiego prawa w obszarze cyberbezpieczeństwa.

Planowane działania NASK w 2024 r.

- CSIRT NASK planuje kontynuować dotychczas prowadzoną współpracę krajową i międzynarodową w zakresie monitorowania działań grup APT, w szczególności z CSIRT-ami poziomu krajowego (CSIRT GOV i CSIRT MON) oraz z zespołami odpowiednich polskich służb specjalnych, a także w ramach CSIRTs Network oraz z partnerami komercyjnymi.
- Artemis – rozwój skanera wykrywającego najczęściej występujące podatności i błędy konfiguracyjne obecne w ramach usług sieciowych. Narzędzie przeznaczone jest do weryfikacji przede wszystkim podmiotów z *constituency* CSIRT NASK, czyli np. szkół, szpitali, instytutów badawczych, uczelni, jednostek samorządu terytorialnego. Znalezione podatności i błędne konfiguracje są i będą zgłaszane osobom odpowiedzialnym za dany system.
- Rozwój platformy n6 służącej do zbierania informacji o wykrytych zagrożeniach i podatnościach.
- W odpowiedzi na rosnącą skalę zagrożeń w sieci, a także skokową zmienność liczby zgłoszeń, prowadzone będą prace podnoszące efektywność obsługi oraz zwiększające szybkość udzielania informacji zwrotnej dla zgłaszających podejrzane wiadomości.
- CERT Polska/CSIRT NASK pełniący funkcję CNA (ang. CVE Numbering Authorities) w dalszym ciągu będzie współtworzyć bazę podatności poprzez nadawanie numerów CVE, które służą do identyfikacji i katalogowania publicznie ujawnionych podatności.

- Kontynuowanie prac związanych z wdrażaniem zapisów ustawy o zwalczaniu nadużyć w komunikacji elektronicznej. Zgodnie z ustawą CSIRT NASK monitoruje występowanie smishingu oraz tworzy wzorce wiadomości, które posiadają cechy pozwalające na uznanie ich za smishing; obsługuje system wymiany informacji o smishingu, prowadzi wykaz zastrzeżonych nadpisów dla podmiotów publicznych.
- CSIRT NASK będzie w dalszym ciągu opracowywał rekomendacje oraz zalecenia dotyczące występujących podatności.
- CSIRT NASK planuje kontynuować działania informacyjno-edukacyjne, w szczególności mające na celu podnoszenie świadomości obywateli w zakresie cyberzagrożeń i higieny cyfrowej.

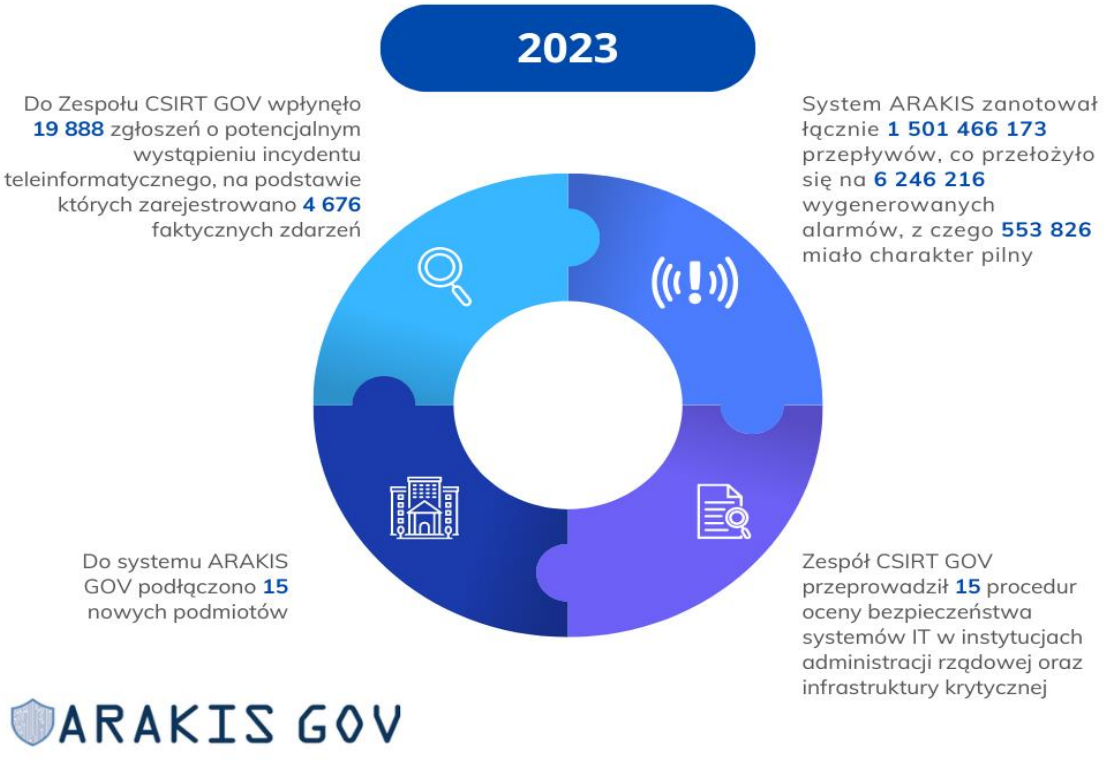
1.2.2 CISRT GOV

CSIRT GOV Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego

Agencja Bezpieczeństwa Wewnętrznego (ABW) i wchodzący w jej skład Zespół CSIRT GOV realizuje ustawowe zadania obejmujące także obszar cyberbezpieczeństwa. Zespół CSIRT GOV, w zakresie swojej właściwości, zapewnia wsparcie przy wykrywaniu incydentów i przeciwdziałaniu zagrożeniom godzącym w bezpieczeństwo systemów kluczowych dla funkcjonowania państwa oraz współpracuje z organami odpowiedzialnymi za rozpoznawanie przestępstw popełnianych w cyberprzestrzeni i ściganie ich sprawców.

ABW przyjmowała i analizowała zgłoszenia o incydentach oraz wydawała rekomendacje zgłaszającym, mając na celu podniesienie poziomu bezpieczeństwa systemów IT, a także formułowała rekomendacje wprowadzenia działań zmierzających do minimalizacji lub neutralizacji zagrożeń, w tym przywrócenia prawidłowego działania systemów teleinformatycznych. W 2023 r. do Zespołu CSIRT GOV wpłynęło 19 888 zgłoszeń o potencjalnym wystąpieniu incydentu teleinformatycznego, na podstawie których zarejestrowano 4 676 faktycznych zdarzeń (ich obsługa realizowana jest w ramach krajowego systemu cyberbezpieczeństwa we współpracy z pozostałymi uczestnikami tego systemu).

Agencja prowadzi system wczesnego ostrzegania o zagrożeniach ARAKIS GOV na podstawie art. 32aa ustawy o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu. W 2023 r. system ARAKIS zanotował łącznie 1 501 466 173 przepływów, co przełożyło się na 6 246 216 wygenerowanych alarmów, z czego 553 826 miało charakter pilny, tzn. wymagało natychmiastowej reakcji na zagrożenie ze strony administratorów i niosło duże ryzyko przełamania zabezpieczeń. W 2023 r. do systemu ARAKIS GOV podłączono 15 nowych podmiotów.



ABW wspierała podmioty administracji publicznej oraz operatorów usług kluczowych i infrastruktury krytycznej w zakresie rozpoznawania i przeciwdziałania zagrożeniom cyberbezpieczeństwa. Agencja dystrybuowała ostrzeżenia o zagrożeniach bezpieczeństwa systemów teleinformatycznych (w tym w zakresie bezpieczeństwa systemów teleinformatycznych operatorów usług kluczowych oraz operatorów infrastruktury krytycznej) oraz przekazywała rekomendacje w zakresie zagadnień organizacyjnych i technicznych, mających na celu podniesienie poziomu bezpieczeństwa systemów IT. W 2023 r. Zespół CSIRT GOV rozesłał do podmiotów administracji publicznej i operatorów infrastruktury krytycznej 766 ostrzeżeń o potencjalnym lub wykrytym zagrożeniu. Ich tematyka obejmowała zarówno informacje o podatnościach w oprogramowaniu, konieczności blokowania szkodliwych adresów IP, wzmożonej aktywności sieciowej, jak i kampaniach phishingowych.

Agencja prowadzi bieżącą i bezpośrednią współpracę z CSIRT MON i CSIRT NASK oraz sektorowymi zespołami cyberbezpieczeństwa w zakresie przeciwdziałania zagrożeniom w cyberprzestrzeni RP, w szczególności dotyczącej sposobów obsługi incydentów, wymiany informacji technicznych i systemowych, w tym w ramach Projektu Połączonego Centrum Operacyjnego Cyberbezpieczeństwa. Agencja współpracuje także z CSIRT MON oraz CSIRT NASK przy identyfikacji i reagowaniu na incydenty krytyczne, w tym mogące mieć wpływ na usługi kluczowe, usługi cyfrowe oraz infrastrukturę krytyczną, a także wspiera podmioty dotknięte incydentem oraz ostrzega podmioty zagrożone jego wystąpieniem. W ubiegłym roku realizowano także kooperację z innymi podmiotami krajowego systemu cyberbezpieczeńswa oraz międzynarodowymi instytucjami odpowiedzialnymi za cyberbezpieczeństwo w zakresie wymiany informacji o zagrożeniach, podatnościach systemów, a także incydentach noszących znamiona działań przestępczych.

ABW wykorzystywała System S46 do rejestrowania i obsługi incydentów teleinformatycznych w zakresie cyberbezpieczeństwa z operatorami infrastruktury krytycznej oraz operatorami usług kluczowych oraz wydawania ostrzeżeń o zidentyfikowanych zagrożeniach dla systemów i sieci teleinformatycznych.

W minionym roku ABW realizowała współpracę z NASK w zakresie przygotowania mobilnego systemu komunikacji niejawnej o nazwie SKR-Z, historycznie rozpatrywanego również jako element Systemu Kierowania Bezpieczeństwem Narodowym, który w swojej architekturze i funkcjonalności bazuje na rozwiązaniu opracowanym przez ABW pk. CATEL (zarówno w obszarze budowy, jak i akredytacji).

W 2023 r. kontynuowano wykorzystanie instrumentów prawnych, wprowadzonych ustawą o działaniach antyterrorystycznych, w tym w szczególności stopni alarmowych CRP.

ABW zgodnie ze swoją właściwością brała czynny udział (opracowywano zarówno stanowiska Szefa ABW, jak również uczestniczono w posiedzeniach komisji sejmowych) w pracach legislacyjnych dotyczących ustawy z dnia 17 sierpnia 2023 r. o zmianie ustawy – Kodeks karny oraz niektórych innych ustaw, która wprowadziła nową definicję przestępstwa szpiegostwa oraz jej kwalifikowane postaci, w tym związanej z prowadzeniem dezinformacji w ramach działalności wywiadowczej. Dodatkowo przedmiotowa ustawa rozszerzyła uprawnienia teleinformatyczne funkcjonariuszy ABW na kwestie związane z podejrzeniem popełnienia przestępstwa szpiegostwa – art. 32a, art. 32aa, art. 32b i art. 32c.

Z inicjatywy ABW, w ramach ww. nowelizacji, do Kodeksu karnego został dodany przepis art. 112a mający na celu eliminację ewentualnych wątpliwości dotyczących tego, które przepisy karne mają być stosowane w przypadku popełnienia przestępstwa popełnionego w cyberprzestrzeni. Zgodnie z nową regulacją polska ustawa karna ma być stosowana wobec obywatela polskiego oraz cudzoziemca w razie popełnienia przestępstwa przy użyciu systemu informatycznego, systemu teleinformatycznego lub sieci teleinformatycznej, jeżeli czyn ten na terytorium Rzeczypospolitej Polskiej wywołał lub mógł wywołać skutek naruszający interes państwa w zakresie ochrony niepodległości, integralności terytorialnej, bezpieczeństwa

zewnętrznego i wewnętrznego, obronności, polityki zagranicznej, pozycji międzynarodowej lub potencjału naukowego lub gospodarczego.

Aktywność ABW obejmowała także podnoszenie poziomu świadomości i wiedzy na temat cyberzagrożeń poprzez wydawanie rekomendacji dotyczących stosowania dobrych praktyk w zakresie zabezpieczania i bezpiecznego użytkowania środowiska teleinformatycznego.

Agencja brała udział (na wniosek zainteresowanych podmiotów administracji publicznej) w opiniowaniu wykorzystywanych oraz potencjalnie wykorzystywanych narzędzi, produktów i usług IT w zakresie ich dostawy, eksploatacji oraz utrzymania.

ABW wykonywała oceny bezpieczeństwa systemów teleinformatycznych istotnych z punktu widzenia ciągłości funkcjonowania państwa na podstawie art. 32a ust. 1 ustawy o Agencji Bezpieczeństwa Wewnętrznego oraz Agencji Wywiadu. W 2023 r. Zespół CSIRT GOV przeprowadził 15 procedur oceny bezpieczeństwa systemów IT w instytucjach administracji rządowej oraz infrastruktury krytycznej.

Aktywność ABW obejmowała realizację własnych prac badawczo-rozwojowych, związanych z przygotowaniem nowych rozwiązań technologicznych ukierunkowanych na podniesienie poziomu cyberbezpieczeństwa kluczowych zasobów RP.

ABW prowadziła także szkolenia dla osób sprawujących funkcje publiczne, podmiotów administracji rządowej, operatorów usług kluczowych i operatorów infrastruktury krytycznej, dotyczących zagrożeń w cyberprzestrzeni oraz ukierunkowanych na podnoszenie kwalifikacji i kompetencji w zakresie cyberbezpieczeństwa. ABW dystrybuowała również zalecenia i rekomendacje zmierzające do wzrostu świadomości w zakresie bezpieczeństwa teleinformatycznego dla organów władzy publicznej.

Na arenie międzynarodowej Agencja brała udział w forach wymiany informacji o cyberzagrożeniach, np. CSIRTs Network, MISP NATO.

1.2.3 CSIRT MON

C:[SIRT/MON]

CSIRT Ministerstwa Obrony Narodowej

Zgłoszenia i incydenty

W 2023 r. CSIRT MON:

- zarejestrował 5841 incydenty;
- nie zarejestrował żadnego incydentu sklasyfikowanego jako krytyczny;
- nie zarejestrował żadnego zgłoszenia od operatora usługi kluczowej dot. incydentu poważnego;
- nie zarejestrował żadnego zgłoszenia od dostawcy usługi cyfrowej dot. incydentu istotnego;
- zarejestrował 81 incydentów dotyczących wojskowych uczelni publicznych.

Opis najważniejszych incydentów

W 2023 r. odnotowano próby ataków na infrastrukturę resortu obrony narodowej (ron). Ataki te miały na celu uzyskanie dostępu do infrastruktury, kradzież istotnych danych, w szczególności dotyczących dostaw sprzętu wojskowego dla Ukrainy. W większości były to ataki typu phishing na konta poczty elektronicznej (służbowe i prywatne) personelu ron. Próby zdobycia danych uwierzytelniających do dostępu do infrastruktury wojskowej prowadzone były również za pomocą kampanii rozpowszechniającej oprogramowanie złośliwe typu stealer, które wykrada te dane z przeglądarek internetowych. Obserwowane są również, prowadzone z dużą regularnością, próby uzyskania dostępu do kont w usługach chmurowych personelu ron za pomocą ataków typu brute-force i password-spraying.

Odnotowano ataki DDoS mające na celu zakłócenie ciągłości świadczenia usług sieciowych organizowanych przez DKWOC.

Odnotowano ataki na uczelnie wojskowe i inne podmioty związane z procesem kształcenia w Siłach Zbrojnych. Adwersarze poprzez wykorzystanie wiadomości phishingowych jako wektorów inicjujących prowadzili ataki z wykorzystaniem taktyk zmierzających do eskalacji uprawnień, uzyskania persystencji, użycia kanałów C&C, aż do prób osiągnięcia zamierzonego wpływu w infrastrukturze ofiary.

Celem ataków były również przedsiębiorstwa branży zbrojeniowej.

Informacje na temat grup dokonujących cyberataków wymierzonych w Polskę

Zasadnicza aktywność w cyberprzestrzeni w 2023 r., podobnie jak w 2022 r., została zdeterminowana działaniami zbrojnymi w Ukrainie, wsparciem przez kraje zachodnie społeczeństwa ukraińskiego, jak i bezpośrednio struktur biorących udział w walce i obronie Ukrainy.

- Aktywność grup powiązanych z Federacją Rosyjską obserwowane w 2023 r.

W 2023 r. DKWOC zidentyfikowało aktywności przeciwko systemom ron, za które odpowiedzialność przypisuje się grupom aktywności o charakterze APT powiązanym z Federacją Rosyjską, Republiką Białorusi oraz Chińską Republiką Ludową. Największą aktywnością wykazały się grupy powiązane ze Służbą Wywiadu Wojskowego Federacji Rosyjskiej. CSIRT MON zaobserwował działania atrybuowane do grupy APT28 polegające na: skanowaniu infrastruktury ron, atakach brute-force oraz atakach phishingowych.

W ramach prowadzonej operacji analitycy CSIRT MON zaobserwowali wykorzystywanie techniki polegającej na modyfikacji uprawnień do folderów skrzynki pocztowej w ramach serwerów Microsoft Exchange pozwalającej na skryty i nieuprawniony dostęp do korespondencji pocztowej. W wyniku przeprowadzonych analiz stwierdzono wykorzystanie tej techniki przeciwko wielu podmiotom publicznym i prywatnym w Polsce. Działania te pokrywają się również z aktywnością atrybuowaną do grupy APT28.

W zakresie działań prowadzonych przeciwko ron przez grupy powiązane z innymi służbami FR, zidentyfikowano aktywność grupy TURLA (FSB) polegającą na próbie uzyskiwania nieuprawnionego dostępu do usług poczty elektronicznej i usługi udostępniania plików oraz grupy APT29 (SVR) polegającą na kompromitacji konta M365 żołnierza WOT.

Ponadto CSIRT MON obserwuje stałą aktywność adwersarzy powiązanych z Federacją Rosyjską dot. zbierania informacji oraz zakłócania procesu dostaw do Ukrainy, przede wszystkim kompromitując podmioty logistyczne, zarówno w sektorze publicznym. jak i prywatnym. Zostało to potwierdzone w ramach operacji NŻ w cyberprzestrzeni prowadzonej przez DKWOC.

- Aktywność grup powiązanych z Republiką Białorusi w 2023 r.

W zakresie aktywności grup APT powiązanych z Republiką Białorusi (RB) przeciwko systemom teleinformatycznym ron, CSIRT MON zidentyfikował aktywność grupy UNC1151 oraz WinterVivern.

W przypadku grupy UNC1151 CSIRT MON zaobserwował trzy główne aktywności w cyberprzestrzeni przeciwko ron:

- Próby dostarczenia złośliwego oprogramowania BADPICK;
- Kampania dezinformacyjna - Rekrutacja do LITPOLUKRBRIG;
- Kampania dezinformacyjna – Wybory Parlamentarne 2023;

W zakresie aktywności grupy WinterVivern w końcówce stycznia 2023 roku CSIRT MON zidentyfikowało kampanię phishingową, w której celem było 116 użytkowników w domenie mon.gov.pl.

- Aktywność grup powiązanych z Chińską Republiką Ludową obserwowana w 2023 r.

Jedyną aktywnością obserwowaną w ubiegłym roku przez CSIRT MON było podszycie się pod aplikacje Signal, będącą dostępną w oficjalnych sklepach z aplikacjami.

- Aktywność grup haktywistycznych w 2023 r.

Do grup, które byłe najbardziej aktywne w działaniach wymierzonych w podmioty w Polsce zalicza się:

- grupę NoName057(16) odpowiedzialną za przeprowadzenie ataków typu DDoS przeciwko podmiotom prywatnym i publicznym w Ukrainie oraz krajach wspierających Ukrainie w konflikcie zbrojnym, tym Polskę;
- grupę Killnet odpowiedzialną za upublicznienie danych z portalu NATO, w tym również danych żołnierzy oraz pracowników ron;
- grupę Solntsepek kojarzoną z atakiem na system nasłuchu radiowego w zakresie HF/VHF.

Zidentyfikowane najpoważniejsze zagrożenia

W 2023 roku znaczący wpływ na bezpieczeństwo systemów IT ron miały zagrożenia wynikające z działań grup APT. Aktywność tych grup kojarzona jest głównie z działalnością sponsorowaną lub wręcz pozostającą w strukturach niektórych państw. Spektrum działań grup APT obejmuje różnorodne czynności – od systematycznie realizowanego rozpoznania infrastruktury teleinformatycznej, poprzez cyberszpiegostwo, zakłócanie działania systemów IT i sieci, aż po niszczenie danych, które się w nich znajdują. Do najpoważniejszych zagrożeń ze strony grup APT można zaliczyć:

- ataki spear-phishingowe mające na celu wykradanie poświadczeń logowania lub infekcji urządzenia złośliwym oprogramowaniem;
- skompromitowanie komercyjnych dostawców usług i rozwiązań IT;
- wykorzystywanie przez grupy APT podatności typu zero-day;
- ataki typu brute-force w celu uzyskania dostępu do zasobów sieciowych i skrzynek pocztowych.

W licznych atakach grupy APT wykorzystywały skompromitowane prywatne urządzenia sieciowe (m.in. zlokalizowane w Polsce) oraz posługiwały się infrastrukturą animizującą typu VPN/proxy w celu ukrycia złośliwej aktywności.

Wybrane działania realizowane przez DKWOC:

- Prowadzono bieżącą analizę podatności oraz zagrożeń w nadzorowanych systemach informatycznych poprzez cykliczne skanowania podatnościowe.
- Monitorowano stan bezpieczeństwa zasobów, usług i aplikacji podłączonych do Internetu w ramach ron oraz PN i współpracujących (EASM).
- Informowano o nowo publikowanych podatnościach sprzętu oraz oprogramowania użytkowanego w RON oraz PN i współpracujących poprzez przygotowanie

i dystrybucję biuletynów CSIRT MON, ostrzeżeń o priorytetowych podatnościach i raportów dotyczących zidentyfikowanych podatności.

- Opracowano: „Plan zapewnienia cyberbezpieczeństwa sc ron" – celem dokumentu jest ukierunkowanie wysiłku komórek oraz jednostek organizacyjnych ron w celu zapewnienia akceptowalnego poziomu cyberbezpieczeństwa w obszarze właściwym Ministrowi Obrony Narodowej.
- Opracowano „Wytyczne do opracowania lokalnych planów reagowania na incydenty" – celem dokumentu jest ujednolicenie w ramach systemu cyberbezpieczeństwa ron sposobu przygotowywania „Lokalnych Planów reagowania na incydenty komputerowe" dotyczących zasad postępowania w obszarze reagowania na incydenty komputerowe w systemach teleinformatycznych lub rozwiązaniach informatycznych.
- Wdrożono i zapewniono ciągłość funkcjonowania i rozwoju dedykowanego systemu teleinformatycznego wraz z systemami informatycznymi budowanymi na potrzeby wykrywania, rozpoznania i zwalczania zagrożeń cyberbezpieczeństwa.
- Rozpoczęto pracę wsparcia i automatyzacji procesu obsługi incydentów oraz PWC (Proaktywnego Wykrywania Cyberzagrożeń).
- Ukompletowano wyposażenie indywidualne przewidziane dla Zespołów Zadaniowych oraz personelu CSIRT MON zabezpieczające pracę w ramach Proaktywnego Wykrywania Cyberzagrożeń oraz wsparcia w obsłudze incydentów,
- Pozyskano pojazdy specjalistyczne dedykowane do realizowania zadań poza miejscem stałej dyslokacji (MSD) na potrzeby Zespołów Zadaniowych CSIRT MON, wraz z niezbędnym wyposażeniem.
- Rozwijano współpracę między sektorem publicznym i prywatnym poprzez realizację:
  - uczestnictwa w spotkaniach technicznych z udziałem przedstawicieli przemysłu i sektora publicznego na arenie krajowej i międzynarodowej,
  - uczestnictwa w realizacji badań naukowych w obszarze cyberbezpieczeństwa na poziomie krajowym oraz międzynarodowym,
  - współpracy w zakresie podniesienia poziomu cyberbezpieczeństwa RP na podstawie podpisanych porozumień o współpracy.
- Rozpoczęto proces budowy zdolności do prowadzenia rozpoznania w cyberprzestrzeni lub z wykorzystaniem elementów cyberprzestrzeni potencjalnych przeciwników.
- Przygotowywano zalecenia dla użytkowników systemów ron w ramach realizacji zadań wynikających z ustawy o krajowym systemie cyberbezpieczeństwa.
- W zakresie współpracy w ramach UE uczestniczono w nw. projektach:
  - PESCO – Cyber Rapid Response Teams (CRRTs),
  - PESCO – Cyber and Information Domain Coordination Center (CIDCC),
  - PESCO – Cyber Academia and Innovation Hub (EU CAIH),
  - PESCO – Mutual Assistance in Cyber Security.
- Kontynuowano współpracę:
  - z NATO Cyber Operations Centre (CyOC) w zakresie wymiany informacji o zagrożeniach i incydentach w cyberprzestrzeni,

  - rozwijano funkcjonowanie Narodowego Punktu Kontaktowego do współpracy z Organizacją Traktatu Północnoatlantyckiego.

- Prowadzono analizę doświadczeń z trwających konfliktów zbrojnych pod kątem bezpiecznego korzystania z infrastruktury teleinformatycznej.
- Prowadzono bieżącą analizę podatności oraz zagrożeń w nadzorowanych systemach informatycznych. Wdrażano środki zaradcze mitygujące zagrożenia i podatności.
- Prowadzono integrację systemów i usług użytkowych z systemami bezpieczeństwa (klasy SIEM, analizy i korelacji logów, oceny podatności).
- Prowadzono prace mające na celu zwiększenie cyberbepieczeństwa usług poprzez udział w międzynarodowych (w ramach NATO) grupach roboczych w ramach partnerstwa AirC2 oraz NST C&IP.
- Opracowano oraz wdrożono przez DKWOC mobilną stację roboczą MocVPN do zapewnienia zdalnego dostępu kadry kierowniczej ron do systemu MILNET-Z.
- Opracowano przez DKWOC rodzinę algorytmów kryptograficznych do ochrony danych o klauzuli TAJNE na potrzeby narodowych urządzeń oraz narzędzi kryptograficznych.
- Przeprowadzono 42 testy bezpieczeństwa systemów teleinformatycznych wprowadzanych do użytku lub eksploatowanych w Siłach Zbrojnych RP .
- Zrealizowano ćwiczenia Purple Team (4 edycje w 2023 r.) jako aktywne testowanie systemów bezpieczeństwa IT ron w wybranych aspektach, weryfikacja procedur reagowania CN CSIRT MON na incydenty komputerowe oraz sposobów przeciwdziałania atakom na ST ron.
- Wdrożono i zapewniono ciągłość funkcjonowania i rozwoju dedykowanego systemu teleinformatczynego ST RYŚ wraz z systemami informatycznymi budowanymi na potrzeby wykrywania, rozpoznania i zwalczania zagrożeń cyberbezpieczeństwa.
- Realizowano prace nad dokumentami standaryzacji operacyjnej: Regulamin działań Wojsk Obrony Cyberprzestrzeni DU-3.20.2.
- Opracowano i administrowano szkolenia e-learningowe z zakresu cyberbezpieczeństwa, które poruszają kwestie: cyberhigieny, dobrych praktyk, metod wykrywania zagrożeń, sposobów utwardzania urządzeń.
- Prowadzono szkolenia on-site dla kadry i pracowników ron w najważniejszych obszarach funkcjonowania Sił Zbrojnych RP m.in. dla: departamentów MON, Centrum Operacyjnego MON, Komendy Głównej Żandarmerii Wojskowej.
- Budowano i rozwijano kompetencje żołnierzy zawodowych i pracowników ron poprzez uzupełnianie, rozszerzanie, pogłębianie i aktualizowanie wiedzy oraz podniesienie umiejętności praktycznych z zakresu cyberbezpieczeństwa w ramach kursów i szkoleń specjalistycznych.

W ramach Sił Zbrojnych RP działania w zakresie cyberbezpieczeństwa realizowało także Dowództwo Wojsk Obrony Terytorialnej, w skład których wchodzi Zespół Działań Cyberprzestrzennych. Wśród działań tych można wskazać m.in. obsługę incydentów w WOT we współpracy z CSIRT MON, szkolenia z zakresu cyberbezpieczeństwa we wszystkich Brygadach Obrony Terytorialnej, czy współpracę z Estonian Defence League's Cyber Unit.

Wnioski i rekomendacje DKWOC

Zgodnie ze zobowiązaniami sojuszniczymi w ramach Sojuszu Północnoatlantyckiego, związanymi z budowaniem odporności państw członkowskich, gotowość cywilna opiera się między innymi na zapewnianiu ciągłości sprawowania rządów i krytycznych usług rządowych. Pomimo że zakres tego zagadnienia jest bardzo rozległy, to jednak należy mieć na uwadze również budowanie zdolności struktur państwowych do komunikowania się, czyli zapewnienia łączności. Aspekt ten jest związany z koniecznością utrzymania ciągłości podejmowania decyzji. Rekomendowane jest sprawdzenie stanu rozwiązań związanych z utrzymaniem łączności na wypadek kryzysu i wojny, ale również wypracowanie alternatywnych sposobów na wypadek odcięcia od sygnału GSM lub sieci internetowej. Mając na uwadze doświadczenia płynące z rosyjskiej inwazji na Ukrainę konieczne jest zapewnienie kanałów komunikacji kryzysowej z obywatelami. NATO w ramach przygotowania społeczeństwa na funkcjonowanie w czasie kryzysów wskazuje na konieczność przygotowania systemów komunikacji cywilnej odpornych na zakłócenia mogące wystąpić w wypadku działań stricte militarnych lub niemilitarnych. Sojusz Północnoatlantycki wskazuje na wypracowanie zdolności państwa do zapewnienia funkcjonowania sieci telekomunikacyjnych i sieci Internet nawet w warunkach kryzysowych, z wystarczającymi zdolnościami rezerwowymi. Niezwykle ważne w tym aspekcie jest rozwijanie potencjału satelitarnego Polski rozpoczętego przez MON.

Dotychczasowe doświadczenia międzynarodowe wskazują na możliwość czasowego unicestwienia kluczowych elementów infrastruktury energetycznej (Ukraina), bankowej (Estonia), zakłócenie dostaw surowców strategicznych (USA), działalności przedstawicieli polityki (Polska) czy ingerowania w procesy wyborcze (USA). W Polsce wykryto dotychczas m.in. lukę związaną z możliwością ataku na lokalne serwisy gminne, które z kolei były wykorzystywane do prowadzenia działań dezinformacyjnych. Cyberbezpieczeństwo infrastruktury krytycznej związane jest z koniecznością przygotowania systemów infrastruktury krytycznej oraz innej istotnej infrastruktury z punktu widzenia bezpieczeństwa i obronności kraju, w tym również na kryzysy wywołane poprzez cyberataki. Rekomendowane jest dokonanie audytu stanu zabezpieczeń elementów infrastruktury krytycznej, również pod względem wykorzystania technologii z krajów uznanych za kraje podwyższonego ryzyka wywiadowczego. Równie newralgicznym obszarem co służby, czy elementy infrastruktury krytycznej, mogą okazać się elementy i przedsiębiorstwa odpowiedzialne za zasilanie sił zbrojnych w dostawy, za produkcję broni i amunicji oraz remonty. Równie ważnym obszarem będą te systemy, których naruszenie może spowodować kryzys zdrowotny lub podważyć zaufanie do procesów demokratycznych, np. systemów stosowanych w ochronie zdrowia czy do przeprowadzenia procesu wyborczego. Rekomenduje się przeprowadzenie audytu stanu zabezpieczenia:

- systemów odpowiedzialnych za transport lotniczy, kolejowy, morski - audyt ma na celu wykrycie luk w celu wprowadzenia planu naprawczego;
- elementów infrastruktury krytycznej;
- systemów wykorzystywanych przez służby;
- systemów odpowiedzialnych za transport surowców strategicznych;
- systemów uzdatniania wody;
- systemów wykorzystywanych przez podmioty odpowiedzialne za dostawy do wojska,
- systemów wykorzystywanych do przeprowadzenia procesu wyborczego.

Dotychczasowe doświadczenie w zakresie wrogich działań informacyjnych pokazuje konieczność przygotowania instytucji kluczowych dla funkcjonowania państwa, w tym również tych, w których uderzenie może naruszyć dobre imię lub prestiż państwa. Konieczne jest stałe

dbanie o struktury odpowiedzialne za pomoc we wczesnym wykrywaniu zagrożeń oraz w odpieraniu cyberataków, a w razie niepowodzenia do minimalizacji skutków oraz szybkiego przywrócenia zdolności do normalnego funkcjonowania systemów, które zostaną naruszone w celu zademonstrowania potencjału przeciwnika. Dużym wyzwaniem jest pomoc podmiotom medialnym, w szczególności lokalnym serwisom, które wykorzystywane są często poprzez włamania do systemów publikowania do rozpowszechniania niesprawdzonych informacji przez rosyjskie ośrodki dezinformacyjne. Z problemami spotykają się również organy samorządowe, których serwisy internetowe są słabo chronione.

Rekomendacje:

- przeprowadzenie audytu stanu funkcjonowania 3 funkcjonujących obecnie CSIRT-ów, sprawdzenie poprawności ulokowania kompetencji oraz ewentualnych luk (np. pomoc prywatnym przedsiębiorcom, mediom i samorządom);
- wprowadzenie jednolitej platformy komunikacji rządowej i samorządowej (rozszerzenie gov.pl na wszystkie samorządy - obligatoryjnie).

Kolejnym kluczowym obszarem związanym z bezpieczeństwem kontrwywiadowczym oraz rozwojem gospodarczym jest wypracowanie systemowych rozwiązań związanych z bezpieczeństwem sieci 5G i kolejnych generacji. Obecnie dominującą technologią, która przysparza problemów nie tylko w wymiarze krajowym, ale i globalnym jest technologia 5G oraz produkcja półprzewodników. Technologia 5G, której wdrożenie jest niezbędne do rozwoju gospodarczego jest obecnie blokowana poprzez wątpliwości związane z bezpieczeństwem tworzenia tego typu infrastruktury. Obecnie Unia Europejska nie posiada zdolności do skutecznego zastąpienia technologii proponowanej przez niewątpliwego lidera w tym zakresie – chińskiego dostawcę Huawei.

Rekomendacje:

- prowadzenie stałego lobbingu na rzecz podnoszenia zdolności Unii Europejskiej do produkcji zarówno półprzewodników, jak i rozwijania zdolności firm europejskich do produkcji elementów potrzebnych do budowy sieci 5G i kolejnych generacji;
- stopniowe odchodzenie od wykorzystywania technologii z państw budzących wątpliwości, co do stosowania zasad państwa demokratycznego.

Zespół Działań Cyberprzestrzennych WOT może stanowić jednostkę ściśle współpracującą z CSIRT MON lub innymi jednostkami w ramach KSC, zapewniając im odpowiednie siły i środki w postaci Operatorów/Analityków SOC oraz Audytorów posiadających odpowiednie kompetencje, wyszkolenie, doświadczenie oraz certyfikaty zgodne z wymogami KSC. Analitycy/Operatorzy SOC z ramienia ZDC mogliby wspierać CSIRT-y w zapewnieniu monitoringu cyberbezpieczeństwa w ramach KSC oraz współdziałać z operatorami usług kluczowych lub JST w zakresie dostosowania do standardów KSC i zapewnienia wsparcia w temacie szkoleń i budowania usług cyberbezpieczeństwa. Audytorzy z ramienia ZDC mogliby przeprowadzać audyty u operatorów usług kluczowych oraz w JST w ramach dostosowania i spełnienia norm do KSC (posiadają odpowiednie kompetencje i doświadczenie) oraz ocenę zdolności i dojrzałości operatorów usług kluczowych. Propozycja wymagałaby dokonania zmian w przepisach KSC, które regulowałyby miejsce, rolę, zakres i uprawnienia ZDC w ramach CSIRT MON.

UKSC może być istotnym narzędziem wsparcia dla Security Operation Center, zapewniając ramy prawne, standardy bezpieczeństwa oraz promując współpracę między różnymi instytucjami. Jednak konieczne jest zachowanie elastyczności, ciągła aktualizacja przepisów oraz dbałość o równowagę pomiędzy bezpieczeństwem a efektywnością działań SOC.

Rekomendacje:

- Edukacja i świadomość: rząd powinien kontynuować działania edukacyjne i promować świadomość społeczną na temat cyberbezpieczeństwa, wspierając w ten sposób działania SOC.
- Konsultacje z sektorem prywatnym: istotne jest prowadzenie konsultacji z sektorem prywatnym, w tym z przedstawicielami SOC, podczas tworzenia i aktualizacji przepisów, aby uwzględnić ich potrzeby i wyzwania.
- Zachowanie elastyczności: przepisy ustawy powinny być elastyczne, umożliwiając SOC dostosowanie się do zmieniających się warunków operacyjnych i technologicznych.
- Wsparcie finansowe: rząd powinien zapewnić odpowiednie wsparcie finansowe dla SOC, zwłaszcza dla mniejszych organizacji, aby umożliwić im efektywne wdrażanie wymagań ustawy.
- Monitoring i ocena skuteczności: istotne jest prowadzenie systematycznego monitorowania oraz oceny skuteczności działań SOC w celu zapewnienia ciągłego doskonalenia i dostosowywania się do zmieniających się zagrożeń.
- Kształcenie personelu: istotne jest kształcenie personelu SOC w zakresie zgodności z przepisami ustawy oraz w praktycznym wykorzystaniu standardów bezpieczeństwa.
- Ochrona danych i poufność: zapewnienie środków ostrożności w zakresie ochrony danych i zachowania poufności informacji, szczególnie podczas współpracy zewnętrznej.
- Stałe doskonalenie: konieczne jest stałe doskonalenie procedur i technologii w SOC, wraz z regularnymi ćwiczeniami i szkoleniami personelu.
- Współpraca i wymiana informacji: zachęcanie do aktywnej współpracy i wymiany informacji między różnymi SOC oraz instytucjami rządowymi i prywatnymi.

Państwo, w tym Siły Zbrojne RP, powinny posiadać zdolność do zapewnienia dostępu do krytycznych systemów teleinformatycznych w ramach kraju i poza granicami państwa (w szczególności centrów bazodanowych). Dlatego też należy rozważyć możliwość wykorzystania rozwiązań chmury publicznej/prywatnej/hybrydowej. Zdaniem DKWOC kluczowe elementy wojskowej sieci teleinformatycznej powinny być rozpraszane, decentralizowane i utwardzane (lepiej zabezpieczane) celem zapewnienia odporności i nadmiarowości (rezerwy natychmiastowego użycia).

Rekomendacje:

- Budowanie świadomości sytuacyjnej w cyberprzestrzeni – spektrum informacji z wielu źródeł, wymiana informacji na poziomie krajowym i międzynarodowym, z sojusznikami, koalicjantami, partnerami, środowiskiem naukowo-badawczym i przemysłem ma kluczowe znaczenie dla utrzymania cyberbezpieczeństwa.
- Ochrona ST ron oraz obrona przed atakami w cyberprzestrzeni wymaga działań proaktywnych (wyprzedzających) w zakresie rozpoznania cyberzagrożeń i właściwego zabezpieczenia urządzeń końcowych na podstawie pozyskanych informacji o adwersarzu, potencjalnych podatnościach i wektorach ataku. Zasadne jest zatem wdrażanie koncepcji defence forward, threat hunting.
- Zasadnicze znaczenie ma również budowanie zdolności ofensywnych do działań w cyberprzestrzeni, celem stworzenia asymetrii w środowisku operacyjnym, jak również zapewnienie zdolności do odstraszania.

- Potrzeba adaptacji potencjału zespołów przeznaczonych do obsługi incydentów komputerowych do warunków panujących w cyberprzestrzeni poprzez stosowną aktualizację narzędzi już wykorzystywanych w procesie monitorowania, a także systematyczne budowanie świadomości personelu na temat wyzwań wynikających z dynamicznie zmieniającej się sytuacji w cyberprzestrzeni.
- Celem osiągnięcia zdolności do rozpoznania, odstraszania, aktywnej odpowiedzi, mając świadomość o intensywności prowadzonych działań w cyberprzestrzeni, zasadne jest przygotowanie odpowiednich struktur organizacyjnych (rozbudowa istniejących struktur) przewidzianych do realizacji tych zadań i wyposażonych w odpowiednie narzędzia i rozwiązania, nie tylko komercyjne, ale również wytworzone przez DKWOC. Zasadne jest zatem budowanie tych zdolności w DKWOC, które jest odpowiedzialne za realizację pełnego spektrum operacji w cyberprzestrzeni, które zgodnie art. 15 ust. 4 pkt. 2 ustawy z dnia 11 marca 2022 r. o obronie Ojczyzny. Wojska Obrony Cyberprzestrzeni, jako specjalistyczny komponent Sił Zbrojnych RP są właściwe do realizacji pełnego spektrum działań w cyberprzestrzeni, w szczególności w zakresie proaktywnej ochrony oraz aktywnej obrony elementów i zasobów cyberprzestrzeni kluczowych z punktu widzenia Sił Zbrojnych RP.
- Zintensyfikowanie w ron szkolenia z zakresu cyberbezpieczeństwa. Należy podjąć działania mające na celu praktyczną weryfikację zdobytej wiedzy np. poprzez realizację Red i Purple Teamingu.
- Efektywne podnoszenie wiedzy oraz umiejętności personelu zaangażowanego w realizację działań z obszaru obsługi incydentów oraz monitorowania stanu sieci i systemów.
- Dokonanie stosownych zmian legislacyjnych i nadanie Dowódcy KWOC uprawnień do samodzielnego podejmowania decyzji w zakresie neutralizacji zagrożeń w cyberprzestrzeni dla ron.
- Monitorowanie światowych trendów i implementacja nowych rozwiązań z obszaru cyberbezpieczeństwa w ron.

Ponadto w związku ze skokowym wzrostem aktywności grup APT i społeczności haktywistycznych w 2023 r., w stosunku do roku 2022., celem wzmocnienia bezpieczeństwa systemów IT, jak i skuteczności w dziedzinie identyfikowania aktywności APT, społeczności haktywistycznych, należy konsekwentnie dążyć do rozwijania i wzmacniania zdolności w obszarach:

- rozpoznania, identyfikacji i analiz cyberzagrożeń;
- właściwego zarządzania i wdrażania aktualizacji bezpieczeństwa, celem doprowadzenia do znacznego zredukowania możliwości ugrupowań APT w zakresie prowadzenia aktywności wymierzonej w systemy IT ron;
- wdrożenia efektywnych środków kontroli bezpieczeństwa sieci oraz efektywnego zarządzania uprawnieniami użytkowników, celem zapobiegania ewentualnemu poruszaniu się przeciwnika między hostami systemów IT ron;
- stałego kontrolowania i zarządzania procesami bezpiecznego logowania (zarówno w przestrzeniach lokalnych, jak i chmurowych) oraz utrzymywania właściwych polityk zarządzania zawartością wiadomości e-mail;
- ciągłego szkolenia personelu i zwracania uwagi na tak zwaną „cyberhigienę”;
- zapewniania, że informacje dotyczące architektury sieci oraz bezpieczeństwa sieci są właściwie zabezpieczone.

Planowane działania CSIRT MON w 2024 r.

- Wprowadzanie uregulowań prawnych niezbędnych z punktu widzenia uprawnień WOC do działań aktywnych w cyberprzestrzeni.
- Przygotowanie specjalistyczne WOC do działań w cyberprzestrzeni.
- Opracowanie strategii cyberbezpieczeństwa ron obejmującej systemy teleinformatyczne, systemy uzbrojenia, systemy automatyki, systemy teletechniczne oraz systemy zewnętrzne kluczowe dla Sił Zbrojnych RP, a następnie opracowanie polityk i wytycznych pozwalających implementować strategię.
- Wdrożenie procesu ciągłego zarządzania ryzykiem w cyberprzestrzeni oraz oceny wpływu tego ryzyka na realizację działań i operacji Sił Zbrojnych RP (mission assurance) oraz procesów prowadzonych w MON.
- Opracowanie architektury systemów łączności i informatyki Sił Zbrojnych RP, z uwzględnieniem w szczególności wniosków płynących z wojny w Ukrainie.
- Wdrożenie strategii integracji systemów łączności i informatyki.
- Działania na rzecz wprowadzenia uregulowań prawnych umożliwiających przetwarzanie informacji wrażliwych lub niejawnych z wykorzystaniem rozwiązań chmurowych.
- Wprowadzanie elementów sztucznej inteligencji do nowo opracowywanych rozwiązań informatycznych dla Sił Zbrojnych RP.
- Utrzymanie motywatorów umożliwiających posiadanie przez WOC wysoce specjalistycznego personelu niezbędnego do realizacji zadań w zakresie działań w cyberprzestrzeni.
- Analiza możliwości budowy zdolności do działań w środowisku elektromagnetycznym.
- Redukcja zagrożenia odpływu personelu o wysokich kompetencjach specjalistycznych do sfery cywilnej.
- Stworzenie warunków do rozwoju zdolności WOC w kierunku prowadzenia działań w domenie kognitywnej, w tym wykrywania i przeciwdziałania dezinformacji.

1.3 Organy właściwe do spraw cyberbezpieczeństwa i sektorowe zespoły cyberbezpieczeństwa

Organy właściwe i ich zadania zdefiniowane są w art. 41 UKSC. Przepisy te przewidują istnienie następujących sektorów i odpowiedzialnych za nich organów:

1) **sektor energii** – minister właściwy do spraw energii (Minister Klimatu i Środowiska);
2) **sektor transportu z wyłączeniem podsektora transportu wodnego** – minister właściwy do spraw transportu (Minister Infrastruktury);
3) **podsektor transportu wodnego** – minister właściwy do spraw gospodarki morskiej i minister właściwy do spraw żeglugi śródlądowej (Minister Infrastruktury);
4) **sektor bankowy i infrastruktury rynków finansowych** – Komisja Nadzoru Finansowego;
5) **sektor ochrony zdrowia (z wyłączeniem podmiotów podległych MON)** – minister właściwy do spraw zdrowia (Minister Zdrowia);
6) **sektor ochrony zdrowia obejmujący podmioty podległe MON** - Minister Obrony Narodowej;
7) **sektor zaopatrzenia w wodę pitną i jej dystrybucji** – minister właściwy do spraw gospodarki wodnej (Minister Infrastruktury);
8) **sektor infrastruktury cyfrowej (z wyłączeniem podmiotów podległych MON)** – minister właściwy do spraw informatyzacji (Minister Cyfryzacji);
9) **sektor infrastruktury cyfrowej obejmujący podmioty podległe MON** - Minister Obrony Narodowej;
10) **dostawcy usług cyfrowych (z wyłączeniem podmiotów podległych MON)** - minister właściwy do spraw informatyzacji (Minister Cyfryzacji);
11) **dostawcy usług cyfrowych obejmujący podmioty podległe MON** - Minister Obrony Narodowej.

Ministerstwo
Klimatu i Środowiska

1.3.1 Sektor energii

Ministerstwo Klimatu i Środowiska realizowało zadania organu właściwego dla sektora energii. W sektorze energii podmioty uznane za operatorów usług kluczowych od momentu wejścia w życie UKSC podniosły swój poziom dojrzałości o czym świadczy m.in. mniejsza liczba niezgodności w sprawozdaniach z przeprowadzonych audytów, czy ogólna ocena poziomu dojrzałości, którą operatorzy usług kluczowych przeprowadzili na początku 2022 r.

Identyfikacja oraz prowadzenie postępowań administracyjnych wobec operatorów usług kluczowych z sektora energii

W 2023 r. organ właściwy ds. cyberbezpieczeństwa sektora energii prowadził bieżącą analizę podmiotów w danym sektorze lub podsektorze pod kątem uznania ich za operatora usługi kluczowej lub niespełniania warunków kwalifikujących podmiot jako operatora usługi kluczowej. Ponadto w 2023 r. Minister Klimatu i Środowiska wydał 5 decyzji o uznaniu podmiotu za operatora usługi kluczowej oraz 1 decyzję stwierdzającą wygaśnięcie decyzji o uznaniu podmiotu za operatora usługi kluczowej. Organ starał się również na bieżąco przekazywać wnioski do ministra właściwego do spraw informatyzacji o wpisanie do wykazu operatorów usług kluczowych albo wykreślenie z tego wykazu, a także wnioski o zmianę danych w wykazie operatorów usług kluczowych w związku z licznymi zmianami właścicielskimi.

Nadzór nad podmiotami krajowego systemu cyberbezpieczeństwa w sektorze energii

W latach 2022/23 r. miała miejsce kolejna tura audytu bezpieczeństwa systemów informacyjnych operatorów usług kluczowych w sektorze energia na gruncie przepisów UKSC. W związku z powyższym w 2023 roku prowadzony był szereg działań nadzorczych względem operatorów usług kluczowych, polegających m.in. na weryfikacji realizacji obowiązku przeprowadzania przez nich okresowych audytów bezpieczeństwa systemów informacyjnych służących do świadczenia usługi kluczowej, analizie sprawozdań z przeprowadzonych audytów pod kątem wykrytych niezgodności, terminowości ich przeprowadzenia czy weryfikacji obowiązku zgłaszania incydentów poważnych do odpowiednich jednostek (właściwego CSIRT).

W Ministerstwie Klimatu i Środowiska prowadzona jest elektroniczna tabela realizacji wymagań cyberbezpieczeństwa, służąca ocenie zarządzania cyberbezpieczeństwem przez operatorów usług kluczowych w sektorze energii. Narzędzie jest uzupełniane w oparciu o informacje ze sprawozdań z audytu bezpieczeństwa systemu informacyjnego, co pozwala prowadzić analizę prawdopodobieństwa naruszenia prawa oraz stanowi istotne narzędzie do oceny spółek w obszarze funkcjonowania cyberbezpieczeństwa. Poddane analizie dane audytowe spółek energetycznych wskazują na stopniowy wzrost na poziomie organizacji zdolności z zakresu cyberbezpieczeństwa, w sferze technicznej (logicznej), bezpieczeństwa fizycznego, a także w obszarze zasobów ludzkich. Na podstawie oszacowanego ryzyka wdrażane są zabezpieczania systemów informacyjnych automatyki przemysłowej pod kątem zagrożeń z zakresu cyberbezpieczeństwa, zapewniana jest ciągłość działania usług kluczowych, rozwijane są zdolności w zakresie reagowania na incydenty, a także ma miejsce rozbudowa struktur dedykowanych cyberbezpieczeństwu u operatorów usług kluczowych w sektorze energia.

W 2023 r. Minister Klimatu i Środowiska przeprowadził postępowanie administracyjne zakończone wydaniem decyzji o nałożeniu administracyjnej kary pieniężnej na jednego operatora usługi kluczowej z sektora energii, który naruszył przepisy UKSC zgłaszając incydent

poważny po terminie wskazanym w UKSC, czyli po upływie 24 godzin od momentu jego wykrycia.

Wśród innych czynności nadzorczych w 2023 r. znalazła się również weryfikacja realizacji Zaleceń Komisji (UE) 2019/553 z dnia 3 kwietnia 2019 r. w sprawie cyberbezpieczeństwa w sektorze energetycznym (notyfikowana jako dokument nr C(2019) 2400)1). Na tej podstawie sporządzone stosowne podsumowanie.

Zespół ds. monitorowania cyberbezpieczeństwa sektora energii

W 2023 r. Ministerstwo Klimatu i Środowiska kontynuowało spotkania Zespołu ds. monitorowania cyberbezpieczeństwa sektora energii. Zespół jest swoistym forum wymiany i analizy informacji pomiędzy operatorami usług kluczowych oraz pomiędzy operatorami a ministrem nadzorującym. W ramach Zespołu funkcjonują grupy zadaniowe, których głównym celem jest usprawnienie działania i rozwój krajowego systemu cyberbezpieczeństwa, poprzez wzmocnienie cyberbezpieczeństwa sektorowego oraz zbudowanie zaufania i mechanizmów współpracy pomiędzy jednostkami funkcjonującymi w sektorze. Efektami prac Zespołu są m.in. platforma MISP, czy tygodniowe biuletyny informacyjne Zespołu dotyczące m.in. certyfikacji produktów i bezpieczeństwa łańcucha dostaw. W czerwcu i listopadzie 2023 r. odbyły się stacjonarne spotkania członków Zespołu.

W 2023 r. przedstawiciele CSIRT-ów poziomu krajowego brali udział w spotkaniach Zespołu ds. monitorowania cyberbezpieczeństwa sektora energii, omawiając podczas nich m.in. aktualne zagrożenia cyberbezpieczeństwa dla tego sektora, czy funkcjonalności i sposób korzystania z narzędzi takich jak m.in. N6, MWDB, Artemis, bezpiecznapoczta +Snitch.

Zorganizowano także udział przedstawiciela Centralnego Biura Zwalczania Cyberprzestępczości w spotkaniu stacjonarnym Zespołu ds. monitorowania cyberbezpieczeństwa sektora energii, który przedstawił procedury zgłaszania przestępstw związanych z cyberbezpieczeństwem. Spotkanie miało również na celu omówienie możliwości uzyskania bezpośrednich kontaktów i szybkiej ścieżki komunikacji między spółkami z sektora energii a CBZC.

CSIRT sektora energii

Organ właściwy ds. cyberbezpieczeństwa sektora energii w 2023 r. kontynuował prace mające na celu opracowanie koncepcji utworzenia CSIRT sektorowego dla sektora energii. Będą one kontynuowane w 2024 r.

ISAC-Energia

Opracowano trzy koncepcje utworzenia ISAC w sektorze energia – ISAC-Energia. Dalsze prace będą kontynuowane we współpracy z operatorami usług kluczowych w 2024 roku.

Prowadzenie akcji podnoszących świadomość w obszarze cyberbezpieczeństwa sektora energia

W czerwcu 2023 r. został wydany dokument pt. „Rekomendacje dotyczące cyberbezpieczeństwa dla prosumentów OZE". Powstał on w efekcie prac prowadzonych przez przedstawicieli MKiŚ we współpracy z Ministerstwem Cyfryzacji, Polskimi Sieciami Elektroenergetycznymi S.A. oraz CERT Polska.

Udział w ćwiczeniach cyberbezpieczeństwa poziomu krajowego i międzynarodowego

W 2023 r. Ministerstwo Klimatu i Środowiska było zaangażowane w liczne ćwiczenia cyberbezpieczeństwa. Wśród najważniejszych należy wymienić udział przedstawicieli MKiŚ oraz przedstawicieli operatorów usług kluczowych z sektora energii w warsztatach cyberbezpieczeństwa „Energy Sector Cybersecurity Training Workshop" zorganizowanych w Polsce przez Departament Energii USA, Idaho National Laboratory oraz Ministerstwo

Cyfryzacji w styczniu 2023 r. Ponadto, MKiŚ brało czynny udział ćwiczeniach NATO CMX 2023 (Crisis Management Exercise). Należy również wspomnieć o udziale przedstawicieli MKiŚ w ćwiczeniach w formie testów warunków skrajnych dla operatorów infrastruktury krytycznej (tzw. „stress testy") AMBER 2023, polegających na ocenie sposobu działania spółek w sytuacjach kryzysowych.

Inne działania w sektorze energii

- Wsparcie Pełnomocnika Rządu ds. Bezpieczeństwa Przestrzeni Informacyjnej RP

Na prośbę Pełnomocnika Rządu ds. Bezpieczeństwa Przestrzeni Informacyjnej RP opracowano i przekazano wkład do raportu na temat powiązań gospodarczych i ich skali łączących państwo polskie z Chińską Republiką Ludową, uwzględniającego te obszary funkcjonowania państwa, które w sposób szczególny są uzależnione od powiązań z ChRL, a także zawierającego dane, analizy i rekomendacje w tym zakresie. MKiŚ w konsultacjach z operatorami usług kluczowych, dokonał analizy czy w ramach usług kluczowych spółki z sektora energii zaobserwowały zjawisko uzależnienia od produktów, usług lub kontrahentów pochodzących z Chin.

- Bezpieczeństwo rozwiązań chmurowych w OZE

Zorganizowano spotkanie z przedstawicielami wybranych operatorów usług kluczowych z sektora energii oraz pozostałymi zainteresowanymi organizacjami (m.in. CSIRT GOV). Spotkanie dotyczyło bezpieczeństwa wykorzystywania rozwiązań chmurowych w instalacjach odnawialnych źródeł energii.

- Certyfikacja cyberbezpieczeństwa w energetyce

Przedstawiciele MKiS uczestniczyli, wraz z przedstawicielami Urzędu Dozoru Technicznego, Polskich Elektrowni Jądrowych sp. z o.o. oraz Polskiej Agencji Atomistyki, w spotkaniu dotyczącym kwestii związanych z certyfikacją urządzeń w zakresie cyberbezpieczeństwa, co będzie musiało zostać w przyszłości uwzględnione przy projektowaniu i budowie elektrowni.

- Zalecenia Komisji Europejskiej ws. cyberbezpieczeństwa w sektorze energetycznym

Pod koniec listopada 2022 roku MKiŚ zwrócił się do operatorów usług kluczowych sektora energii z prośbą o uzupełnienie ankiet w celu przekazania informacji na temat wdrożenia założeń Zalecenia Komisji (UE) 2019/553 z dnia 3 kwietnia 2019 r. w sprawie cyberbezpieczeństwa w sektorze energetycznym. W roku 2023 r. dokonano szczegółowej analizy wyników zebranych informacji, wyciągnięto wnioski w zakresie takich obszarów jak: wymogi czasu rzeczywistego dotyczące elementów infrastruktury energetycznej, efekty kaskadowe, dotychczasowa i najnowocześniejsza technologia. Na podstawie wyników opracowano także rekomendacje dla kierownictwa resortu.

- Sprawozdania z przeprowadzonych audytów

Organ właściwy na bieżąco występuje do operatorów usług kluczowych z wnioskiem o przekazanie sprawozdań z przeprowadzonych audytów. Dokumenty te są na bieżąco analizowane przez organ właściwy ds. cyberbezpieczeństwa dla sektora energii, a wnioski będą służyły dalszym czynnościom nadzorczym.

- Podręcznik kontroli organu właściwego ds. cyberbezpieczeństwa sektora energii względem operatorów usług kluczowych

MKiŚ opracowało i wydało dokument "Podręcznik kontroli organu właściwego ds. cyberbezpieczeństwa sektora energii względem operatorów usług kluczowych". 13 stycznia 2023 r. podręcznik został udostępniony na stronie BIP Ministerstwa oraz przekazany do wszystkich operatorów usług kluczowych sektora energii.

- Budowanie świadomości i kompetencji społecznych w zakresie cyberbezpieczeństwa w sektorze energii

Na stronie internetowej Ministerstwa Klimatu i Środowiska funkcjonuje zakładka nt. cyberbezpieczeństwa w sektorze energii. Są w niej umieszczone podstawowe informacje m.in. o tym kim jest operator usługi kluczowej i jakie ma zadania i obowiązki, o organie właściwym, a także liczne publikacje w języku polskim i angielskim oraz akty prawne krajowe i międzynarodowe dotyczące cyberbezpieczeństwa. Co więcej, na stronie zamieszczone są również informacje dotyczące bieżących działań m.in. w zakresie legislacji w obszarze cyberbezpieczeństwa, a także wydane przez Ministra Klimatu i Środowiska "Rekomendacje dotyczące działań mających na celu wzmocnienie cyberbezpieczeństwa w sektorze energii oraz wytyczne sektorowe dotyczące zgłaszania incydentów".

- Szkolenia dla sektora energii

Między innymi przygotowano i skoordynowano szkolenie z przedstawicielem ENISA, który przeprowadził szkolenie dla spółek z sektora energii z zakresu stosowania narzędzia opracowanego przez ENISA – Awareness Raising in a Box. Zorganizowano szkolenie z przedstawicielami NASK-PIB, którzy zaprezentowali członkom Zespołu ds. monitorowania cyberbezpieczeństwa sektora energii, głównie operatorom usług kluczowych, funkcjonalności systemu S46 oraz proces podłączania się do systemu.

- Udział w grupach roboczych Grup Współpracy

W ramach Grupy Współpracy funkcjonuje Grupa Robocza 8 (Work Stream 8 on Energy Sector), która zajmuje się kwestią cyberbezpieczeństwa w sektorze energii, a zwłaszcza opracowaniem dokumentów wspierających implementację dyrektywy NIS, realizację wymagań bezpieczeństwa w sektorze, jak i dokumentów służących zarządzaniu ryzykiem. W 2023 r. odbyły się 2 stacjonarne spotkania w ramach WS8 w Atenach - w maju miał miejsce warsztat poświęcony krajowym planom szacowania ryzyka cyberbezpieczeństwa sektora, zaś we wrześniu zorganizowano stacjonarne posiedzenie grupy. W obu tych spotkaniach uczestniczyli przedstawiciele organu właściwego ds. cyberbezpieczeństwa dla sektora energii, przedstawiając polski punkt widzenia na omawiane kwestie.

Ministerstwo Infrastruktury

1.3.2 Sektor transportu

Ministerstwo Infrastruktury realizowało zadania organu właściwego dla sektora transportu. Wiąże się to przede wszystkim z:

- prowadzeniem bieżącej analizy podmiotów w sektorach transportu oraz zaopatrzenia w wodę pitną i jej dystrybucji pod kątem uznania za operatora usługi kluczowej lub niespełniania warunków kwalifikujących podmiot jako operatora usługi kluczowej (stan na dzień 6 marca 2024 r. to łącznie 32 podmioty będące we właściwości Ministra Infrastruktury);
- monitorowaniem stosowania przepisów UKSC przez operatorów usług kluczowych;
- prowadzeniem kontroli operatorów usług kluczowych (w 2023 r. przeprowadzono 4 kontrole planowe oraz 1 kontrolę doraźną);
- stałą współpracą z operatorami usług kluczowych z zakresu realizacji przepisów UKSC;
- współpracą z CSIRT GOV i CSIRT NASK w zakresie powiadamiania o cyberzagrożeniach, w tym dystrybucją rekomendacji dotyczących działań mających na celu wzmocnienie cyberbezpieczeństwa;
- prowadzeniem spraw związanych z postępowaniami administracyjnymi w stosunku do operatorów usług kluczowych, a także spraw wpływających na kształt krajowego systemu cyberbezpieczeństwa.

Inne przedsięwzięcia zrealizowane w 2023 r. w ramach sektora transportu

W podsektorze transportu lotniczego ustanowiono trzecie w Polsce (a drugie w sektorze transportu) Centrum Wymiany Informacji i Analiz: Aviation-ISAC. Bazując na doświadczeniach oraz współpracy z podsektorem kolejowym, w którym Centrum Wymiany Informacji i Analiz (ISACKolej) funkcjonuje w Polsce najdłużej, można niezaprzeczalnie stwierdzić, że taka inicjatywa stanowi wartość dodaną dla cyberbezpieczeństwa. Dlatego też Ministerstwo Infrastruktury podejmowało działania mające na celu ustanowienie takich struktur w sektorze zaopatrzenia w wodę pitną i jej dystrybucji oraz w podsektorze transportu wodnego.

Ministerstwo Infrastruktury wspólnie z Europejską Agencją ds. Cyberbezpieczeństwa oraz firmą Deloitte zrealizowało projekt Cybersecurity Support Action w ramach Cybersecurity Maturity Assessment, w ramach którego zostało przeprowadzone badanie dojrzałości cyberbezpieczeństwa sektora zaopatrzenia w wodę pitną i jej dystrybucji obejmujące zakres nie tylko obecnie wyznaczonych operatorów usług kluczowych, ale także podmiotów, które już po implementacji Dyrektywy NIS2 staną się podmiotami kluczowymi.

Ministerstwo Infrastruktury zbudowało przestrzeń do ścisłej współpracy z NASK-PIB w ramach zagadnień szeroko rozumianego cyberbezpieczeństwa, zastosowania metod sztucznej inteligencji, rozwoju e-usług administracji państwowej i szeroko rozumianego rozwoju społeczeństwa informacyjnego, w szczególności w obszarze wspierania Ministerstwa Infrastruktury przez NASK-PIB w tworzeniu rozwiązań podnoszących poziom cyberbezpieczeństwa, poprzez podpisanie listu intencyjnego oraz zapewnienie możliwości wymiany wiedzy w ramach zawartej umowy o zachowaniu poufności pomiędzy NASK-PIB a MI.

Podjęte zostały działania zmierzające do rozbudowy już posiadanej przez Ministerstwo Infrastruktury komunikacji w ramach PCOC, które wspiera wymianę informacji na potrzeby kierowania bezpieczeństwem narodowym w obszarze cyberbezpieczeństwa.

W ramach poprawy cyberbezpieczeństwa urzędu Ministerstwo Infrastruktury dołączyło do platformy N6 – stworzonego przez CERT Polska systemu, służącemu do gromadzenia, przetwarzania i przekazywania informacji o zdarzeniach bezpieczeństwa w sieci.

Realizowano dystrybucję rekomendacji wydanych przez Agencję Bezpieczeństwa Wewnętrznego, w których zawarto najważniejsze kwestie dot. rozwiązań technicznych, organizacyjnych i funkcjonalnych, których zastosowanie wpłynie na zwiększenie poziomu cyberbezpieczeństwa, wśród operatorów usług kluczowych i jednostek podległych i nadzorowanych (w tym podmiotów infrastruktury krytycznej), ale także podmiotów przewidzianych zakresem Dyrektywy NIS2.

Zapewniano wsparcie operatorów usług kluczowych w nadzorowanych przez MI sektorach w objęciu projektem Artemis (narzędziem mającym za zadanie badanie stron internetowych w poszukiwaniu podatności, luk bezpieczeństwa i błędów konfiguracyjnych oraz pomagającym weryfikować zabezpieczenia systemów udostępnianych w Internecie). Działaniem zostały objęte również podmioty z sektora zaopatrzenia w wodę pitną i jej dystrybucji, które najpewniej obejmie Dyrektywa NIS2.

Realizowano wsparcie w przyłączeniu jednostek podległych i nadzorowanych przez Ministra Infrastruktury, jak i samego Ministerstwa, do projektu ochrony przed atakami DDoS w ramach ADDoS, zapewnianego przez Ministerstwo Cyfryzacji i NASK-PIB.

Ministerstwo Infrastruktury aktywnie promuje również System S46 wśród nadzorowanych operatorów usług kluczowych, który służy m.in. do wspierania szacowania ryzyka na poziomie krajowym. Na koniec 2023 r. spośród 32 operatorów usług kluczowychpodłączonych do systemu było 11 podmiotów, 2 miały status w trakcie podłączenia, a jeden był w trakcie podpisywania porozumienia z Ministerstwem Cyfryzacji.

Ministerstwo Infrastruktury podejmuje też szereg działań mających na celu podniesienie cyberbezpieczeństwa w ramach resortu, p.. „Cyberbiuletyn MI", rożnego typu szkolenia, czy modernizacja własnej infrastruktury teleinformatycznej.

Nowa perspektywa prawna ukazuje rolę Ministerstwa Infrastruktury nie tylko jako organu nadzorującego, ale również podmiotu wykonawczego do obowiązków ujętych w dyrektywie NIS2.

Znaczny wzrost podmiotów pozostających w nadzorze, czy rozszerzenie katalogu zadań dla podmiotów nadzorujących, bezpośrednio wpływają na zwiększenie zakresu obowiązków realizowanych przez organ właściwy, co przekłada się na konieczność zapewnienia odpowiednich zasobów kadrowych. Należy przy tym zauważyć, że Minister Infrastruktury jest organem właściwym ds. cyberbezpieczeństwa dla dwóch sektorów: transportu oraz zaopatrzenia w wodę pitną i jej dystrybucji. Dlatego jednym z najistotniejszych wyzwań będzie utworzenie CSIRTu sektorowego odpowiadającego potrzebom obu tych sektorów. Jest to niezwykle istotne w kontekście występowania zróżnicowanych systemów informacyjnych wykorzystywanych do świadczenia usług nie tylko w poszczególnych dziedzinach transportu (sektor ten dzieli się na cztery podsektory: kolejowy, lotniczy, wodny oraz drogowy), jak i w podmiotach odpowiadających za dostawę i dystrybucję wody oraz przedsiębiorstwa zbierające, odprowadzające lub oczyszczające ścieki komunalne, bytowe lub przemysłowe. Pomocne w realizacji tego zadania niewątpliwie okazały się działania podjęte w ubiegłym roku przez Ministerstwo Infrastruktury, których zwieńczeniem był raport zawierający opis procesu utworzenia zespołu reagowania na incydenty bezpieczeństwa komputerowego (CSIRT) poziomu sektorowego we wszystkich istotnych aspektach, takich jak usługi, kompetencje, procesy i perspektywa techniczna.

W świetle powyższego należy podkreślić, że przeprowadzone w nadzorowanych sektorach analizy wskazują, że podsektor transportu kolejowego już teraz posiada zdolności operacyjne do świadczenia usług odpowiadającym kompetencjom CSIRT-u dla tego podsektora. Wobec tego rozważana jest delegacja części zadań wynikających z nowelizowanych przepisów UKSC do podsektora transportu kolejowego. Decyzja kierunkowa w tym zakresie jeszcze nie zapadła, niemniej ważne jest, aby takie działanie było możliwe do przeprowadzenia w ramach ustanawianych nowelizowanych przepisów.

Jednym z najistotniejszych zadań będzie weryfikacja szczegółowa podmiotów z nadzorowanych sektorów, które zostaną objęte zakresem dyrektywy NIS2. Ministerstwo Infrastruktury przewiduje realizację projektu polegającego na przeprowadzeniu badania dojrzałości cyberbezpieczeństwa i gotowości na wdrożenie dyrektywy NIS2 w sektorze transportu (Ministerstwo Infrastruktury zrealizowało w zeszłym roku taki projekt dla drugiego z nadzorowanych sektorów, tj. w sektorze zaopatrzenia w wodę pitną i jej dystrybucję). Jednocześnie, w celu zapewnienia wsparcia podmiotom w nadzorowanych sektorach w zakresie spełnienia wymogów dyrektywy NIS2, przewiduje się podjęcie działań promujących System S46, jako system wspomagający spełnienie tychże obowiązków.

Kolejnym zadaniem, do którego przygotowuje się Ministerstwo Infrastruktury jest utworzenie CSIRTu sektorowego, którego zakres obejmie dwa sektory pozostające we właściwości Ministra Infrastruktury: transportu oraz zaopatrzenia w wodę pitną i jej dystrybucję. Na potrzeby realizacji zadania w ubiegłym roku przygotowano do tego odpowiednią przestrzeń, poprzez podpisanie listu intencyjnego i zawarcie umowy o zachowaniu poufności pomiędzy MI a NASK-PIB oraz przeprowadzono badanie, w wyniku którego opracowano raport zawierający mapę drogową do zbudowania sektorowego CSIRT i model jego funkcjonowania. W 2024 r. planowany jest szereg dalszych prac związanych z realizacją tego celu.

W 2024 r. Ministerstwo Infrastruktury będzie kontynuować starania mające na celu formalne ustanowienie ISAC w podsektorze transportu wodnego oraz w sektorze zaopatrzenia w wodę pitną i jej dystrybucji. Planowane są również spotkania z operatorami usług kluczowych (oraz podmiotami kluczowymi i ważnymi przewidzianymi zakresem dyrektywy NIS2) z sektorów transportu i zaopatrzenia w wodę pitną i jej dystrybucji, poświęcone tematyce cyberbezpieczeństwa oraz przygotowania się do wdrożenia i spełnienia nowych wymogów.

KNF | KOMISJA NADZORU FINANSOWEGO

1.3.3 Sektor bankowy i infrastruktury rynków finansowych

Komisja Nadzoru Finansowego realizowała zadania organu właściwego dla sektora bankowego i infrastruktury rynków finansowych.

Analiza podmiotów w sektorze oraz postępowania administracyjne

Analiza podmiotów rynku finansowego w zakresie spełnienia kryteriów

W ramach realizacji zadań organu właściwego prowadzono czynności obejmujące bieżącą analizę podmiotów w sektorze bankowym i infrastruktury rynków finansowych pod kątem uznania ich za operatora usługi kluczowej lub niespełniania warunków kwalifikujących podmiot jako operatora usługi kluczowej.

Postępowania administracyjne

W oparciu o wyniki w/w analiz realizowane były dalsze czynności następcze w postaci wydawania odpowiednich decyzji administracyjnych: w przedmiocie uznania danego podmiotu za operatora usługi kluczowej albo stwierdzenia wygaśnięcia decyzji o uznaniu podmiotu za operatora usługi kluczowej. Obejmowało to uznanie w 2023 r. jednego podmiotu w sektorze bankowym i infrastruktury rynków finansowych za operatora usługi kluczowej, a także wydanie jednej decyzji stwierdzającej wygaśnięcie decyzji o uznaniu podmiotu za operatora usługi kluczowej. Na podstawie wydanych w ten sposób decyzji KNF, jako organ właściwy, kierowała następnie wnioski do ministra właściwego do spraw informatyzacji o wpisanie podmiotu do wykazu operatorów usług kluczowych lub wykreślenie z tego wykazu.

Bieżący nadzór, w tym przekazywanie informacji oraz kontrole

Kontrole Operatorów Usług Kluczowych

W ramach nadzoru sprawowanego nad operatorami usług kluczowych w sektorze bankowym i infrastruktury rynków finansowych przeprowadzono w 2023 r. 5 kontroli, w ramach których dokonano szczegółowej analizy objętych kontrolą obszarów działalności operatorów usług kluczowych w kontekście obowiązków przewidzianych w UKSC. W oparciu o wyniki kontroli wydawano zalecenia oraz podejmowano dalsze czynności związane z monitorowaniem ich realizacji.

Metodyki kontroli

Działania organu właściwego w obszarze kontroli obejmowały również doskonalenie procesów w ramach Urzędu KNF. Dotyczy to przygotowania w 2023 r. wewnętrznych metodyk dotyczących kontroli operatorów usług kluczowych.

Nadzór bieżący

Działania podejmowane przez KNF w ramach nadzoru bieżącego koncentrowały się na monitorowaniu stosowania przepisów UKSC przez operatorów usług kluczowych sektora bankowego i infrastruktury rynków finansowych. W tym zakresie KNF kierowała do operatorów usług kluczowych m.in. pisemne stanowiska nadzorcze i pisma sygnalizacyjne, a także wnioski o wyjaśnienia bądź przekazanie dodatkowych informacji na temat realizacji określonych obowiązków wynikających z przepisów UKSC.

W ramach działań obejmujących bieżący nadzór nad operatorami usług kluczowych KNF, jako organ właściwy w ramach UKSC, podejmowała także działania mające na celu wzmacnianie wymiany informacji w obszarze cyberbezpieczeństwa podmiotów rynku finansowego, w tym operatorów usług kluczowych. Do podmiotów rynku finansowego, w tym operatorów usług kluczowych, dystrybuowano więc przede wszystkim informacje o cyberzagrożeniach. Jednocześnie KNF organizowała cykliczne spotkania podmiotów rynku finansowego (w tym operatorów usług kluczowych) w celu wymiany informacji o aktualnych zagrożeniach cyberbezpieczeństwa.

Ponadto do wyżej wymienionych podmiotów przekazywano również zalecenia dotyczące kwestii związanych z cyberbezpieczeństwem, w tym rekomendacje i zalecenia odnoszące się do cyberbezpieczeństwa łańcucha dostaw. Dodatkowo KNF jako organ właściwy do spraw cyberbezpieczeństwa opracowywała i przekazywała operatorom usług kluczowych również dobre praktyki i standardy w zakresie cyberbezpieczeństwa. Działania informacyjne KNF jako organu właściwego podejmowane były również w ramach współpracy z innymi podmiotami krajowego systemu cyberbezpieczeństwa. Można w tym kontekście wskazać na skierowanie do operatorów usług kluczowych informacji z Ministerstwa Cyfryzacji w sprawie Systemu S46 wraz z ulotką informacyjną oraz formularzem kontaktowym dla realizacji porozumienia i umów podłączenia do omawianego systemu.

Budowanie świadomości i kompetencji społecznych w zakresie cyberbezpieczeństwa oraz inne wybrane działania

Budowanie świadomości i działania edukacyjne

W 2023 roku w ramach działań KNF jako organu właściwego do spraw cyberbezpieczeństwa na gruncie UKSC zrealizowano także szereg inicjatyw w zakresie budowania świadomości i kompetencji społecznych w zakresie cyberbezpieczeństwa. W tym zakresie KNF organizowała m.in. szkolenia dla operatorów usług kluczowych oraz pracowników Urzędu KNF w obszarze cyberbezpieczeństwa. Obejmowało to również prowadzenie szkoleń dedykowanych wybranym grupom społecznym (seniorzy, uczniowie, nauczyciele itd.) w obszarach takich jak bezpieczeństwo środków finansowych, bezpieczeństwo urządzeń mobilnych, metody działania cyberprzestępców, czy też bezpieczne korzystanie z Internetu. Dodatkowo podejmowano także inne działania w celu dystrybucji wiedzy na temat cyberbezpieczeństwa – m.in. poprzez wystąpienia na konferencjach i udział w panelach dyskusyjnych dot. obszaru cyberbezpieczeństwa i cyberprzestępczości. Jednocześnie, w ramach projektu CEDUR KNF organizowano również szkolenia dla organów ścigania oraz służb specjalnych w zakresie cyberbezpieczeństwa rynku finansowego. We współpracy z Wyższą Szkołą Policji w Szczytnie prowadzone były kierowane do funkcjonariuszy Policji, w tym CBZC, studia podyplomowe na kierunku "Cyberbezpieczeństwo" oraz "Zwalczanie cyberprzestępczości".

Współpraca krajowa i międzynarodowa

W ramach działań organu właściwego do spraw cyberbezpieczeństwa w sektorze bankowym i infrastruktury rynków finansowych podejmowane były działania w celu rozwijania współpracy krajowej i międzynarodowej. Obejmowało to przede wszystkim współpracę z przedstawicielami Policji i prokuratury w zakresie zapobiegania cyberprzestępstwom popełnianym na polskim rynku finansowym, której uzupełnieniem były omówione powyżej wspólne działania edukacyjne. Kontynuowano współpracę z dostawcami mediów społecznościowych w zakresie wykrywania i zwalczania działań cyberprzestępczych z wykorzystaniem takich mediów oraz kontynuowano współpracę w międzynarodowych organizacjach w obszarze wymiany informacji o cyberprzestępstwach na rynkach finansowych. Istotna pozostawała także współpraca CSIRT KNF z zespołem CSIRT NASK w ramach działań mających na celu zwalczanie zagrożeń na rynku finansowym, a także współpraca z pozostałymi zespołami CSIRT poziomu krajowego, podejmowana w celu wymiany informacji o incydentach i cyberzagrożeniach.

Na szczególną uwagę zasługuje także nawiązanie współpracy z Ministerstwem Cyfryzacji w celu omawiania kierunków legislacji w obszarze relacji między dyrektywą NIS 2 a rozporządzeniem DORA.

Działania zespołu CSIRT KNF, w tym zgłoszenia incydentów

Działania sektorowego zespołu cyberbezpieczeństwa CSIRT KNF

W 2020 r. Komisja Nadzoru Finansowego, jako organ właściwy do spraw cyberbezpieczeństwa, ustanowiła w ramach sektora bankowego i infrastruktury rynków finansowych sektorowy zespół cyberbezpieczeństwa – CSIRT KNF. Przez okres swojego funkcjonowania zespół ten stale rozbudowuje kompetencje i intensyfikuje realizowane działania.

- **Przyjmowanie i obsługa incydentów**

Zespół CSIRT KNF odpowiedzialny jest w szczególności za przyjmowanie od operatorów usług kluczowych zgłoszeń o incydentach poważnych oraz wsparcie w obsłudze tych incydentów. W tym zakresie zespół podejmuje również między innymi czynności związane z analizą takich incydentów, wyszukiwaniem powiązań pomiędzy nimi oraz opracowywaniem wniosków z ich obsługi, a także działania związane ze współpracą z właściwym CSIRT poziomu krajowego w zakresie koordynowania obsługi tego rodzaju incydentów poważnych. Wymaga podkreślenia, że w 2023 r. zgłoszono do CSIRT KNF 31 incydentów poważnych, w stosunku do 34 tego rodzaju zgłoszeń w roku 2022 (brak trendu wzrostowego). Rozkład zgłaszanych incydentów poważnych w poszczególnych kwartałach roku 2023 przedstawia się następująco:

1) I kwartał – 6 zgłoszonych incydentów poważnych;
2) II kwartał – 6 zgłoszonych incydentów poważnych;
3) III kwartał – 8 zgłoszonych incydentów poważnych;
4) IV kwartał – 11 zgłoszonych incydentów poważnych.

Przeważająca większość zgłaszanych incydentów poważnych, tj. 27 z nich (około 87% wszystkich zgłoszonych do CSIRT KNF incydentów poważnych w 2023 r.) dotyczyła kategorii „Utrata dostępności usługi", 1 incydent poważny dotyczył kategorii „Bezpieczeństwo informacji", zaś 3 incydenty poważne dotyczyły kategorii „Inne". Zgłoszone incydenty poważne w głównej mierze dotyczyły awarii w infrastrukturze teleinformatycznej operatorów usług kluczowych lub awarii w podmiotach zewnętrznych dostarczających usługi dla operatorów usług kluczowych – obejmowało to incydenty poważne zaklasyfikowane jako „Utrata dostępności usługi". Najczęściej występującym czynnikiem zaklasyfikowania incydentu jako poważny w wyniku awarii były:

1) niedostępność usług bankowości elektronicznej dla klientów,
2) opóźnienia w realizacji przelewów oraz płatności,
3) problemy z realizacją zleceń na skutek awarii systemów związanych z otrzymywaniem SMS autoryzacyjnych,
4) aktualizacja kursów walut.

Na skutek prowadzonych ataków DDoS, wśród incydentów poważnych zgłoszonych w 2023 r. znalazły się 4 incydenty poważne związane z takimi atakami. W ich wyniku dochodziło do częściowej lub całkowitej niedostępności usług bankowości elektronicznej. CSIRT KNF koordynował również działania podmiotów rynku finansowego, w tym operatorów usług kluczowych, w sytuacji występowania incydentów w obszarze łańcucha dostaw.

- **Analiza infrastruktury podmiotów rynku finansowego**

Oprócz otrzymywania zgłoszeń poważnych incydentów oraz wsparcia w ich obsłudze, działania CSIRT KNF podejmowane w 2023 r. obejmowały m.in. aktywne wyszukiwanie i ograniczanie cyberzagrożeń na rynku finansowym, a także dystrybucję ostrzeżeń odnośnie zagrożeń w infrastrukturze podmiotów z rynku finansowego. W tym zakresie dokonywano m.in. analizy infrastruktury teleinformatycznej operatorów usług kluczowych oraz dystrybuowano informacje o zidentyfikowanych podatnościach lub nieprawidłowościach, jak również regularnie przekazywano do podmiotów rynku finansowego, w tym operatorów usług kluczowych, informacje i ostrzeżenia o podatnościach i zagrożeniach cyberbezpieczeństwa.

W 2023 roku CSIRT KNF przygotował i przesłał do podmiotów rynku finansowego, w tym operatorów usług kluczowych, 471 ostrzeżeń zawierających szczegółowe opisy zagrożeń oraz proponowane działania mitygujące, zwiększające poziom cyberbezpieczeństwa.

- **Analizy zagrożeń i przygotowywanie raportów**

Elementem aktywności CSIRT KNF było również prowadzenie działań CTI (Cyber Threat Intelligence) i działań analitycznych w zakresie działalności grup cyberprzestępczych ukierunkowanych na podmioty i klientów polskiego rynku finansowego. Ponadto działania CSIRT KNF w przedmiotowym obszarze skoncentrowane były także na wykrywaniu, analizie, przygotowywaniu i dystrybuowaniu informacji i raportów na temat działania złośliwego oprogramowania wykorzystywanego przez cyberprzestępców do kradzieży środków finansowych.

- **Utrzymywanie systemów przeznaczonych do wymiany informacji o cyberzagrożeniach**

Działania CSIRT KNF w opisywanej sferze dotyczyły również udostępniania na rzecz podmiotów rynku finansowego, w tym operatorów usług kluczowych, narzędzi do komunikacji bezpośredniej pomiędzy podmiotami rynku finansowego a zespołem CSIRT KNF, a także wymiany informacji o cyberzagrożeniach.

- **Wykrywanie domen phishingowych**

Istotnym aspektem działań CSIRT KNF jest aktywne poszukiwanie i wykrywanie domen o charakterze phishingowym oraz zgłaszanie ich do zablokowania z wykorzystaniem listy ostrzeżeń CERT Polska, jak również wykrywanie, analiza i blokowanie we współpracy z dostawcami mediów społecznościowych reklam tzw. „fałszywych inwestycji", publikowanych za pośrednictwem takich mediów. W wyniku tych działań, w 2023 roku zidentyfikowanych i zgłoszonych do zablokowania zostało 30140 domen służących do wyłudzeń (w 2023 r. zespół CERT Polska zablokował w ramach swojej działalności łącznie 79493 tego rodzaju domeny). Zidentyfikowano i zgłoszono do zablokowania także 7693 reklamy „fałszywych inwestycji".

- **Działania edukacyjne**

Pracownicy CSIRT KNF biorą m.in. udział w prowadzeniu szkoleń z zakresu cyberbezpieczeństwa dla profesjonalnych i nieprofesjonalnych uczestników rynku finansowego. W prowadzonych przez zespół CSIRT KNF profilach mediów społecznościowych publikowane są ostrzeżenia i informacje o zagrożeniach w obszarze cyberbezpieczeństwa rynku finansowego. Ostrzeżenia te były źródłem wiedzy o cyberzagrożeniach w obszarze rynku finansowego również dla dziennikarzy i przedstawicieli mediów. Na podstawie informacji

i ostrzeżeń publikowanych przez zespół CSIRT KNF powstawały materiały wykorzystywane i dystrybuowane do szerokiego grona odbiorców w Internecie. W 2023 roku w mediach społecznościowych zespołu CSIRT KNF zamieszczono 256 tego rodzaju ostrzeżeń, a na ich podstawie powstało 1256 artykułów oraz publikacji dystrybuowanych w mediach internetowych o zasięgu ogólnopolskim. W ramach wymiany wiedzy CSIRT KNF prowadzi cykliczne spotkania z przedstawicielami rynku finansowego a także organów ścigania, takich jak prokuratura i CBZC. W ramach spotkań omawiane są aktualne kampanie i nowe metody przestępcze wykorzystywane przez cyberprzestępców. Dla celów edukacyjnych CSIRT KNF publikuje także na stronach internetowych raporty i analizy opisujące różnego rodzaju cyberzagrożenia, sposoby działania złośliwego oprogramowania oraz kampanie realizowane przez cyberprzestępców.

Opierając się na doświadczeniach zdobytych w ramach realizowanych zadań, a także wynikających ze współpracy z innymi podmiotami krajowego systemu cyberbezpieczeństwa, KNF jako organ właściwy do spraw cyberbezpieczeństwa dla sektora bankowego i infrastruktury rynków finansowych pozytywnie ocenia funkcjonowanie krajowego systemu cyberbezpieczeństwa.

Doświadczenia zdobyte w ramach realizacji zadań przez CSIRT KNF oraz perspektywa współpracy KNF w ogólnoeuropejskich ramach koordynacji dla odpowiednich organów w odniesieniu do cyberincydentów o charakterze systemowym zgodnie z zaleceniem Europejskiej Rady ds. Ryzyka Systemowego z dnia 2 grudnia 2021 r. w sprawie ogólnoeuropejskich ram koordynacji dla odpowiednich organów w odniesieniu do cyberincydentów o charakterze systemowym (ERRS/2021/17) uzasadniają również postulat umożliwienia sektorowym zespołom cyberbezpieczeństwa udziału w Sieci CSIRT (CSIRT Network). Zmiana taka mogłaby zostać wprowadzona w ramach kolejnej nowelizacji UKSC, a uczestnictwo CSIRT KNF w Sieci CSIRT mogłoby pozytywnie wpłynąć na nawiązanie relacji omawianego zespołu z innymi zespołami CSIRT w Europie, co powinno przełożyć się m.in. na skuteczniejszą współpracę z takimi zespołami w ramach reagowania na cyberincydenty o charakterze systemowym, bądź poważne incydenty związane z ICT w rozumieniu rozporządzenia DORA.

W bieżącym roku planowana jest dalsza realizacja działań w dotychczasowych obszarach oraz analizowanie pola dla podejmowania nowych aktywności dla zapewnienia cyberbezpieczeństwa na rynku finansowym. Może to dotyczyć w szczególności wykorzystania możliwości płynących z nowego prawodawstwa europejskiego, jak rozporządzenie Parlamentu Europejskiego i Rady (UE) 2022/2065 z dnia 19 października 2022 r. w sprawie jednolitego rynku usług cyfrowych oraz zmiany dyrektywy 2000/31/WE (akt o usługach cyfrowych), którego przepisy mogą przysłużyć się walce z oszustwami na rynku finansowym. Obejmuje to w szczególności kwestię zgłaszania nielegalnych treści, w rozumieniu art. 3 lit. h) tego rozporządzenia, do dostawców usług pośrednich objętych zakresem jego zastosowania. Przykładem takich treści mogą być bowiem reklamy tzw. „fałszywych inwestycji", wykorzystywane przez cyberprzestępców do popełniania przestępstw na szkodę obywateli RP, o których wspomniano w ramach opisu działań CSIRT KNF.

Ministerstwo Zdrowia

1.3.4 Sektor ochrony zdrowia

Ministerstwo Zdrowia w roku 2023 prowadziło wielokierunkowe działania związane z wykonywaniem obowiązków organu właściwego w sektorze ochrony zdrowia, w którym ustanowiono 239 operatorów usług kluczowych.

Ministerstwo Zdrowia ustawicznie monitorowało operatorów usług kluczowych pod kątem realizacji obowiązków nałożonych na nich przepisami ustawy. Przeprowadzano analizy przekazywanych przez operatorów sprawozdań z audytów zgodności w wymogami UKSC, o których mowa w art. 15 ust. 1. Cyklicznie badano również poziom dojrzałości cyberbezpieczeństwa operatorów. Ministerstwo wydawało także rekomendacje w zakresie wdrażania rozwiązań mających na celu usuwanie podatności w systemie cyberbezpieczeństwa operatorów. Istotnym przedsięwzięciem była ponadto koordynacja projektu dofinansowania podmiotów leczniczych podejmujących działania mające na celu podniesienie poziomu cyberbezpieczeństwa.

W minionym roku Ministerstwo Zdrowia koordynowało projekt podłączania operatorów w sektorze do Systemu S46. Na dzień 31.12.2023 r. status podłączeń do Systemu S46 przedstawiał się następująco:

- 60 operatorów podłączonych,
- 16 operatorów w trakcie podłączania,
- 2 operatorów w trakcie podpisywania porozumienia z Ministerstwem Cyfryzacji,
- 169 operatorów wytypowanych do podłączenia w nowej architekturze zaproponowanej przez NASK-PIB.

Ministerstwo Zdrowia współpracowało z NASK-PIB w zakresie cyklicznego wykonywania przez CSIRT NASK skanów podatności w infrastrukturze teleinformatycznej operatorów, jak również usprawniło komunikację z operatorami, w tym na drodze usuwania problemów zakłócających proces nawiązywania łączności z osobami wyznaczonymi przez operatorów do utrzymywania kontaktów z podmiotami krajowego systemu cyberbezpieczeństwa.

Inne zadania realizowane przez Ministerstwo Zdrowia w zakresie cyberbezpieczeństwa

- Koordynowanie działań związanych z utworzeniem sektorowego zespołu cyberbezpieczeństwa dla sektora ochrony zdrowia – CSIRT CeZ

Zespół rozpoczął funkcjonowanie we wrześniu 2023 r. CSIRT CeZ odpowiedzialny jest za świadczenie usług dla podmiotów sektora ochrony zdrowia, w tym m. in. za przyjmowanie zgłoszeń o incydentach poważnych, wsparcie w obsłudze tych incydentów, analizowanie incydentów poważnych, wyszukiwanie powiązań między nimi, opracowanie wniosków z obsługi incydentów, czy wspieranie operatorów usług kluczowych w wykonywaniu obowiązków określonych przepisami UKSC.

- Wsparcie podmiotów sektora ochrony zdrowia przy usuwaniu skutków incydentów bezpieczeństwa w cyberprzestrzeni

Zadanie to realizuje z ramienia Ministerstwa Zdrowia podległa mu wyspecjalizowana i doświadczona jednostka Centrum e-Zdrowia (CeZ).

- Opracowanie procesu przeprowadzania kontroli operatorów
- Realizacja projektów finansowanych ze środków Europejskiej Agencji ds. Cyberbezpieczeństwa (ENISA), w tym polegających na:
    a) opracowaniu (przy współpracy z Ministerstwem Cyfryzacji) dokumentu opisującego krajobraz cyberzagrożeń polskiego systemu ochrony zdrowia, ukazującego najpoważniejsze zagrożenia oraz główne trendy zaobserwowane w odniesieniu do zagrożeń cyberprzestepców i technik ataku; w dokumencie przedstawiono także wyniki analizy wpływu i motywacji poszczególnych cyberprzestępców oraz rekomendowane do wdrożenia środki zaradcze;
    b) opracowaniu (przy współpracy z Ministerstwem Cyfryzacji) dokumentu „Krajobraz bezpieczeństwa IT";
    c) przeprowadzeniu testów penetracyjnych w infrastrukturze teleinformatycznej 8 wytypowanych operatorów;
    d) opracowaniu podręcznika reagowania na incydenty, który będzie pełnił rolę narzędzia wspierającego proces zarządzania incydentami cyberbezpieczeństwa w jednostkach publicznej opieki zdrowotnej; podręcznik ma pomóc jednostkom leczniczym w identyfikacji i zrozumieniu zagrożeń, poprzez przedstawienie realistycznych sytuacji kryzysowych związanych z cyberbezpieczeństwem oraz wyjaśnienie ich potencjalnych skutków dla pacjentów, podmiotów medycznych oraz ich personelu (w dokumencie przedstawiono przejrzyste i skuteczne procedury reagowania na incydenty cyberbezpieczeństwa, w tym ataki typu ransomware, utratę danych pacjentów czy naruszenia poufności informacji medycznych);
    e) przeprowadzeniu ćwiczeń symulacyjnych (w formie gry sztabowej), mających na celu zweryfikowanie użyteczności ww. podręcznika w realnych działaniach; ćwiczenia, w których wzięło udział 3 operatorów wykazały, że podręcznik może być z powodzeniem wykorzystywany w trakcie przejmowania kontroli nad incydentami cyberbezpieczeństwa.

Cele projektów, o których mowa w punktach d) i e) zostały osiągnięte, dzięki czemu zespoły reagowania na incydenty w jednostkach medycznych zostaną wyposażone w kompleksowe narzędzie do zarządzania incydentami cyberbezpieczeństwa we współpracy z CSIRT-em sektorowym.

W 2024 r. Ministerstwo Zdrowia planuje realizację następujących działań w obszarze odpowiedzialności ustanowionej przepisami UKSC:

1) kontynowanie procesu podłączania Operatorów do S46;
2) prowadzenie kontroli operatorów;
3) uczestnictwo w pracach nad nowelizacją UKSC;
4) uczestnictwo w projektach finansowanych przez ENISA w następujących obszarach:
    a) prowadzenia testów penetracyjnych,
    b) ćwiczeń symulacyjnych w oparciu o podręcznik zarządzania incydentami,
    c) wspierania obsługi zarządzania incydentami na poziomie CSIRT oraz SOC,
    d) aktualizacji dokumentów pn. „Krajobraz cyberzagrożeń polskiego systemu ochrony zdrowia" oraz „Krajobraz bezpieczeństwa IT";
5) organizowanie stacjonarnych konferencji z udziałem przedstawicieli Operatorów.

Ministerstwo Cyfryzacji

1.3.5 Sektor infrastruktury cyfrowej

Ministerstwo Cyfryzacji w 2023 r. realizowało zadania organu właściwego do spraw cyberbezpieczeństwa dla sektora infrastruktury cyfrowej, prowadziło bieżącą analizę pod kątem identyfikacji nowych, potencjalnych podmiotów spełniających kryteria uznania za operatora usługi kluczowej oraz ustalenia, czy nadal spełnione są przesłanki przyjęte za podstawę do wydania decyzji identyfikacyjnej (o uznaniu za operatora usługi kluczowej). W oparciu o powyższe analizy nie wydano żadnej decyzji o uznaniu podmiotu za operatora usługi kluczowej, ani również decyzji stwierdzającej wygaśnięcie decyzji o uznaniu podmiotu za operatora usługi kluczowej. Nie przedłożono również żadnego wniosku o zmianę danych w wykazie operatorów usług kluczowych.

Ponadto Ministerstwo Cyfryzacji w ramach nadzoru nad operatorami usług kluczowych w zakresie wykonywania obowiązków wynikających z UKSC dotyczących przeciwdziałania zagrożeniom cyberbezpieczeństwa i zgłaszania incydentów:

- Przeprowadziło 3 kontrole operatorów usług kluczowych we wskazanym wyżej zakresie. Na podstawie zgromadzonych w toku kontroli informacji Minister Cyfryzacji stwierdził naruszenie przepisów UKSC oraz wydał zalecenia pokontrolne wzywające do usunięcia uchybień i nieprawidłowości, a także monitorował stopień ich realizacji;
- Nałożyło dwie administracyjne kary pieniężne za nieprzeprowadzenie pierwszego audytu bezpieczeństwa systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej w terminie, o którym mowa w art. 15 ust. 1 w związku z art. 16 pkt 3 UKSC.

Inne działania realizowane przez Ministerstwo Cyfryzacji, nie związane bezpośrednio z pełnieniem funkcji organu właściwego, przedstawione są w rozdziale 2.

1.4 Służby specjalne

Ważnym ogniwem krajowego systemu cyberbezpieczeństwa są służby specjalne o charakterze wywiadowczym i kontrwywiadowczym[5], czyli Agencja Bezpieczeństwa Wewnętrznego (ABW), Agencja Wywiadu (AW), Służba Kontrwywiadu Wojskowego (SKW) oraz Służba Wywiadu Wojskowego (SWW). Służby te realizują zadania w zakresie cyberbezpieczeństwa zarówno w ramach obowiązków wynikających z UKSC, jak i innych ustaw określających zakres działania i kompetencje służb specjalnych.

Rola służb specjalnych w zapewnianiu bezpieczeństwa teleinformatycznego na poziomie krajowym jest szczególna zarówno co do ilości realizowanych zadań, ich ciężaru gatunkowego oraz specyfiki działania. Jednak większość działań służb specjalnych pozostaje niejawnych, dlatego też szczegółowe informacje w tym zakresie zawarte są w niejawnym załączniku do niniejszego Sprawozdania.

Ponadto zgodnie z art. 34 ust. 1 UKSC CSIRT MON, CSIRT NASK, CSIRT GOV i sektorowe zespoły cyberbezpieczeństwa oraz podmioty świadczące usługi z zakresu cyberbezpieczeństwa zobowiązane są współpracować nie tylko z organami ścigania i wymiaru sprawiedliwości, ale także ze służbami specjalnymi przy realizacji ich ustawowych zadań.

Działania służb specjalnych w zakresie bezpieczeństwa polskiej cyberprzestrzeni ogniskują się wokół aktywnej cyberobrony, cyberkontrwywiadu, cyberwywiadu, a także identyfikowaniu zagrożeń oraz zbieraniu i analizowaniu informacji, dzięki czemu dostarczają kluczowe dane dla najważniejszych osób w państwie.

Ponadto należy dodać, że w strukturze ABW znajduje się Zespół CSIRT GOV realizujący szczególne zadania wynikające z UKSC, których jawna część została opisana w części Sprawozdania poświęconej działalności CSIRT-ów poziomu krajowego.

Poza tym służby specjalne biorą aktywny udział w Połączonym Centrum Operacyjnym Cyberbezpieczeństwa, co ma szczególne znaczenie dla koordynowania działań najważniejszych instytucji i sprawnego działania w odpowiedzi na pojawiające się zagrożenia. Służby te biorą także udział w posiedzeniach Kolegium do Spraw Cyberbezpieczeństwa.

[5] Ponadto status służby specjalnej posiada także Centralne Biuro Antykorupcyjne, które realizuje zadania o charakterze policyjnym. Dlatego też działania Biura zostały opisane w części Sprawozdania dotyczącej zwalczania cyberprzestępczości.

Publikacje kompromitujące rosyjskie cyberoperacje

W ramach współpracy na poziomie krajowym opracowano raporty o wrogich kampaniach w cyberprzestrzeni, prowadzonych grupy wiązane z rosyjskimi służbami specjalnymi, a tym samym kompromitując wykorzystywane przez nie metody i narzędzia. W 2023 r. ukazały się następujące publikacje:

- Kampania szpiegowska wiązana z rosyjskimi służbami specjalnymi (SKW, NASK)[6];
- Analiza zagrożeń dla cyberbezpieczeństwa placówek dyplomatycznych NATO (AW, MC)[7];
- Russian Foreign Intelligence Service (SVR) Cyber Actors Use JetBrains TeamCity CVE in Global Targeting (FBI, CISA, NSA, SKW, NASK, NCSC)[8].

Publikacje służb specjalnych wydane w 2023 r.

[6] https://www.gov.pl/web/baza-wiedzy/kampania-szpiegowska-wiazana-z-rosyjskimi-sluzbami-specjalnymi
[7] https://www.gov.pl/web/baza-wiedzy/analiza-zagrozen-dla-cyberbezpieczenstwa-placowek-dyplomatycznych-nato
[8] https://www.gov.pl/web/baza-wiedzy/rosyjski-wywiad-wykorzystuje-cve-jetbrains-w-globalnej-kampanii

1.5 Zwalczanie cyberprzestępczości

Centralne Biuro Zwalczania Cyberprzestępczości Policji

Jako jednostka Policji ukierunkowana na zwalczanie cyberprzestępczości, Centralne Biuro Zwalczania Cyberprzestępczości Policji (CBZC) dostrzega istotną trudność w zwalczaniu najbardziej złożonych form cyberprzestępczości, związanych z wykorzystaniem zaawansowanych narzędzi i wyrafinowanych form ataku na systemy informatyczne i sieci telekomunikacyjne. Z tym aspektem wiąże się również rosnące zagrożenie, jakim jest oferowanie takich narzędzi i określonych usług przestępczych w tzw. ciemnym internecie (Darknet).

Zauważalne jest również dynamiczne tempo pojawiania się zupełnie nowych zagrożeń, związanych z aktywnym adoptowaniem przez przestępców najnowszych technologii, które czynią ich ataki bardziej skutecznymi, a jednocześnie trudniejszymi do wykrycia. Dotyczy to chociażby wykorzystania narzędzi sztucznej inteligencji (np. duże modele językowe). W tym kontekście należy również wskazać na rosnące i potencjalnie istotne w przyszłości zagrożenie nielegalnymi działaniami w tzw. światach wirtualnych (Metaverse). Tymczasem zagadnienie to nie zostało jeszcze w pełni opracowane w kontekście działania organów ścigania.

Kolejny istotny aspekt wiąże się z faktem, że cyberprzestępstwa w zdecydowanej większości mają charakter międzynarodowy, gdzie bardzo często przestępcza infrastruktura lub niezbędne dane umożliwiające wykrycie sprawców są dostępne poza granicami kraju, a dostęp do nich jest często utrudniony, bądź niemożliwy.

Dane dotyczące wyników w zwalczaniu cyberprzestępczości w kategoriach będących w szczególnym zainteresowaniu CBZC za rok 2023 przedstawiają poniższe tabele.

0		zatrzymani	podejrzani	Tymczasowo Aresztowani	Liczba przestępstw stwierdzonych	Mienie zabezpieczone w złotych	Mienie odzyskane w złotych
OSZUSTWA	286 §1 kk	134	165	68	2340	127 904 412,07 zł	4 153 385,57 zł
	287 §1 kk	13	31	7	69	64 540,00 zł	1 140,00 zł
	297 § 1 kk	1	24	0	35	0,00 zł	0,00 zł
Przeciwko ochronie informacji	267 kk	2	3	0	39	0,00 zł	0,00 zł
	268 kk	0	0	0	0	0,00 zł	0,00 zł
	268 a kk	0	0	0	9	0,00 zł	0,00 zł
	269 kk	4	4	1	0	0,00 zł	0,00 zł
	269a kk	0	0	0	2	1 300,00 zł	0,00 zł
	269b kk	13	47	1	21	486 756,00 zł	0,00 zł
Przeciwko wolności seksualnej	200 kk	9	8	7	4	0,00 zł	0,00 zł
	200a kk	2	2	0	2	0,00 zł	0,00 zł
	200b kk	0	0	0	0	0,00 zł	0,00 zł
	202 kk	143	167	65	96	495 016,00 zł	0,00 zł
Podszywanie się pod inną osobę / kradzież tożsamosci	190a § 2 kk	3	5	3	0	0,00 zł	0,00 zł
Fałszywe alarmy	224a kk	0	0	0	159	0,00 zł	0,00 zł
Prawo autorskie i przemysłowe	art. 6 i 7 (sharing)	0	0	0	0	0,00 zł	0,00 zł
	116 upa	0	1	0	1	1 048 120,00 zł	0,00 zł
	117 upa	0	0	0	0	0,00 zł	0,00 zł
	118 upa	0	0	0	0	0,00 zł	0,00 zł
	305 kk	0	2	0	3	0,00 zł	0,00 zł
INNE	sprzedaż/posiadanie narkotyków	6	7	5	10	3 592,00 zł	0,00 zł
	sprzedaż/posiadanie broni	0	1	0	2	4 826,00 zł	0,00 zł
	sprzedaż wyrobów akcyzowych	0	0	0	0	0,00 zł	0,00 zł
	nielegalna sprzedaż leków	0	0	0	3	23 000,00 zł	0,00 zł
	inne...	129	151	59	275	310 318 092,00 zł	10 006 161,09 zł
Suma		**459**	**618**	**216**	**3070**	**440 349 654,07 zł**	**14 160 686,66 zł**

Zestawienie danych dotyczących cyberprzestępczości, zarejestrowanych przez CBZC – 2023 r.

Bazując na dotychczasowych doświadczeniach, CBZC formułuje następujące rekomendacje w zakresie zwalczania zaawansowanych form cyberprzestępczości:

- rozwijanie szerokiej współpracy organów ścigania w kontekście międzynarodowym, w szczególności na forum takich organizacji jak Agencja Unii Europejskiej Europol oraz Międzynarodowa Organizacja Policji Kryminalnych INTERPOL;
- rozwijanie skutecznych kanałów komunikacji i współpracy z dostawcami usług elektronicznych;
- potrzeba ciągłego podnoszenia kompetencji funkcjonariuszy w zakresie najnowszych technologii;
- rozwijanie i wdrażanie narzędzi inteligentnego przetwarzania dużych wolumenów danych (w szczególności z zabezpieczonych nośników danych);
- stałe monitorowanie najnowszych trendów technologicznych i związanych z nimi zagrożeń, w celu identyfikacji nowych rodzajów cyberprzestępczości;
- wdrażanie najnowszych rozwiązań (np. z obszaru sztucznej inteligencji) dla potrzeb skutecznego zwalczania i zapobiegania cyberprzestępczości;
- prowadzenie działań i kampanii prewencyjnych skierowanych do społeczeństwa.

CBZC w ramach swojej działalności planuje podjąć następujące działania:

- o charakterze ogólnym:
  - zapobieganie cyberprzestępczości poprzez budowanie bezpieczeństwa cyberprzestrzeni w oparciu o właściwą komunikację ze społeczeństwem;
  - zoptymalizowanie pracy operacyjnej i procesowej w ramach CBZC;
  - zacieśnienie współpracy z krajowymi podmiotami publicznymi i prywatnymi oraz instytucjami międzynarodowymi;
  - ustanowienie „hubu" informacyjnego w zakresie danych dotyczących cyberprzestępczości;
  - wdrażanie/rozwijanie nowoczesnych technologii i innowacji;
  - stałe podnoszenie kompetencji funkcjonariuszy i pracowników CBZC;
- o charakterze szczegółowym:
  - rozpoznawanie, eliminowanie lub redukowanie prawdopodobieństwa wystąpienia cyberprzestępstw;
  - dialog ze społeczeństwem za pośrednictwem dostępnych form komunikacji (np. media społecznościowe, kampanie uświadamiające, spoty, itp.);
  - wdrożenie ujednoliconego podejścia do pracy operacyjnej i procesowej w ramach CBZC;
  - wypracowanie kryteriów doboru spraw prowadzonych przez CBZC oraz efektywnych algorytmów postępowania w sprawach procesowych;
  - współpraca z krajowymi i zagranicznymi podmiotami oraz innymi organami ścigania w zakresie podnoszenia poziomu wiedzy w zakresie cyberbezpieczeństwa oraz zwalczania cyberprzestępczości;
  - rozwój współpracy z Prokuraturą zakresie wymiany informacji, jak i pogłębiania wiedzy dotyczących znajomości metod i narzędzi używanych przez sprawców, istniejących zagrożeń i sposobów ich rozpoznawania, prawnych i faktycznych możliwości pozyskiwania i zabezpieczania dowodów, metod identyfikacji i przeciwdziałania zagrożeniom związanym z cyberatakami;
  - rozwijanie współpracy z krajowymi i międzynarodowymi podmiotami prywatnymi w zakresie zapobiegania i zwalczania cyberprzestępczości;
  - rozwijanie zdolności w zakresie zintegrowanego gromadzenia danych dotyczących cyberprzestępczości i budowanie jej obrazu w Polsce;
  - prognozowanie, diagnozowanie i analizowanie nowych zagrożeń, a także trendów technologicznych w celu rozwijania strategii i metodyki ich wykorzystania dla potrzeb funkcjonowania CBZC (np. AI, quantum computing, cloud computing, IoT, metaverse).

Ministerstwo Sprawiedliwości

Ustawa z dnia 6 czerwca 1997 roku Kodeks Karny definiuje szereg artykułów kwalifikujących się do szeroko pojętej cyberprzestępczości. Poniższe tabele przedstawiają dane Ministerstwa Sprawiedliwości dotyczące osądzonych i skazanych w I instancji sądów rejonowych i okręgowych za przestępstwa z art. 200a § 1 kk, art. 200a § 2 kk, art. 267 § 1 kk, art. 268a kk, art. 269 kk, art. 269a kk, art. 269b kk, art. 287 kk.

Rodzaje przestępstw	OSĄDZENI ogółem		SKAZANI W I INSTANCJI	
	2023	Zmiana do 2022	2023	Zmiana do 2022
Ogółem	**295 921**	*-5%*	**252 627**	*-6%*
w tym:				
Art. 200a § 1 kk	**40**	*33%*	**36**	*38%*
Art. 200a § 2 kk	**120**	*-35%*	**108**	*-36%*
Art. 267 § 1 kk	**159**	*15%*	**98**	*14%*
Art. 268a kk	**45**	*246%*	**32**	*256%*
Art. 269 kk	**3**	*200%*	**3**	*200%*
Art. 269a kk	**4**	*400%*	**2**	*200%*
Art. 269b kk	**21**	*62%*	**5**	*-50%*
Art. 287 kk	**189**	*13%*	**159**	*17%*
Suma dla ww. art. kk	**581**		**443**	

Osadzeni, skazani za wybrane przestępstwa w I instancji sądów rejonowych.

Rodzaje przestępstw	OSĄDZENI ogółem		SKAZANI W I INSTANCJI	
	2023	Zmiana do 2022	2023	Zmiana do 2022
Ogółem	**8 466**	*-9%*	**7 631**	*-8%*
w tym:				
Art. 165 § 1 i 3 kk	**33**	*-57%*	**31**	*-52%*

Osadzeni, skazani za wybrane przestępstwa w I instancji sądów okręgowych.

Cyberbezpieczeństwo wymiaru sprawiedliwości

Zespół do spraw Cyberbezpieczeństwa w Sądach Apelacyjnych pod przewodnictwem Biura Cyberbezpieczeństwa Ministerstwa Sprawiedliwości tworzy i przekazuje standardy oraz rekomendacje dotyczące działań podnoszących poziom cyberbezpieczeństwa w obszarze zarówno Ministerstwa Sprawiedliwości, jak i sądów powszechnych. Jednocześnie celem jest, aby tworzone w ten sposób dokumenty były zgodne z Narodowymi Standardami Cyberbezpieczeństwa. Ponadto standardy i rekomendacje uzgadniane są podczas kwartalnych spotkań w ramach Zespołu do spraw analizy i oceny ryzyk cyberbezpieczeństwa w resorcie sprawiedliwości oraz środków ich zapobiegania. Ponadto Ministerstwo Sprawiedliwość w zakresie cyberbezpieczeństwa współpracuje z takimi instytucjami jak Prokuratura Krajowa, Służba Więzienna, ABW, NASK i inne podmioty administracji publicznej.

Centralne Biuro Antykorupcyjne

Centralne Biuro Antykorupcyjne w 2023 r. prowadziło czynności analityczno-informacyjne i kontrolne dotyczące szeroko rozumianej branży IT, które mogą być potencjalnie związane z cyberprzestępczością i jej zwalczaniem, jak również z sektorem cyberbezpieczeństwa.

- 82 działania realizowane przez Departament Kontroli i Wydziały Postępowań Kontrolnych:
  - 24 sprawy kontrolne,
  - 45 analiz przedkontrolnych,
  - 13 postępowań kontrolnych;
- 2 działania realizowane przez Departament Operacyjno-Śledczy;
- 23 przedsięwzięcia realizowane przez Departament Analiz.

W zależności od wyniku działań realizowanych działań podejmowane odpowiednie dalsze kroki.

Ponadto CBA w zakresie zwiększenia własnych i krajowych zdolności w zakresie cyberbezpieczeństwa brało udział w spotkaniach Połączonego Centrum Operacyjnego Cyberbezpieczeństwa, jak również ściśle współpracowało z CSIRT GOV m.in. poprzez zgłaszanie IoC (ang. Indicator of Compromise) w zakresie aktów teleinformatycznych skierowanych na CBA oraz wdrażanie zaleceń CSIRT GOV.

2. Realizowane działania w zakresie zapewnienia cyberbezpieczeństwa na poziomie krajowym

W niniejszej części Sprawozdania przedstawiono inne niż w rozdziale 1. kluczowe działania wpisujące się w realizację celu głównego Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019-2024, jakim jest „podniesienie poziomu odporności na cyberzagrożenia oraz zwiększenie poziomu ochrony informacji w sektorze publicznym, militarnym, prywatnym oraz promowanie wiedzy i dobrych praktyk umożliwiających obywatelom lepszą ochronę ich informacji". Poniżej przedstawione są działania w podziale na cele szczegółowe Strategii.

2.1 Rozwój krajowego systemu cyberbezpieczeństwa

Wdrożenie Dyrektywy NIS 2

Ministerstwo Cyfryzacji rozpoczęło prace nad implementacją do krajowego porządku prawnego przepisów Dyrektywy Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniająca rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylająca dyrektywę (UE) 2016/1148 (Dyrektywa NIS 2).

Strategia Cyberbezpieczeństwa RP na lata 2025-2029

Jesienią 2023 r. Ministerstwo Cyfryzacji zainicjowało działania związane z opracowaniem projektu nowej Strategii Cyberbezpieczeństwa RP na lata 2025-2029. Dokument ten będzie odpowiedzią na bieżące wyzwania i zagrożenia występujące w obszarze cyberbezpieczeństwa (m.in. uwzględniając doświadczenia związane z cyfryzacją wielu dziedzin życia, trwającą wojną Rosji z Ukrainą, działaniami hybrydowymi Rosji i innych państw, jak również rozwoju nowych technologii). Nowa Strategia uwzględni również planowane zmiany związane z implementację do krajowego porządku prawnego Dyrektywy NIS 2.

Centrum Cyberbezpieczeństwa NASK

W celu wzmocnienia krajowego systemu cyberbezpieczeństwa, we współpracy z Ministerstwem Cyfryzacji, w październiku 2023 r. rozpoczęto realizację projektu utworzenia Centrum Cyberbezpieczeństwa NASK (CCN), na które złożą się jakościowo nowe tematyczne specjalistyczne centra, ośrodki i laboratoria kluczowe dla wzmocnienia krajowego systemu cyberbezpieczeństwa. Realizacja projektu pozwoli na podniesienie poziomu bezpieczeństwa informacji, poprzez wzmacnianie odporności oraz zdolności do skutecznego zapobiegania i reagowania na incydenty w systemach informacyjnych państwa oraz podmiotów mających kluczowe znaczenie dla gospodarki. Projekt ten stanowi odpowiedź na szereg zdefiniowanych wyzwań i potrzeb oraz szybko rosnącą liczbę coraz poważniejszych zagrożeń cyberprzestrzeni i wynikających z nich strat gospodarczych. Zgodnie z przyjętymi założeniami zakres Projektu obejmuje m.in.:

- Budowę obiektu CCN;
- Utworzenie specjalistycznych centrów, ośrodków i laboratoriów:
  - Krajowego Centrum Odzyskiwania Danych (KCOD),
  - Krajowego Centrum Operacyjnego Cyberbezpieczeństwa (KCOC),
  - modelowego Ośrodka treningowo – szkoleniowego w obszarze Cyberbezpieczeństwa (OSC),

  - Laboratorium Bezpieczeństwa AI (AITAS),
  - Laboratorium Fuzzingu i Badania Złośliwego Oprogramowania (FUMAL),
  - Krajowego Centrum Wsparcia Security dla JST (KCWS),
  - Ośrodka Modelowania Certyfikacji Cyberbezpieczeństwa (OMCC);
- Rozbudowę infrastruktury NASK-PIB działającej na rzecz CSIRT NASK, w tym aktualizację procesów i realizację szkoleń wewnętrznych.

Utworzone w ramach projektu CCN centra, ośrodki i laboratoria nie będą stanowiły odrębnych jednostek, lecz wzajemnie współpracujące i wspierające się w realizacji zadań. Projekt jest dofinansowany ze środków Europejskiego Funduszu Rozwoju Regionalnego w ramach Programu Fundusze Europejskie na Rozwój Cyfrowy 2021-2027. Łączna wartość projektu CCN to 310 mln zł.

Projekty KPO

W celu realizacji inwestycji C3.1.1. Cyberbezpieczeństwo – CyberPL, infrastruktura przetwarzania danych oraz optymalizacja infrastruktury służb państwowych odpowiedzialnych za bezpieczeństwo – komponent Cyberbezpieczeństwo, w ramach Krajowego Planu Odbudowy i Zwiększania Odporności, Ministerstwo Cyfryzacji w 2023 r. prowadziło prace nad rewizją zakresu tej inwestycji. W grudniu 2023 r. rewizja KPO została zatwierdzona przez Radę UE. W ramach inwestycji dofinansowanie uzyskają 4 nw. projekty:

- Utworzenie lub rozwój przynajmniej 5 sektorowych Zespołów Reagowania na Incydenty Bezpieczeństwa Komputerowego (CSIRT) w sektorach kluczowych w rozumieniu UKSC, tj. sektorach: energii, transportu, ochrony zdrowia, bankowości i infrastruktury rynków finansowych, infrastruktury cyfrowej, zaopatrzenia w wodę oraz dla przedsiębiorców komunikacji elektronicznej;
- Podłączenie 385 nowych podmiotów krajowego systemu cyberbezpieczeństwa do Systemu S46 oraz dalszy rozwój tego systemu;
- Utworzenie wojewódzkich zespołów specjalistów cyberbezpieczeństwa działających lokalnie i wspierających podmioty publiczne w obsłudze incydentów i odzyskiwaniu danych oraz prowadzeniu działań podnoszących świadomość o cyberbezpieczeństwie;
- Wsparcie 500 podmiotów krajowego systemu cyberbezpieczeństwa w modernizacji i rozbudowie infrastruktury cyberbezpieczeństwa w sieciach IT, w tym wsparcie podmiotów wykorzystujących technologie informacyjne (IT) oraz operacyjne (OT) stosowane w przemysłowych systemach sterowania (ICS).

Zakończenie realizacji tych projektów zaplanowane jest na połowę 2026 r.

System S46

Ministerstwo Cyfryzacji we współpracy z NASK-PIB kontynuowało rozwój i utrzymanie Systemu S46, o którym mowa w art. 46 ust. 1 UKSC. System wdrożono 1 stycznia 2021 r., zgodnie z art. 89 tej ustawy. S46 wspiera zgłaszanie i obsługę incydentów, wymianę informacji i współpracę pomiędzy podmiotami KSC, a także szacowanie ryzyka na poziomie krajowym.

W 2023 r. – do wcześniej już obsługiwanych m.in. CSIRT-ów poziomu krajowego, Ministerstwa Cyfryzacji / Pełnomocnika Rządu ds. Cyberbezpieczeństwa, Urzędu Komunikacji Elektronicznej (UKE), Organów Właściwych (OW), wybranych operatorów usług kluczowych i dostawców usług cyfrowych – podłączono 134 podmioty KSC (100 z projektu S46-REACT, 34 z dotacji

celowej). Na zakończenie 2023 r. z Systemu S46 korzystało razem 157 podmiotów, w tym operatorzy usług kluczowych, dostawcy usług cyfrowych oraz podmioty publiczne, takie jak Jednostki Samorządu Terytorialnego. W obszarze utrzymania ustandaryzowano proces podłączania nowych uczestników do Systemu S46, uruchomiono również rozwiązania SOC/NOC. W obszarze rozwoju wprowadzono kolejne wydania mające na celu wprowadzenie integracji z zewnętrznymi systemami ticketowymi do obsługi zgłoszeń incydentów. Zwiększono również odporność systemu w aspekcie ciągłości działania oraz bezpieczeństwa.

Forum Organów Właściwych

W 2023 r. odbyły się cztery fora organów właściwych krajowego systemu cyberbezpieczeństwa (inicjatywa została zapoczątkowana pod koniec 2022 r. przez resort cyfryzacji w celu stworzenia, pomiędzy organami właściwymi do spraw cyberbezpieczeństwa, wspólnej przestrzeni do wymiany doświadczeń, wiedzy, nawiązania współpracy, wypracowywania wspólnych stanowisk oraz diagnozowania aktualnych potrzeb). Podczas forów poruszano m.in. problematykę Centrów Analizy i Wymiany Informacji (ISAC), CSIRT-ów sektorowych, Systemu S46, czynności podejmowanych przez poszczególne organy właściwe w ramach monitorowania realizacji obowiązków przez operatorów usług kluczowych, dojrzałości organizacyjnej podmiotów krajowego systemu cyberbezpieczeństwa w zakresie cyberbezpieczeństwa (w tym oceny dojrzałości cyberbezpieczeństwa operatorów usług kluczowych) czy implementacji dyrektywy NIS 2.

Systemowe Forum Ochrony Infrastruktury Krytycznej Ministerstwa Cyfryzacji

Uczestnikami Systemowego Forum Ochrony Infrastruktury Krytycznej Ministerstwa Cyfryzacji w dniu 29 września 2023 r. byli Operatorzy Infrastruktury Krytycznej dla systemów: łączności, sieci teleinformatycznych i zapewniającego ciągłość działania administracji publicznej oraz prelegenci (przedstawiciele świata nauki i administracji tj. Komendy Głównej Policji, Rządowego Centrum Bezpieczeństwa, Politechniki Poznańskiej, IDEAS NCBR Sp. z o.o.). Systemowe Forum Ochrony Infrastruktury Krytycznej Ministerstwa Cyfryzacji w głównej mierze poświecono zagrożeniom stwarzanym przez systemy bezzałogowe oraz zagadnieniom związanym z zabezpieczeniem fizycznym obiektów Infrastruktury Krytycznej.

Zarządzanie kryzysowe w zakresie cyberbezpieczeństwa

Zgodnie z art. 5a ust. 1 i 2 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym Rządowe Centrum Bezpieczeństwa (RCB) koordynuje przygotowanie Raportu o zagrożeniach bezpieczeństwa narodowego, który obejmuje zagrożenia cyberbezpieczeństwa mogące doprowadzić do sytuacji kryzysowej.

Zgodnie z art. 5 ust. 1 oraz art. 11 ust. 2 ww. ustawy RCB opracowuje i aktualizuje Krajowy Plan Zarządzania Kryzysowego (KPZK). W dokumencie tym uwzględniono m.in. zagrożenie funkcjonowania systemów i sieci teleinformatycznych. Scharakteryzowano zagrożenie, oszacowano skutki dla ludzi, mienia i środowiska oraz określono wartości ryzyka. Ponadto wskazano podmiot wiodący i współpracujący w przeciwdziałaniu i minimalizowaniu skutków jego wystąpienia. Natomiast zgodnie z art. 12 oraz art. 14 ust. 4 ww. ustawy - ministrowie, kierownicy urzędów centralnych i wojewodowie przygotowują plany zarządzania kryzysowego (uwzględniające również ww. zagrożenie), które stanowią załączniki funkcjonalne do KPZK. W 2023 r. RCB na bieżąco uzgadniało i opiniowało projekty tych planów.

RCB przygotowało nowelizację Narodowego Programu Ochrony Infrastruktury Krytycznej (NPOIK) w zakresie załącznika nr 2 - dobre praktyki. Uchwałą Rady Ministrów nr 23/2013

NPOIK został znowelizowany i przekazany do stosowania. W 2023 roku RCB zorganizowało dla operatów infrastruktury krytycznej dwa seminaria, których celem było promowanie dobrych praktyk w zakresie cyberbezpieczeństwa. W 2024 roku planowane są również dwa dwudniowe seminaria, poświęcone bezpieczeństwu systemów IT i OT. RCB poprzez proces zatwierdzania planów ochrony infrastruktury krytycznej kontroluje na bieżąco poziom bezpieczeństwa, w tym cyberbezpieczeństwa w podmiotach przemysłowych i technologicznych, które są operatorami IK.

RCB rozwijało także systemy teleinformatyczne na potrzeby zarządzania kryzysowego.

Europejski kodeks łączności elektronicznej

W 2023 r. Ministerstwo Cyfryzacji realizowało prace legislacyjne nad projektem ustawy Prawo komunikacji elektronicznej, wdrażającej w głównej mierze dyrektywę Parlamentu Europejskiego i Rady (UE) 2018/1972 z dnia 11 grudnia 2018 r. ustanawiającą Europejski kodeks łączności elektronicznej. Prace nad tym projektem nie zostały zakończone. W 2024 r. po rewizji przepisów wszczęto nowy proces legislacyjny względem projektu ustawy – Prawo komunikacji elektronicznej (UC 7) oraz projektu ustawy – Przepisy wprowadzające ustawę – Prawo komunikacji elektronicznej (UC 8). Celem regulacji jest m.in. zapewnienie podstaw prawnych do stabilnego funkcjonowania sieci i usług telekomunikacyjnych. W projekcie znalazły się regulacje przenoszące zapisy ustawy Prawo telekomunikacyjne obejmujące także zagadnienia związane z wykonywaniem przez przedsiębiorcę telekomunikacyjnego zadań i obowiązków na rzecz obronności, bezpieczeństwa państwa oraz bezpieczeństwa i porządku publicznego. W porównaniu do obecnie obowiązujących regulacji uległy doprecyzowaniu, udoskonaleniu celem zapewnienia efektywniejszego ich stosowania.

Plany działania przedsiębiorców telekomunikacyjnych w sytuacjach szczególnych zagrożeń

Ministerstwo Cyfryzacji w 2023 r. realizowało stałe zadanie w zakresie uzgadniania planów działania przedsiębiorców telekomunikacyjnych w sytuacjach szczególnych zagrożeń. Obowiązek sporządzenia planu i zakres uzgodnień wynika z art. 176a ust. 2 ustawy Prawo telekomunikacyjne oraz rozporządzenia Rady Ministrów z dnia 19 sierpnia 2020 r. w sprawie planu działań przedsiębiorcy telekomunikacyjnego w sytuacjach szczególnych. Posiadanie planu działań jest istotne z punktu widzenia potrzeby efektywnego reagowania na przypadki wystąpienia sytuacji kryzysowych, stanów nadzwyczajnych i bezpośrednich zagrożeń dla bezpieczeństwa lub integralności infrastruktury telekomunikacyjnej[9]. Zadanie to będzie kontynuowane w 2024 r.

W 2023 r. znowelizowano także rozporządzenie Rady Ministrów z dnia 19 sierpnia 2020 r. w sprawie planu działań przedsiębiorcy telekomunikacyjnego w sytuacjach szczególnych zagrożeń, z powodu uchylenia z dniem wejścia w życie ustawy z dnia 11 marca 2022 r. o obronie Ojczyzny, ustawy z dnia 23 sierpnia 2001 r. o organizowaniu zadań na rzecz obronności

[9] Z tego względu plan powinien zawierać, m.in. zasady współpracy z innymi przedsiębiorcami telekomunikacyjnymi, z podmiotami i służbami wykonującymi zadania w zakresie ratownictwa, niesienia pomocy ludności, a także zadania na rzecz obronności, bezpieczeństwa państwa oraz bezpieczeństwa i porządku publicznego; wykaz przygotowanych technicznych i organizacyjnych środków zapewnienia bezpieczeństwa i integralności infrastruktury telekomunikacyjnej i świadczonych usług, w tym ochrony przed wystąpieniem incydentów w rozumieniu ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa; opis sposobów utrzymania ciągłości świadczenia usług telekomunikacyjnych lub dostarczania sieci telekomunikacyjnej oraz ich odtworzenia w przypadku utraty możliwości świadczenia tych usług (ważne, w sytuacji świadczenia usług dla służb ratowniczych oraz wykonujących zadania na rzecz bezpieczeństwa i obronności państwa).

państwa realizowanych przez przedsiębiorców, a co za tym idzie wydanych na podstawie tej ustawy aktów wykonawczych. Fakt ten spowodował usunięcie z porządku prawnego wykazu przedsiębiorców o szczególnym znaczeniu gospodarczo-obronnym, którzy na podstawie decyzji i umów, wydawanych i zawieranych z właściwymi ministrami, byli zobligowani do realizowania zadań obronnych, a także mieli dodatkowe obowiązki w zakresie sporządzenia planu działań. Nowelizacja rozporządzenia zapewniła, że te dodatkowe obowiązki w zakresie planu zostały zaadresowane do przedsiębiorców realizujących zadania na rzecz Sił Zbrojnych, o których mowa w art. 648 ustawy z dnia 11 marca 2022 r. o obronie Ojczyzny. W ten sposób usunięto lukę prawną oraz zabezpieczono interes państwa w zakresie skuteczniejszej realizacji obowiązków przez tę szczególną kategorię przedsiębiorców telekomunikacyjnych.

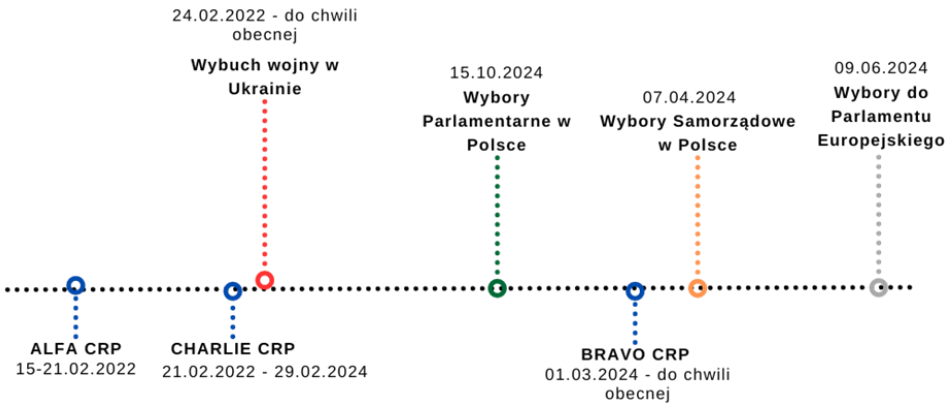
Ustawa o kryptoaktywach

Pod koniec 2023 r. Ministerstwo Finansów zaczęło prace nad sporządzeniem projektu ustawy o kryptoaktywach, która ma za zadanie zapewnienie stosowania przepisów Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2023/1114 z dnia 31 maja 2023 r. w sprawie rynków kryptoaktywów oraz zmiany rozporządzeń (UE) nr 1093/2010 i (UE) nr 1095/2010 oraz dyrektyw 2013/36/UE i (UE) 2019/1937 (tzw. Rozporządzenie MiCA). Rozporządzenie zostało opublikowane dnia 9.06.2023 r. oraz wprowadza ramy regulacyjne w zakresie rynku kryptoaktywów zapewniające m.in. bezpieczeństwo uczestników tego rynku oraz systemu finansowego. Biorąc pod uwagę cyfrową naturę regulowanych instrumentów rozporządzenie to ma wpływ na cyberbezpieczeństwo kraju.

2.2 Podniesienie poziomu odporności systemów informacyjnych administracji publicznej i sektora prywatnego oraz osiągnięcie zdolności do skutecznego zapobiegania i reagowania na incydenty

Stopnie alarmowe CRP

Od 21 lutego 2022 r. na terytorium Rzeczypospolitej Polskiej obowiązywał trzeci stopień alarmowy CHARLIE-CRP. Zgodnie z ustawą o działaniach antyterrorystycznych stopnie alarmowe CRP są wprowadzane przez Prezesa Rady Ministrów w przypadku zagrożenia wystąpieniem zdarzenia o charakterze terrorystycznym, dotyczącego systemów teleinformatycznych organów administracji publicznej lub systemów teleinformatycznych wchodzących w skład infrastruktury krytycznej albo w przypadku wystąpienia takiego zdarzenia. Stopień CHARLIE-CRP jest trzecim z czterech stopni alarmowych określonych w ustawie.



Stopnie alarmowe CRP wprowadzane w Polsce

Rozporządzenie Prezesa Rady Ministrów z dnia 25 lipca 2016 r. w sprawie zakresu przedsięwzięć wykonywanych w poszczególnych stopniach alarmowych i stopniach alarmowych CRP określa szczegółowe zakresy przedsięwzięć wykonywanych w ramach kompetencji ustawowych przez organy administracji publicznej oraz kierowników służb i instytucji właściwych w sprawach bezpieczeństwa i zarządzania kryzysowego w poszczególnych stopniach alarmowych CRP, w tym we współpracy z właścicielami, posiadaczami samoistnymi i posiadaczami zależnymi obiektów infrastruktury krytycznej w zakresie ochrony tych obiektów. Przy obowiązywaniu stopnia CHARLIE-CRP należy wykonać zadania przewidziane w rozporządzaniu dla stopni ALFA-CRP i BRAVO-CRP, ponadto należy wykonać w szczególności następujące zadania:

1) wprowadzić całodobowe dyżury administratorów systemów kluczowych dla funkcjonowania organizacji oraz personelu uprawnionego do podejmowania decyzji w sprawach bezpieczeństwa systemów;
2) dokonać przeglądu dostępnych zasobów zapasowych pod względem możliwości ich wykorzystania w przypadku zaistnienia ataku;
3) przygotować się do uruchomienia planów umożliwiających zachowanie ciągłości działania po wystąpieniu potencjalnego ataku, w tym:
    a) dokonać przeglądu i ewentualnego audytu planów awaryjnych oraz systemów,
    b) przygotować się do ograniczenia operacji na serwerach, w celu możliwości ich szybkiego i bezawaryjnego zamknięcia.

Od czasu wprowadzenia stopnia CHARLIE-CRP w lutym 2022 r. był on cyklicznie przedłużany. Od 1 marca 2024 r. stopień alarmowy CRP został obniżony do poziomu BRAVO.

Cyberbezpieczeństwo wyborów parlamentarnych w 2023 r.

Wiodącą rolę w zapewnieniu cyberbezpieczeństwa październikowych wyborów parlamentarnych odgrywała Agencja Bezpieczeństwa Wewnętrznego, zgodnie ze swoimi ustawowymi kompetencjami. W ramach działań mających na celu zabezpieczenie infrastruktury Krajowego Biura Wyborczego (KBW) Zespół CSIRT GOV funkcjonujący w strukturze ABW pod koniec 2022 r. rozpoczął współpracę z KBW mającą na celu weryfikację stanu bezpieczeństwa systemów i sieci teleinformatycznych wykorzystywanych w KBW. W ramach podjętej współpracy od początku maja 2023 r. prowadzona była ocena bezpieczeństwa, ze szczególnym uwzględnieniem tych systemów, które były wykorzystywane w procesie wyborczym. Dodatkowo Zespół CSIRT GOV przeprowadził cykl szkoleń z zakresu cyberbezpieczeństwa i higieny cyfrowej dla m.in. kadry kierowniczej KBW, członków Państwowej Komisji Wyborczej (PKW) oraz całego Zespołu Informatyki KBW. Ponadto w sieci KBW funkcjonują sondy narodowego systemu wczesnego ostrzegania o zagrożeniach pochodzących z sieci Internet - ARAKIS GOV, którego gestorem jest ABW. Działania związane z cyberbezpieczeństwem wyborów w odniesieniu do innych instytucji państwowych realizowane były w ramach ustawowych zadań ABW.

Działania związane z cyberbezpieczeństwem wyborów realizowane były także w ramach krajowego systemu cyberbezpieczeństwa, w tym m.in. w ramach Projektu Połączonego Centrum Operacyjnego Cyberbezpieczeństwa w zakresie wymiany informacji o zagrożeniach w cyberprzestrzeni, współpracy między CSIRT-ami i komórkami bezpieczeństwa instytucji biorących udział w PCOC. Sytuacja była stale monitorowana pod kątem ewentualnego występowania zagrożeń. Incydenty, które wystąpiły, były analizowane i na tej podstawie podejmowano odpowiednie środki prewencyjne. Należy także podkreślić, że w trakcie kampanii wyborczej i samych wyborów obowiązywał stopień alarmowy CHARLIE-CRP co wiązało się z

konkretnymi obowiązkami dla wielu podmiotów w zakresie bezpieczeństwa teleinformatycznego.

Realizowane były także zadania związane z osłoną informacyjną kampanii wyborczej trwającej w 2023 r. Ministerstwo Cyfryzacji udzieliło NASK-PIB dotacji celowej w wysokości 4 000 000 zł na realizację zadania publicznego pn. „Osłona informacyjna kampanii wyborczej 2023 r.". Zadanie było realizowane od 1 lipca do 31 grudnia 2023 r. Zadanie składało się z 3 głównych działań:

- Budowa portalu „bezpieczne wybory", związanego z wyborami do Sejmu i Senatu, który stanowił platformę do zgłaszania treści szkodliwych oraz był miejscem publikowania informacji oraz gromadzenia materiałów edukacyjnych.
- Monitoring mediów społecznościowych w zakresie rozpowszechnianej dezinformacji wyborczej. W ramach tego działania stworzona została m.in. baza profili z mediów społecznościowych publikujących treści dezinformujące związane z wyborami oraz dostosowano narzędzia do monitoringu mediów zgodnie ze specyfiką projektu (narzędzia, słowa kluczowe, zapytania itp.).
- Przygotowanie raportów (otwarcia i zamknięcia) zawierających opisy trendów w zakresie publikacji treści o charakterze szkodliwym. W ramach tego działania przygotowana została m.in. pogłębiona analiza publikacji z pierwszego miesiąca kampanii wyborczej pod kątem najpopularniejszych narracji dezinformujących.

SKR-Z

Resort cyfryzacji (ówcześnie w ramach KPRM) w 2021 r. zlecił NASK-PIB realizację zadania publicznego pn. „Budowa systemu łączności mobilnej umożliwiającej przetwarzanie informacji niejawnych do klauzuli „zastrzeżone" (SKR-Z) w oparciu o system CATEL". Zadanie zostało zrealizowane na podstawie umowy dotacji celowej i zakończyło się uruchomieniem produkcyjnym systemu SKR-Z.

W grudniu 2022 r. resort cyfryzacji zlecił NASK-PIB kontynuację rozbudowy systemu SKR-Z w ramach dotacji celowej z budżetu państwa, w ramach zadania publicznego na okres do końca 2024 r. Zadanie obejmuje zarówno utrzymanie systemu SKR-Z, jak i jego rozbudowę i rozwój.

System SKR-Z ma na celu ochronę informacji niejawnych z klauzulą „zastrzeżone", przetwarzanych w administracji publicznej oraz zapewnienie bezpiecznego systemu komunikacji do wymiany tych informacji i ograniczenie możliwości ich niepowołanego przejęcia. System ten stanie się docelowo częścią Sieci Komunikacji Rządowej i będzie zapewniał dostęp do kanału komunikacji niejawnej z klauzulą „zastrzeżone" osobom realizującym zadania publiczne oraz powiązane z cyberbezpieczeństwem.

Rozwój systemu SKR-Z przyczyni się bezpośrednio do:

- zwiększenia poziomu bezpieczeństwa informatycznego poprzez zapewnienie kluczowym interesariuszom narzędzi, które będą mogły być wykorzystywane do realizacji bezpiecznej wymiany informacji o klauzuli „zastrzeżone" i ograniczą możliwość ich niepowołanego przejęcia;
- umożliwienia szyfrowanej wymiany informacji na potrzeby podejmowania decyzji;
- skoordynowania działań i środków, w tym także w ramach działań w trybie zrządzania kryzysowego.

Ponadto Dowództwo Wojsk Obrony Cyberprzestrzeni przeprowadziło integrację infrastruktury CATEL z ST MILNET-Z oraz realizowało budowę resortowej wyspy CATEL RON (dla mobilnej komunikacji zastrzeżonej - projekt SmartWOC).

Bezpieczny komunikator

W 2022 r. resort cyfryzacji uruchomił aplikację Komunikator w celu zapewnienia bezpiecznej komunikacji rządowej i Krajowego Systemu Cyberbezpieczeństwa. Komunikator został uruchomiony w wersji mobilnej, webowej, dzięki najnowocześniejszemu szyfrowaniu „end to end" w obszarze komunikacji „jawnej".

Dzięki lokalnemu zarządzaniu zapewnia on bezpieczniejsze i w pełni kontrolowalne rozwiązanie, zarządzane i nadzorowane przez Ministerstwo Cyfryzacji, z powodzeniem wykorzystywane do celów służbowych w komunikacji służbowej przez pracowników administracji rządowej, samorządowej, w urzędach centralnych, instytutach badawczych, a także w sektorze służb mundurowych i organów państwa w kraju i za granicą. Aktualnie z Komunikatora korzysta kilka tysięcy użytkowników w skali kraju. Liczba ta stale rośnie, a system umożliwia udział nawet 10 tys. osób.

Komunikator jest dostępny jako aplikacja mobilna oraz przez przeglądarkę WWW i służy do prowadzenia szyfrowanych rozmów tekstowych, połączeń głosowych, połączeń wideo oraz do przesyłania multimediów.

Komunikator zapewnia:

- komunikację szyfrowaną „end-to-end" z wykorzystaniem kluczy szyfrujących rozmówców;
- ograniczenie dostępu do niektórych funkcjonalności aplikacji;
- zamkniętą listę kontaktów, która jest nadzorowana, weryfikowana i zarządzana przez administratora i same podmioty publiczne;
- możliwość dodatkowego, podwyższonego poziomu weryfikacji kontaktów.

W 2023 r. realizowany był dalszy rozwój aplikacji w zakresie funkcjonalności i liczby podłączonych użytkowników. Aplikacja wspiera codzienne działania operacyjne i ułatwia codzienną komunikację swoim użytkownikom.

Aplikacja jest stale monitorowana, audytowana i rozwijana zgodnie z aktualnymi standardami, praktykami i rekomendacjami w zakresie bezpieczeństwa aplikacji, m.in. zgodnie z wymaganiami ISO 27001 i całą rodziną ISO 27000 oraz OWASP Top 10 (ang. Open Web Application Security Project), ochrony danych osobowych oraz najlepszymi praktykami wypracowanymi przez Ministerstwo Cyfryzacji. Dzięki szyfrowaniu „end-to-end" jest to komunikacja w pełni bezpieczna.

W 2024 r. planowany jest dalszy rozwój funkcjonalności obu aplikacji, zwiększenie liczby użytkowników do 10 tys. w perspektywie do marca 2025, a także działania informacyjno-marketingowe w celu dalszej promocji tego rozwiązania wśród pracowników administracji rządowej.

Z kolei DKWOC na potrzeby resortu obrony narodowej uruchomiło użytkowo resortowy komunikator MERKURY 2.0.

AntyDDoS

DDoS (ang. Distributed Denial of Service) jest to atak na system komputerowy lub usługę w celu uniemożliwienia działania poprzez zajęcie wszystkich dostępnych zasobów lub pasma. Ataki te wykonywane są najczęściej przez zainfekowane komputery, nad którymi przejęto kontrolę przy użyciu szkodliwego oprogramowania. Ochrona przed atakami DDoS polega

na przekierowaniu całego ruchu skierowanego do serwisu objętego ochroną do centrum oczyszczania (tzw. Scrubbing Center), celem oddzielenia ruchu pożądanego od niepożądanego.

W obecnej sytuacji wzrostu zagrożenia atakami typu DDoS, mając na względzie krytyczne znaczenie realizowanych zadań publicznych, konieczne było wzmocnienie ochrony serwisów instytucji publicznych poprzez zapewnienie bezpiecznego i możliwie niezawodnego świadczenia usługi chmurowej ochrony przed atakami DDoS. W związku z tym Ministerstwo Cyfryzacji zleciło NASK-PIB realizację projektu AntyDDoS, którego celem jest zapewnienie ochrony przed tego typu atakami.

Dzięki tym działaniom na chwilę obecną osłonę przed atakami DDoS Ministerstwo Cyfryzacji zapewnia centralnie dla 67 instytucji, w tym np. także dla Sił Zbrojnych RP, służb specjalnych oraz urzędów centralnych.

Rozpoznawanie zagrożeń w cyberprzestrzeni

W 2023 r. Ministerstwo Cyfryzacji rozpoczęło postępowanie o udzielenie zamówienia publicznego dotyczącego pozyskania dostępu do platformy rozpoznawania zagrożeń w cyberprzestrzeni (Cyber Threat Intelligence, CTI) na poziom operacyjny na potrzeby Ministerstwa oraz siedmiu instytucji zapewniających bezpieczeństwo teleinformatyczne na poziomie krajowym. Wdrożenie systemu planowane jest w 2024 r.

Pozyskiwanie oraz przetwarzanie informacji dotyczących aktywności grup APT, stanowiących zagrożenie dla bezpieczeństwa państwa, jest konieczne do zapobiegania występowania incydentów oraz minimalizowania negatywnych skutków ich wystąpienia. Platforma CTI poziomu operacyjnego zostanie wykorzystana m.in. przez zespoły reagowania na incydenty komputerowe wchodzące w skład krajowego systemu cyberbezpieczeństwa. Będą to narzędzia umożliwiające znaczące podniesienie bezpieczeństwa polskiej cyberprzestrzeni poprzez między innymi:

- wykrycie przeprowadzenia planowanych ataków hakerskich;
- wykrycie wystąpienia incydentu komputerowego;
- śledzenie skutków wystąpienia incydentu oraz identyfikację ofiar danej kampanii;
- badanie głębokich zasobów Internetu (dark-web, deep-web) poprzez dostęp do zamkniętych forów zrzeszających cyberprzestępców;
- badanie mediów społecznościowych celem zbierania informacji o zagrożeniach w cyberprzestrzeni;
- wykrycie wycieku danych uwierzytelniających użytkowników oraz przeciwdziałanie ich nielegalnej sprzedaży;
- monitorowanie rejestracji domen wykorzystywanych w atakach phishingowych;
- pozyskiwanie informacji o taktykach, technikach oraz procedurach stosowanych przez adwersarzy;
- pozyskiwanie informacji o podatnościach na rozwiązania stosowane w systemach teleinformatycznych.

Pozyskanie platformy zostanie zrealizowane na rzecz podmiotów wchodzących w skład krajowego systemu cyberbezpieczeństwa, co w sposób znaczący przyczyni się do podniesienia bezpieczeństwa państwa oraz w konsekwencji sektora publicznego i prywatnego.

Rosnąca liczba cyberataków w Polsce i na świecie wskazuje na eskalację zagrożeń w sferze cyberprzestrzeni. Ataki te mogą powodować znaczne szkody finansowe, utratę danych, naruszenie prywatności. Wykorzystanie platformy CTI poziomu operacyjnego umożliwi

skuteczną i szybką reakcję na te zagrożenia i minimalizację potencjalnych strat. Pozyskanie rozwiązania to strategiczny krok, który pomoże utrzymać stabilność systemów teleinformatycznych w Polsce oraz w czasie rzeczywistym ochronić kluczowe zasoby przed atakami – również w zakresie funkcjonowania infrastruktury krytycznej państwa. Dodatkowo w kontekście wojny w Ukrainie i napiętej sytuacji geopolitycznej, istnieje zwiększone ryzyko cyberataków skierowanych przeciwko infrastrukturze naszego kraju – czego dowodem jest przedłużony kolejny raz podwyższony stopień alarmowy CRP. Natychmiastowe zaopatrzenie w rozwiązanie z zakresu CTI wzmocni zdolności do skutecznego śledzenia oraz przeciwdziałania zagrożeniom w cyberprzestrzeni.

Rozwój systemów teleinformatycznych

Instytucje krajowe rozwijały swoje systemy teleinformatyczne, w tym niejawne (m.in. Ministerstwo Spraw Wewnętrznych i Administracji i służby podległe pod MSWiA, Ministerstwo Finansów i inne). Wiązało się to nie tylko z kwestiami technicznymi i infrastrukturalnymi, ale także przeszkoleniem pracowników i zapewnieniem odpowiedniej kadry administrującej nimi.

Cyberbezpieczeństwo rejestrów państwowych i cyfrowych usług publicznych COI

Centralny Ośrodek Informatyki (COI) jest największą w kraju firmą realizującą projekty IT dla sektora publicznego. COI wykonuje zadania wyznaczane przez Ministerstwo Cyfryzacji, m.in. opracowuje cyfrowe usługi publiczne (m.in. mObywatel) oraz odpowiada za rejestry państwowe znajdujące się właściwości ministra właściwego ds. informatyzacji. W COI funkcjonuje zespół SOC monitorujący w trybie 24/7 bezpieczeństwo utrzymywanych systemów (w tym systemów powierzonych). Zespół ten ściśle współpracuje z CSIRT GOV i CSIRT NASK oraz stale podnosi zdolności do monitorowania i reagowania na incydenty poprzez wdrażanie nowych rozwiązań technologicznych oraz systemowych. Stale doskonali procedury operacyjne i playbooki związane z obsługą zdarzeń bezpieczeństwa.

Utrzymywane systemy przechodzą cykliczne testy ciągłości działania, mające na celu zweryfikowanie prawidłowości funkcjonowania systemu w przypadku wystąpienia sytuacji kryzysowej np. awarii, a także weryfikacji i doskonalenia działań poszczególnych zespołów.

Obecnie we wszystkie działania związane z budową i rozwojem utrzymywanych rozwiązań włączani są Architekci Bezpieczeństwa, tak aby zminimalizować możliwość wystąpienia słabości w tworzonym oprogramowaniu. Stanowi to element podejścia shift-left, którego celem jest włączenie w proces wytwórczy na jak najwcześniejszym etapie działań związanych z bezpieczeństwem. Zespół bezpieczeństwa COI raportuje wszystkie zdarzenia bezpieczeństwa do CSIRT GOV, CSIRT NASK oraz organu nadrzędnego - Ministerstwa Cyfryzacji. Ponadto COI uczestniczy w pracach nad dołączeniem do systemu analitycznego S46 wspierającego krajowy system cyberbezpieczeństwa.

W całym roku 2023 zrealizowano kilkaset testów bezpieczeństwa dotyczących badania infrastruktury i aplikacji utrzymywanych przez COI, w tym też Systemów Powierzonych. Prowadzono również technologiczno-biznesowe testy ciągłości. W ramach COI prowadzone były też szkolenia podnoszące świadomość wśród pracowników w obszarze SZBI oraz w obszarze zagrożeń w cyberprzestrzeni.

Ponadto COI uczestniczyło wraz z NASK-PIB w opracowaniu, wdrożeniu i utrzymaniu usługi bezpiecznedane.gov.pl, dzięki której obywatele mają możliwość weryfikowania ujawnienia danych w sytuacji ujawnionego wycieku informacji.

Narodowe Standardy Cyberbezpieczeństwa

W 2023 r. Ministerstwo Cyfryzacji opracowało i zamieściło w bazie wiedzy o cyberbezpieczeństwie na portalu gov.pl 10 rekomendacji w postaci Narodowych Standardów Cyberbezpieczeństwa dotyczących stosowania zalecanych środków bezpieczeństwa i ochrony prywatności w ramach skutecznego zarządzania ryzykiem, osiągania bezpieczeństwa w systemach informacyjnych oraz przetwarzania w chmurze. Ponadto, dokonano rewizji czterech Narodowych Standardów Cyberbezpieczeństwa wydając kolejne wersje tych publikacji. Dotychczas opublikowano już 39 Narodowych Standardów Cyberbezpieczeństwa w zakresie wymagań organizacyjno-technicznych rekomendujących rozwiązania bezpieczeństwa informacji.

BezpieczeneDane.gov.pl

W maju 2023 r. doszło do upublicznienia loginów i haseł części polskich użytkowników internetu w wyniku działania cyberprzestępców wykorzystujących złośliwe oprogramowanie instalowane na wykorzystywanych przez tych użytkowników urządzeniach. Ministerstwo Cyfryzacji we współpracy z NASK-PIB i COI uruchomiło portal BezpieczeDane.gov.pl, który umożliwia sprawdzenie przy wykorzystaniu prostej w użyciu wyszukiwarki, czy twoje dane mogły trafić w ręce cyberprzestępców. Serwis został później uzupełniony o informacje związane z innymi wyciekami, w tym głośnego wycieku, w ramach którego doszło do ujawniania danych wielu osób wykonujących badania w laboratoriach jednej z firm. Dzięki działaniu portalu BezpieczneDane.gov.pl możliwe jest ograniczenie negatywnych skutków wycieku danych polskich użytkowników internetu.

Ustawa o zwalczaniu nadużyć w komunikacji elektronicznej

W minionym roku weszły w życie przepisy opracowanej przez Ministerstwo Cyfryzacji ustawy z dnia 28 lipca 2023 r. o zwalczaniu nadużyć w komunikacji elektronicznej, mającej na celu zwiększenie ochrony użytkowników przed szkodliwymi działaniami dokonywanymi za pośrednictwem technologii komunikacyjnych. Na jej podstawie m.in. przedsiębiorcy telekomunikacyjni zostali zobowiązani do przeciwdziałania nadużyciom za pomocą różnorakich środków organizacyjnych i technicznych np. poprzez blokowanie SMS-ów, zawierających treści wyczerpujące znamiona smishingu oraz połączeń głosowych, których celem jest podszywanie się pod inną osobę lub instytucję.

Nowe przepisy mają na celu zwiększenie ochrony użytkowników przed szkodliwymi działaniami dokonywanymi za pośrednictwem technologii komunikacyjnych, w szczególności przed tzw. Caller ID (CLI) spoofingiem i smishingiem. Ustawa o zwalczaniu nadużyć w komunikacji elektronicznej ma za zadanie stworzyć mechanizmy, które pozwolą na ograniczenie tych niekorzystnych zjawisk. Z tego względu, nowe obowiązki zostały nałożone przede wszystkim na przedsiębiorców telekomunikacyjnych, dostawców poczty elektronicznej i podmioty publiczne. Szczególną rolę w realizacji ustawowych zadań ma odegrać CSIRT NASK.

Ramowy Program Cyberbezpieczeństwa Resortu Finansów

Opracowano Ramowy Program Cyberbezpieczeństwa Resortu Finansów, w tym m.in.: przeprowadzono ocenę obecnego stopnia dojrzałości Resortu Finansów w zakresie cyberbezpieczeństwa w oparciu o standard NIST CSF, zidentyfikowano obszary w RF wymagające naprawy i wskazano rekomendowane działania do podjęcia w celu podniesienia poziomu cyberbezpieczeństwa oraz uzgodniono priorytety i sposób wdrożenia rekomendacji.

W Ministerstwie Finansów ustanowiono także Pełnomocnika do spraw cyberbezpieczeństwa.

2.3 Zwiększenie potencjału narodowego w zakresie technologii cyberbezpieczeństwa

Krajowe Centrum Kompetencji Cyberbezpieczeństwa

W 2023 r. Ministerstwo Cyfryzacji kontynuowało realizację zadań polskiego Krajowego Ośrodka Koordynacji (NCC-PL) w rozumieniu Rozporządzenia Parlamentu Europejskiego i Rady (UE) 2021/887 z dnia 20 maja 2021 r. *ustanawiającego Europejskie Centrum Kompetencji Przemysłowych, Technologicznych i Badawczych w dziedzinie Cyberbezpieczeństwa oraz sieć krajowych ośrodków koordynacji*.

Celem tych działań było wspieranie rozwoju polskich podmiotów działających w obszarze cyberbezpieczeństwa, polegały one w szczególności na:

- Udzielaniu pomocy technicznej podmiotom zainteresowanym aplikowaniem o granty z Programu Cyfrowa Europa (DEP) na dofinansowanie swoich projektów w obszarze cyberbezpieczeństwa – poprzez bezpośrednie przekazywanie informacji i udzielanie odpowiedzi na pytania, publikowanie informacji na stronie internetowej, udzielanie pomocy przy tworzeniu międzynarodowych konsorcjów projektowych;
- Organizacji wydarzenia matchmakingowego Access2Market, którego celem było wsparcie polskich małych i średnich przedsiębiorców oferujących rozwiązania w obszarze cyberbezpieczeństwa - wydarzenie to, zorganizowane w dniu 22 czerwca 2023 r. podczas Cybersec Forum/Expo 2023 przez ECCC, NCC-PL, Instytut Kościuszki i Polski Klaster Cyberbezpieczeństwa przy wsparciu zespołu projektowego ECCO, umożliwiło spotkanie i nawiązanie kontaktów biznesowych pomiędzy tymi przedsiębiorcami a potencjalnymi odbiorcami ich rozwiązań i inwestorami;
- Dalszym rozwijaniu działalności NCC-PL zgodnie z katalogiem zadań przewidzianym w Rozporządzeniu 2021/887, poprzez ubieganie się (z wynikiem pozytywnym)

o grant z DEP – podpisanie umowy grantowej z Komisją Europejską nastąpiło w dniu 14 grudnia 2023 r. W ramach projektu planowane jest również udzielenie grantów małym i średnim przedsiębiorcom działającym w obszarze cyberbezpieczeństwa. Realizacja projektu rozpoczęła się w styczniu 2024 r. i jest planowana na 2024 i 2025 r.;

- Udziale w pracach koordynowanych przez Europejskie Centrum Kompetencji Przemysłowych, Technologicznych i Badawczych w dziedzinie Cyberbezpieczeństwa (ECCC) i Komisję Europejską: organizacja posiedzenia Rady Zarządzającej ECCC oraz spotkania sieci Krajowych Ośrodków Koordynacji w dniach 15-17 marca 2023 r. w Warszawie, udział w pracach Grup Roboczych ECCC w obszarach określenia kierunków strategicznych i planu działań ECCC, rozwoju kompetencji w obszarze cyberbezpieczeństwa, budowania Społeczności kompetentnej w zakresie cyberbezpieczeństwa.

Certyfikacja w cyberbezpieczeństwie

W 2023 r. Ministerstwo Cyfryzacji zleciło realizację zadania pn. „Wsparcie funkcjonowania, rozwoju i wykonywania zadań Uczestnika oraz akredytowanej Jednostki Certyfikującej spełniającej wymagania". NASK-PIB w ramach udzielonej dotacji realizował zadania na poziomie operacyjnym, polegające na wykonywaniu w imieniu Rządu RP zadań Uczestnika w ramach Umowy o wzajemnym uznawaniu certyfikatów oceny bezpieczeństwa teleinformatycznego oraz w ramach Porozumienia o sprawie uznawania Certyfikatów Common Criteria w dziedzinie bezpieczeństwa teleinformatycznego, a także wykonywaniu zadań Jednostki Certyfikującej Spełniającej Wymagania (ang. *Compliant Certification Body*), odpowiedzialnej za zarządzanie Programem Oceny i Certyfikacji Bezpieczeństwa IT oraz za autoryzację laboratoriów badawczych.

CYBERSECIDENT

Ministerstwo Cyfryzacji prowadziło związane z realizacją programu CYBERSECIDENT „Cyberbezpieczeństwo i eTożsamość", którego celem jest wytwarzanie rozwiązań nakierowanych na podniesienie poziomu bezpieczeństwa cyberprzestrzeni RP. Zadania te polegały na koordynacji procesu zawierania umów, w wyniku których Minister Cyfryzacji nabył autorskie prawa majątkowe do rozwiązań w obszarze cyberbezpieczeństwa wypracowanych w ramach programu, a także procesu udzielania wykonawcy projektu licencji na ww. rozwiązania.

Program Współpracy w Cyberbezpieczeństwie (PWCyber)

Ministerstwo Cyfryzacji kontynuowało rozwój współpracy o charakterze partnerstwa publiczno-prywatnego w ramach programu Program Współpracy w Cyberbezpieczeństwie (PWCyber) uruchomionego w 2019 r. W 2023 r. do PWCyber dołączyło 14 nowych partnerów. Na koniec roku 2023 w ramach Programu współpracowało łącznie 38 firm technologicznych (polskich i zagranicznych) oraz organizacji.

Kluczowym obszarem współpracy w ramach partnerstwa jest podnoszenie kompetencji podmiotów krajowego systemu cyberbezpieczeństwa w zakresie świadomości zagrożeń, metod ataków w cyberprzestrzeni oraz prawnych, organizacyjnych i technicznych umiejętności przeciwdziałania zagrożeniom w systemach i sieciach teleinformatycznych. Od początku uruchomienia Programu w ramach szkoleń organizowanych przez partnerów PWCyber przeszkolono blisko 20 tys. przedstawicieli podmiotów krajowego systemu

Cyberbezpieczeństwa. Wspólnie z partnerami Programu w 2023 r. zorganizowano 17 szkoleń online dla kadr podmiotów krajowego systemu cyberbezpieczeństwa, a także rozpoczęto cykl szkoleń dla podmiotów publicznych realizujących działalność leczniczą.

Partnerzy Programu o przyszłości programu dyskutowali podczas V Forum Cyberbezpieczeństwa organizowanego w ramach XXXII Forum Ekonomicznego w Karpaczu. Spotkanie było okazją do podsumowania dotychczasowej współpracy oraz dyskusji o rozwoju programu. Partnerzy PWCyber dzielili się swoimi doświadczeniami ze współpracy z podmiotami publicznymi w kraju i za granicą, a także oczekiwaniami, jakie mogłyby zostać zaadresowane w programie na rzecz podnoszenia bezpieczeństwa krajowego systemu cyberbezpieczeństwa.

W 2023 r. w ramach współpracy z partnerami Programu zorganizowano 4 warsztaty eksperckie z:

- IBM Polska Sp. z o.o. oraz Sevenet S.A. w dniu 27 czerwca w siedzibie IBM Polska w Warszawie, udział w nim wzięli przedstawiciele kadry kierowniczej odpowiadającej za cyberbezpieczeństwo w Ministerstwie Cyfryzacji, Ministerstwie Klimatu i Środowiska, Ministerstwie Infrastruktury, Komisji Nadzoru Finansowego, Urzędzie Komunikacji Elektronicznej oraz w Urzędzie Transportu Kolejowego. Głównym celem spotkania było omówienie budowy sektorowych zespołów CSIRT.
- Amazon Web Services (AWS) w dniu 27 września w siedzibie Ministerstwa Cyfryzacji - zaawansowane 4-godzinne warsztaty techniczne Tabletop Exercises w jaki sposób można udoskonalić proces reagowania na incydent w organizacji.
- AWS w dniach 9-13 października w siedzibie AWS warsztaty z zakresu zarządzania infrastrukturą organizacji w chmurze AWS i poszczególnymi usługami oferowanymi przez firmę.
- AWS w dniach 7-9 listopada w siedzibie AWS w USA odbyła się wizyta studyjna. Uczestniczyli w niej eksperci Ministerstwa Cyfryzacji oraz NASK. Program wizyty uwzględniał zarówno kwestie techniczne, jak i te związane z najlepszymi praktykami oraz zapewnianiem zgodności z normami i rekomendacjami w aspekcie rozwiązań chmurowych.

Dodatkowo przy współpracy z firmą AWS rozpoznano możliwości technologiczne związane m.in z zagadnieniami dot. confidential computing - usług gwarantujących bezpieczeństwo przetwarzania danych w modelu uniemożliwiającym odczyt danych przez administratorów, czy też samej specyfiki zarządzania chmurą i budowaniu infrastruktury z wykorzystaniem gotowych usług. Tym sposobem PWCyber umożliwia przygotowanie pracowników do wyzwań technologicznych, które cyklicznie się pojawiają, a kompetencje w ich zakresie są i będą niezbędne.

Partnerzy Programu są zaangażowani w rozwijanie współpracy. Prowadzenie wspólnych działań w dynamicznie zmieniającym się środowisku technologicznym otwiera przed sektorem publicznym nowe możliwości związane z gromadzeniem eksperckiej wiedzy i doświadczeń. Współpraca w ramach programu PWCyber przynosi pozytywne rezultaty w postaci rozwoju kompetencji w zakresie cyberbezpieczeństwa oraz promowania nowych rozwiązań w sektorze publicznym. Beneficjentami wspólnych działań są m.in.: jednostki administracji państwowej, jednostki samorządu terytorialnego, urzędy, szpitale i placówki ochrony zdrowia oraz pracujący w nich specjaliści IT.

W 2024 r. przypada jubileusz 5-lecia funkcjonowania Programu PWCyber. W ramach obchodów zaplanowano konferencję podsumowującą dotychczasowe działania i ogłoszenie kolejnych kierunków rozwoju Programu.

Swój program współpracy między sektorem publicznym i prywatnym realizowało także DKWOC. W ramach tych działań uczestniczono w spotkaniach technicznych z udziałem

przedstawicieli przemysłu i sektora publicznego na arenie krajowej i międzynarodowej, brano udział w realizacji badań naukowych w obszarze cyberbezpieczeństwa na poziomie krajowym oraz międzynarodowym, jak również realizowano współpracę w zakresie podniesienia poziomu cyberbezpieczeństwa RP na podstawienie podpisanych porozumień o współpracy.

Projekt PIONIER-Q w ramach European Quantum Communication Infrastructure

Projekt PIONIER-Q jest oficjalnym wkładem Polski do europejskiej inicjatywy - European Quantum Communication Infrastructure (EuroQCI[10]) uruchomionej w 2019 roku. EuroQCI będzie bezpieczną infrastrukturą łączności kwantowej obejmującą całą UE.

Komisja Europejska współpracuje ze wszystkimi 27 państwami członkowskimi UE oraz Europejską Agencją Kosmiczną (ESA) w celu zaprojektowania, opracowania i wdrożenia EuroQCI, który będzie składał się z segmentu naziemnego opartego na sieciach łączności światłowodowej, łączących strategiczne obiekty na poziomie krajowym i transgranicznym oraz segmentu kosmicznego opartego na satelitach. Będzie ona integralną częścią IRIS[211], nowego unijnego systemu bezpiecznej komunikacji opartej na przestrzeni kosmicznej. EuroQCI będzie chronić wrażliwe dane i infrastrukturę krytyczną poprzez integrację systemów kwantowych z istniejącą infrastrukturą komunikacyjną, zapewniając dodatkową warstwę bezpieczeństwa opartą na fizyce kwantowej. Wzmocni ochronę europejskich instytucji rządowych, ich centrów danych, szpitali, sieci energetycznych i innych.

Realizacja projektu PIONIER-Q jest kluczowym elementem dla efektywnego udziału Polski w tej inicjatywie. W ramach Projektu zostanie uruchomiona infrastruktura oraz usługi związane z generowaniem oraz przesyłaniem kluczy w technologii kwantowej dystrybucji kluczy (QKD – Quantum Key Distribution). Jest to metoda bezpiecznego generowania oraz dystrybucji kluczy oparta na zasadach mechaniki kwantowej, które następnie mogą zostać wykorzystane np. do szyfrowania danych lub uwierzytelniania usług i użytkowników. Technologia QKD może zostać wykorzystana w aktualnych algorytmach do symetrycznego szyfrowania danych lub do przyszłych rozwiązań algorytmów szyfrowania danych typu post quantum, będących aktualnie przedmiotem standaryzacji. Sieci komunikacji kwantowej są potencjalnym elementem do łączenia oraz skalowania infrastruktur obliczeń kwantowych. Długofalowym celem projektu jest wypracowanie rozwiązań oraz zbudowanie fundamentów pod sieci bezpiecznej komunikacji między innymi dla jednostek administracji lokalnej, centralnej oraz na poziomie transgranicznym (pomiędzy państwami członkowskimi i instytucjami UE). Dotyczy to zarówno komunikacji w segmencie naziemnym, jak i satelitarnym.

W grudniu 2023 r. Prezes Rady Ministrów powierzył Konsorcjum PIONIER-Q realizację zadania z zakresu informatyzacji sektora publicznego oraz innowacji cyfrowych, polegającego na utrzymaniu zdolności zleceniobiorców do realizacji projektu pn. „PIONIER-Q: Ogólnopolska Kwantowa Infrastruktura Komunikacyjna", będącego wkładem Polski do inicjatywy EuroQCI – budowy europejskiej infrastruktury komunikacji kwantowej. Po stronie rządowej działania w tym zakresie realizowane są przez Ministerstwo Cyfryzacji.

W skład Konsorcjum PIONIER-Q wchodzą:

- Poznańskie Centrum Superkomputerowo-Sieciowe
- Akademickie Centrum Komputerowe Cyfronet AGH

[10] https://digital-strategy.ec.europa.eu/pl/policies/european-quantum-communication-infrastructure-euroqci
[11] https://defence-industry-space.ec.europa.eu/eu-space-policy/iris2_en

- Interdyscyplinarne Centrum Modelowania Matematycznego i Komputerowego
- Naukowa i Akademicka Sieć Komputerowa - Państwowy Instytut Badawczy
- Centrum Informatyczne TASK
- Wrocławskie Centrum Sieciowo-Superkomputerowe

Ministerstwo Cyfryzacji współfinansuje projekt PIONIER-Q w wysokości 25%.

Narodowe Centrum Badań i Rozwoju

Powstałe w 2007 r. Narodowe Centrum Badań i Rozwoju jest pierwszą polską rządową agencją wykonawczą powołaną do realizowania zadań z zakresu polityki naukowej, naukowo-technicznej i innowacyjnej państwa. W ramach NCBR realizowane są także projekty badawczo-rozwojowe dotyczące cyfryzacji oraz cyberbezpieczeństwa.

KONKURSY NCBR:

- SMART Konsorcja

W listopadzie 2023 r. ogłoszony został konkurs SMART Konsorcja, gdzie w ramach Modułu Cyfryzacja możliwe jest uzyskanie dofinansowania na realizację inwestycji związanych z zastosowaniem rozwiązań cyfrowych w przedsiębiorstwie, zmierzających do cyfryzacji produkcji, procesów w przedsiębiorstwie, jak i cyfryzacji produktów, usług, modelu biznesowego oraz zapewnienia cyberbezpieczeństwa.

- Ścieżka SMART na rzecz dostępności

W ramach Ścieżki SMART na rzecz dostępności (nabór FENG.01.01-IP.01-003/23 zakończony w listopadzie 2023 r.), w ramach Modułu Cyfryzacja, możliwe jest uzyskanie dofinansowania na realizację inwestycji związanych z zastosowaniem rozwiązań cyfrowych w przedsiębiorstwie zmierzających do cyfryzacji produkcji, procesów w przedsiębiorstwie, jak i cyfryzacji produktów, usług, modelu biznesowego oraz zapewnienia cyberbezpieczeństwa.

- Ścieżka SMART

W ramach Ścieżki SMART (nabór FENG.01.01-IP.01-002/23 zakończony w listopadzie 2023 r.) aspekt cyberbezpieczeństwa również został uwzględniony.

- INFOSTRATEG

W 2023 r. ogłoszono też VI i VII edycję konkursu INFOSTRATEG. Program INFOSTRATEG został przygotowany, by wspierać rozwój polskiego potencjału sztucznej inteligencji (SI) poprzez

opracowanie rozwiązań wykorzystujących sztuczną inteligencję i blockchain, mających bezpośrednie zastosowanie w praktyce.

- XI polsko-tajwański konkurs

W minionym roku ogłoszono również XI polsko-tajwański konkurs. Był on skierowany do organizacji badawczych i innowacyjnych przedsiębiorstw z Polski i Tajwanu. Konsorcja złożone z partnerów polskich i tajwańskich miały możliwość uzyskania w konkursie dofinansowania na aplikacyjne projekty badawcze trwające maksymalnie trzy lata. Projekty mogły obejmować badania w obszarach, m. in., neuronauki, efektywności energetycznej, inżynierii materiałowej, inteligentnego transportu, technologii kwantowej, cyberbezpieczeństwa, badań kosmicznych i półprzewodników.

- Program TEF AI

Zakres tematyczny obejmuje współfinansowanie utworzenia i funkcjonowania Centrów testów i eksperymentowania technologicznego sztucznej Inteligencji (TEF AI); usługi TEF AI, które mają w szczególności umożliwić przedsiębiorcom z grupy MŚP eksperymentowanie, testowanie oraz walidację rozwiązań AI zarówno w środowisku wirtualnym jak i rzeczywistym.

Ponadto, również w ramach programów strategicznych, ustanowionych i realizowanych przez NCBR, tematyka cyberbezpieczeństwa stanowi ważny obszar.

REALIZOWANE PROJEKTY NCBR

W 2023 r. w zakresie cyberbezpieczeństwa realizowano projekt opracowania nowej wersji cyberpoligonu umożliwiającej symulowanie cyberataków z wykorzystaniem agenta sztucznej inteligencji w celu zidentyfikowania luk w systemie i sieci dla poprawy poziomu bezpieczeństwa infrastruktury komputerowej (IT i OT) i podniesienia kompetencji zespołów odpowiedzialnych za nią.

Wartość ogółem: 9 722 007,54 zł

Data rozpoczęcia realizacji: 01.01.2023

Data zakończenia realizacji: 31.12.2023

Nazwa beneficjenta: CDEX PSA

Szkolnictwo wyższe

Dane w Zintegrowanym Systemie Informacji o Szkolnictwie Wyższym i Nauce POL-on wskazują, że uczelnie dostrzegają potrzebę kształcenia studentów w obszarze cyberbezpieczeństwa. W 2023 r. uczelnie prowadziły m.in. następujące kierunki dot. cyberbezpieczeństwa: "Bezpieczeństwo w cyberprzestrzeni", "Cyberbezpieczeństwo", "Informatyka i cyberbezpieczeństwo", "Inżynieria cyberprzestrzeni", "IT Cyber Security", "Kryptologia i cyberbezpieczeństwo" i "Master of Business Administration MBA - Cyberbezpieczeństwo i compliance".

Doktorat wdrożeniowy

W 2023 r. kontynuowano program Ministerstwa Nauki i Szkolnictwa Wyższego "Doktorat wdrożeniowy", którego przedmiotem jest tworzenie warunków do rozwoju współpracy podmiotów systemu szkolnictwa wyższego i nauki z otoczeniem społeczno-gospodarczym, prowadzonej w ramach szkół doktorskich i polegającej na kształceniu doktorantów we współpracy z zatrudniającymi ich przedsiębiorcami albo innymi podmiotami, której efektem będzie wdrażanie w tych podmiotach wyników prowadzonej przez doktorantów działalności naukowej. W roku 2023 było realizowanych 11 projektów badawczych z zakresu

cyberbezpieczeństwa. Odbyła się 1 obrona rozprawy doktorskiej. W roku 2023 rozpoczęła się realizacja 1 nowego projektu badawczego w powyższym zakresie.

Projekty badawcze i rozwojowe resortu obrony narodowej

DKWOC prowadził nadzór nad realizacją badań pk. MIKOK, OptoKrypt i APQ finansowanych przez NCBR. Głównymi celami realizacji tych przedsięwzięć są:

- budowa modułowej infrastruktury komputera kwantowego (MIKOK),
- budowa urządzenia realizującego kwantową wymianę klucza i generatora kwantowego oraz kodowania fazowego do ochrony transmisji (OptoKrypt),
- opracowanie algorytmów postkwantowych szyfrowania, podpisu cyfrowego i uzgadniania klucza (APQ).

Wymienione przedsięwzięcia uruchomiono w celu opracowania nowych metod zabezpieczenia danych z uwzględnieniem zagrożeń związanych z powstaniem komputerów kwantowych oraz rozwoju technologicznego w zakresie budowy komputera kwantowego.

Resort obrony narodowej realizował także projekty związane z łącznością. Natomiast do projektów odnoszących bezpośrednio do cyberbezpieczeństwa można zaliczyć projekt "Badanie podatności radiostacji na ofensywne działania w cyberprzestrzeni" realizowany przez Wojskowy Instytut Łączności (WIŁ) w ramach umowy na wykonywanie w 2023 roku zadań na rzecz Sił Zbrojnych nałożonych przez Ministra Obrony Narodowej. Ponadto WIŁ realizował także własne tematy badawcze dotyczące m.in. bezpieczeństwa elektromagnetycznego technologii NFC czy technologii kwantowych.

Projekt Krajowego planu działania do programu polityki „Droga ku cyfrowej dekadzie" do 2030 r.

Ministerstwo Cyfryzacji, we współpracy z właściwymi interesariuszami na poziomie krajowym, opracowało projekt Krajowego planu działania do programu polityki „Droga ku cyfrowej dekadzie" do 2030 r. Konieczność przygotowania ww. dokumentu wynika z Decyzji Parlamentu Europejskiego i Rady (UE) 2022/2481 z dnia 14 grudnia 2022 r. ustanawiająca program polityki „Droga ku cyfrowej dekadzie" do 2030 r., która wyznacza konkretne cele ogólne i cyfrowe na poziomie UE oraz jednocześnie zobowiązała kraje członkowskie UE do przedłożenia Komisji krajowych planów działania. Obecny projekt Krajowego planu działania jest owocem współpracy z jednostkami administracji rządowej, a także ze stroną społeczną (organizacjami pozarządowymi, przedsiębiorcami i obywatelami).

Projekt Krajowego planu wskazuje m.in. na wdrożone i planowane polityki, interwencje i działania, które Polska zobowiązuje się podjąć w celu przyśpieszenia transformacji cyfrowej, zmierzając do osiągnięcia celów ogólnych i celów cyfrowych programu polityki „Droga ku cyfrowej dekadzie" do 2030 r. Jednym z celów ogólnych ww. programu polityki jest poprawa odporności na cyberataki, przyczynianie się do zwiększenia świadomości ryzyka oraz szerzenia wiedzy na temat procedur cyberbezpieczeństwa, przy intensyfikacji wysiłków organizacji publicznych i prywatnych na rzecz osiągnięcia co najmniej podstawowego poziomu cyberbezpieczeństwa.

Z uwagi na międzyresortowy charakter projektu Krajowego planu i działań w nim wskazanych przyjęcie dokumentu wymaga podjęcia uchwały przez Radę Ministrów. Na obecnym etapie projekt Krajowego planu nie został jeszcze przyjęty na poziomie krajowym.

Prace nad dokumentem strategicznym w dziedzinie informatyzacji

Ministerstwo Cyfryzacji prowadzi prace nad dokumentem o charakterze strategicznym w dziedzinie informatyzacji, zwanym dalej „Strategią informatyzacji". Podstawę prawną dla dokumentu będzie stanowić art. 12aa-12ad ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne. Przepisy stanowiące podstawę prawną dla Strategii informatyzacji zostały zamieszczone w projekcie ustawy, który zgodnie z harmonogramem zostanie zgłoszony do wykazu prac legislacyjnych i programowych Rady Ministrów w I kwartale 2024 r. Wejście w życie przepisów ustawy planuje się na IV kwartał 2024 r.

Strategia informatyzacji będzie uwzględniała m.in. wizję informatyzacji państwa, cele i priorytety informatyzacji oraz środki służące ich realizacji, a także możliwości finansowania projektowanych działań. Głównymi priorytetami Strategii informatyzacji będą: telekomunikacja i 5G, cyberbezpieczeństwo, kompetencje cyfrowe, e-administracja oraz lepsza koordynacja cyfryzacji. W celu realizacji Strategii informatyzacji, minister kierujący działem administracji rządowej będzie mógł powołać pełnomocnika do spraw informatyzacji, którego podstawowymi zadaniami będzie koordynacja realizacji strategii, nadzorowanie jej wdrażania oraz diagnozowanie obszaru koniecznych zmian w zakresie działu.

Pomiary jakości i dostępności sygnałów globalnych systemów nawigacji satelitarnej (GNSS)

W ramach umowy dotacji celowej zawartej pomiędzy Ministrem Cyfryzacji a Instytutem Łączności-Państwowym Instytutem Badawczym (IŁ-PIB), w 2023 r. IŁ-PIB przeprowadził m.in. pomiary jakości i dostępności sygnałów globalnych systemów nawigacji satelitarnej (GNSS), ze szczególnym uwzględnieniem unijnego systemu Galileo, w różnych środowiskach propagacyjnych w Polsce. Istotnym aspektem testów było sprawdzenie występowania celowych zakłóceń sygnałów GNSS. W tym celu przeprowadzona została dedykowana kampania pomiarowa w pobliżu wschodniej granicy Polski. Przeprowadzone badania wykazały jednoznacznie obecność zakłóceń w pasmach GNSS, których kierunek wskazywał na lokalizację po stronie białoruskiej. W 2024 r. planowana jest kontynuacja monitorowania jakości usług

systemów GNSS. Dodatkowo planowane jest opracowanie koncepcji sondy do monitorowania zakłóceń (interferencji) w zakresach częstotliwości wykorzystywanych przez system Galileo, co w kolejnych latach umożliwi budowę rozproszonego na terytorium RP systemu wczesnego ostrzegania przed wrogim jammingiem i spoofingiem GNSS.

Analiza ryzyk dla ochrony danych i prywatności związanych korzystaniem z komercyjnych usług cyfrowych

W wyniku ogłoszonego przez Ministerstwo Cyfryzacji przetargu nieograniczonego i zawartej umowy z wykonawcą sporządzona została analiza prawna dotycząca ryzyk odnoszących się do ochrony danych i prywatności, jakie wiążą się z korzystaniem z komercyjnych usług cyfrowych, w tym korzystaniem z usług komunikacji elektronicznej, usług świadczonych drogą elektroniczną, serwisów społecznościowych, sklepów internetowych, platform streamingowych, usług w chmurze, z uwzględnieniem obecnych na rynku usług i przewidywanych kierunków ich rozwoju oraz przedstawienia działań zmierzających do niwelowania tych ryzyk. Wykonana analiza pozwoli na tworzenie regulacji lepiej chroniących użytkowników oraz skuteczniejsze egzekwowanie ich stosowania. Działania te przełożą się zarówno na poprawę bezpieczeństwa danych użytkowników w sieci, jak i umocnią budowę społeczeństwa informacyjnego.

Zwalczanie niegodziwego traktowania dzieci w celach seksualnych w Internecie

Ministerstwo Cyfryzacji uczestniczyło w pracach Grupy Roboczej Rady UE ds. Egzekwowania Prawa (LEWP) w zakresie opiniowania projektu rozporządzenia Parlamentu Europejskiego i Rady zmieniającego rozporządzenie Parlamentu Europejskiego i Rady (UE) 2021/1232 w sprawie tymczasowego odstępstwa od niektórych przepisów dyrektywy 2002/58/WE w celu zwalczania niegodziwego traktowania dzieci w celach seksualnych w Internecie. Nowelizacja zakładała wydłużenie o dwa lata, tj. do 3 sierpnia 2026 r., okresu obowiązywania rozporządzenia 2021/1232. W pozostałym zakresie nie zmieniła przepisów tego aktu. Zgodnie z obecnymi regulacjami rozporządzenie 2021/1232 obowiązuje do dnia 3 sierpnia 2024 r. Przedłużenie obowiązywania tymczasowych regulacji umożliwi dalsze stosowanie przepisów dotyczących wykrywania i usuwania pornografii dziecięcej, wykrywania praktyk nagabywania dzieci w Internecie w celach pedofilskich do czasu uchwalenia docelowych, długookresowych przepisów unijnych dotyczących ochrony dzieci przed niegodziwym traktowaniem w celach seksualnych w Internecie.

Obecnie w instytucjach unijnych trwają prace nad takimi docelowymi przepisami. Ze względu jednak na złożoność tej tematyki nie ma pewności, czy zakończą się w terminie gwarantującym wejście w życie rozporządzenia długoterminowego przed wygaśnięciem rozporządzenia przejściowego. Wygaśnięcie rozporządzenia 2021/1232 przed wejściem w życie docelowych regulacji, uniemożliwi zgodną z prawem i skuteczną ochronę najmłodszych użytkowników sieci Internet. Z tego względu Komisja Europejska przedstawiła projekt przedłużający stosowanie obecnych regulacji. Ministerstwo Cyfryzacji przygotowało projekt stanowiska Rządu, które następnie zostało przyjęte dnia 29 grudnia 2023 r. przez KSE.

W 2023 r. przygotowano ponadto dla Komisji Europejskiej, na podstawie art. 8 rozporządzenia 2021/1232, sprawozdanie w sprawie wykrytych przypadków niegodziwego traktowania dzieci w celach seksualnych w internecie. W 2024 r. planowane jest przekazanie kolejnej informacji dla Komisji.

Ogólnopolska Sieć Edukacyjna

W 2023 r. swoje funkcjonowanie kontynuowała Ogólnopolska Sieć Edukacyjna (OSE). Jest to program funkcjonujący na mocy ustawy z dnia 27 października 2017 r. o Ogólnopolskiej Sieci Edukacyjnej. Zgodnie z ustawą OSE jest publiczną siecią telekomunikacyjną, dzięki której szkoły otrzymują nieodpłatny dostęp do szybkiego Internetu wraz z usługami bezpieczeństwa sieciowego i teleinformatycznego oraz usługami ułatwiającymi dostęp do technologii cyfrowych. Operatorem OSE jest NASK-PIB, nadzorowany przez Ministerstwo Cyfryzacji.

Świadczenie usług bezpieczeństwa teleinformatycznego obejmuje ochronę przed szkodliwym oprogramowaniem, monitorowanie zagrożeń i bezpieczeństwa sieciowego oraz przeciwdziałanie dostępowi do treści, które mogą stanowić zagrożenie dla prawidłowego rozwoju uczniów. Usługa Bezpieczny Internet OSE jest włączona domyślnie wraz z rozpoczęciem świadczenia usług OSE w szkole. Usługa realizuje funkcje ochronne w zakresie blokowania niepożądanej komunikacji sieciowej. Usługa pozwala na zabezpieczenie sieci szkolnej w podstawowym zakresie. Umożliwia także ochronę urządzeń niedziałających prawidłowo w ramach zaawansowanych usług bezpieczeństwa OSE plus wymagających inspekcji SSL, w tym np. tablic interaktywnych, monitorów multimedialnych, gogli VR, smart TV, a także urządzeń mobilnych (smartfonów, tabletów). W przypadku każdej szkoły możliwe jest jednak indywidualne dostosowanie ochrony do potrzeb, w tym również połączenie obu wariantów usług bezpieczeństwa w sieci szkoły (np. wyższy poziom zabezpieczeń w pracowni komputerowej wyposażonej w komputery stacjonarne/przenośne i niższy poziom zabezpieczeń dla urządzeń mobilnych/interaktywnych, czy komputerów w sekretariacie).

Firma Bezpieczna Cyfrowo

Ministerstwo Rozwoju i Technologii we współpracy z NASK-PIB przeprowadził pilotaż programu Firma Bezpieczna Cyfrowo, który pozwolił na przebadanie poziomu cyberbezpieczeństwa w formie ankiety samooceny ponad 1600 przedsiębiorców. To pozwoliło na sformułowanie wniosków, które przełożą się na uruchomienie programu wsparcia rozwoju kompetencji małych i średnich przedsiębiorstw w zakresie cyberbezpieczeństwa.

2.4 Budowanie świadomości i kompetencji społecznych w zakresie cyberbezpieczeństwa

Cyberbezpieczny Samorząd

W celu zwiększenia poziomu bezpieczeństwa informacji jednostek samorządu terytorialnego (JST) poprzez wzmacnianie odporności oraz zdolności do skutecznego zapobiegania i reagowania na incydenty w systemach informacyjnych Ministerstwo Cyfryzacji uruchomiło program Cyberbezpieczny Samorząd. W lipcu 2023 r. rozpoczęty został nabór wniosków grantowych, który zakończył się w grudniu ub. r. Wnioski zostały złożone przez 2517 z 2807

(90%) JST objętych projektem. Łącznie na wsparcie JST przeznaczonych zostanie ok. 1,5 mld zł. Realizacja projektu przyczyni się w szczególności do:

- wdrożenia lub aktualizacji w JST polityk bezpieczeństwa informacji (SZBI),
- wdrożenia w JST środków zarządzania ryzykiem w cyberbezpieczeństwie,
- wdrożenia w JST mechanizmów i środków zwiększających odporność na ataki z cyberprzestrzeni,
- podniesienia poziomu wiedzy i kompetencji personelu JST kluczowego z punktu widzenia SZBI wdrożonego w urzędzie,
- przeprowadzenia w JST audytów SZBI potwierdzających uzyskanie wyższego poziomu odporności na cyberzagrożenia.

Projekt jest dofinansowany ze środków Europejskiego Funduszu Rozwoju Regionalnego w ramach Programu Fundusze Europejskie na Rozwój Cyfrowy 2021-2027.

W ramach programu NASK-PIB opracował publikację pt. "Cyberbezpieczny Samorząd – poradnik". Głównym celem opracowania jest ułatwienie każdej jednostce samorządu terytorialnego identyfikacji aktualnego stanu cyberbezpieczeństwa i rzeczywistych potrzeb jednostki w tym zakresie oraz określenie realnych możliwości podniesienia przez JST poziomu cyberbezpieczeństwa. Jednocześnie w poradniku przedstawiono podstawowe zagadnienia formalne, prawne, organizacyjne i techniczne umożliwiające analizę stanu rozwoju JST w obszarze cyberbezpieczeństwa. Wskazano również przykłady przedsięwzięć, jakie mogą podjąć JST w celu zwiększenia bezpieczeństwa informacji przez wzmacnianie odporności oraz zdolności do skutecznego zapobiegania incydentom, wykrywania ich i reagowania na nie.

Fundusz Cyberbezpieczeństwa

Fundusz Cyberbezpieczeństwa, którego dysponentem jest minister właściwy do spraw informatyzacji, został powołany ustawą z dnia 2 grudnia 2021 r. o szczególnych zasadach wynagradzania osób realizujących zadania z zakresu cyberbezpieczeństwa. Głównym zadaniem Funduszu, jako państwowego funduszu celowego, jest wsparcie działań zmierzających do zapewnienia bezpieczeństwa systemów teleinformatycznych przed cyberzagrożeniami poprzez finansowanie świadczenia teleinformatycznego, tj. dodatku do wynagrodzenia za pracę, a w przypadku funkcjonariuszy i żołnierzy zawodowych świadczenia pieniężnego.

Świadczenie teleinformatyczne może zostać przyznane osobom realizującym zadania z zakresu cyberbezpieczeństwa na rzecz podmiotów wymienionych w ustawie, m.in. w CSIRT poziomu

krajowego, służbach odpowiedzialnych za bezpieczeństwo państwa oraz bezpieczeństwo powszechne, a także w urzędach administracji publicznej.

Warunkiem ubiegania się o wsparcie ze środków Funduszu jest złożenie przez uprawniony podmiot wniosku do ministra właściwego do spraw informatyzacji. Wnioski spełniające wymagania formalne przekazywane są do Kolegium do Spraw Cyberbezpieczeństwa, które wydaje opinię w zakresie wnioskowanych kwot.

W 2023 r. umowy o udzielenie wsparcia ze środków Funduszu Cyberbezpieczeństwa zostały zawarte z 79 beneficjentami na łączną kwotę 267 513 986,00 zł, zaś świadczenie teleinformatyczne otrzymało ponad 4 000 osób realizujących zadania w zakresie zapewnienia cyberbezpieczeństwa w kluczowych instytucjach w kraju.

W 2023 r., zgodnie z art. 31a ustawy z dnia 1 grudnia 2022 r. o szczególnych rozwiązaniach służących realizacji ustawy budżetowej na rok 2023, wprowadzonym ustawą z dnia 7 lipca 2023 r. o zmianie ustawy o szczególnych rozwiązaniach służących realizacji ustawy budżetowej na rok 2023 oraz niektórych innych ustaw, powstała możliwość sfinansowania ze środków Funduszu Cyberbezpieczeństwa zadań ministra właściwego do spraw informatyzacji związanych z cyberbezpieczeństwem innych niż świadczenie teleinformatyczne i koszty z nim związane. W ramach ww. dodatkowego celu Funduszu w 2023 r. sfinansowano 4 dotacje na łączną kwotę 9 953 839,52 zł.

W połowie 2023 r. przeprowadzona została ewaluacja funkcjonowania ustawy z dnia 2 grudnia 2021 r. o szczególnych zasadach wynagradzania osób realizujących zadania z zakresu cyberbezpieczeństwa.

Zgodnie z zebranymi w ramach ww. badania danymi, wprowadzenie świadczenia teleinformatycznego w opinii podmiotów, które uzyskały wsparcie ze środków Funduszu Cyberbezpieczeństwa w 2023 r., pozwoliło na:

- zmniejszenie odpływu specjalistów realizujących zadania z zakresu cyberbezpieczeństwa z tych podmiotów – aż 79% beneficjentów obniżyło wskaźnik rezygnacji kadr;
- pozyskanie nowych specjalistów na wakujące do tej pory stanowiska – 40% beneficjentów zatrudniło nowych pracowników przy wsparciu Funduszu, zaś 49% beneficjentów planuje zatrudnić nowych pracowników w latach kolejnych;
- planowanie utworzenia dodatkowych stanowisk pracy, na których będą realizowane zadania z zakresu cyberbezpieczeństwa – 58% beneficjentów planuje utworzenie nowych stanowisk pracy przy wsparciu Funduszu;
- podniesienie poziomu cyberbezpieczeństwa – aż 96% beneficjentów wskazało, że uzyskane wsparcie z Funduszu wpłynęło na zmniejszenie liczby zagrożeń i incydentów bezpieczeństwa w ich jednostkach.

Szkolenia z cyberbezpieczeństwa dla najważniejszych osób w państwie – projekt SecureV

W 2023 r. Ministerstwo Cyfryzacji kontynuowano prowadzone od 2021 r. działania prewencyjno-edukacyjne dla najważniejszych osób w państwie (projekty SecureV). W ramach działania prowadzone są specjalistyczne szkolenia z zakresu cyberbezpieczeństwa adresowane do najważniejszych osób w państwie. Początkowo projekt SecureV obejmował wyłącznie parlamentarzystów i kadrę kierowniczą administracji centralnej. Jednak z uwagi na dynamiczną sytuację w cyberprzestrzeni kraju oraz duże zainteresowanie szkoleniami, kolejne edycje projektu uwzględniają coraz większą grupę odbiorców.

Terminy i zakres merytoryczny szkoleń dostosowywane są do konkretnych potrzeb szkolonej osoby. Dodatkowo, każda indywidualnie przeszkolona osoba zostaje wyposażona w uniwersalne narzędzia służące do silnego uwierzytelnienia wraz z instruktażem stosowania narzędzia.

W 2023 r. zasięg działań prewencyjno-edukacyjnych objął już terytorium całego kraju, a projektem szkoleniowym objęci są parlamentarzyści, kadra kierownicza administracji centralnej i samorządowej, przedstawiciele Krajowego Biura Wyborczego oraz pracownicy Podstawowej Opieki Zdrowotnej. W edycji SecureV 2023 udział w szkoleniach wzięło 5288 osób. Od 2021 r., w ramach działań SecueV przeszkolono ponad 6700 osób. Działania prewencyjno-edukacyjne są kontynuowane w 2024 r.

Szkolenia online dla podmiotów krajowego systemu cyberbezpieczeństwa

W roku 2023 Ministerstwo Cyfryzacji kontynuowało prowadzone od 2020 r. szkolenia online dla podmiotów krajowego systemu cyberbezpieczeństwa. Szkolenia prowadzone są przez ekspertów i praktyków na co dzień zajmujących się kwestiami cyberbezpieczeństwa – ekspertów NASK-PIB, partnerów technologicznych PWCyber, oraz COI. Szkolenia realizowane są na różnym poziomie zaawansowania wiedzy z zakresu cyberbezpieczeństwa, dostosowane do bieżącej sytuacji i zgłaszanych potrzeb.

W ramach szkoleń online w 2023 r. zorganizowano:

- 8 szkoleń z zakresu higieny cyfrowej (4 cykle) we współpracy z NASK-PIB. Cykl składa się z dwóch szkoleń: *Cyberzagrożenia - bądź na bieżąco*! oraz *Podstawowe zasady cyberhigieny w pracy i w życiu prywatnym*. Z uwagi na ogromne zainteresowanie szkoleniami z podstaw cyberbezpieczeństwa, od 2023 roku cykl jest powtarzany regularnie raz na kwartał.
- 2 szkolenia dla użytkowników Systemu Rejestrów Państwowych we współpracy z Centralnym Ośrodkiem Informatyki. W szkoleniach udział wzięło 1591 osób.
- 3 szkolenia w ramach nowego cyklu szkoleń dla podmiotów publicznych wykonujących działalność leczniczą. W październiku 2023 r. uruchomiono nowy cykl specjalistycznych szkoleń skierowany do kadry kierowniczej, personelu IT i osób zarządzających cyberbezpieczeństwem w podmiotach świadczących usługi z zakresu ochrony zdrowia. Cykl obejmuje 10 szkoleń online, które są realizowane średnio raz w miesiącu. W 3. pierwszych szkoleniach zrealizowanych w 2023 r. udział wzięło 1294 osoby. Cykl jest kontynuowany w 2024 r.
- 17 szkoleń online zrealizowanych we współpracy z partnerami PWCyber, w których udział wzięło 7 760 osób. Celem szkoleń jest nie tylko zwiększenie świadomości kadr KSC na temat cyberzagrożeń, ale również podniesienie umiejętności praktycznych związanych z wykorzystywaniem narzędzi informatycznych oraz radzenia sobie w sytuacjach kryzysowych.

Łącznie w 2023 r. zrealizowano 30 szkoleń online, w których uczestniczyło ponad 18 tys. osób.

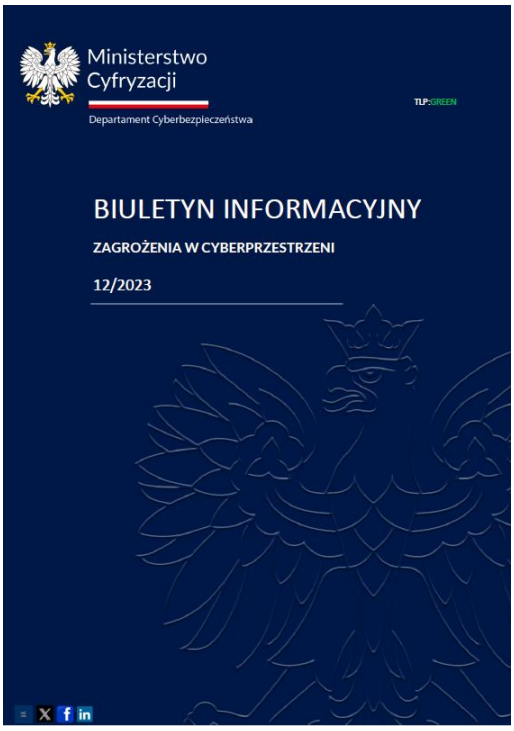
Numer 8080

W związku z wejściem w życie w 2023 r. ustawy o zwalczaniu nadużyć w komunikacji elektronicznej Ministerstwo Cyfryzacji podjęło szereg działań informacyjnych dotyczących nowych rozwiązań. W szczególności informowano o numerze 8080, na który należy przesyłać podejrzane sms-y w celu ich zbadania przez CSIRT NASK. Informowano również o liście ostrzeżeń, na którą wpisywane są domeny internetowe wykorzystywane do wprowadzania

w błąd użytkowników internetu i doprowadzenia do wyłudzenia ich danych lub niekorzystnego rozporządzenia mieniem. W wyniku prowadzonych działań informacyjnych dotyczących porozumienia o liście ostrzeżeń systematycznie dołączają do porozumienia nowe podmioty dzięki czemu wzrasta grono podmiotów mogących blokować dostęp do stron internetowych wykorzystujących nazwy domen internetowych wpisanych na listę ostrzeżeń.

Biuletyn „Bezpieczeństwo cyberprzestrzeni”

Ministerstwo Cyfryzacji opracowywało i dystrybuowało wśród podmiotów krajowego systemu cyberbezpieczeństwa comiesięczny biuletyn „Bezpieczeństwo cyberprzestrzeni” (dokument początkowo oznaczony jako TLP:AMBER, a następnie TLP:GREEN). Biuletyn propaguje wiedzę na temat najnowszych trendów w zakresie cyberbezpieczeństwa.



Baza wiedzy o cyberbezpieczeństwie na portalu gov.pl

W roku 2023 r. Ministerstwo Cyfryzacji rozwijało prowadzoną od 2019 r. bazę wiedzy o cyberbezpieczeństwie na portalu gov.pl, gdzie publikowane są informacje o wydarzeniach z obszaru cyberbezpieczeństwa, w tym ostrzeżenia o bieżących zagrożeniach, poradniki,

rekomendacje i standardy cyberbezpieczeństwa. Materiały adresowane są do różnych kategorii odbiorców (zarówno do profesjonalistów, jak i każdego zainteresowanego bezpieczeństwem nowych technologii). Publikowane są tam również informacje o realizowanych szkoleniach online. W 2023 r. powstała nowa zakładka: *Porozumienie ws. listy ostrzeżeń*. W zakładce znajdują się wszystkie niezbędne informacje o prowadzeniu listy ostrzeżeń dotyczących domen internetowych, które służą do wyłudzeń danych i niekorzystnego rozporządzania mieniem użytkowników Internetu. W bazie wiedzy w 2023 r. pojawiło się ponad 170 nowych publikacji dotyczących problematyki bezpieczeństwa w cyberprzestrzeni.

www.cyber.gov.pl

Działania wspierające edukację o cyberbezpieczeństwie

W 2023 r. zaktualizowano projekt edukacyjny Cyberlekcje (Cyberlekcje 3.0) realizowany w ramach współpracy Ministra Cyfryzacji oraz NASK-PIB. Projekt adresowany jest do nauczycieli szkół podstawowych i ponadpodstawowych. Przygotowane materiały pomagają pedagogom usystematyzować wiedzę z zakresu cyberbezpieczeństwa, a także umożliwią zorganizowanie lekcji na temat mądrego i odpowiedzialnego korzystania z nowych technologii. W nowej odsłonie projektu wszystkie materiały przystosowano do jednej, spójnej metodyki nauczania - metodologii PBL (ang. *Problem-Based Learning*). PBL, czyli nauczanie oparte na rozwiązywaniu problemów, rzuca wyzwanie uczniom, aby aktywnie uczestniczyli w procesie uczenia się, a nie biernie „otrzymywali" informacje.

18 gotowych scenariuszy lekcji oraz materiały multimedialne opracowane w 2021 r. oraz w 2023 r. obejmują każdy etap edukacji. Treści zawarte w scenariuszach są zgodne z obowiązującą podstawą programową, a ich tematyka odpowiada rosnącemu zapotrzebowaniu na wiedzę i kompetencje z zakresu efektywnego wykorzystywania mediów cyfrowych.

Wszystkie scenariusze oraz materiały dodatkowe projektu Cyberlekcje 3.0 są dostępne w bazie wiedzy o cyberbezpieczeństwie na portalu gov.pl w zakładce CyberEdukacja, a także na rekomendowanej przez Ministerstwo Edukacji i Nauki Zintegrowanej Platformie Edukacyjnej (ZPE).

Szkolenia „Cyberhigiena. Służbowo i prywatnie”

Ministerstwo Cyfryzacji prowadziło szkolenia dla pracowników Ministerstwa i KPRM z zakresu cyberbezpieczeństwa pn. „Cyberhigiena. Służbowo i prywatnie”. W trakcie szkoleń przekazywane były informacje m.in. o stosowaniu kluczy 2FA, menadżerów haseł, kryptografii symetrycznej i asymetrycznej. W roku 2023 wzięło w nich udział 569 osób. Ze strony uczestników szkoleń pojawiały się prośby o przygotowanie praktycznych warsztatów z korzystania ww. narzędzi. Wychodząc naprzeciw tym potrzebom Departament Cyberbezpieczeństwa Ministerstwa Cyfryzacji planuje uruchomienie takich szkoleń w bieżącym roku.

Forum Cyberbezpieczeństwa

We wrześniu 2023 r. Ministerstwo Cyfryzacji po raz 5. zorganizowało Forum Cyberbezpieczeństwa w ramach Forum Ekonomicznego. Podczas 30 paneli eksperckich, zaproszeni goście dyskutowali o największych wyzwaniach związanych z cyberbezpieczeństwem, sztuczną inteligencją, cyfryzacją kraju, dezinformacją. Podczas Forum odbyły się także spotkania Cyfrowej Dekady z udziałem ministrów ds. cyfrowych, konsultacje dwustronne z Wielką Brytanią, USA, Rwandą.

Ustawa o ochronie małoletnich przed dostępem do treści nieodpowiednich w internecie

Ministerstwo Cyfryzacji w 2023 r. procedowało projekt ustawy o ochronie małoletnich przed dostępem do treści nieodpowiednich w internecie. Projekt stanowił odpowiedź na zidentyfikowany problem powszechnego i niemal nieograniczonego dostępu przez dzieci i młodzież do treści pornograficznych. Treści pornograficzne, w przeważającej części dostępne bezpłatnie w internecie, wymieniane są jako jeden z głównych czynników przyczyniających się do destabilizacji psychiki i zdrowia małoletnich, co może również prowadzić do zachwianego postrzegania seksualności i ról płciowych w okresie dojrzewania i dorosłości. Stanowi to poważne zagrożenie dla zdrowia publicznego. Prace nad projektem ustawy nie zostały zakończone z powodu wyborów parlamentarnych w październiku 2023 r. a co za tym idzie zasady dyskontynuacji prac legislacyjnych. Zaszła również potrzeba szerszej dyskusji na temat zakresu podmiotowego i przedmiotowego planowanej regulacji.

W 2024 r. Ministerstwo Cyfryzacji planuje nowe rozwiązania legislacyjne, mające zapewnić bezpieczeństwo małoletnim w internecie i ograniczenie negatywnego dla ich rozwoju wpływu treści szkodliwych. Analizowane są przy tym rozwiązania wdrażane w innych krajach europejskich, w tym regulacje brytyjskie i francuskie. Rozważane regulacje mogłyby objąć szerszy zakres treści, tj. ochronę dzieci przed treściami nie tylko pornograficznymi, ale i innymi dla nich szkodliwymi, jak np. treściami zawierającymi drastyczne sceny przemocy, nawoływanie do samookaleczania, popełnienia samobójstwa, a zatem też patostreaming. Ze względu na złożony charakter przedmiotowej tematyki, przed wszczęciem formalnych prac legislacyjnych Ministerstwo Cyfryzacji planuje zgromadzenie szerokiego grona specjalistów – środowiska naukowego, prawniczego, przedstawicieli NGO-sów oraz przedsiębiorców, celem odbycia wspólnej dyskusji m.in. nad definicjami, zakresem podmiotowym i przedmiotowym regulacji, możliwymi środkami technicznymi.

Edukacja szkolna na rzecz cyberbezpieczeństwa

Działania Ministerstwa Edukacji Narodowej w zakresie przeciwdziałania zagrożeniom płynącym z cyberprzestrzeni koncentrują się na projektowaniu systemowych rozwiązań

gwarantujących bezpieczne warunki kształcenia, wychowania i opieki oraz wspierania szkół i placówek systemu oświaty w realizacji zadań. Zadaniem systemu oświaty jest również upowszechnianie wśród dzieci i młodzieży wiedzy o cyberbezpieczeństwie oraz kształtowanie właściwych postaw wobec zagrożeń, w tym związanych z korzystaniem z technologii informacyjno-komunikacyjnych.

Szkoły i placówki zapewniające uczniom dostęp do Internetu są obowiązane podejmować działania zabezpieczające uczniów przed dostępem do treści, które mogą stanowić zagrożenie dla ich prawidłowego rozwoju, w szczególności zainstalować i aktualizować oprogramowanie zabezpieczające. Kompetencje cyfrowe są rozwijane w ramach realizacji obszaru Edukacja informatyczna (klasy I-III), a następnie na lekcjach informatyki (klasy IV-VIII), gdzie uczniowie zapoznają się m.in. z normami prawnymi w zakresie stosowania technologii informacyjno-komunikacyjnych dotyczących rozpowszechniania programów komputerowych, przestępczości komputerowej, poufności, bezpieczeństwa i ochrony danych oraz informacji w komputerze i w sieciach komputerowych. Podstawa programowa mocno akcentuje potrzebę rozwijania u uczniów świadomości i zachowań gwarantujących odpowiedzialne korzystanie z narzędzi ICT. Ponadto w ramach rządowego programu „Bezpieczna+" realizowane było zadanie mające na celu umiejętne korzystanie przez dzieci i młodzież z Internetu, jak również podniesienie umiejętności reagowania przez rodziców i nauczycieli na zagrożenia płynące z cyberprzestrzeni.

Poza tym na stronie Ośrodka Rozwoju Edukacji udostępniane są materiały informacyjne i publikacje dotyczące m.in. zagrożeń związanych z korzystaniem przez uczniów z nowych technologii komunikacyjnych oraz badań tego zagadnienia. Równocześnie na Zintegrowanej Platformie Edukacyjnej zgromadzono wiele zasobów nt. bezpiecznego korzystania z nowych technologii i Internetu wśród dzieci i młodzieży. Ponadto, na stronie internetowej Ministerstwa Edukacji Narodowej zamieszczono poradnik Bezpieczna szkoła. Poradnik obejmuje również zagadnienia bezpieczeństwa w cyberprzestrzeni.

W kwestii bezpieczeństwa teleinformatycznego systemów wewnętrznych Ministerstwa Edukacji Narodowej (MEN), jak i systemów publicznie dostępnych (w tym Systemu Informacji Oświatowej i Krajowego Systemu Danych Oświatowych), CIE i dla części systemów Ośrodka Rozwoju Edukacji (ORE) oraz Centralnej Komisji Egzaminacyjnej (CKE) Centrum Informatyczne Edukacji. W 2023 roku w celu zapewnienia i zwiększenia cyberbezpieczeństwa MEN oraz jednostek podległych MEN w CIE został powołany Zespół ds. Cyberbezpieczeństwa składający się z wybranych pracowników CIE, którzy są specjalistami z różnych specjalizacji IT. Zespół w poprzednim roku ukończył i zaraportował w wewnętrznym systemie łącznie 761 zadań związanych z zapewnieniem lub zwiększeniem poziomu cyberbezpieczeństwa w obsługiwanych jednostkach. Zadania realizowane w ramach prac zespołu to zadania ściśle związane z bezpieczeństwem IT, ale także prace nad procedurami bezpieczeństwa będące częścią Systemu Zarządzania Bezpieczeństwem Informacji.

Ponadto CIE współpracowało z CSIRT GOV w zakresie zgłaszania i obsługi incydentów oraz wdrażało otrzymane zalecenia, a także monitorowało i usuwało podatności. Wdrożono m.in.: Procedurę Łańcucha Dostaw, rozpoczęto prace nad Procedurą Zabezpieczania Śladów Cyfrowych, przeprowadzono testy antyphishingowe zwiększające świadomość użytkowników końcowych, rozbudowano infrastrukturę o nowe systemy bezpieczeństwa, przeprowadzono testy stron www utrzymywanych i zarządzanych przez CIE. Utrzymywano również współpracę i wymianę informacji z jednostkami zewnętrznymi (CSIRT GOV, ABW, ORE, OKE, CKE). W celu rozwijania świadomości społecznej w kierunku bezpiecznego korzystania z cyberprzestrzeni ministerstwo wśród swoich pracowników podejmowało działania uświadamiające nt. zagrożeń występujących w Internecie. Organizowane były szkolenia wewnętrzne i zewnętrzne dotyczące bezpiecznej pracy w cyberprzestrzeni, a także rozpowszechniane były informacje o aktualnie występujących zagrożeniach w sieci i o konieczności zachowania szczególnej ostrożności w Internecie w okresach wzmożonej aktywności cyberprzestępców.

Ćwiczenia resortu obrony narodowej

Personel cyberbezpieczeństwa resortu obrony narodowej doskonalił umiejętności w trakcie: Cyber Net 2023, Cyber Blitz (Baltic Blitz), Cyber Spartan 2023, Locked Shields 2023, Cyber Expert Games 2023, Cyber Coalition 2023, Joint Fury 2023, Anakonda 2023, ćwiczenia CWIX 2023 przez wydzielone zespół CIAT (Coalition Incident Assessment Team) Cyber Flag 2023, Guardian Blue 2023, CWIX 2023, System 23, Metoda 23, Crossed Swords 2023, narodowych i międzynarodowych treningach, warsztatach, szkoleniach i kursach, w czasie których rozwijano zdolności w zakresie planowania i prowadzenia działań w cyberprzestrzeni.

Zgrywano także komórki dowództwa w zakresie planowania i dowodzenia działaniami w cyberprzestrzeni jako wsparcie wielodomenowej operacji połączonej, pełniąc rolę Dowództwa SOCC podczas ćwiczenia CYBER COALITION 2024.

Na zwrócenie uwagi zasługuje również zwiększenie kompetencji w zakresie planowania i prowadzenia operacji ofensywnej w cyberprzestrzeni poprzez uczestnictwo w ćwiczeniu CROSSED SWORDS 2023.

Ćwiczenia Locked Shields 2023

Seminarium CyberBEZPIECZNI

Wydarzenie skupiające przedstawicieli resortu obrony narodowej, ze szczególnym uwzględnieniem pionów wsparcia dowodzenia, łączności, informatyki i cyberbezpieczeństwa, dowódców oraz kadry zarządzającej ron, administracji państwowej Krajowego Systemu Cyberbezpieczeństwa. Pierwsza edycja Seminarium CyberBEZPIECZNI odbyła się w dniu 29 marca 2023 r. i była poświęcona praktycznym zastosowaniom cyberbezpieczeństwa w działalności służbowej. Druga edycja odbyła się w dniu 18 maja 2023 r., a tematem przewodnim było wykorzystanie niekonwencjonalnych rozwiązań do obrony państwa w czasie konfliktu zbrojnego.

Konferencja CyberEXPERT

Coroczna konferencja organizowana przez Eksperckie Centrum Cyberbezpieczeństwa (ECSC) skupiająca ekspertów, naukowców i inżynierów działających w branży szeroko pojętego IT, cyberbezpieczeństwa oraz kryptologii. Poprzednia edycja CyberEXPERT odbyła się w dniach 15-16 listopada 2023 r. i poświęcona była technologii kwantowej oraz sztucznej inteligencji w kontekście ich wykorzystania w służbie cyberbezpieczeństwa.

Warsztaty CyberEXPERT GAME

Organizowane raz w roku 3-dniowe warsztaty mające na celu koordynację i zgrywanie zespołów CSIRT oraz podmiotów, które wchodzą w skład Krajowego Systemu Cyberbezpieczeństwa. W roku 2023 zorganizowano trzecią edycję warsztatów, na której pojawiły się zespoły z następujących podmiotów: DKWOC, DWOT, ENEA, Gaz-SYSTEM, KGHM, NBP, PGE, PGZ, PKO BP, ZUS. Ponadto działania adwersarza zapewnił zespół z Jednostki Działań w Cyberprzestrzeni A i B. W dniach 28-30.11.2023 r. w warsztatach wzięło udział 147 osób.

Certyfikacja

W roku 2023 wysiłki ECSC skupiały się na przygotowaniu procesu certyfikacji i uzyskaniu statusu akredytowanej jednostki, prowadzącej certyfikację osób w obszarze cyberbezpieczeństwa. W tym zakresie w minionym roku zrealizowano poniższe przedsięwzięcia:

- w strukturze ECSC utworzono Oddział Certyfikacji odpowiedzialny za przygotowanie i realizację procesów certyfikacji osób,
- opracowano dokumenty systemowe wraz z pięcioma programami certyfikacji osób,
- opracowano bazę pytań egzaminacyjnych na potrzeby programu ECSC-PR-04 Specjalista ds. cyberbezpieczeństwa,
- przeprowadzono audyty wewnętrzne systemu,
- powołano Radę Programową i Komitet Naukowy,
- przeprowadzono pierwsze procesy certyfikacji osób zgodnie z programem ECSC-PR-04 Specjalista ds. cyberbezpieczeństwa,
- uzyskano akredytację Polskiego Centrum Akredytacji do programu ECSC-PR-04 Specjalista ds. cyberbezpieczeństwa.

Kontynuowane są prace mające na celu uzyskanie akredytacji Polskiego Centrum Akredytacji na kolejne 4 programy.

Opracowanie szkoleń dla zdefiniowanych ścieżek szkoleniowych kluczowych ról zawodowych cyberbezpieczeństwa w oparciu o Standard NIST 800-181 (NICE Framework)

Celem projektu realizowanego przez ECSC jest wdrożenie modelu do zarządzania kompetencjami w obszarze cyberbezpieczeństwa w oparciu o standard NICE Framework, co ma umożliwić sprawne zarządzanie kompetencjami w obszarze cyberbezpieczeństwa oraz planowanie rozwoju zawodowego kadry i pracowników ron. Zgodnie z zakresem kompetencji opracowano model (program, moduł) szkolenia dla zdefiniowanych ścieżek szkoleniowych dla otrzymanej z DKWOC kluczowej roli zawodowej cyberbezpieczeństwa w oparciu o Standard NIST 800-181 (NICE Framework). Ponadto powołano zespół roboczy do opracowania modeli szkolenia kolejnych ról zawodowych. Rozpoczęto ich opracowywanie i mapowanie na podstawie otrzymanego projektu dokumentu „Zakresy kompetencji i ścieżki szkoleniowe dla kluczowych ról zawodowych cyberbezpieczeństwa w oparciu o standard NIST 800-181 (NICE Framework)".

Współpraca ECSC z European Security And Defence College

W minionym roku ECSC dokończyło pilotażową edycję (pilot course) szkoleń oraz rozpoczęło realizację drugiej edycji, zakwalifikowanych przez ESDC, jako standard course, szkoleń organizowanych wspólnie z ESDC. Zobowiązanie poczynione na rok 2023 obejmowało przygotowanie i realizację nw. szkoleń:

- Cyber Range – Cybersecurity in Practice (pilot), 21 – 23.03.2023 r.;
- Cyber Range – Defensive Capabilities (standard), 26 – 28.09.2023 r.;
- Cyber Range – Pentester Tools (standard), 24 – 26.10.2023 r.

Przygotowane przez ECSC szkolenia adresowane były do personelu technicznego średniego szczebla państw Unii Europejskiej, którzy w ramach swoich obowiązków odpowiadają za kwestie związane z cyberbezpieczeństwem.

Współpraca ECSC z NATO

Szkolenia adresowane do NATO są inicjatywą równoległą do działalności na arenie Unii Europejskiej i obejmują zbieżny zakres tematyczny szkoleń. Podczas posiedzenia NATO Cyber Defence Committee w dniu 7 listopada 2022 r. przedstawiciele ECSC przedstawili ofertę szkoleniową na rok akademicki 2023/2024 adresowaną do NATO. W ramach tej oferty znalazły się trzy niżej wymienione szkolenia:

- Cyber Range – Defensive Capabilities, zrealizowany w terminie 19-21.09.2023 r.;
- Cyber Range – Pentester Tools, zrealizowany w terminie 7-9.11.2023 r.;
- Cyber Range – Cybersecurity in Practice, planowany w marcu 2024 r.

W ramach prowadzonych szkoleń w 2023r. uczestniczyli przedstawiciele sił zbrojnych Czech, Kanady, Litwy, Norwegii, Słowacji, Węgier.

Szkolenia ESCS dla Ukrainy

Odpowiadając na zapotrzebowanie zgłoszone przez stronę ukraińską, w ramach współpracy w obszarze szkoleniowym na rzecz wsparcia Sił Zbrojnych Ukrainy (SZ UA), w ubiegłym roku ECSC zadeklarowało przygotowanie i przeprowadzenie nw. kursów:

- Certified Ethical Hacker, 17 – 21 kwietnia 2023 r.;
- Administration and securing Windows and Linux based systems, 12 – 14 września 2023 r.;
- Malware Analysis - Reverse Engineering and Digital Forensic, 04 – 08 września 2023 r.

Kursy przygotowane przez ECSC były jedynymi szkoleniami oferowanymi SZ UA w obszarze bezpieczeństwa cyberprzestrzeni. Całość inicjatywy zorganizowana została w ramach UE Millitary Assistance Mission in support of Ukraine.

2.5 Budowanie silnej pozycji międzynarodowej Rzeczypospolitej Polskiej w obszarze cyberbezpieczeństwa

Współpraca w ramach Unii Europejskiej

W ramach współpracy unijnej Ministerstwo Cyfryzacji realizowało zadania związane z koordynacją współpracy między organami właściwymi ds. cyberbezpieczeństwa RP z odpowiednimi organami w innych państwa członkowskich UE. Dotyczy to udziału w Grupie Współpracy NIS oraz w pracach następujących zespołów: WS5 - dostawcy usług cyfrowych, WS3 - raportowanie incydentów, WS7 – WS2 – środki bezpieczeństwa, WS5 - dostawcy usług cyfrowych, WS8 - sektor energii, WS10 - infrastruktura cyfrowa, WS12 - sektor zdrowia, WS on 5G and Telecom Security, WS on Supply Chain Security, 5G Toolbox, Sub-group standaryzacja i certyfikacja, europejska sieć zarządzania kryzysami cyfrowymi CyCLONE, Europejska Sieć Bezpieczeństwa Wyborów (ECNE), Horyzontalna Grupa Robocza ds. Cyberprzestrzeni (Cyber) (HWPCI), Grupa Robocza ds. Egzekwowania Prawa (LEWP) w zakresie CSAM. Przy czym warto podkreślić, że Polska przewodniczyła pracom zespołu WS10 - infrastruktura cyfrowa.

Ministerstwo Cyfryzacji realizowało również zadania Pojedynczego Punktu Kontaktowego, o którym mowa w Dyrektywie NIS, oraz koordynowało współpracę z podmiotami odpowiedzialnymi za cyberbezpieczeństwo, jak również prowadziło konsultacje z przedstawicielami resortów kluczowych w ramach współpracy w ramach cyberbezpieczeństwa.

MSZ realizowało działania na rzecz operacjonalizacji i wzmocnienia narzędzi cyberdyplomacji, szczególnie poprzez zgłoszenie non-paper ws. rozszerzenia narzędzi restrykcyjnych Cyber Diplomacy Toolbox o sankcje sektorowe. Resort ten brał też udział w pracach Horyzontalnej Grupy Roboczej ds. Cyberbezpieczeństwa (HWPCI), przede wszystkim w zakresie tematyki cyberdyplomacji. Bierze również aktywny udział w pracach unijnej sieci ambasadorów/krajowych koordynatorów ds. cyberbezpieczeństwa (cyber ambassador's network) oraz wsparcie udziału Polski w sieci dyplomacji cyfrowej (digital diplomacy).

Ponadto, Polska brała udział w ćwiczeniach na poziomie UE, w m.in. takich jak ćwiczenia BlueOLex 2023 oraz warsztatach organizowanych przez poszczególne zespoły robocze.

Ministerstwo Cyfryzacji brało ponadto udział w pracach legislacyjnych na poziomie europejskim nad:

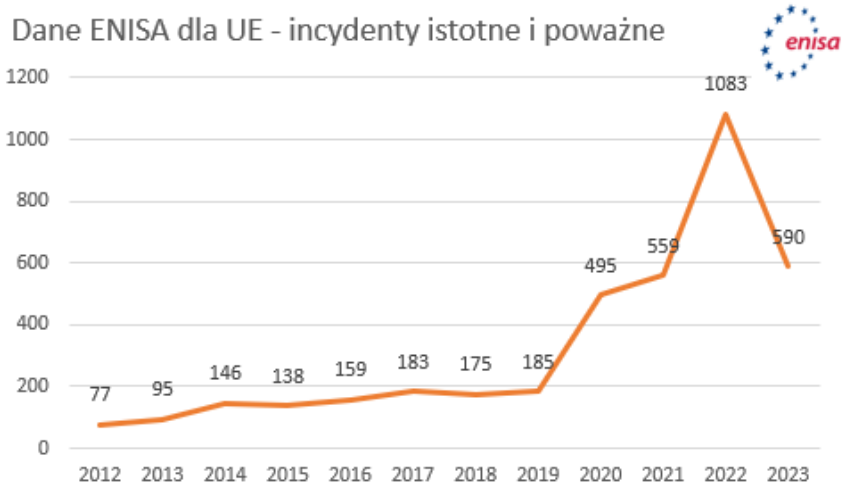
- Dyrektywą Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniająca rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylająca dyrektywę (UE) 2016/1148 (dyrektywa NIS2),

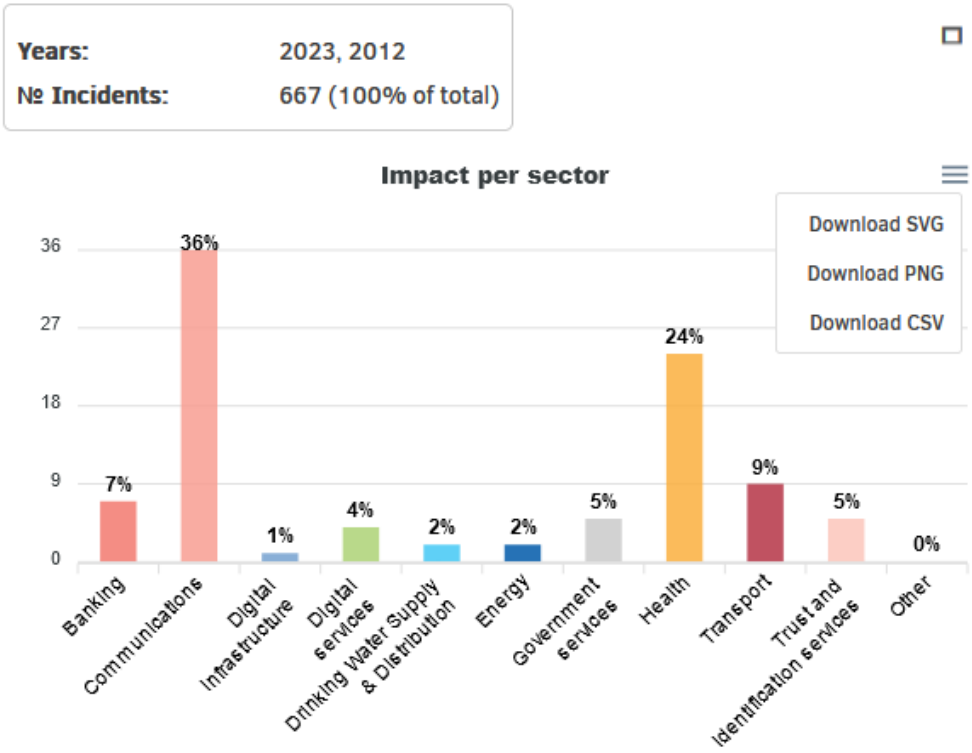
- Rozporządzeniem Parlamentu Europejskiego i Rady ustanawiającym środki mające na celu zwiększenie solidarności i zdolności w Unii w zakresie wykrywania zagrożeń cyberbezpieczeństwa i incydentów w cyberbezpieczeństwie oraz przygotowywania się i reagowania na takie zagrożenia i incydenty 2023/0109 (Cyber Solidarity Act),
- Rozporządzeniem Parlamentu Europejskiego i Rady w sprawie horyzontalnych wymogów cyberbezpieczeństwa w odniesieniu do produktów z elementami cyfrowymi i zmieniające rozporządzenie (UE) 2019/1020 (Cyber Resilience Act), Rozporządzeniem UE ustanawiającym przepisy mające na celu zapobieganie i zwalczanie seksualnego wykorzystywania dzieci (CSAM).

Ministerstwo Cyfryzacji brało także udział w pracach Europejskiej Grupy ds. Certyfikacji Cyberbezpieczeństwa oraz Europejskiego Komitetu Certyfikacji Cyberbezpieczeństwa. W ramach tych prac prezentowane było stanowisko Polski dotyczące europejskich programów certyfikacji cyberbezpieczeństwa. W szczególności Ministerstwo brało udział w przyjęciu pierwszego aktu implementującego europejski program certyfikacji cyberbezpieczeństwa – European Union Common Criteria.

ENISA

W 2023 r. Ministerstwo Cyfryzacji było zaangażowane w ENISA Support Action Fund - krótkoterminowe wsparcie zapewnione przez Komisję Europejską za pośrednictwem Agencji Unii Europejskiej ds. Cyberbezpieczeństwa (ENISA) państwom członkowskim w świetle podwyższonego zagrożenia złośliwymi działaniami w cyberprzestrzeni w związku z trwającymi konfliktami. Wsparcie ma na celu uzupełnienie już realizowanych działań przez państwa członkowskie na rzecz zwiększenia poziomu bezpieczeństwa i odporności na cyberzagrożenia. To wsparcie odbywa się poprzez realizowanie przez ENISA usług ex-ante i ex-post. ENISA wspiera państwa członkowskie w ich działaniach na rzecz zapobiegania, wykrywania, analizowania oraz wzmacniania zdolności w zakresie reagowania na zagrożenia i cyberincydenty. Ministerstwo Cyfryzacji, jako punkt kontaktowy, przekazuje do ENISA listę beneficjentów wraz z określonym priorytetem, współpracując z podmiotami KSC, mogącymi ubiegać się o środki.





Dane ENISA dla poszczególnych sektorów. Źródło: ENISA

Współpraca w ramach NATO

MSZ brało aktywny udział w kształtowaniu polityki cyberbezpieczeństwa NATO w kierunku wzmocnienia potencjału odstraszania Sojuszu, wsparcia Ukrainy, zacieśnienia współpracy cywilno-wojskowej oraz współpracy z sektorem prywatnym (m.in. poprzez prace CDC oraz aktywny udział w pierwszej NATO Cyber Defence Conference). MSZ było również zaangażowanie na rzecz spójnej współpracy UE-NATO w zwalczaniu zagrożeń cybernetycznych, hybrydowych i w zakresie dezinformacji (m.in. poprzez prace grup CDC NATO i HWPCI EU).

W działania w ramach NATO zaangażowane było również Ministerstwo Obrony Narodowej, zarówno na szczeblu strategiczno-politycznym, jak i operacyjnym oraz technicznym.

Ćwiczenia w zakresie cyberbezpieczeństwa i warsztaty

Pełnomocnik Rządu ds. Cyberbezpieczeństwa aktywnie uczestniczył wraz z podmiotami KSC m.in. w międzynarodowych ćwiczeniach NATO CMX 23 oraz Stress Testach „AMBER", co pozwoliło na wzmocnienie i zacieśnienie współpracy międzyinstytucjonalnej. Ćwiczenia te pozwoliły na przetestowanie obecnie obowiązujących procedur. Wypracowane na podstawie ćwiczeń wnioski pozwolą na sprawniejsze i efektywniejsze podejmowanie działań w sytuacjach kryzysowych w przyszłości.

Ministerstwo Cyfryzacji jest pomysłodawcą międzynarodowych warsztatów dla infrastruktury krytycznej. Celem zorganizowanych przez Departament Cyberbezpieczeństwa MC wraz z Departamentem Energii USA i NASK-PIB warsztatów, które odbyły się po raz drugi 5-9 lutego 2024 r. (poprzednie ćwiczenia - styczeń 2023 r.), jest zacieśnianie współpracy i wzajemnych stosunków z USA oraz krajami biorącymi udział (w edycji 2024 eksperci z Polski,

Ukrainy, Holandii, Niemiec, Litwy, Słowacji, Słowenii, Mołdawii, Albanii, Estonii, Łotwy, Rumunii).

Współpraca bilateralna i multilateralna

W kwietniu 2023 r. zawarto *Memorandum Of Understanding* pomiędzy Polską a Mołdawią dotyczące m.in. polsko-mołdawskiej współpracy w obszarze cyberbezpieczeństwa. Należy także odnotować aktywność MSZ poprzez stymulację partnerów krajowych i zaangażowanie własne we wsparcie rozwoju systemu cyberbezpieczeństwa Mołdawii.

Ministerstwo Cyfryzacji prowadzi uzgodnienia ze stroną amerykańską w celu podpisania porozumienia o wzajemnej współpracy w ramach cyberbezpieczeństwa.

Ministerstwo Cyfryzacji we współpracy z MSZ w listopadzie 2023 r. zorganizowało w Warszawie 11. edycję Chińsko-Europejskiego Dialogu nt. Cyberbezpieczeństwa (Sino-European Cyber Dialogue - SECD).

Koordynator ds. międzynarodowych aspektów bezpieczeństwa cybernetycznego i technologicznego MSZ brał regularnie udział w spotkaniach sieci ambasadorów UE ds. cyber, sieci ambasadorów/koordynatorów grupy państw podobnie myślących (like-minded) – w tym ds. kontaktów z sektorem prywatnym, dialogach cyberbezpieczeństwa np. UE-Indie.

Współpraca dwu- i wielostronna była także realizowana przez resort obrony narodowej, np. Dowództwo Wojsk Obrony Terytorialnej współpracowało z Estonian Defence League's Cyber Unit.

Counter Ransomware Initiatives

Ministerstwo Cyfryzacji uczestniczyło w międzynarodowej inicjatywie koordynowanej przez USA pn. „Counter Ransomware Initiatives", która ma na celu połączenie wysiłku działań zaangażowanych państw w zwalczanie zagrożeń typu ransomware. Inicjatywa została zapoczątkowana w październiku 2021 r. przez U.S. National Security Council przy Białym Domu i aktualnie liczy 50 członków. Ministerstwo Cyfryzacji aktywnie uczestniczy w pracach grup roboczych CRI. W szczególności w ramach filaru ICRTF (The International Counter Ransomware Task Force), wspólnie z NASK-PIB, amerykańskim DHS oraz instytutem SANS Ministerstwo Cyfryzacji rozwija projekt RACER (Ransomware Attack Collective Effective Resilience). Obecnie wraz z NASK-PIB prowadzone są prace mające na celu wydanie ostatecznych raportów z projektu. Planowane zakończenie to I kw. 2024 r.

Wsparcie dla Ukrainy i współpraca z Ukrainą

Mechanizm Talliński

Polska bierze aktywny udział w inicjatywach wspierających Ukrainę zaatakowaną przez Federację Rosyjską. Jedną z nich jest Mechanizm Talliński. Jest to grupa państw sojuszniczych w ramach NATO, która ma na celu koordynację i wzajemne wspieranie działań poprawiających cyberbezpieczeństwo Ukrainy oraz budowanie jej odporności na cyberzagrożenia. W ramach tej inicjatywy Polska pełni rolę tzw. Back Office zbierającego zapotrzebowanie strony ukraińskiej w zakresie cyberbezpieczeństwa z jednej strony, a z drugiej oferty konkretnej pomocy i wsparcia od członków grupy.

Inne działania

Ponadto Ministerstwo Cyfryzacji, MON, MSZ i inne krajowe instytucje realizowały także inne działania na rzecz wzmocnienia cyberbezpieczeństwa Ukrainy. Przykładowo, dzięki działaniom

Ministerstwa Cyfryzacji, Polska jest największym donatorem terminali Starlink zapewniających dostęp do Internetu, co ma kluczowe znaczenie dla zapewnienia ciągłości funkcjonowania państwa ukraińskiego, udzielania pomocy humanitarnej oraz zagwarantowania bezpiecznej łączności, także dla realizowania zadań wojskowych. Nie do przeceniania jest też udział Polski w przeniesieniu (i utrzymywaniu) ukraińskiej administracji publicznej i krytycznych usług komercyjnych do zasobów chmurowych. Z kolei resort obrony narodowej m.in. prowadził szkolenia z zakresu cyberbezpieczeństwa dla Sił Zbrojnych Ukrainy, a MSZ brał udział w przygotowaniu projektu TIARA, który ma na celu m.in. zapewnienie bezpośredniego wsparcia podmiotów infrastruktury krytycznej Ukrainy (głównie w obszarze energetyki i transportu).

Inne organizacje międzynarodowe

MSZ obsługuje udział Polski w pracach OBWE w wymiarze cyberbezpieczeństwa. Polska wraz z UE, Szwajcarią i Macedonią zorganizowała wydarzenie towarzyszące spotkaniu Nieformalnej Grupy Roboczej OBWE ds. cyberbezpieczeństwa (IWG), poświęcone środkowi budowy zaufania nr 12 pt. „Development and implementation of confidence building measures in cyber security. Learning from regional experiences and looking for cross-regional synergies". Polska wraz z trzema partnerami poinformowała oficjalnie o zaadoptowaniu CBM12 (rozbudowy systemu praktycznej współpracy pomiędzy państwami OBWE) i przedstawiła non-paper w tej sprawie. Ponadto MSZ brało udział w regularnych spotkaniach Nieformalnej Grupy ds. Cyberbezpieczeństwa OBWE (Informal Working Group) i dorocznej konferencji dot. cyberbezpieczeństwa, jak również obsługiwało sieć punktów kontaktowych ds. cyberbezpieczeństwa w ramach OBWE.

W ramach Organizacji Narodów Zjednoczonych (ONZ) MSZ reprezentował Polskę w pracach Otwartej Grupy Roboczej ds. odpowiedzialnego zachowania państw w cyberprzestrzeni (OEWG). Ponadto MSZ wraz z Ministerstwem Sprawiedliwości i Prokuraturą Krajową reprezentował Polskę w pracach Komitetu Ad Hoc ds. negocjacji konwencji o zwalczaniu cyberprzestępczości. Ambasador Polski przy ONZ w Wiedniu pełniła także funkcję wiceprzewodniczącej Komitetu.

Także Ministerstwo Cyfryzacji było zaangażowane w działania w zakresie cyberbezpieczeństwa w ramach Organizacji Współpracy Gospodarczej i Rozwoju (OECD); Organizacji Bezpieczeństwa i Współpracy w Europie (OBWE); Międzynarodowego Związku Telekomunikacyjny (ITU).

3. Wnioski i rekomendacje

1) Doświadczenia z funkcjonowania Krajowego Systemu Cyberbezpieczeństwa wskazują na potrzebę powołania instytucji koordynującej, dysponującej odpowiednią pozycją ustrojową, kompetencjami, zasobami osobowymi, budżetem i infrastrukturą. Pozwoli to zwiększyć efektywność Systemu i zapewni sprawniejsze reagowanie na zagrożenia w cyberprzestrzeni. Wnioski krajowe oraz z innych państw pokazują, że potrzebna jest instytucja pełniąca centralną rolę w KSC, będąca też jedną „bramą" dla zgłaszania incydentów, a następnie przekazując ich obsługę, w sposób skoordynowany, do właściwego CSIRT-u. Instytucja ta mogłaby również wykorzystywać narzędzia takie jak System S46 dla zautomatyzowania wymiany informacji w ramach systemu.

2) Istnieje potrzeba dalszego zwiększenia zdolności operacyjnych podmiotów Krajowego Systemu Cyberbezpieczeństwa, w szczególności instytucji zapewniających bezpieczeństwo teleinformatyczne na poziomie krajowym, w tym do rozpoznawania zagrożeń w cyberprzestrzeni.

3) Istnieje potrzeba uregulowania kwestii działań ofensywnych w cyberprzestrzeni, aktywnej obrony oraz rozwoju zdolności do tego rodzaju działań, w tym uszczegółowienie zadań służb specjalnych. Szczyt NATO w Warszawie w 2016 r. i uznanie cyberprzestrzeni jako nowej domeny działań zbrojnych Sojuszu Północnoatlantyckiego sprawił, iż wroga aktywność w przestrzeni cyfrowej jest traktowana na równi z atakiem kinetycznym na członków Sojuszu i umożliwia zastosowanie art. 5 Traktatu Północnoatlantyckiego. Oznacza to radykalny wzrost znaczenia bezpieczeństwa cyfrowego również w sferze relacji politycznych i stosunków międzynarodowych. Przedefiniowanie i formalizacja treści omawianego pojęcia oraz uznanie podmiotowości aktywności w cyberprzestrzeni dla warunków traktatowych NATO, powoduje wzrost odpowiedzialności za prowadzone działania i wpływa na wrażliwość czynności podejmowanych w domenie cyfrowej.

   W dobie napiętej sytuacji międzynarodowej i ataków na RP w sferze informacyjnej, umożliwienie prowadzenia samodzielnych działań aktywnych (ofensywnych) jednostkom podległym Siłom Zbrojnym RP może prowadzić do wzrostu napięcia w sferze stosunków międzynarodowych oraz zostać uznane za działania prowokacyjne. Przy trudnej do udowodnienia działalności w cyberprzestrzeni aktywność ta mogłaby zostać określona jako działania zaczepne. W konsekwencji może skutkować to wzrostem napięć w sferze stosunków i prawa międzynarodowego w związku z legalnością prawną i umocowaniem takiej aktywności, a w następstwie do eskalacji napięć i przeniesienia zagrożeń ze sfery cyfrowej do kinetycznej.

   W opinii Pełnomocnika działania jednostek Sił Zbrojnych RP wykonywanych w czasie pokoju w sferze cyberprzestrzeni powinny być skoncentrowane na działaniach defensywnych. Natomiast kompetencje aktywne, z pogranicza działalności specjalnej, należy pozostawić instytucjom do tego powołanym w zakresie ich kompetencyjnym (SKW, SWW, ABW, AW oraz organy ścigania), a działania podmiotów zależnych od SZ RP jako wsparcie wskazanych podmiotów.

   Należy rozważyć doprecyzowanie przepisów dotyczących realizacji czynności operacyjno-rozpoznawczych uprawnionych służb celem rozszerzenia oraz doszczegółowienia ich o działania mające na celu neutralizację zagrożeń w cyberprzestrzeni.

4) Zasadne jest opracowanie krajowego planu przejścia na kryptografię postkwantową, aby Polska była gotowa na tzw. „DzieńQ". Potrzebne jest systemowe podejście do przystosowania wszelkich rozwiązań kryptograficznych (w sektorze publicznym i prywatnym), aby wykorzystywane algorytmy szyfrowania były kwantoodporne, a tym samym zapewniona była poufność informacji w momencie, gdy technologie kwantowe osiągną odpowiedni poziom dojrzałości.

5) Należy budować świadomość ryzyk i znaczenia odpowiedniej strategii bezpieczeństwa, aby organizacje odpowiednio doceniały powagę zagrożeń związanych z cyberbezpieczeństwem oraz wdrażały klarowne strategie bezpieczeństwa.

6) Należy kłaść nacisk na stosowanie najnowszych technologii i aktualizację oprogramowania. Niedoinwestowanie w infrastrukturę teleinformatyczną skutkuje korzystaniem z przestarzałych technologii odbiegających od aktualnych standardów bezpieczeństwa.

7) Kwestią kluczową jest zapewnienie odpowiednich zasobów kadrowych, w aspekcie ilościowym i jakościowym, w szczególności pod kątem skali zagrożeń i związanych z tym stopni alarmowych CRP, które nakładają na podmioty KSC liczne zadania, takich jak obowiązek utrzymywania całodobowych dyżurów komórek bezpieczeństwa i administratorów systemów w trakcie dwuletniego obowiązywania stopnia alarmowego CHARLIE-CRP. Przedłużający się stopień alarmowy CHARLIE-CRP po początkowym okresie, w którym przyczynił się do podniesienia poziomu bezpieczeństwa, po pewnym czasie mógł raczej obniżać zdolności z uwagi na przeciążenie kadr zadaniami wynikającymi ze stopnia alarmowego oraz wkradającą się rutynę (od marca 2024 r. obniżono stopień alarmowy do poziomu BRAVO-CRP).

8) Dobrym krokiem było wprowadzenie Funduszu Cyberbezpieczeństwa. Stanowi on istotny krok w budowaniu silniejszego i bardziej odpornego środowiska cyberbezpieczeństwa w Polsce. Jest to inicjatywa, która nie tylko zapewnia stabilne finansowanie dla działań związanych z ochroną cyberprzestrzeni, ale również promuje świadomość oraz umiejętności w zakresie cyberbezpieczeństwa na szeroką skalę. Fundusz wspiera organy administracji publicznej zapewniając dodatkowe środki dla pracowników jednostek publicznych odpowiedzialnych za zadania dotyczące cyberbezpieczeństwa. Dzięki temu możliwe jest finansowanie inwestycji w nowoczesne narzędzia i technologie, które są niezbędne do zapewnienia bezpieczeństwa w dynamicznym i zmiennym środowisku bezpieczeństwa. Jednak problem pozyskania nowych wykwalifikowanych i doświadczonych kadr wciąż jest obecny. O ile świadczenie teleinformatyczne zmniejszyło odpływ specjalistów ds. cyberbezpieczeństwa z sektora publicznego, o tyle w ograniczony sposób mogło wpłynąć na zwiększenie możliwości ściągnięcia fachowców z rynku prywatnego. Wiąże się to m.in. z tym, iż świadczenie nie jest częścią wynagrodzenia, a „dodatkiem" czasowym, uznaniowym, a przez to pracownicy nie mają pewności czy i w jakiej kwocie mogą się jego spodziewać w kolejnych okresach.

9) Należy szerzej stosować audyty bezpieczeństwa, gdyż wiele podmiotów nie prowadzi ich regularnie, co prowadzi do braku wiedzy na temat słabych punktów w infrastrukturze.

10) Brak wiążącego charakteru przekazywanych zaleceń w zakresie cyberbezpieczeństwa (np. związanych z koniecznością aktualizacji systemów czy niekorzystania/wyłączenia systemów i oprogramowania w podatnych wersjach) wydawanych przez Pełnomocnika czy CSIRT-y poziomu krajowego. W związku z tym zasadne są odpowiednie zmiany legislacyjne. Incydenty, które miały miejsce

w ostatnich latach w sektorze publicznym - wynikające m.in. z niestosowania się do rekomendacji i zaleceń CSIRT-ów poziomu krajowego pokazują, że zasadne jest zwiększenie skuteczności egzekwowania stosowania tych rekomendacji i zaleceń w instytucjach publicznych. Ponadto częściej należałoby stosować mechanizm rekomendacji Pełnomocnika dotyczących konkretnych podatności w rozwiązaniach teleinformatycznych.

11) Zasadne jest usprawnienie i zautomatyzowanie procesu wymiany informacji pomiędzy podmiotami KSC oraz rozważenie utworzenia platformy do wymiany informacji np. ISAC. Jednym ze sposób rozwiązania tego problemu jest wykorzystanie Systemu S46, który będzie dostosowany, rozbudowywany o takie funkcjonalności.
12) W zakresie zakupu pilnych usług i produktów związanych z cyberbezpieczeństwem zasadne jest wprowadzenie rozwiązań umożliwiających wyłączenie stosowania Prawa Zamówień Publicznych (PZP), co usprawniłoby proces zakupowy oraz zwiększyło bezpieczeństwo informacji. Realizacja tego rodzaju zakupów jest czasochłonna, a w przypadku zagrożeń dotyczących cyberbezpieczeństwa kluczowy jest czas reakcji.
13) Systematycznie rośnie liczba incydentów oraz nadużyć w komunikacji elektronicznej. Zasadne jest dostosowanie systemu wymiany informacji o tych zdarzeniach do jednolitych standardów, zarówno z punktu widzenia rozwiązań technicznych, jak również przygotowania odpowiednich regulacji prawnych. Wpływ na powyższą ocenę ma również różnorodność i złożoność rynku telekomunikacyjnego, na którym obecni są zarówno mali, jak i duzi operatorzy. Dlatego też istotne jest stworzenie odpowiednich warunków prawnych do wymiany informacji pomiędzy podmiotami funkcjonującymi na rynku telekomunikacyjnym. Izby gospodarcze oraz inne podmioty zrzeszające operatorów telekomunikacyjnych oczekują od organów państwa właściwych w sprawach telekomunikacji wsparcia merytorycznego oraz koordynacji takiej wymiany. Dlatego też wskazuje się na zasadność powołania CSIRT Telco dla sektora telekomunikacyjnego.
14) Organizacja kolejnej edycji ćwiczeń KSC EXE – do tej pory tego typu ćwiczenia odbyły się jeden raz w 2020 r. W związku ze zmieniająca się sytuacją geopolityczną i krajobrazem zagrożeń, powinno się dokonywać regularnych ćwiczeń z zakresu cyberbezpieczeństwa, aby w sytuacji zmaterializowania się różnych ryzyk podmioty wchodzące w zakres krajowego systemu cyberbezpieczeństwa wiedziały co dokładnie należy robić, z kim się kontaktować i jakie informacje przekazywać. Warto również rozważyć organizację ćwiczeń typu cyberpoligon dla operatorów usług kluczowych.
15) Zasadne jest wprowadzenie rozwiązań teleinformatycznych oraz przepisów prawnych, które spowodują wykorzystanie rządowych sieci odseparowanych od Internetu jako głównych mediów służących do wymiany danych pomiędzy instytucjami rządowymi. Pozwoli to zmniejszyć powierzchnię ataków na systemy teleinformatyczne, a tym samym zmniejszyć ryzyko wycieku danych, w szczególności informacji wrażliwych przesyłanych obecnie przez instytucje w sieci Internet. Rozwój systemu łączności głosowej i transmisji danych dla organów właściwych, podmiotów wchodzących w zakres constituency danego organu właściwego ds. cyberbezpieczeństwa, CSIRT poziomu krajowego i sektorowych, jednostek administracji rządowej na wypadek niedostępności komercyjnych systemów łączności, np. GSM. Zasadne byłoby też powołanie specjalnych podmiotów, które odpowiedzialne będą za zapewnienie dostępu do bezpiecznych rozwiązań

infrastrukturalnych, wpisujących się w Program Wspólnej Infrastruktury Informatycznej Państwa (WIIP).

16) Wprowadzenie Narodowych Standardów Cyberbezpieczeństwa, choć niezwykle ważne, to brak jednoznacznego wskazania co do obowiązku stosowania NSC jako standardu implementacyjnego stanowił pewne wyzwanie dla niektórych instytucji. Ponadto zapisy NSC są bardzo szczegółowe i złożone, co dodatkowo utrudniało ich wdrożenie. Brak odpowiednich funduszy na realizację zadań zmuszał jednostki do korzystania z własnych środków. W przypadku wyboru między procedurami a infrastrukturą, zawsze priorytetem były inwestycje w infrastrukturę kosztem budowy kompleksowego i efektywnego systemu zarządzania bezpieczeństwem informacji w organizacji.
17) Implementacja wypracowanego na forum UE tzw. Toolbox'a 5G, który docelowo pozwoli na bezpieczne wdrażanie technologii sieci mobilnej piątej generacji. Należy również właściwie zaadresować wyzwania związane z bezpieczeństwem łańcucha dostaw (tzw. dostawcy wysokiego ryzyka).
18) Zasadne jest pogłębienie współpracy w obszarze pozyskiwania i wymiany informacji na temat zagrożeń i podatności – rozbudowa struktury Kolegium ds. Cyberbezpieczeństwa.

4. Planowane działania w 2024 roku

W 2024 r. przewidziano wprowadzenie daleko idących zmian, które znacząco przemodelują Krajowy System Cyberbezpieczeństwa.

Na 2024 r. zaplanowane zostało wdrożenie dyrektywy NIS 2. Obecnie w Ministerstwie Cyfryzacji trwają prace nad projektem ustawy wdrażającej ww. dyrektywę. W drugim kwartale 2024 r. wspomniany projekt zostanie skierowany do uzgodnień, konsultacji społecznych i opiniowania. Istotą projektowanych przepisów jest uspójnienie krajowego systemu cyberbezpieczeństwa z przepisami NIS 2 oraz wprowadzenie do niego innych niezbędnych zmian. Ponadto do polskiego porządku prawnego wdrożona będzie dyrektywa CER, w zakresie której wiodące jest RCB.

Na 2024 r. zaplanowano również uchwalenie ustawy mającej na celu dostosowanie polskiego porządku prawnego do obowiązków wynikających z wejścia w życie (w czerwcu 2019 r.) rozporządzenia Parlamentu Europejskiego i Rady (UE) 2019/881 z dnia 17 kwietnia 2019 r. w sprawie ENISA (Agencji Unii Europejskiej ds. Cyberbezpieczeństwa) oraz certyfikacji cyberbezpieczeństwa w zakresie technologii informacyjno-komunikacyjnych oraz uchylenia rozporządzenia (UE) nr 526/2013 (akt o cyberbezpieczeństwie). Projektowane w Ministerstwie Cyfryzacji przepisy przyczynią się do rozwoju rynku certyfikacji cyberbezpieczeństwa w Polsce, a przez to do zwiększenia bezpieczeństwa w tej dziedzinie. Projektowana regulacja ma też ułatwić przedsiębiorstwom konkurowanie na rynku unijnym przez wzajemne uznawanie certyfikatów opartych o programy unijne.

W 2024 r. planowane jest także przyjęcie nowej Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej, która będzie obowiązywać w latach 2025-2029.

Obecny rok upłynie także nad przygotowaniem Prezydencji Rzeczypospolitej Polskiej w Radzie Europejskiej. Jednym z priorytetów prezydencji Polski w Radzie UE będzie cyberbezpieczeństwo.

Polska będzie aktywnie działać na arenie międzynarodowej również w innych formatach współpracy, m.in. planowane jest podpisanie porozumienia w ramach współpracy w zakresie cyberbezpieczeństwa z USA i Wielką Brytanią.

Jako zaangażowany członek Sojuszu Północnoatlantyckiego RP odgrywa ważną rolę we wspieraniu jedności, spójności i solidarności w regionie. Jej strategiczne położenie geograficzne sprawia, że pełni ona istotną funkcję w obronie wschodniej flanki NATO. Obecnie jednym z głównych zadań jest utrzymanie zdolności obronnej NATO i wzmocnienie współpracy w dziedzinie cyberbezpieczeństwa, aby zapewnić skuteczną ochronę przed atakami hakerskimi, które mogą zagrażać jedności, stabilności i bezpieczeństwu Sojuszu oraz wartościom przyświecającym jego istnieniu. Polska uczestniczy w działaniach mających na celu wspieranie stabilności w regionie i przeciwdziałanie zagrożeniom hybrydowym, w tym cyberatakom. Skuteczna obrona cyberprzestrzeni wymaga zintegrowanego podejścia i współdziałania zarówno poszczególnych krajów ze sobą, jak i organów rządowych oraz firm prywatnych, tak aby „żelazne zobowiązanie do obrony siebie nawzajem i każdego centymetra terytorium Sojuszu” pozostało naszym wspólnym, nadrzędnym celem.