

X kadencja



KANCELARIA SEJMU

Biuro Komisji Sejmowych

PEŁNY ZAPIS PRZEBIEGU POSIEDZENIA

■ **KOMISJI ADMINISTRACJI I SPRAW
WEWNĘTRZNYCH
(NR 38)**
z dnia 18 grudnia 2024 r.

Pełny zapis przebiegu posiedzenia Komisji Administracji i Spraw Wewnętrznych (nr 38)

18 grudnia 2024 r.

Komisja Administracji i Spraw Wewnętrznych, obradująca pod przewodnictwem poseł **Marii Małgorzaty Janyskiej (KO)**, przewodniczącej Komisji, oraz posła **Konrada Frysztaka (KO)**, zastępcy przewodniczącej Komisji, rozpatrzyła:

- informację na temat funkcjonowania krajowego systemu cyberbezpieczeństwa z uwzględnieniem podnoszenia odporności systemów teleinformatycznych administracji publicznej;
- informację na temat funkcjonowania Centralnego Biura Zwalczania Cyberprzestępczości w Policji.

W posiedzeniu udział wzięli: **Dariusz Nowak-Nova** dyrektor Departamentu Teleinformatyki w Ministerstwie Spraw Wewnętrznych i Administracji wraz ze współpracownikami, **Agata Furgała** dyrektor Departamentu Porządku Publicznego w MSWiA, **Marcin Wysocki** zastępca dyrektora Departamentu Cyberbezpieczeństwa w Ministerstwie Cyfryzacji, nadinsp. **dr Tomasz Michulka** zastępca komendanta głównego Policji wraz ze współpracownikami, nadbryg. **Józef Galica** zastępca komendanta głównego Państwowej Straży Pożarnej wraz ze współpracownikiem, płk SG **Mariusz Kijowski** dyrektor Biura Łączności i Informatyki w Komendzie Głównej Straży Granicznej, nadinsp. **Adam Cieślak** komendant Centralnego Biura Zwalczania Cyberprzestępczości, płk SOP **Radosław Ryński** dyrektor Zarządu Łączności i Informatyki w Służbie Ochrony Państwa oraz **Mariusz Stolarz** doradcy techniczny Najwyższej Izby Kontroli.

W posiedzeniu udział wzięli pracownicy Kancelarii Sejmu: **Igor Amarowicz**, **Anna Ornat** i **Kamila Pawluczuk** – z sekretariatu Komisji w Biurze Komisji Sejmowych.

Przewodnicząca poseł Maria Małgorzata Janyska (KO):

Dzień dobry, witam państwa serdecznie na posiedzeniu Komisji Administracji i Spraw Wewnętrznych. Stwierdzam kworum. W dzisiejszym porządku obrad mamy propozycję uzyskania informacji na temat funkcjonowania krajowego systemu cyberbezpieczeństwa z uwzględnieniem podnoszenia odporności systemów teleinformatycznych administracji publicznej. Informację przedstawia przedstawiciel Ministerstwa Spraw Wewnętrznych i Administracji oraz Ministerstwa Cyfryzacji. I drugi punkt porządku dziennego to informacja na temat funkcjonowania Centralnego Biura Zwalczania Cyberprzestępczości w Policji – przedstawia minister spraw wewnętrznych i administracji. Czy państwo posłowie mają jakieś uwagi do przedstawionego porządku obrad. Nie widzę zgłoszeń, w takim razie porządek obrad przyjęliśmy.

Szanowni państwo, witam na naszym dzisiejszym posiedzeniu przedstawicieli resortów, które wymieniałam. Miał być z nami pan Tomasz Szymański, minister spraw wewnętrznych i administracji, ale nie będzie obecny z uwagi na to, że ma Komisję Wspólną Rządu i Samorządu i musi w związku z tym brać w niej udział. Witam zastępcę komendanta głównego Państwowej Straży Pożarnej pana nadbryg. Józefa Galicę. Witam zastępcę komendanta głównego Policji pana nadinsp. Tomasza Michulkę. Witam komendanta Centralnego Biura Zwalczania Cyberprzestępczości pana nadinsp. Adama Cieślaka oraz pana Marcina Wysockiego, zastępcę dyrektora Departamentu Cyberbezpieczeństwa w Ministerstwie Cyfryzacji. Witam pana Mariusza Stolarza, doradcę technicznego Najwyższej Izby Kontroli. Witam pana Dariusza Nowaka-Nowę, dyrektora Departamentu Teleinformatyki w Ministerstwie Spraw Wewnętrznych i Administracji, który – z tego, co mi wiadomo – będzie przedstawiał informację w imieniu ministra Tomasza Szymańskiego.

Witam pana Tomasza Świątkowskiego, naczelnika wydziału w Departamencie Teleinformatyki w MSWiA, pana insp. Przemysława Więclawa, dyrektora Biura Łączności i Informatyki w Komendzie Głównej Policji. Witam pana płk. Mariusza Kijowskiego, dyrektora Biura Łączności i Informatyki w Komendzie Głównej Straży Granicznej, oraz st. bryg. Jarosława Pozieraka, dyrektora Biura Bezpieczeństwa Informacji w Komendzie Głównej Państwowej Straży Pożarnej. Witam pana płk. SOP Radosława Ryńskiego, dyrektora Zarządu Łączności i Informatyki w Służbie Ochrony Państwa, panią Agatę Furgalę, dyrektora Departamentu Porządku Publicznego w MSWiA, która będzie przedstawiała informację w imieniu pana ministra Czesława Mrocza. Witam pana Konrada Kaczora, głównego specjalistę w Departamencie Porządku Publicznego w MSWiA. Chyba wszystkich państwa, których mam w wykazie, przedstawiłam, a jeśli popełniłam jakiś błąd w precedencji, to proszę wybaczyć.

Szanowni państwo, w związku z tym, że nam się dzisiaj harmonogramy mocno pozmieniały i jesteśmy..., ale w dużej części Komisji, to zwracam się do państwa z resortu, żebyście nam to wybaczyli. Bardzo wyczerpująca informacja z resortu do nas wpłynęła, posłowie mieli możliwość zapoznania się, a jeśli nie, to na pewno z tego skorzystają, bo to niezwykle ważne informacje, o które sami do planu pracy wnioskowaliśmy. W tej chwili, szanowni państwo, przekażę już głos przedstawicielowi ministerstwa przedstawiającemu pkt 1, czyli informację na temat funkcjonowania krajowego systemu cyberbezpieczeństwa z uwzględnieniem podnoszenia odporności systemów teleinformatycznych administracji publicznej. Bardzo proszę, panie dyrektorze, o przedstawienie tego tematu.

Dyrektor Departamentu Teleinformatyki w Ministerstwie Spraw Wewnętrznych i Administracji Dariusz Nowak-Nova:

Dzień dobry, Dariusz Nowak-Nova, MSWiA. Pani przewodnicząca, Wysoka Komisjo, chciałbym przedstawić krótką informację na temat funkcjonowania krajowego systemu cyberbezpieczeństwa z uwzględnieniem podnoszenia odporności systemów teleinformatycznych administracji publicznej w obszarach odpowiedzialności ministra spraw wewnętrznych i administracji.

Cyberbezpieczeństwo jest pojęciem odnoszącym się do zapewnienia ochrony i przeciwdziałania zagrożeniom, które dotyczą cyberprzestrzeni. W krajowym systemie prawnym za obszary te odpowiada Ministerstwo Sprawiedliwości, w którym umocowany jest także pełnomocnik rządu do spraw cyberbezpieczeństwa. Minister spraw wewnętrznych może opisywać tylko funkcjonowanie krajowego systemu w obszarach: sprawy wewnętrzne i administracja, czyli w obszarach, za które odpowiada, i w takim kontekście została przygotowana informacja, która została państwu przekazana.

Informacja ta została podzielona na dwie części. Część pierwsza koncentruje się na opisie funkcjonowania krajowego systemu bezpieczeństwa w obszarze sprawy wewnętrzne i zawiera opis działań tego systemu cyberbezpieczeństwa, który jest tworzony przez MSWiA i służby mu podległe: Policję, Straż Graniczną, Państwową Straż Pożarną...

Przewodnicząca poseł Maria Małgorzata Janyska (KO):

Przepraszam bardzo, ale trochę te rozmowy i śmiechy przeszkadzają w wypowiedaniu się. Bardzo proszę.

Dyrektor departamentu w MSWiA Dariusz Nowak-Nova:

Przedstawiciele tych służb są obecni dzisiaj na sali, więc jeśli będziecie państwo mieli w trakcie posiedzenia szczegółowe pytania, to będziemy gotowi udzielać odpowiedzi na te zagadnienia.

Część druga opisuje szczegóły związane z działaniami mającymi na celu podnoszenie odporności konkretnych systemów, za działanie których odpowiada minister spraw wewnętrznych. Podzielone to jest na trzy duże grupy tematów: systemy wewnętrzne, które są warstwą transportową dla administracji rządowej, systemy, które są wykorzystywane głównie w obszarze bezpieczeństwa, porządku publicznego i numeru ratunkowego, a także warstwa transportowa paneuropejskiej sieci TESTA-ng. Warstwa ta znalazła się w tym opisie z tego względu, że z punktu widzenia Unii Europejskiej odpowiadamy również za obszar, który unia definiuje jako obszar sprawy wewnętrzne i sądownictwo, i w takim kontekście minister spraw wewnętrznych i administracji uczestniczy

w tych działaniach. To, co dla nas może być na przykład związane tylko z ochroną granicy, z punktu widzenia UE jest też dbaniem o porządek całej UE, stąd znalazł się również taki kontekst. W ostatniej części krótko opisujemy nasze wnioski i pewnego rodzaju rekomendacje na przyszłość. My je opracowujemy dla siebie, po to żeby zaplanować rozwój tych zagadnień w przyszłości.

Nawiązując jeszcze do tematu związanego z systemami paneuropejskimi, szczególnego podkreślenia wymaga bardzo dobra współpraca pomiędzy Policją, Strażą Graniczną, Urzędem do Spraw Cudzoziemców, które bezpośrednio realizują te tematy, a także ministerstwami, które uczestniczą w obszarach wielkoskalowych systemów informatycznych, bo to jest ten obszar. I to jest Ministerstwo Spraw Zagranicznych, Ministerstwo Finansów, Ministerstwo Sprawiedliwości, Ministerstwo Cyfryzacji i Agencja Bezpieczeństwa Wewnętrznego.

MSWiA oraz organy, jednostki organizacyjne nadzorowane lub podległe ministrowi sukcesywnie rozwijają się w zakresie transformacji cyfrowej, wysoko stawiając zagadnienia dotyczące cyberbezpieczeństwa, cyberodporności, a także zapewnienia ciągłości działania usług. W ramach aktywów resortu znajdują się różnorodne technologicznie systemy, użytkowane także przez inne organy administracji publicznej, a także systemy teletransmisyjne, które wymieniają informacje na szczeblu rządowy, a także na szczeblach międzynarodowych. MSWiA odpowiada za bezpieczeństwo infrastruktury telekomunikacyjnej, zapewniającej niezawodną i bezpieczną transmisję danych dla klientów wchodzących w skład administracji rządowej. To jest głównie sieć GovNet, która jest szczegółowo opisana w informacji. Za ogólnopolską platformę teletransmisyjną, wykorzystywaną przez służby bezpieczeństwa i porządku publicznego oraz ratownictwa uznawany jest system OST 112, również szeroko opisany w informacji, a za infrastrukturę umożliwiającą przesyłanie danych i realizację usług z interesariuszami europejskimi – paneuropejska sieć TESTA-ng, również opisana. Aktywa te odgrywają istotną rolę w realizacji zadań zarówno przez MSWiA, jak i podległe mu służby, odpowiedzialne za bezpieczeństwo obywateli i utrzymanie porządku publicznego. Systemy te stanowią nieodłączną część infrastruktury krytycznej w obszarze ochrony bezpieczeństwa publicznego, granic, ochrony przeciwpożarowej oraz bezpieczeństwa państwa. Infrastruktura ta podlega ochronie realizowanej przez CSIRT GOV, prowadzonej przez szefa ABW. Bezpośrednio za bezpieczeństwo tych systemów MSWiA odpowiada Departament Teleinformatyki.

W MSWiA funkcjonuje system zarządzania bezpieczeństwem informacji, zapewniona jest ochrona przetwarzanych informacji przed ich kradzieżą, nieuprawnionym dostępem, uszkodzeniem. Istnieją mechanizmy zabezpieczające informacje w sposób uniemożliwiający nieuprawnione ich udostępnienie i przekazanie. W 2023 r. w ramach przeglądu systemu zaktualizowano polityki i procedury na potrzeby zarówno obszaru bezpieczeństwa informacji, jak i obszaru cyberbezpieczeństwa, ponieważ obszar cyberbezpieczeństwa staje się coraz poważniejszym wyzwaniem. Z tego też względu wszystkie umowy podpisywane pomiędzy MSWiA a dostawcami usług, głównie w obszarze teleinformatyki, posiadają instrukcje bezpieczeństwa, czyli pewnego rodzaju zbiór wymagań organizacyjnych i technicznych, jakie muszą spełniać podmioty chcące dostarczać usługi do MSWiA.

W MSWiA powołany został pełnomocnik do spraw bezpieczeństwa cyberprzestrzeni, odpowiadający między innymi za monitorowanie stanu bezpieczeństwa sieci i systemów teleinformatycznych, monitorowanie informacji o zagrożeniach cybernetycznych, a także inicjowanie i koordynowanie zadań w zakresie bezpieczeństwa. Nie mamy w MSWiA dedykowanego SOC-u, czyli specjalnej grupy security operations center, która nadzorowałaby administrację rządową. Sami podlegamy CSIRT-owi organizowanemu przez ABW, natomiast zauważyliśmy taką potrzebę i w latach przyszłych będziemy rozwijali taki SOC dla administracji rządowej szczebla wojewódzkiego i administracji zespolonej.

Policja wdraża zaawansowane rozwiązania w obszarach informatyki, teletransmisji, telekomunikacji, a także radiokomunikacji. Projektowane i wdrażane są rozwiązania teleinformatyczne w obszarach cyberbezpieczeństwa zasobów informacyjnych. W celu wymiany informacji o incydentach i zagrożeniach Policja współpracuje również z CSIRT-em górnym prowadzonym przez szefa ABW. Realizując zadania związane z zapewnieniem bezpieczeństwa cyberprzestrzeni na poziomie krajowym, Policja współpracuje także z wiodącymi

podmiotami w zakresie cyberbezpieczeństwa. Mowa tu o pomiotach komercyjnych, z którymi zawierane są odpowiednio klauzulowane umowy i porozumienia zapewniające operacyjność działań. Policja zapewnia zgodność swoich systemów z normami dotyczącymi bezpieczeństwa, nadzoruje krajowy system informatyczny, który zawiera wiele systemów realizujących usługi objęte również procedurami bezpieczeństwa. Zarządza tym Biuro Łączności i Informatyki KGP. Jednocześnie biuro łączności realizuje w sposób praktyczny szkolenia dla funkcjonariuszy w obszarach dotyczących cyberbezpieczeństwa.

Straż Graniczna wykorzystuje szereg programów teleinformatycznych do kontroli ruchu granicznego. Głównie są to systemy budowane bezpośrednio przez funkcjonariuszy SG, ponieważ podjęto tam decyzję o stworzeniu siłami wewnętrznymi dużej grupy programistycznej odpowiedzialnej za budowanie aplikacji dla uniknięcia sytuacji, w której pewnego rodzaju rozwiązania są kupowane na rynku. Od kilku lat SG realizuje te procedury, one się sprawdzają i dalej jest planowany rozwój tego rodzaju działań. Obszar cyberbezpieczeństwa SG objęty został kompleksowym systemem o nazwie KORUND, który obejmuje systemy monitorowania, reagowania i ochrony przed cyberzagrożeniami. Jednocześnie system KORUND stanowi zewnętrzną barierę ochronną dla strategicznych aplikacji budowanych samodzielnie przez SG. Te aplikacje, które buduje SG, działają wewnętrznie, a jednocześnie są one końcówkami europejskich systemów w ramach działań paneuropejskich. W SG realizowane są okresowe audyty bezpieczeństwa, w ramach których weryfikowana jest zgodność stanu rzeczywistego z zapisami dokumentacji. Realizowane są też procedury inwentaryzacyjne sprzętu. Decyzją Komendanta Głównego SG powołany został komitet do spraw bezpieczeństwa teleinformatycznego oraz zespół security operations center, do zadań którego należy, poza bieżącą obsługą incydentów, wynikającą z ustawy, również wymiana informacji z pozostałymi CSIRT-ami poziomu krajowego.

Komenda Główna Państwowej Straży Pożarnej prowadzi działania mające na celu bezpieczne użytkowanie środowiska teleinformatycznego. W SG zauważono, że problem cyberbezpieczeństwa powinien zostać sformalizowany, dlatego przygotowano projekt wdrożenia zintegrowanego systemu zarządzania bezpieczeństwem informacji. Straż pożarna ma swój wewnętrzny zespół odpowiedzialny za cyberbezpieczeństwo i również podlega ochronie przez CSIRT GOV. Wymienia się również informacjami o zagrożeniach z pozostałymi CSIRT-ami. W 2023 r. wykonywane były okresowe audyty oraz skanowania sieci i są to już czysto technologiczne zagadnienia. Oprócz dużych audytów, takich prawie że horyzontalnych, realizowano też audyty dedykowane, dziedzinowe, po to żeby odnajdywać luki w zabezpieczeniach i móc im przeciwdziałać.

Jeżeli chodzi o Służbę Ochrony Państwa, to powiem jedynie, że sukcesywnie rozwija swoje systemy i to w zasadzie wszystko, co powinno dotyczyć tej służby.

Wszystkie szczegółowe działania związane z odpłatnością systemów są opisane w przedstawionej państwu informacji, nie chciałbym powielać treści tam zawartych. Dlatego myślę, że tytułem wprowadzenia zakończyłbym teraz i pozostajemy do dyspozycji, jeśli będą jakieś pytania. Dziękuję.

Przewodnicząca poseł Maria Małgorzata Janyska (KO):

Dobrze, dziękuję bardzo. Czy ktoś jeszcze z przedstawicieli resortu i podległych służb chciałby w tym momencie zabrać głos? Nie widzę zgłoszeń. W takim razie otwieram dyskusję... Przepraszam, może jeszcze wysłuchamy informacji przedstawiciela MC, bo to jest w tym samym temacie i wtedy otworzymy dyskusję. Od pana ministra Standerskiego z MC wiemy, że informację przedstawi pan Marcin Wysocki, zastępca dyrektora Departamentu Cyberbezpieczeństwa, tak że bardzo proszę.

Zastępca dyrektora Departamentu Cyberbezpieczeństwa w Ministerstwie Cyfryzacji Marcin Wysocki:

Bardzo dziękuję, pani przewodnicząca. Marcin Wysocki, zastępca dyrektora Departamentu Cyberbezpieczeństwa w MC. Pani przewodnicząca, Wysoka Komisjo, szanowni państwo, kilka słów o krajobrazie bezpieczeństwa cyberprzestrzeni.

Utrzymuje się wysoki poziom zagrożeń w cyberprzestrzeni w skali globalnej, co powoduje oczywiście także wysoki poziom cyberzagrożeń w Polsce. Wzrasta aktywność różnego rodzaju grup prowadzących nielegalne działania w świecie cyfrowym, począwszy

od hakywistów, przez grupy cyberprzestępcze o charakterze zarobkowym, po grupy powiązane z innymi państwami, tzw. grupy APT. Wysoki poziom cyberzagrożeń w dzisiejszym dynamicznym środowisku cyfrowym ma wpływ na codzienne funkcjonowanie obywateli, przedsiębiorstw i instytucji państwa, wymaga ciągłego doskonalenia funkcjonowania krajowego systemu cyberbezpieczeństwa. Polska pozostaje celem licznych cyberataków, w tym operacji prowadzonych przez służby wrogich państw, obliczonych na pozyskanie kluczowych informacji, rozpoznanie systemów ICT na potrzeby potencjalnych przyszłych cyberataków, zakłócanie infrastruktury krytycznej i innych kluczowych zasobów, jak również szerzenie dezinformacji mającej na celu rozpropagowanie nieprawdziwych informacji i własnych narracji oraz pogłębianie polaryzacji społecznej. Wobec trwającej wojny Rosji z Ukrainą, w której Polska pełni rolę hubu do wsparcia Ukrainy oraz sama udziela wielkoskalowej pomocy, intensyfikacji uległy cyberataki wymierzone w infrastrukturę, logistykę i systemy transportowe. Co istotne, w samym roku 2023 zespół CSIRT NASK, czyli jeden z trzech CSIRT-ów poziomu krajowego, obsłużył ponad 80 tys. incydentów cyberbezpieczeństwa, czyli takich incydentów, które mają lub mogą mieć wpływ na bezpieczeństwo systemów informacyjnych, z których korzystają kluczowe przedsiębiorstwa. Oznacza to wzrost o ponad 100% rok do roku. W bieżącym roku natomiast od stycznia CSIRT NASK obsłużył już ponad 100 tys. takich incydentów.

Pani przewodnicząca, mam jeszcze dwa komponenty wystąpienia. Pierwszy dotyczy przybliżenia podstawowych podmiotów krajowego systemu cyberbezpieczeństwa i projektów realizowanych przez MC. Czy to ujęcie podmiotowe przedstawić ogólnie, czy zakładamy, że członkowie Komisji zapoznali się z tymi materiałami?

Przewodnicząca poseł Maria Małgorzata Janyska (KO):

Myślę, że możemy przyjąć, że członkowie Komisji zapoznali się z materiałami i będą pytali ewentualnie w swoich wystąpieniach, żeby doprecyzować.

Zastępca dyrektora departamentu w MC Marcin Wysocki:

Dziękuję, pani przewodnicząca. W związku z tym tylko jedno słowo. Pan dyrektor opowiedział o roli MSWiA i służb podległych. Krajowy system cyberbezpieczeństwa to wiele podmiotów o różnych funkcjach, z CSIRT-ami poziomu krajowego, z organami właściwymi do spraw cyberbezpieczeństwa, z administracją publiczną, z operatorami usług kluczowych, których jest prawie 400. Szczegółowa informacja została przekazana Komisji, więc przejdę do zadań, które są realizowane przez MC.

Obecnie z MC mamy to szczęście, że kumulujemy wiele bardzo ważnych funkcji z perspektywy krajowego systemu cyberbezpieczeństwa. Mamy ministra cyfryzacji, który ma swoje zadania, jak również pełnomocnika rządu do spraw cyberbezpieczeństwa, którym obecnie jest pan premier Krzysztof Gawkowski. Pełnomocnik rządu do spraw cyberbezpieczeństwa odpowiada za koordynowanie działań i realizowanie polityki rządu w zakresie zapewnienia cyberbezpieczeństwa w RP. Liczne zadania na poziomie krajowym realizowane przez MC mogą być należycie skoordynowane z działaniami innych instytucji zapewniających cyberbezpieczeństwo. Pełnomocnik i MC stanowią centralny element kształtujący obecnie krajowy system cyberbezpieczeństwa. Obecnie procesowany projekt nowelizacji ustawy o krajowym systemie cyberbezpieczeństwa przewiduje na stałe przypisanie funkcji pełnomocnika do MC oraz rozszerzenie jego kompetencji. Jednym z istotnych instrumentów będących już obecnie w rękach pełnomocnika, który pozwala na podnoszenie cyberbezpieczeństwa kraju, są rekomendacje, które mogą wykluczyć na przykład podatne rozwiązania. W bieżącym roku pełnomocnik rządu do spraw cyberbezpieczeństwa wydał rekomendacje oraz komunikaty z zaleceniami, reagując na pojawiające się zagrożenia. To były rekomendacje dotyczące bezzwłocznej aktualizacji produktów Fortinet, rekomendacja dotycząca obowiązku niestosowania systemów SmoBIP i MegaBIP jako platform Biuletynu Informacji Publicznej do udostępniania informacji publicznej. Ponadto rekomendacja dotycząca oprogramowania Zimbra Collaboration, komunikat w związku ze zwiększeniem zagrożenia atakami DDoS, komunikat w sprawie zabezpieczenia infrastruktury teleinformatycznej administracji samorządowej na terenach zagrożonych powodzią, komunikat w sprawie oszustw w komunikacji z osobami publicznymi, podszywanie się pod przedstawicieli innych państw między innymi,

komunikat z zaleceniami w związku ze wzrostem liczby incydentów związanych z wyciekiem danych.

Przy Radzie Ministrów działa również taki organ jak Kolegium do Spraw Cyberbezpieczeństwa. Jest to organ opiniodawczo-doradczy w sprawach cyberbezpieczeństwa oraz działalności w tym zakresie: CSIRT-ów poziomu krajowego, sektorowych zespołów cyberbezpieczeństwa i organów właściwych do spraw cyberbezpieczeństwa. Do zadań kolegium należy także opracowanie rekomendacji dla Rady Ministrów dotyczących działań w zakresie zapewnienia cyberbezpieczeństwa na poziomie krajowym. W tym roku odbyły się organizowane przez MC cztery posiedzenia kolegium, którym przewodniczył wicepremier i minister cyfryzacji. Na posiedzeniach zapadły decyzje na temat przyznania dodatkowych świadczeń teleinformatycznych dla ekspertów do spraw cyberbezpieczeństwa sektora publicznego. Wydano także opinie Kolegium do Spraw Cyberbezpieczeństwa w sprawie aukcji i wymagań bezpieczeństwa dla sieci 5G w paśmie 700 MHz oraz 800 MHz. Analizowano również aktualne zagrożenia w cyberprzestrzeni, w tym te związane z wyludzeniami finansowymi.

Jak już wspominałem, MC w porozumieniu w Rządowym Centrum Bezpieczeństwa, ze służbami podległymi i z ministrami, prowadzimy wspólnie połączone centrum operacji cyberbezpieczeństwa. Funkcjonowanie takiego połączonego centrum na poziomie roboczym umożliwia szybką wymianę informacji, co również pozwala podnieść poziom cyberbezpieczeństwa w kraju i reagować na incydenty. W procedowanej nowelizacji ustawy o krajowym systemie cyberbezpieczeństwa jest planowane sformalizowanie tej współpracy i dalszy rozwój.

MC, szanowni państwo, prowadzi masę projektów kluczowych z zakresu cyberbezpieczeństwa Polski. Ja powiem superzwężle: od projektu Anty-DDoS – to jest projekt, który minister cyfryzacji zlecił Naukowej i Akademickiej Sieci Komputerowej – Państwowemu Instytutowi Badawczemu – zapewnienie ochrony przed atakami DDoS dla instytucji centralnych. MC chroni przed atakami DDoS 76 instytucji, w tym Siły Zbrojne Rzeczypospolitej Polskiej oraz służby. System rozpoznawania zagrożeń w cyberprzestrzeni jako drugi projekt, dostęp do platformy rozpoznawania zagrożeń w cyberprzestrzeni CTI na potrzeby MC i ośmiu innych instytucji zapewniających bezpieczeństwo teleinformatyczne na poziomie krajowym, pozyskiwanie oraz przetwarzanie informacji dotyczących aktywności grup APT, stanowiących zagrożenie dla bezpieczeństwa państwa. Platforma jest aktywnie wykorzystywana przez zespoły CSIRT. Trzeci projekt, system 46, to system teleinformatyczny, który wspiera zgłaszanie i obsługę incydentów, wymianę informacji, współpracę pomiędzy uczestnikami krajowego systemu cyberbezpieczeństwa. Jest projekt ABW, o którym również warto wspomnieć, system wczesnego ostrzegania o zagrożeniach w Internecie. Powstał na potrzeby wsparcia ochrony zasobów teleinformatycznych podmiotów administracji państwowej oraz operatorów infrastruktury krytycznej w 2023 r. System zanotował łącznie ponad 1,5 mld przepływów, co przełożyło się na ponad 6 mln wygenerowanych alarmów, z czego ponad 500 tys. miało charakter pilny, czyli wymagało natychmiastowej reakcji i mogło stwarzać poważne zagrożenie.

Kolejny projekt to Artemis, projekt CSIRT NASK – narzędzie służące do wykrywania najczęściej występujących podatności i błędów konfiguracyjnych, obecnych w ramach usług sieciowych, przekazywania osobom odpowiedzialnym za dany system informacji o znalezionych podatnościach i błędach konfiguracyjnych. Od początku roku łącznie przeskanowano 250 tys. domen i adresów IP i około 580 tys. subdomen. Każdego miesiąca NASK wysyła kilka tysięcy powiadomień do placówek oświatowych, uczelni, jednostek samorządu terytorialnego, placówek medycznych, mediów lokalnych, osób odpowiedzialnych za bezpieczeństwo systemów w domenie gov.pl, a także operatorów usług kluczowych.

I jeszcze dwa projekty. Bezpieczna łączność – w ramach bezpiecznej łączności MC uruchomiło aplikację komunikator w celu zapewnienia bezpiecznej komunikacji rządowej i krajowego systemu cyberbezpieczeństwa na urządzeniach służbowych. Komunikator został uruchomiony w wersji mobilnej, webowej, dzięki najnowocześniejszemu szyfrowaniu end-to-end. Dzięki lokalnemu zarządzaniu zapewnia on bezpieczniejsze i w pełni kontrolowane rozwiązywanie zarządzane i nadzorowane przez MC, z powodzeniem

wykorzystywane do celów służbowych w komunikacji 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 i liczba ta stale rośnie. System umożliwia udział w nim nawet 10 tys. osób. Planowany jest dalszy rozwój komunikatora, aplikacja jest stale monitorowana, updatowana i rozwijana zgodnie z aktualnymi standardami. W ramach komunikacji również projekt ministra cyfryzacji dotyczący zwiększenia zdolności do przetwarzania informacji niejawnych z klauzulą „zastrzeżone” – jest to system mobilny łączności niejawnej, również na potrzeby kluczowych partnerów administracji publicznej, ponieważ dostęp do łączności, zapewnienie bezpiecznych łączy jest niewątpliwie kwestią fundamentalną do zapewnienia bezpieczeństwa.

Z ważnych przedsięwzięć wzmacniających krajowy system cyberbezpieczeństwa – Fundusz Cyberbezpieczeństwa i świadczenia teleinformatyczne. Coraz większe wyzwania stoją przed instytucjami publicznymi odpowiedzialnymi za cyberbezpieczeństwo państwa, ponadto trzeba zadbać o wysoko wykwalifikowaną kadrę ekspertów do spraw cyberbezpieczeństwa, która jest bardzo pożądana również na rynku prywatnym, z którym my jako instytucja publiczna musimy nieraz rywalizować. W 2021 r. został utworzony Fundusz Cyberbezpieczeństwa; środki przeznacza się na wyrównanie poziomu wynagrodzeń w sektorze prywatnym i publicznym, ustabilizowanie fluktuacji zatrudnienia specjalistów do spraw cyberbezpieczeństwa. W bieżącym roku Fundusz Cyberbezpieczeństwa zwiększono do prawie 350 mln zł, w tym 173 mln zł z budżetu państwa, a w 2025 r. wyniesie on 355 mln zł, w tym 250 mln zł z budżetu państwa, zgodnie z projektem ustawy budżetowej.

Cyberbezpieczeństwo rejestrów państwowych, cyfrowych usług publicznych. Ciągłe rozwijamy usługi cyfrowe dla obywateli, utrzymujemy i rozwijamy państwowe systemy i rejestry, również kluczowe dla ciągłości funkcjonowania państwa w Centralnym Ośrodku Informatyki, który jest odpowiedzialny za rozwój i utrzymanie wielu rejestrów państwowych i usług cyfrowych, takich jak mObywatel. Funkcjonuje zespół security operations center – czym zajmuje się taki zespół, nie będę powtarzał wypowiedzi pana dyrektora; odpowiedź na aktualne zagrożenia, które pojawiają się w czasie rzeczywistym.

I już zupełnie krótko – projekt „Cyberbezpieczny Samorząd”. Do jednostek samorządu terytorialnego trafi ponad 1,5 mld zł na wzmocnienie potencjału ochrony przed zagrożeniami i obejmie 2500 jednostek samorządu terytorialnego. Centrum Cyberbezpieczeństwa NASK – budowa centrum oraz utworzenie siedmiu nowych ośrodków i laboratoriów; całkowita wartość projektu to 310 mln zł. CSIRT-y sektorowe w ramach nowelizacji ustawy o krajowym systemie cyberbezpieczeństwa; w poszczególnych sektorach mogą funkcjonować takie zespoły z większymi kompetencjami w stosunku do tych, które mają obecnie. W myśl przygotowanej nowelizacji na realizację takich inwestycji na CSIRT-y sektorowe zostanie przeznaczonych 66 mln zł z Krajowego Planu Odbudowy.

Bezpieczna chmura dla administracji publicznej – pod koniec października wprowadziliśmy ważne zmiany w inicjatywie Wspólna Infrastruktura Informatyczna Państwa, które poprawiają efektywność i bezpieczeństwo usług świadczonych publicznie oraz umożliwiają korzystanie przez podmioty administracji rządowej z usług przetwarzania w publicznej chmurze obliczeniowej. Powszechniejsze korzystanie z usług przetwarzania w chmurze przyczyni się do podniesienia poziomu bezpieczeństwa przetwarzanych danych, trwałego obniżenia kosztów stałych przetwarzania danych, efektywności wydatkowania środków, skrócenia czasu realizacji nowych przedsięwzięć informatycznych. W kolejnych latach chcielibyśmy uruchomić także we współpracy z partnerami chmurę dla administracji rządowej. Są jeszcze stopnie alarmowe CRP, na pewno administracja publiczna doskonale wie, jakie wyzwania się z tym wiążą – wzmocnienie monitorowania systemów informatycznych.

Współpracujemy oczywiście w ramach różnych gremiów międzynarodowych, w ramach UE. Jednym ze sztandarowych elementów naszych działań jest projekt Secure V prowadzony od 2021 r. we współpracy z NASK PIB. Projekt koncentruje się na zapewnieniu specjalistycznych indywidualnych szkoleń z zakresu cyberbezpieczeństwa dla osób pełniących kluczowe funkcje publiczne. Jest to bardzo ważne, żeby świadomość w tej grupie jak najbardziej podnosić. W ramach projektu Secure V przeszkolono ponad

2 tys. najważniejszych osób w państwie. Mamy też szkolenia dla podmiotów krajowego systemu cyberbezpieczeństwa, inne działania szkoleniowe skierowane do kadr podmiotów krajowego systemu cyberbezpieczeństwa, pracowników administracji publicznej, jednostek samorządu terytorialnego i w tym zakresie również jest współpraca z NASK PIB.

Mógłbym tak jeszcze długo, pani przewodnicząca, ale może na tym zakończę. Bardzo dziękuję.

Przewodnicząca poseł Maria Małgorzata Janyska (KO):

Dziękuję bardzo. To bardzo ważne, interesujące informacje. Szanowni państwo, otwieram dyskusję na ten temat. Zgłosił się pan poseł Rutnicki, ale zanim panu Jakubowi oddam głos, to pozwolę sobie zadać kilka pytań, bo niestety z powodu innej aktywności za chwilę będę musiała państwa opuścić. Ale oczywiście zapoznam się później z odpowiedziami, których państwo udzielicie.

Chciałabym dopytać o zagrożenie dla infrastruktury krytycznej, o której jest mowa w informacji, którą państwo przedstawiliście. Czy jakieś dane liczbowe możecie państwo nam podać, jeśli chodzi o liczbę ataków na infrastrukturę krytyczną? Jak to się kształtuje w porównaniu do lat poprzednich i na jakich etapach te cyberataki były wykrywane? Chciałabym też skierować pytanie dotyczące rekomendacji i zaleceń MC, bo zainteresowały mnie rekomendacje i zalecenia dotyczące platformy do biuletynów informacji publicznej. Jakie były zagrożenia, jaka statystyka w tym zakresie i jakie ewentualnie skutki z tym związane? I jeszcze kadra, którą państwo pozyskujecie i macie zamiar pozyskiwać w ramach Funduszu Cyberbezpieczeństwa oraz wyrównywania wynagrodzeń w relacji do specjalistów ze sfery prywatnej – chciałabym uzyskać kilka bliższych informacji dotyczących tego, na jakim poziomie jesteśmy w tej chwili? Czy te wynagrodzenia już są porównywalne? W jakim zakresie, na przykład procentowo, te wynagrodzenia nie przystają do sfery prywatnej? A teraz bardzo proszę, pan poseł Rutnicki.

Poseł Jakub Rutnicki (KO):

Bardzo dziękuję, pani przewodnicząca. Wysoka Komisjo, mówimy na temat cyberbezpieczeństwa i szerzenia dezinformacji w Internecie. Chciałem państwu przytoczyć kilka wpisów z portalu X, bo sam byłem ofiarą takiego ataku na moją osobę kilka dni temu, gdzie próbowano mnie dyskredytować w związku z moim wystąpieniem sejmowym. Nagle pojawiły się infografiki zarzucające mi przestępstwa seksualne w miejscach, w których nigdy nie byłem. Oczywiście chodziło o maksymalne zaatakowanie danej osoby.

Jak wejście państwo na portal X, w tej chwili, to jest taki człowiek jak Robert Wiśniewski: „Tusk, Siemoniak, Wiczorek, Brejzowie zamordowali 27-latkę w Inowrocławiu”. Polecicie dalej, zobaczycie twarz premiera najjaśniejszej Rzeczypospolitej, Hitlera, Stalina, rzeczy absolutnie skandaliczne, rzeczy, które są karalne pod każdym względem. I te treści cały czas są sączone w Internecie, często na zamówienie polityczne. Chciałabym się dowiedzieć albo też chciałabym do państwa zaapelować, bo zdajemy sobie sprawę, że kwestia dotycząca tego, w jaki sposób łatwo można kogoś zdyskredytować, w jaki sposób łatwo można kogoś zaatakować... ja oczywiście z mojej strony tę sprawę zgłosiłem na Policję i mam nadzieję, że Policja wykaże się skutecznością w tej kwestii, aby osoby, które przecież w sposób cyniczny szerzą dezinformacje... Szanowni państwo, to jest pomówienie premiera, ministra spraw wewnętrznych i administracji. Jak państwo wejście na portal X i wpisze Robert Wiśniewski – proszę zobaczyć te treści, szanowni państwo, naprawdę proszę zobaczyć te treści. To jest nienawiść, kłamstwo, to są pomówienia, to jest dyskredytowanie wszystkich osób. Oczywiście na tym portalu jest tylko jeden pozytywny wpis, tu są setki wpisów, które atakują polityków, które po prostu kłamią w sposób bardzo bolesny. Jeden pozytywny wpis jest na tym portalu i oczywiście rośnie poparcie dla kandydata PiS w wyborach prezydenckich. To jest jedyny wpis, który jest tylko i wyłącznie pozytywny, wszystko inne są totalnym hejtem, totalnym kłamstwem.

Uważam, że takie rzeczy każdy z nas powinien zgłaszać, ale czasami po prostu nie ma na to siły, jeżeli chodzi o ilość tego typu kłamliwych treści. Odpowiednie instytucje powinny tego typu kwestiami się zajmować, bo naprawdę, szanowni państwo, warto... może nie warto, ale trzeba zobaczyć, jakiego typu treści są tam sączone i w jaki sposób to działa. Takich rzeczy nie powinno być i myślę, że one powinny być z automatu

usuwane, bo są wierutnym kłamstwem i dyskredytacją ludzi zajmujących najważniejsze urzędy publiczne w naszym kraju. Bardzo dziękuję.

Przewodnicząca poseł Maria Małgorzata Janyska (KO):

Teraz pan Łukasz Ściebiorowski, bardzo proszę.

Poseł Łukasz Ściebiorowski (KO):

Dziękuję, pani przewodnicząca. Szanowna Komisjo, szanowni goście, oczywiście to bardzo ważny temat, bo nasze życie jest tak teraz zależne od świata cyfrowego, że nie da się tego rozdzielić. Jesteśmy atakowani i to praktycznie wszyscy, niezależnie od stanowisk, od funkcji przez maile, telefony itd., itd. – było o tym mówione. I na pewno tak jak już wybrzmiało w wypowiedzi posła, wiele tych rzeczy jest realizowanych w naszym kraju przez różne środowiska, pewnie też w części polityczne.

Ale chciałem zapytać, z jakich innych krajów jesteśmy najczęściej atakowani, jeżeli chodzi o cyberprzestępczość? Jeden kraj sam się nasuwa na myśl, ale czy mamy dane, skąd te ataki się pojawiają i jak my sobie z nimi radzimy? Czy istnieje współpraca z policją z tamtych krajów, z instytucjami, żeby to zwalczać, czy to jest utrudnione poza UE, jeżeli dotyczy to innych krajów? Bo pewnie z tamtego kierunku tych ataków jest najwięcej. Prosiłbym, żeby przybliżyć ten temat. Dziękuję bardzo.

Przewodniczący poseł Konrad Fryszak (KO):

Bardzo dziękuję. Proszę o zabranie głosu pana posła Kaletę.

Poseł Piotr Kaleta (PiS):

Bardzo dziękuję, panie przewodniczący. Wysoka Komisjo, panowie generałowie, panowie oficerowie, nie chciałem zabierać głosu, bo wydaje mi się, że wypowiedzi przedstawicieli resortów są wyczerpujące, ale inspiracją jest oczywiście wypowiedź pana posła Rutnickiego.

W takich żyjemy czasach, że jesteśmy narażeni na różne wpisy na różnych portalach, nie tylko na portalu X, ale także w innych miejscach. I to, co przedstawia pan poseł, rzeczywiście jest karygodne, bo wobec rzeczy, które nas bezpośrednio dotyczą, być może my politycy powinniśmy być bardzo gruboskórni, ale niestety dotyka to także naszych rodzin. Rzeczywiście pan poseł ma rację, w pełni się z tym zgadzam, że jeżeli pojawiają się jakieś takie obrzydliwe wpisy, to trzeba je niewątpliwie wyjaśniać, dyskredytować i tych, którzy się tego dopuszczają, karać. Idąc w duchu tej wypowiedzi, chciałbym panów zapytać, czy również w podobny sposób takie bezczelne kłamstwa jak to, że pan premier Jarosław Kaczyński jest odpowiedzialny za śmierć swojego brata, też państwo będziecie ścigać, też będziecie sprawdzać, kto takie bezczelne rzeczy robi? Bo rzeczywiście z tym kłamstwem, bezczelnością trzeba walczyć, należy odcinać, wypalać gorącym żelazem takie rzeczy, które są skandaliczne, które oskarżają w tak bezczelny sposób. Dziękuję uprzejmie.

Przewodniczący poseł Konrad Fryszak (KO):

Dziękuję. Pan poseł Bogucki.

Poseł Zbigniew Bogucki (PiS):

Dziękuję. Panie przewodniczący, Wysoka Komisjo, szanowni państwo, rzadko mi się to zdarza, ale z większością wypowiedzi pana posła Rutnickiego wypada się zgodzić, że tego rodzaju hejt, ataki, w szczególności jakieś posądzenia o różnego rodzaju przestępstwa, w tym przestępstwa – jak zrozumiałem – o charakterze seksualnym, jest czymś obrzydliwym i powinniśmy tutaj absolutnie stanąć w jedno i z tym walczyć. To jest dla mnie zupełnie oczywiste. Chociaż nasuwa mi się takie polskie powiedzenie, które mówi: kto sieje wiatr, ten zbiera burzę, bo przypominają mi się reakcje dzisiaj rządzących, a wówczas totalnej opozycji odnośnie do sprawy z Wrocławia i tych karygodnych działań, które – jak wszystko wskazuje – doprowadziły do śmierci młodego człowieka. Przypomnę, co wtedy się działo, i myślę, że warto uderzyć się w pierś i spojrzeć na to, jakie wtedy były komentarze pod adresem polityków PiS i kto to wtedy inspirował.

Natomiast co do tego portalu czy miejsca w Internecie, w którym treści, o których pan poseł Rutnicki mówił, są publikowane, to my, tak jak pan poseł Kaleta powiedział, co miesiąc, każdego 10 dnia miesiąca spotykamy się z falą hejtu, nienawiści, utrudnień

w oddawaniu czci osobom zmarłym i hasłami wypisywanymi, chronionymi niestety przez Policję. Nie mam powodu, żeby mieć pretensje do szeregowych funkcjonariuszy, ale do tych, którzy wydają rozkazy, już tak. Tam jest ewidentne kłamstwo, na które nie ma żadnego potwierdzenia ani w organach międzynarodowych, ani w polskich organach ścigania, obarczające prezydenta Najjaśniejszej Rzeczypospolitej ś.p. prof. Lecha Kaczyńskiego o zbrodnię, o zabójstwo 95 osób. To też jest bezczelność i mam nadzieję, że pan poseł Rutnicki, tak jak ja, jak pan poseł Kaleta, również będzie przeciwko temu protestował, tak jak przeciwko temu hejtowi, o którym pan poseł mówił.

I na koniec: to jest tylko dowód na to, że prowokatorzy są wszędzie. Nie wiem, kto tę stronę tworzy, pan mówi o jednym wpisie, ale takiego wpisu może dokonać każdy, więc prowokacje mogą być czynione w jedną i w drugą stronę. A dowodem tego jest na przykład kwestia badana przez ABW, którą ujawniła akurat, bo przeciek poszedł do tego medium, „Gazeta Wyborcza”; chociaż zmanipulowany, pokazywał, jak próbowano wpływać na kampanię wyborczą w Polsce w zeszłym roku. I na pewno nie był to wpływ korzystny dla PiS, bo gdyby wczytać się w ten artykuł, to te wiadomości były skrajnie niekorzystne z punktu widzenia PiS, ale tytuł sugerował, że były esemesy namawiające do głosowania na PiS. Warto by było również i tą sprawą się zająć, zbadać tę publikację i to, co zostało napisane, że było 187 tys. esemesów agitujących za PiS, chociaż były tam na przykład takie hasła jak PiS = ... De facto sprowadzało się to do tego, że PiS = bezpieczeństwo, bezpieczeństwo = zabranie świadczeń socjalnych. Jeżeli to jest agitacja, jeżeli to jest namawianie do głosowania na PiS, to konia z rzędem temu, kto tak to zrozumiał. To takie refleksje odnośnie do sprawy, którą pan poseł Rutnicki podniósł, dziękuję.

Przewodniczący poseł Konrad Fryszak (KO):

Bardzo dziękuję i o zabranie głosu poproszę pana posła Goska.

Poseł Mariusz Gosek (PiS):

Dziękuję, panie przewodniczący. Ja oczywiście podzielam pogląd pana posła Rutnickiego, bo absolutnie takie zdarzenia, wpisy na portalu X, Facebooku czy innych social mediach należy z całą surowością identyfikować i karać.

Natomiast chciałbym odczytać – zaraz powiem, dlaczego – komunikat Sądu Najwyższego, mianowicie pana prof. dra hab. Aleksandra Stępkowskiego. To jest komunikat sprzed kilkunastu godzin. Cytuję: „Osobiście traktuję tego typu wypowiedzi zarówno Państwowej Komisji Wyborczej, jak i takich organów jak chociażby minister sprawiedliwości, które podważają kompetencje Izby Kontroli Nadzwyczajnej i Spraw Publicznych, jako działanie dezinformacyjne, mieszczące się w arsenale środków prowadzenia wojny hybrydowej. Te działania dezinformacyjne, jak wskazują na to dokumenty zarówno NATO, Rady Europy, jak i UE zmierzają do polaryzacji społeczeństwa, do wywoływania podziałów społecznych, zaostrzenia tych podziałów, destabilizacji instytucji państwowych i podważania zaufania obywateli do funkcjonowania demokratycznych instytucji. Wypowiedzi te wpisują się dokładnie w logikę prowadzenia hybrydowych działań dezinformacyjnych w naszym kraju”.

W związku z powyższym i z wypowiedzią pana rzecznika prasowego Sądu Najwyższego prof. dra hab. Aleksandra Stępkowskiego proszę o interwencję względem pana prokuratora generalnego, ministra sprawiedliwości Adama Bodnara oraz członków PKW, którzy prowadzą takie działania dezinformacyjne, jak wskazał pan prof. dr hab. Aleksander Stępkowski w programie „Polski punkt widzenia” w TV Trwam. Ten wpis jest opublikowany na oficjalnej stronie SN i uważam, że również, a może przede wszystkim minister sprawiedliwości nie ma prawa do prowadzenia działań dezinformacyjnych w demokratycznym państwie prawa, którego model jest wpisany do konstytucji. Prosiłbym polską Policję, żeby podjęła działania w kierunku ministra sprawiedliwości i usunęła te – jak wskazał prof. dr hab. Aleksander Stępkowski – oczywiście naruszenia prawa. Dziękuję.

Przewodniczący poseł Konrad Fryszak (KO):

Oczywiście się z panem nie zgadzamy, a o zabranie głosu proszę pana posła Łackiego.

Posel Artur Jarosław Łacki (KO):

Panie przewodniczący, panie i panowie parlamentarzyści, szanowni goście, ja nie w tej sprawie, politycy narzekają i sami się bronią, chciałem tylko powiedzieć, że obrona przed cyberatakami to nie jest obrona polityków, tylko obrona Rzeczypospolitej. Jeśli politycy nie chcą, żeby był na nich wylewany hejt, to proponuję zrezygnować z roli polityka i zająć się pieczeniem ciasta na święta, wtedy będą chwalić.

Ja w innej sprawie. Jutro odbędzie się posiedzenie Zespołu do Spraw Prewencji Suicydalnej. Państwu ze służb pewnie nie muszę o tym mówić, ale kolegom tak – o tym, że giną ludzie na drogach, wszyscy wiemy, bo codziennie o tym nas informują telewizje, że tu zginęły dwie osoby, tu trzy, wielkie tragedie. Rocznie ginie na drogach około 3 tys. ludzi. W Polsce rocznie popełnia samobójstwo ponad 5 tys. ludzi – 5200, 5300, od 10 lat ta liczba nie spadła chyba poniżej 5 tys. Wśród tej ogromnej rzeszy ludzi, którzy popełniają samobójstwo, jest wiele osób młodych i dzieci. Co ich do tego skłania? Jedną z przyczyn jest to, co jest właśnie w Internecie. Jedną z przyczyn tych wszystkich tragedii ludzkich jest hejt, który wylewa się w Internecie. Chciałbym się dowiedzieć – oprócz tego jak państwo chcą bronić infrastruktury krytycznej RP – jak my jako politycy i wy jako ludzie służb zamierzacie próbować bronić przed tym naszą młodzież, nasze dzieci? Bo nie da się tego oddzielić, nie da się chronić dzieci, nie da się chronić młodzieży, jeśli nie będziemy jej chronić od złych wpisów w mediach społecznościowych, w Internecie. Ja nie wiem, jak to zrobić, wy jesteście fachowcami i chciałbym, żebyśmy my jako Sejm Rzeczypospolitej zajęli się głęboko tą sprawą, bo z tego robi się już ogólnopolska tragedia. Dziękuję bardzo.

Przewodniczący poseł Konrad Fryszak (KO):

Bardzo dziękuję i o głos poprosiła pani posłanka Urszula Nowogórska.

Posel Urszula Nowogórska (PSL-TD):

Szanowny panie przewodniczący, Wysoka Komisjo, zacni goście, powszechnie wiadomo, że ci, którzy planują i realizują ataki związane z cyberbezpieczeństwem, mają swoje z góry założone cele, które osiągają lepiej albo gorzej. I jako adresatów swoich działań wybierają osoby, które zajmują czołowe stanowiska w państwie, albo też instytucje, które są w posiadaniu ważnych, wrażliwych – również dla bezpieczeństwa państwa – danych. Chciałam zapytać np. w przełożeniu na dwa ostatnie lata, jak wygląda, jeżeli chodzi o służby podległe MSWiA, liczba ataków skierowanych na instytucje podległe temu resortowi? I czy w wyniku tych cyberataków dochodziło do wycieku danych wrażliwych, które mogły być wykorzystywane w niecnym celu, jeżeli chodzi o bezpieczeństwo państwa?

Drugie moje pytanie dotyczy umów podpisywanych z podmiotami zewnętrznymi. Jakie muszą spełnić kryteria związane z bezpieczeństwem, żeby umowy z takimi przedstawicielami czy instytucjami mogły być podpisywane?

I jeszcze jedno pytanie, które kieruję do Państwowej Straży Pożarnej. Wiadomo, że gdy mają miejsce jakieś bardzo poważne zagrożenia, trzeba uruchomić łączność awaryjną. Czy ta łączność awaryjna pokryciem radiowym jest realizowana przy użyciu sił i środków podległych PSP? A jeżeli nie, to czy realizację takich usług są zlecane firmom zewnętrznym, które podpisują stosowne umowy z poszczególnymi komendami wojewódzkimi na terenie Polski? Bardzo dziękuję.

Przewodniczący poseł Konrad Fryszak (KO):

Bardzo dziękuję. O głos poprosił pan poseł Zieliński.

Posel Jarosław Zieliński (PiS):

Dziękuję, panie przewodniczący. Nie wiem, czy nie szkoda czasu na polemikę z takimi tezami, jakimi, jaką – przynajmniej jedną – wygłosił pan poseł Łacki. Ale ponieważ sprawa jednak jest poważna, to powiem parę słów.

Chodzi o to, że to jest bardzo fałszywa teza, chociaż populistycznie może uznać pan ją za ważną dla siebie – teza, że trzeba chronić państwo, ale niekoniecznie chronić polityków, bo oni muszą być albo odporni, albo ciasto na święta wypiekać. Panie pośle, politycy to część państwa, politycy pełnią funkcje w ważnych państwowych instytucjach i za nie odpowiadają, więc atak na polityków jest też atakiem na państwo. Dlatego niech pan takich tez nie wygłasza, bo to naprawdę jest szkodliwe, a ktoś kto słucha, może mniej

zorientowany, może tak myśleć, że polityków można atakować, bo to nie jest państwo i jak ktoś się tym przejmie, to niech zrezygnuje z polityki, niech się zajmie przysłowiową pietruszką czy ciastami, z całym szacunkiem dla tych innych, ważnych przecież nie tylko przed świętami funkcji, bo i pieczenie ciast, i inne rzeczy to są ważne umiejętności. Ale naprawdę poważnie traktując tę sprawę, proszę, panie pośle, zastanowić się nad tym, bo ludzie nas słuchają, jest transmisja tych obrad i takich... przepraszam, niech się pan nie obrazi, ale głupstw nie wolno wygłaszać.

Przewodniczący poseł Konrad Fryszak (KO):

Bardzo dziękuję. Rzadko zgadzam się z panem posłem Zielińskim, ale w tym jednym przypadku zgadzam się z panem, że trzeba chronić każdą obywatelkę i każdego obywatela polskiego państwa bez względu na to, jaką funkcję w tym państwie pełni, czy jest posłem, czy nie jest, czy jest senatorem, piekarzem, kierowcą, policjantem. Każdy powinien mieć ochronę naszego państwa.

Poseł Artur Jarosław Łacki (KO):

Zapomniał pan o dzieciach i młodzieży, panie przewodniczący.

Przewodniczący poseł Konrad Fryszak (KO):

To też obywatele naszego państwa. Pan poseł Rutnicki i zamykam listę mówców. Będzie odpowiedź na pytanie pani posłanki Nowogórskiej i przejdziemy do punktu drugiego, gdzie większość z państwa otrzyma odpowiedzi na swoje pytania. Jeśli nie będzie tych odpowiedzi, to wtedy poprosimy o doprecyzowanie. Pan poseł Rutnicki.

Poseł Jakub Rutnicki (KO):

Bardzo dziękuję za tę dyskusję, bo myślę, że to jest bardzo ważna rzecz.

Patrzę na odpowiednie służby i chciałem zapytać, czy biorąc pod uwagę to, że taki hejt jest przecież widoczny, nie ma problemu ze zidentyfikowaniem czegoś takiego, to czy jednak nie powinny być tu podejmowane pewne działania z urzędu. Bo jak widzę grób mamy pana premiera z podpisem, kto tam leży – już nie będę cytował – albo widzę mundur gestapo i kogoś, kto przypomina premiera Najjaśniejszej Rzeczypospolitej, widzę faszystowskie symbole, to nie odnoszę wrażenia, że każdy z nas jest zobligowany do zgłaszania tego typu treści, tylko takie rzeczy, takie działania powinny być de facto podejmowane z urzędu. Stąd też chciałem zapytać, czy tego typu działania są podejmowane, bo biorąc pod uwagę ilość tak haniebnych treści, które można znaleźć...

Szanowni państwo, jakby to znalazł mój 10-letni syn, jeżeli chodzi na przykład o moją osobę, to jest to wielki problem – nie dla mnie, bo trzeba mieć twardą skórę, ale jeżeli ktoś dotyka rzeczy bardzo delikatnych, które mogą mieć wielki wpływ także na rodzinę i na wiele innych sytuacji, to uważam, że takie działania powinny być podejmowane. Zupełnie inna jest krytyka działań itd., ale zupełnie inna jest sytuacja, gdy swoje zdjęcie publikujemy, czy ktoś publikuje zdjęcie i może napisać o każdym, że jest złodziejem, zdrajcą, pedofilem, mordercą i wszystkim, co najgorsze. Dlatego uważam, że tego typu działania powinny być bardzo stanowcze i absolutnie trzeba takie osoby, jeżeli takich rzeczy się dopuszczają, bezwzględnie ścigać i karać. Dziękuję bardzo.

Przewodniczący poseł Konrad Fryszak (KO):

Dziękuję, panie pośle. O głos prosi pan poseł Kaleta, ale umówmy się, że to już donikąd nie zmierza, przejdźmy do punktu drugiego. Nie wiem, panie pośle, co jeszcze chce pan wniesić do tej...

Poseł Piotr Kaleta (PiS):

Chciałem po raz kolejny zgodzić się z panem posłem Rutnickim, że te rzeczy naprawdę muszą być piętnowane. Każde nawoływanie do przemocy musi być piętnowane i mam nadzieję, że pan Rutnicki będzie jedną z pierwszych osób, albo może już tak się stało, które doniosły na swojego kolegę wożącego na swoim samochodzie jakieś osiem gwiazdek. Nie wiem, czy pan też wytłumaczył swojego synowi 10-letniemu, co oznacza...

Poseł Jakub Rutnicki (KO):

Niech pan nie porusza tego typu rzeczy, bo zaczyna pan wchodzić w bardzo... proszę nie dotykać mojej rodziny i niech pan przestanie.

Posel Piotr Kaleta (PiS):

Ale pan sam ją przywołał...

Przewodniczący poseł Konrad Fryszak (KO):

Szanowni państwo, na tym zamykam tę dyskusję i zbędną pyskowę. Przywołuję panów do porządku. Panie pośle Rutnicki, panie pośle Kaleta, panie pośle Bogucki, bardzo proszę o spokój, już wystarczy. Przywołuję panów po raz kolejny do porządku. Jeśli chcecie sobie porozmawiać, to proszę wyjść do kuluarów i zakończyć tę dyskusję. Proszę o udzielenie odpowiedzi na pytanie pani posłanki Nowogórskiej.

Zastępca komendanta głównego Państwowej Straży Pożarnej nadbryg. Józef Galica:

Panie przewodniczący, szanowni państwo, odpowiadając na pytanie pani poseł, chciałem się ustosunkować.

Oczywiście mamy problemy z łącznością podczas akcji. Wtedy w zasadzie swoją łączność – oczywiście mówimy o łączności radiowej, bo myślę, że pani poseł o to chodzi – budujemy na swoich samochodach dowodzenia i łączności. Jest to rozwiązanie doraźne, praktycznie każde województwo ma taki samochód dowodzenia i łączności, natomiast w perspektywie czasu, o czym pan dyrektor mówił, szykujemy rewolucję łącznościową w skali całego kraju. Łączność będzie na pewno zmodernizowana, będzie się opierała na troszeczkę innych technologiach, bardziej nowoczesnych – mam na myśli TETRĘ, którą koledzy z Policji będą organizować. Już niektóre miasta, przede wszystkim wojewódzkie, te, które miały EURO, mają te nowoczesne rozwiązania TETRY. Zapewne pyta pani w kontekście rozwiązań w terenie górskim, bo wiem, skąd pani pochodzi i w zasadzie mogę powiedzieć, że jest to problem, z którym się borykamy od lat. Odpowiadając na pytanie, które pani zapewne chciała mi zadać: jeżeli będą nowe rozwiązania TETRY, to ta łączność na pewno się poprawi.

Natomiast jeżeli chodzi o drugie pytanie, czy wspieramy się firmami zewnętrznymi, to oczywiście w kontekście wsparcia technicznego jak najbardziej tak. Wspieramy się firmami zewnętrznymi, które w zasadzie kontrolują i konserwują przede wszystkim, modernizują sprzęt.

Przewodniczący poseł Konrad Fryszak (KO):

Bardzo dziękuję, panie generale. O przedstawienie informacji na temat funkcjonowania Centralnego Biura Zwalczania Cyberprzestępczości w Policji jako pierwszą poproszę panią dyrektor Furgalę.

Dyrektor Departamentu Porządku Publicznego w MSWiA Agata Furgala:

Dziękuję bardzo. Szanowny panie przewodniczący, Wysoka Komisjo, szanowni państwo, o tym, że cyberprzestępczość jest jednym z największych i najbardziej niestety rozwijających się zagrożeń dla bezpieczeństwa wszystkich obywateli, nikogo nie trzeba przekonywać.

Świadczy o tym liczba pytań, a także państwa zaangażowanie, stąd też chcieliśmy przedstawić wspólnie z panami generałami, z panem gen. Tomaszem Michulką, pierwszym zastępcą komendanta głównego Policji, oraz szefem, komendantem Centralnego Biura Zwalczania Cyberprzestępczości szczegółowe informacje, które – jak myślę – w dużej mierze będą uzupełnieniem materiału, który został państwu przekazany. Oczywiście odpowiedzią na ten zwiększający się trend, dynamiczny rozwój skali cyberprzestępczości było uchwalenie 17 grudnia 2021 r. ustawy o zmianie niektórych ustaw w związku z powołaniem CBZC, czyli Centralnego Biura Zwalczania Cyberprzestępczości. Na tej podstawie 12 stycznia 2022 r. powołano tę wyspecjalizowaną jednostkę organizacyjną Policji, która ma cyberprzestępczość zwalczać. Oczywiście skuteczna walka z zagrożeniami, bo taki był cel, który przyświecał i przyświeca nadal skutecznej walce z zagrożeniami płynącymi z Internetu, jest możliwa tylko i wyłącznie wtedy, kiedy organy ścigania nie ustępują cyberprzestępcom zarówno pod względem technologii, jak i umiejętności. Warto zaznaczyć, że prowadzone w CBZC postępowania przygotowawcze charakteryzują się bardzo często wielowątkowością, złożonością i długofalowym charakterem. Często są to śledztwa zbiorcze, obejmujące swoim zasięgiem obszar całego kraju, a nawet mają charakter ponadnarodowy. Specyfika wykrywania tego rodzaju przestępstw wymaga analizy ogromnych ilości danych cyfrowych i różnych innych aspektów. CBZC stale rozwija swój

potencjał, a o zasadności powołania tej jednostki organizacyjnej, wyspecjalizowanej w tym obszarze, mogą świadczyć dane statystyczne, które w sposób szczegółowy sposób panowie generałowie, panowie komendanci za chwilę pokażą. Nadmienię tylko, że w 2023 r. CBZC prowadziło 617 postępowań przygotowawczych, podczas gdy w 2024 r. do dzisiaj, do paru dni wstecz, było prowadzonych blisko 1200 takich postępowań, dokładnie 1198.

Jeśli chodzi o stan etatowy CBZC, to obecnie wynosi 1300 etatów. W 2025 r. planowane jest, zgodnie z ustawą, zwiększenie stanu etatowego o kolejnych 500 etatów, czyli do tego docelowego, zakładanego w ustawie poziomu 1800 etatów.

Krótko, zanim panowie komendanci przedstawiają bardziej szczegółowe informacje: można powiedzieć, że z perspektywy 3 lat funkcjonowania tej jednostki dzięki zapewnieniu lepszej koordynacji działań, prowadzeniu spójnego systemu organizacyjnego i struktury jednostek zwalczających cyberprzestępczość w całym kraju, a także wysokiej profesjonalizacji działań funkcjonariuszy tej jednostki udało się zwiększyć skuteczność reagowania przez państwo na zagrożenia związane z cyberprzestępczością. Tyle tytułem wstępu z perspektywy nadzoru ministra spraw wewnętrznych i administracji. Jeżeli mogę, to płynnie przekazę głos panu komendantowi głównemu Policji. Dziękuję bardzo.

Przewodniczący poseł Konrad Fryszak (KO):

Bardzo dziękuję, pani dyrektor, a o zabranie głosu proszę pana nadinsp. Michułka.

Zastępca komendanta głównego Policji nadinsp. Tomasz Michułka:

Szanowny panie przewodniczący, Wysoka Komisjo, szanowni państwo, nadinsp. Tomasz Michułka, zastępca komendanta głównego Policji odpowiedzialny za służbę kryminalną. Na wstępie chciałbym scharakteryzować obszary, którymi zajmuje się CBZC. Mam nadzieję, że nasze wystąpienia w dużej mierze odpowiedzą przynajmniej na część z pytań, które państwo zadaliście. Kontynuując wypowiedź pani dyrektor, w odniesieniu do prowadzonych postępowań przygotowawczych, tak jak pani dyrektor wspomniała, proszę zwrócić uwagę, szanowni państwo, że porównując dane statystyczne rok do roku, liczba postępowań przygotowawczych prowadzonych przez CBZC wzrosła o 100%. Idąc dalej, 250 postępowań dotyczyło seksualnego wykorzystywania... przepraszam, oszustw w Internecie, kolejny duży odsetek to właśnie postępowania dotyczące seksualnego wykorzystania dzieci, ale było też 97 postępowań z zakresu ataków złośliwym oprogramowaniem, ataków DDoS czy z wykorzystaniem Ransomware.

Chciałbym zwrócić uwagę szanownych państwa posłów na fakt, że to, o czym mówimy, część z tych informacji, które się rozprzestrzeniają w sieci, wyczerpują znamiona art. 12 Kodeksu karnego, czyli zniesławienie. Chciałbym tylko zwrócić uwagę, że są to przestępstwa ścigane w trybie prywatnoskargowym, więc konieczny jest prywatny akt oskarżenia. Jeżeli oczywiście wymaga tego ważny interes społeczny, to mogą być one objęte ściganiem z urzędu i tak w wielu sytuacjach się dzieje. Było pytanie, czy z własnej inicjatywy są podejmowane działania z urzędu. Oczywiście, że są. Pan gen. Cieślak będzie w swojej prezentacji mówił o tym, że zdecydowana większość postępowań jest wszczynana na podstawie materiałów operacyjnych, czyli są skutkiem naszej pracy operacyjnej, między innymi tego, co wychytujemy w necie. Także chcę zapewnić państwa, że każde zawiadomienie o przestępstwie jest traktowane ze szczególną starannością i podlega ocenie prawnokarnej prokuratury, a policja podejmuje stosowne działania. I tutaj chciałbym tę sprawę wyjaśnić, że nie może być inaczej.

Szanowni państwo, chciałbym przy tej okazji powiedzieć o inicjatywie, którą podjęliśmy. Mianowicie z mojego polecenia wyznaczaliśmy stałe dyżury w każdym województwie – w godzinach od 7.00 do 20.00 w stałym dyżurze telefonicznym jest funkcjonariusz CBZC, który ma wiedzę specjalistyczną i jego zadaniem jest udzielanie wsparcia funkcjonariuszom jednostek terenowych przy przyjmowaniu zawiadomień o przestępstwie. Może być bowiem taka sytuacja, że do komisariatu, do komendy powiatowej udaje się obywatel i składa zawiadomienie o przestępstwie w zakresie cyberprzestępstwa. Trzeba mieć świadomość, że sierżant w jednostce terenowej nie ma wiedzy specjalnej, tak aby na etapie przyjmowania zawiadomienia o przestępstwie należycie zabezpieczyć materiał dowodowy w postaci nagłówków, treści, które są w Internecie. W związku z tym wydałem takie polecenia i pan komendant już je zrealizował, żeby funkcjonariusz jednostki

terenowej miał zawsze możliwość skontaktowania się z funkcjonariuszem z biura, który ma wiedzę specjalną i może udzielić wsparcia. Myślę, że to jest bardzo cenne, bo wpływały do nas takie informacje, że obywatele wychodzą z komisariatu bądź z komendy powiatowej nie do końca poinformowani, co mają zrobić w związku z zaistnieniem określonego przestępstwa, ponieważ na przykład dokonano kradzieży tożsamości w Internecie albo przejęcia konta. Chodzi o to, żeby obywatel wychodzący z jednostki terenowej był należycie poinstruowany, a jeżeli funkcjonariusz z komisariatu czy komendy powiatowej nie ma wystarczającej wiedzy, to jest ekspert, który ma pomóc w tym zakresie. Myślę, że to jest cenna inicjatywa prospołeczna, tak żeby nasi mieszkańcy, wychodząc z jednostki terenowej, otrzymali niezbędny pakiet wiedzy, aby skutecznie przeciwdziałać negatywnym skutkom podjętego, przestępczego działania.

Drugim niezmiernie istotnym obszarem, jeżeli chodzi o funkcjonowanie CBZC, jest analiza kryminalna i analiza kryptowalut. W strukturach CBZC służy 42 analityków kryminalnych, w styczniu będzie kolejny kurs dedykowany dla tych analityków. Analiza kryminalna jest tu szalenie istotna, ale to co ważne – nabyliśmy specjalistyczne oprogramowanie, które służy między innymi do analizy przepływów, jeżeli chodzi o kryptowaluty, i to oprogramowanie również przekazaliśmy do jednostek szczebla wojewódzkiego. Mamy tam już 50 osób, które są przeszkolone i mają podstawowe narzędzia służące do nadzoru i kontroli w zakresie transakcji dokonywanych za pomocą kryptowalut.

Kolejny obszar funkcjonowania, działania CBZC to informatyka śledcza, równie istotny obszar działania. Mamy ekspertów, przeszkolonych funkcjonariuszy, którzy są w stanie bardzo skutecznie przełamywać określone zapory w zabezpieczonym już materiale, w zabezpieczonych urządzeniach, które służyły do popełniania przestępstw. Ci eksperci są w stanie dokonać analizy tychże zabezpieczonych nośników czy też urządzeń i takie rzeczy CBZC realizuje również na rzecz jednostek terenowych. Wsparcie dla jednostek szczebla terenowego, oprócz dyżurów, o których wspomniałem, to szereg szkoleń, tak żeby docierać z wiedzą specjalną z zakresu zwalczania cyberprzestępczości jak najniżej, żeby liczba funkcjonariuszy, którzy są w stanie skutecznie działać, była jak największa.

Szanowni państwo, kolejny obszar to działania w trybie emergency. Chciałbym powiedzieć, że w KGP istnieje Sekcja Obsługi Całodobowej Wydziału Wywiadu Kryminalnego CBZC. Jak to przełożyć na proste wy tłumaczenie państwu, na czym polega działanie tej sekcji? Otóż obok stanowiska dyżurnego operacyjnego kraju jest pokój, gdzie urzędują funkcjonariusze komendanta Cieślaka, którzy w systemie całodobowym pracują nad sprawami dotyczącymi zagrożeń życia i zdrowia. Mamy podpisanych szereg umów również z fundacjami, z Biurem Rzecznika Praw Dziecka i wszystkie treści, które pojawiają się w sieci, które wskazują, że może być zagrożone życie bądź zdrowie kogokolwiek, są przekazywane do tego całodobowego centrum. Następnie podejmowane są natychmiastowe działania, żeby ratować życie i zdrowie osób, które gdzieś w swoich wpisach ujawniają przesłanki czy zamiary w zakresie samobójstwa. Chciałbym państwu powiedzieć, że ja szczególnie zwracam na to uwagę, bo martwi mnie skala. Tak jak jeszcze 3 lata temu było od 2 do 3 takich zgłoszeń czy ujawnionych treści przez naszych funkcjonariuszy, to dzisiaj ta liczba wzrosła do średnio 18, 19 na dobę. Tyle podejmujemy skutecznych działań w zakresie ratowania życia i zdrowia ludzi, więc ta sekcja jak najbardziej się sprawdza, jej efektywność jest bardzo wysoka.

Ostatni obszar, o którym chciałbym krótko powiedzieć, to oczywiście profilaktyka. Nie możemy skutecznie działać bez skutecznej, efektywnej wiedzy, w którą wyposażamy mieszkańców naszego państwa, którą przekazujemy społeczeństwu. W związku z tym CBZC prowadzi szereg kampanii uświadamiających, między innymi pod hasłem „Ty możesz być następny”, „Twoje konto, twoje przestępstwo”. To są kampanie społeczne, które mówią o tym, jak należy się chronić przed cyberzagrożeniami. Mamy również wiele skutecznych kooperacji, między innymi ze Związkiem Banków Polskich, przygotowujemy kampanie dedykowane w zależności od okresu, między innymi wtedy, kiedy mieliśmy promocje z okazji Black Friday. Mogliśmy się tu spodziewać wielu prób oszustw, stąd specjalne działania i komunikaty, które dystrybuujemy online do obywateli z ostrzeżeniami przed zagrożeniami.

Szanowni państwo, oczywiście jeżeli chodzi o szczegóły, to pan gen. Cieślak je przekaże. Będziemy mówić również o strukturze CBZC, o sytuacji kadrowej, bo to też na pewno jest w sferze państwa zainteresowania. Dziękuję bardzo, panie przewodniczący.

Przewodniczący poseł Konrad Fryszak (KO):

Bardzo dziękuję panie generale i o zabranie głosu proszę pana nadinsp. Adama Cieślaka.

Komendant Centralnego Biura Zwalczania Cyberprzestępczości nadinsp. Adam Cieślak:

Panie przewodniczący, Wysoka Komisjo, szanowni państwo, oczywiście uzupełnię wypowiedzi pana komendanta Michułki i pani dyrektor Furgały. Na początek trochę informacji o stanie kadrowym, o strukturze organizacyjnej, o tym, jak biuro wygląda. Faktycznie biuro powstało 12 stycznia 2022 r., niemniej jednak półroczny okres przygotowań spowodował, że działalność operacyjną w postaci prowadzenia spraw, ścigania cyberprzestępców biuro zaczęło formalnie 12 lipca 2022 r., więc działamy, jesteśmy w strukturach Policji prawie 2,5 roku.

Szanowni państwo, co roku od momentu powstania biura przyznawane są etaty, docelowo 1800 etatów policyjnych. Aktualnie jest 1300, ale zaczynaliśmy z 300 etatami w roku 2022. Liczba policjantów, którzy są w biurze, rośnie z roku na rok. Oczywiście uzupełnienie, dojście do pełnego stanu etatowego jeszcze trochę zajmie, ale też postaram się wyjaśnić, skąd tyle wakatów. Struktura organizacyjna biura aktualnie wygląda tak, że w każdym mieście wojewódzkim jest komórka CBZC. Na samej górze w strukturze jest oczywiście komendant i trzech zastępców komendanta CBZC, a w każdym mieście wojewódzkim jest komórka albo w randze zarządu, albo w randze wydziału. Oczywiście musi też funkcjonować struktura administracyjna w centrali, tak jak w każdej jednostce Policji – wynika to z wielu przepisów i regulacji: musi być dział kontroli, muszą być osoby odpowiedzialne za bezpieczeństwo i higienę pracy, musi być pełnomocnik do ochrony informacji niejawnych itd., itd. Tych zadań jak na jednostkę jest bardzo dużo. Jeśli chodzi o wielkość komórek, to co roku wraz ze wzrostem liczby etatów rośnie też stan etatowy komórek terenowych. Jak wygląda sytuacja kadrowa w chwili obecnej? W 2022 r. było 18% wakatów przy 388 etatach, liczba wakatów wynosiła 78. Rok 2023 – 35% wakatów, rok 2024 – 40% wakatów. Ale przypomnę, że w marcu tego roku otrzymaliśmy 500 etatów, więc cały czas gonimy tę liczbę, do której powinniśmy docelowo dojść. Oprócz tych zapełnionych etatów w biurze są jeszcze osoby delegowane – aktualnie jest ich 48 – i to są osoby w tzw. okresie próby. Jeżeli przejdą ją pozytywnie, to zostaną przyjęte na etat, więc aktualnie w biurze służbę pełni 825 policjantów. Biuro w momencie wprowadzenia w życie ustawy zyskało możliwość – i bardzo się z tego cieszę – rekrutacji osób bezpośrednio z cywila, czyli osób niebędących policjantami. Takie możliwości zostały też przyznane między innymi Centralnemu Biuru Śledczemu Policji, Biuru Spraw Wewnętrznych oraz Centralnemu Pododdziałowi Kontrterrorystycznemu Policji „BOA”. Bardzo się cieszę, że jest taka możliwość, bo widzieliśmy bardzo dużą potrzebę wzmocnienia biura fachowcami z zakresu informatyki, posiadającymi umiejętności specjalne.

Szanowni państwo, rekrutację zaczęliśmy w listopadzie 2022 r., dlatego że wymagała ona przygotowania wielu testów i egzaminów, które wynikają z przepisów prawa. Każdy bowiem kandydat musi przejść bardzo trudny test teoretyczny, praktyczny, ale też wykazać się znajomością języka obcego w zakresie technicznym. I to wymagało przygotowań, więc ruszyliśmy z rekrutacją w listopadzie 2022 r. Jak widzicie państwo na slajdzie, ten rok pokazuje, że mamy złożonych 720 podań o wstąpienie do CBZC z cywila, a łącznie ponad 1100 podań. Matematyka jest prosta – gdybyśmy przyjęli wszystkich, którzy się zgłosili, to nie mielibyśmy już problemu z wakatami, ale niestety tak nie jest, a może dobrze, że tak nie jest, bo my chcemy przyjąć tych najlepszych, tych, którzy posiadają odpowiednie kwalifikacje. Na tym slajdzie widzicie państwo, jak mniej więcej wygląda proces rekrutacji, bo przyjęliśmy w ciągu tych dwóch lat niespełna 75 osób. I już mówię, dlaczego. Na 1138 złożonych podań o przyjęcie do CBZC już na pierwszym etapie weryfikacji dokumentów odpada 16%. Powodów jest kilka – czasami są to osoby notowane kryminalnie, więc chociażby już z tego powodu nie możemy ich przyjąć do biura. Drugi powód jest taki, że często sami się nie zgłaszają, pomimo trzykrotnych wezwań dotyczących terminów testów, egzaminów. Po prostu jest brak odpowiedzi, czasami kandydaci rezygnują.

Są więc trzy główne powody, dlaczego 16% odpada już na samym początku. Później jest test kompetencji, który składa się z testu teoretycznego, gdzie jest 40 dosyć trudnych pytań – proszę mi wierzyć – trzech zadań technicznych, a jeżeli się przejdzie pozytywnie ten test teoretyczny, to jest jeszcze test z języka obcego. I na tym etapie z tych osób, które przeszły dalej, odpada 61%.

Mamy jeszcze obowiązkowo w procesie kwalifikacji badania psychologiczne, mamy wariograf, więc każdy kandydat, który przychodzi do nas z zewnątrz jest poddany obowiązkowo badaniu na wariograf. Przyczyna jest prosta i oczywista – nie chcemy w naszych szeregach mieć kogoś, kto ma powiązania z obcymi służbami, kto popełniał do tej pory przestępstwa i staramy się przy okazji tego badania, takie osoby wykluczyć. Odpadają też osoby, które nie przejdą pozytywnie komisji lekarskiej. Stąd w opracowaniu, bo ten proces jest płynny – musicie państwo wiedzieć, że te osoby są na różnym etapie – jest jeszcze 120 osób i zakładam, że jakąś część z nich, ale nie potrafię powiedzieć jaką, przyjmujemy, dlatego że my przynajmniej raz w miesiącu robimy testy dla tych osób, gdzie badaniu podlega około 60 osób, w zależności od tego, ile się stawi. Miesiące mamy różne – czasami testy zdaje 15 osób, a czasami 30 z tych 60. Trudno wytłumaczyć, dlaczego tak jest, ale prawdopodobnie w jednym momencie jest kumulacja osób z lepszym przygotowaniem, a innym razem z mniejszym.

Docelowo w 2025 r. struktura etatowa będzie wyglądała tak, że w dużych miastach wojewódzkich takich jak Katowice, miasto stołeczne Warszawa będą komórki, które będą liczyły 140 etatów policyjnych. W mniejszych miastach – nie wiem, czy dobrze widać barwy na slajdach – będą zarządy, które będą liczyły 100 etatów policyjnych, w miastach średnich – 85 etatów i komórki najmniejsze – 67 etatów. Projektując biuro, zakładaliśmy, że ten stan etatowy będzie zbliżony do stanu etatowego komend wojewódzkich. Stan etatowy komend wojewódzkich wynika z zagrożenia, z zaludnienia na danym terenie, więc poszliśmy tą drogą. Być może można było pójść inną, ale akurat tamta wtedy wydawała nam się słuszna i tak to będzie wyglądało, że będziemy mieli w 2025 r. 1800 etatów. Ilu będzie funkcjonariuszy, trudno mi odpowiedzieć, ale zakładam, że ponad 1000 na pewno.

Czym się zajmujemy? Myślę, że to bardzo ważny slajd, dlatego że przestępstw, które są określane mianem cyberprzestępstw, jest bardzo dużo, nie tylko w naszym kraju, ale na świecie, wszyscy się z tym mierzą. Nie ma definicji cyberprzestępstwa w naszym kodeksie karnym, więc przyjęliśmy takie założenia, które są zbliżone do założeń Euro-polu, czyli przyjmujemy, że typowe cyberprzestępstwa to takie, których nie można popełnić, gdyby nie sieć Internet. I to jest hacking, czyli pokonywanie zabezpieczeń systemów informatycznych, teleinformatycznych, są to ataki ransomware, ataki DDoS, złośliwe oprogramowanie, ale też bulletproof hosting, czyli prowadzenie takiej działalności przez dostawców infrastruktury, czasami w Darknecie, żeby skutecznie ukrywać się przed organami ścigania, żeby zostać anonimowym. Dostawcy ci często nie udzielają odpowiedzi na zadane pytania, a nawet potrafią informować osoby, że my się o nie pytamy.

Druga bardzo szeroka i chyba największa grupa przestępstw, którymi też jako biuro się zajmujemy i uważamy, że jest to bardzo ważna potrzeba, bo dotyczy wielu obywateli w naszym kraju, to są oszustwa internetowe. Jest ich bardzo dużo, w skali kraju ponad 60 tys. rocznie i mają one bardzo różny obraz, bardzo różne scenariusze. Pewnie państwu są one znane – to są oszustwa metodą na pracownika banku, przestępstwa inwestycyjne, gdzie przestępcy mają nas szybkimi zyskami, to są oszustwa na platformach sprzedażowych. To są oszustwa, które nazywamy nigeryjskimi, czyli gdzie osoby samotne są najczęściej wykorzystywane, żeby przelać pieniądze, więc tych oszustw jest dosyć dużo, są różne mechanizmy, niemniej jednak wszystkie sprowadzają się do tego, żeby okraść ofiarę.

Trzecia część naszych działań – uznaliśmy, że jest to obszar, którym powinniśmy się zająć jako Policja, jako CBZC – to jest seksualne wykorzystywanie dzieci w sieci Internet. Wiemy, że tych przypadków na świecie jest dużo, trend jest rosnący i obok tych nieszczęść dzieci nie można przejść obojętnie, dlatego też tym zagadnieniem się mocno zajęliśmy. O szczegółach powiem za chwilę. Jest jeszcze taki obszar, o którym nie ma mowy na slajdzie, ale chodzi o wszystkie inne przestępstwa, które też się dzieją w sieci, i to jest handel

narkotykami, handel lekami, to są... tych przestępstw jest mniej, ale to też są dosyć istotne sprawy i się okazuje, że one też są dosyć dużym zagrożeniem.

Jeśli chodzi o liczbę postępowań przygotowawczych, to wraz z rosnącą liczbą policjantów liczba spraw rośnie i to jest naturalne. Jak widać na slajdzie, prawie 1200 postępowań mamy w tym roku, część została zakończona, część wszczęta, jest ich nieporównywalnie więcej niż w roku 2023 i myślę, że w 2025 będzie ich jeszcze więcej.

Natomiast chciałbym zwrócić państwa uwagę, bo przejdę teraz do statystyki, żebyśmy nie popadli w takie... mylne myślenie. Bo statystyka ma to do siebie, że liczby mogą być duże, a pod tymi liczbami niewiele się kryje. Postępowanie nie jest równe postępowaniu. Mamy takie postępowania, gdzie mamy jednego podejrzanego, ale mówiąc kolokwialnie, narozrabiał on tyle, że mógłby obdzielić 150 osób w innych postępowaniach. Zatem ta jedna kreska statystyczna nie zawsze jest równa drugiej kresce statystycznej. Jeśli chodzi o biuro, przyjęliśmy takie założenie, żeby zajmować się sprawami dużymi, ciężkimi, trudnymi technicznie, żeby nie zajmować się drobnymi oszustami, którzy oszukają tylko jedną osobę, bo tych spraw jest bardzo dużo i nie bylibyśmy w stanie ich wszystkich przy tej liczbie policjantów przeprowadzić skutecznie. Dlatego położyliśmy nacisk na pracę operacyjną i to my szukamy tych poważnych przestępstw, my szukamy przestępców. Chcemy doprowadzić do takiej sytuacji, że to my wychodzimy z inicjatywą wszczęcia postępowania przygotowawczego, a nie reagujemy na złożone zawiadomienie. Często jest już bowiem za późno, bo pieniądze już dawno wyszły poza granice kraju albo na giełdy kryptowalutowe, które mogą z nami nie współpracować. Oczywiście w całej masie spraw, które mamy, są też zawiadomienia od instytucji, podmiotów, osób prywatnych, czasami są to postanowienia wynikające z prowadzonego już postępowania, bo na sprzeczne zabezpieczonym znaleźliśmy np. zupełnie inny obszar działań prowadzonych przez daną grupę bądź daną osobę.

Jeżeli chodzi o mapę w jakich obszarach się poruszamy i jak to wygląda procentowo, to oszustwa, których jest dużo, stanowią największą liczbę prowadzonych u nas spraw. Mamy dosyć dużą liczbę spraw, jeżeli chodzi o seksualne wykorzystywanie dzieci, ale one się charakteryzują się tym, że często dotyczą jednej osoby, która krzywdzi kilka osób, ewentualnie jest to siatka. One nie są takie rozległe jak sprawy związane z oszustwami, chociażby z platformami inwestycyjnymi, gdzie mamy setki, jak nie tysiące pokrzywdzonych i ogromną liczbę przelewów bankowych do zbadania oraz ślad pieniądza, jaki trzeba było przeprowadzić.

Niepokojącą i bardzo trudną kategorią do ścigania są ataki ransomware; na pewno państwo o tym słyszeliście. Dla przestępców nie ma świętości, ofiarami padają szpitale na całym świecie, pada administracja, firmy prywatne, a nawet osoby prywatne i jest to naprawdę bardzo trudna kategoria do ścigania, bo za przeciwnika mamy całe korporacje międzynarodowe, które się tym zajmują, często rozsiane po całym świecie, podzielone sektorowo i odpowiedzialne za poszczególną część. Mało tego, coraz bardziej popularna staje się usługa Ransomware-as-a-Service, czyli dla tych przestępców, którzy nie są na tyle dobrzy, sprawni technicznie, przestępcy oferują infrastrukturę przestępczą, którą można kupić i nie będąc zaawansowanym informatycznie, dokonywać ataków. Te ataki są o tyle groźne, że czasami dotyczą naprawdę ważnych obiektów i potrafią sparaliżować prace. Całe szczęście my jako Polska nie jesteśmy na mapie świata jakoś widocznie zaznaczeni, jesteśmy poza takimi krajami jak Stany Zjednoczone, gdzie jest chyba 48% pokrzywdzonych w atakach ransomware – mówię to na podstawie badań firm, które się w tym specjalizują. 48% pokrzywdzonych jest w Stanach Zjednoczonych, znacznie wyprzedzających Francję, Niemcy i inne kraje. Chciałbym więc państwa uspokoić, że Polska wcale nie jest czerwonym punktem na mapie, nawet Europy. Jeśli chodzi o cyferki i statystyki, to proszę pamiętać o tym, co powiedziałem wcześniej, że jeden podejrzanym nie jest równy jednemu podejrzanemu. One wyglądają tak i rosną z roku na rok, teraz mamy już ponad 1000 podejrzanych, w porównaniu do poprzedniego roku to też znaczny wzrost. Mamy spadek zabezpieczonego mienia, ale to wynika z tego, że w tamtym roku mieliśmy taką sprawę, że zabezpieczyliśmy 360 mln zł. W tym roku takiej sprawy nie było, ale jeśli chodzi o zabezpieczone i odzyskane mienie, to udało nam się zabezpieczyć i uratować pieniądze pokrzywdzonych na ponad 100 mln zł. To jest naprawdę wyścig z czasem,

proszę państwa, bo te pieniądze dosyć szybko z konta na konto przechodzą, są wypłacane w bankomatach, przelewane za granicę, więc to jest nasz główny cel, żeby te pieniądze uratować. W tym celu współpracujemy ze Związkiem Banków Polskich, z Komisją Nadzoru Finansowego, z Głównym Inspektoratem Farmaceutycznym, więc staramy się... oczywiście współpraca międzynarodowa jest tu dosyć istotna. Nasz główny cel to uratować pieniądze, i to jest pierwszy etap naszych działań, jeżeli jest czas, a później ściganie przestępców. Oczywiście te działania czasami prowadzone są równolegle. Ponad 300 osób tymczasowo aresztowanych, więc jestem zadowolony, widzę progres, tylko proszę pamiętać, że podejrzany podejrzanemu nie jest równy.

Poproszę o następny slajd. Teraz ta część, o której wspominał już zarówno pan komendant Michulka, jak i pan poseł – to jest ta część działalności biura, która jest realizowana głównie przez dyżurnych w całodobowej sekcji obsługi zdarzeń. Na slajdzie widziecie państwo, jak wyglądała sytuacja na przestrzeni ostatnich lat. To są informacje, które wpływają z różnych źródeł, od Biura Rzecznika Praw Dziecka, od fundacji, czasami od dostawców usług, bo oni też mają ustawione filtry i widzą, że ktoś zgłasza chęć popełnienia samobójstwa, czasami są to znajomi. Te informacje wpływają do dyżurnych i oni we współpracy z operatorami telekomunikacyjnymi i dostawcami usług internetowych jak najszybciej próbują zlokalizować osobę, która zgłasza chęci samobójcze. Trend jest strasznie, niepokojąco wysoki w ostatnich 2 latach. My nie badamy tego socjologicznie, natomiast uznajemy, że może to być wynik pandemii, zamknięcia dzieci i wielu innych czynników. Być może są to też te czynniki, o których była tu mowa, być może hejt w Internecie, natomiast my takich informacji nie mamy i takich badań nie prowadzimy. Proszę zwrócić uwagę, że te liczby niepokojąco rosną i o ile w latach 2018–2022 liczba tych zdarzeń była mniej więcej na podobnym poziomie, to ostatnie 2 lata, a szczególnie ten rok to jest 2675 takich informacji, gdzie trzeba było reagować. Osoby, które wymagały hospitalizacji, więc ich stan był dosyć poważny – 2123. Ja codziennie odbieram informacje od dyżurnych w tym zakresie i proszę mi wierzyć, że niektóre historie są mrozące, bo są to osoby ściągane z torów przed nadjeżdżającym pociągiem, są to osoby, które podcięły sobie żyły, połknęły masę tabletek, więc jest to wyścig z czasem, bardzo obciążające zadanie dla tych policjantów. Czynności na miejscu, już po ustaleniu osoby, realizują policjanci z jednostek terenowych – to rzecz oczywista, bo muszą tam jak najszybciej dojechać. Wśród tych osób są też niestety nieletni – to jest ten pomarańczowy wykres – i też jest ich dosyć dużo.

Coś, co odrywa uwagę policjantów od normalnej pracy, czyli od łapania przestępców – biuro, żeby się mogło rozwijać, to niestety policjanci muszą pracować w warunkach należytych. Ponieważ rzadko się tak zdarzało do tej pory, ja w Policji pracuję wiele lat, ale zwykle reorganizacje polegały na tym, że się przesuwało policjantów z jednego obszaru, z jednej komórki, tworząc następną, bo takie były potrzeby. Natomiast tutaj doszły dodatkowe etaty, więc zwiększył się stan etatowy każdej komendy czy każdej komórki i w związku z tym policjanci w wielu przypadkach nie mieli, gdzie siedzieć. Stąd potrzeba budowania. Chciałem państwu powiedzieć, że my ten aspekt rozwoju biura też realizujemy, została już oddana nowa siedziba w Łodzi, we Wrocławiu, która była budowana wspólnie z komisariatem Wrocław-Stare Miasto. Niedługo będzie oddana siedziba w Szczecinie, kolejne są remontowane bądź budowane, jak widać na załączonych zdjęciach, i ten proces będzie jeszcze trwał. Mam trochę danych statystycznych, jak to wygląda, ale właściwie praktycznie w każdej części kraju albo remontujemy, budujemy, albo co najmniej wynajmujemy, bo musieliśmy też w kilku miejscach w Polsce iść w wynajem siedzib tymczasowych do czasu wybudowania, bo już się przestaliśmy mieścić. Zgodnie z ustawą na budowę było przeznaczonych 450 mln zł i część mogła być pokryta z innych pozycji, jeśli chodzi o częściowe wyposażenie i sprzęt informatyczny. Natomiast w 11 miastach wojewódzkich planujemy budowę – jak państwo widzieliście, część inwestycji już została ukończona, część jest na etapie planów, na niektóre będziemy musieli wnioskować o dodatkowe środki. Modernizację mamy w trzech miastach – w Krakowie, Białymstoku i Poznaniu. Na razie nie planujemy, jest to może bardziej w sferze koncepcji – w dwóch regionach kraju, w Opolu i Gorzowie, na razie nie mamy takich mocno skonkretyzowanych planów, ale też myślimy o polepszeniu warunków pracy policjantów.

Będzie budowana centrala oraz siedziba zarządu warszawskiego i koszt wszystkich inwestycji, które planujemy, to jest prawie 744 mln zł, ale bez tego się nie da. Policjanci, szczególnie z zakresu informatyki śledczej – to jest bardzo specjalistyczna dziedzina – muszą mieć dość szczególne warunki. Pewnie państwo wiecie, że można usunąć zdalnie zawartość telefonu przez chmurę, można wykasować dane, więc te warunki muszą być spełnione, żeby do tego nie dopuścić, bo często można doprowadzić do utraty materiału dowodowego. Dlatego we wszystkich nowych siedzibach, które modernizujemy, są przewidziane bezpieczne pomieszczenia, żeby do tego nie dopuścić. Proszę, żebyśmy przeklikali kilka slajdów.

Może jeszcze bardzo krótko, panie przewodniczący, kilka przykładów spraw, jakie biuro w krótkim okresie zrealizowało, od początku istnienia, żebyście państwo mieli obraz tego, czym się zajmujemy. Obszarów, którymi zajmuje się biuro, jest wiele, natomiast my do tych spraw, oprócz podejścia operacyjnego, chcemy podchodzić od strony technicznej i naszymi przeciwnikami są często osoby tworzące infrastrukturę przestępczą, którą można w masowy sposób wykorzystywać. I o ile walka ze sprawcami ataków ransomware nie jest beznadziejna, tak jak generalnie na całym świecie mówią, bo naprawdę niewielkimi sukcesami może się pochwalić FBI i być może niektóre kraje, to często ruch pieniądza jest dosyć istotny, bo to jest robione po to, żeby uzyskać pieniądze. Stąd ten etap, kiedy dochodzi do zmonetyzowania przestępstwa, jest dosyć istotny i tam są sukcesy. To jest jeden z przykładów spraw dotyczących ataków ransomware – mówimy o ataku o nazwie Play, którym zaatakowany został mazowiecki urząd marszałkowski, Urząd Miejski w Świebodzinie i jeszcze parę innych jednostek na terenie kraju. Zatrzymaliśmy 3 osoby na terenie Polski narodowości ukraińskiej, zabezpieczyliśmy sprzęt komputerowy, który cały czas badamy.

Jeśli chodzi o seksualne wykorzystywanie dzieci, to oprócz pojedynczych spraw, które prowadzimy, co roku od momentu powstania biura dwa razy w roku, na wiosnę i jesienią, organizujemy operacje, w które zaangażowani są wszyscy policjanci CBZC. Przygotowujemy się do nich przez kilka tygodni i nazywamy je po kolei, alfabetycznie, żebyśmy wiedzieli za kilka lat, ile takich akcji zostało przeprowadzonych. W pięciu akcjach, które miały miejsce do tej pory, o kryptonimach: „Anastazja”, „Barbossa”, „Carlos”, „Dakota” i „Enola Gay” dokonaliśmy ponad 480 przeszukań, 119 osób zostało tymczasowo aresztowanych, a zarzuty postawiono 284 osobom. Zabezpieczonych zostało ponad 2 mln plików z obrzydliwymi zdjęciami, filmami. Wielkim sukcesem – i taki cel stawiamy policjantom – jest uderzanie w tych, którzy są producentami pornografii, materiałów z wykorzystaniem seksualnym dzieci. I proszę mi wierzyć, że wiele takich przypadków, o których nie ma tu czasu mówić, udało się zrealizować i ustalić osoby, które nie były do tej pory w ogóle znane służbom w żadnej skali, udało się przerwać cierpienie dzieci. Niestety są to też osoby bliskie dla tych dzieci.

„Genesis Market” to przykład sprawy, międzynarodowej operacji, w której uczestniczyło wiele krajów, którą organizowało FBI. Mówimy tu o grupie, która sprzedawała w Darknecie, czyli na czarnym rynku boty przełamujące zabezpieczenia komputerów. Jeżeli ktoś kupił te boty i komputer został zainfekowany, to zmiana hasła nic nie dawała, ten bot po prostu przekazywał utworzenie nowego hasła. Na rynku na całym świecie były 2 mln skradzionych tożsamości, które można było kupić. Takie tożsamości na innych darknetowych rynkach też można kupić i one są sprzedawane naprawdę za bardzo niskie kwoty. W Polsce też był dosyć ważny epizod tej sprawy, zatrzymaliśmy 35 osób, bo ta sprawa się oczywiście rozwinęła. To jest ten przykład, kiedy się okazuje, że na zabezpieczonym sprzęcie są też inne wątki, zupełnie nieznane do tej pory, i tak było w tym przypadku. Udało się rozbić grupę, która sprzedawała fałszywe certyfikaty zdrowotne, pomagała legalizować pobyt cudzoziemców i to jest właśnie te 35 osób, które tutaj widzimy. Po prawej stronie na zdjęciu jest taka kartka, która została znaleziona podczas przeszukania, napisana odręcznie – nie mam zdjęcia sprawcy, ale jak byście państwo zobaczyli, to czasami naszymi przeciwnikami są nastolatki i to jest kartka narysowana przez niego – to jest jego pomysł na przestępczy biznesplan.

Nielegalna kampania, czyli trochę nawiązanie do dezinformacji. To sprawa, kiedy w listopadzie ubiegłego roku zatrzymano jednego pana, który miał kilkadziesiąt telefonów,

miał portfel kryptowalutowy i wysłał 190 tys. wiadomości sms o takiej treści, że Ministerstwo Obrony Narodowej zaprasza ochotników do służby w litewsko-polsko-ukraińskim korpusie. Tam był link, który oczywiście kradł dane, więc był to typowy fishing.

Simboxy. I dodałbym jeszcze do tego tytułu call centra. Staramy się uderzać w infrastrukturę przestępczą, nie łapać sprawców gdzieś na samym dole, wypłacających pieniądze, tylko tych, którzy to organizują. Naszym celem, który sobie założyliśmy przy wielu sprawach, jest likwidacja call centrów albo simboxów. Simboxy to są urządzenia, które pozwalają masowo wysyłać wiadomości do nas, do obywateli. Państwo pewnie nieraz otrzymaliście wiadomość typu „dopłać do paczki, twoja paczka już czeka, masz nieopłacony rachunek”. Tego było mnóstwo, mam wrażenie, że w ostatnim czasie, ale to też wynik działania ustawy o nadużyciach w komunikacji elektronicznej, jest tego trochę mniej, natomiast nasze działania ukierunkowane są na to, żeby łapać tych ludzi, którzy taką infrastrukturę organizują.

Poproszę następny slajd. Braliśmy też udział w operacji organizowanej przez Niemców. Otóż nasz obywatel był odpowiedzialny za stworzenie i sprawne działanie komunikatora, gdzie przestępcy mogli się bezpiecznie porozumiewać. To nie był żaden ze znanych komunikatorów, tylko taki, który był dedykowany dla przestępców i było to dosyć duże wyzwanie techniczne dla policjantów, bo zastali bardzo dużo szaf rackowych z bardzo dużą ilością sprzętu wewnątrz, który należało umiejętnie zabezpieczyć. Pojemności 30 TB zapewne za wiele państwu nie mówią i ciężko to przełożyć nawet na wydrukowane kartki papieru, ale proszę mi wierzyć, że tego jest ogromnie dużo, a przeanalizowanie tego wymaga bardzo dużo czasu.

Fraudplace to kolejny przykład działalności biura, jeśli chodzi o zwalczanie oszustów, i jest to kolejna grupa przestępcza, która sprzedawała fałszywe strony do Allegro, Allegro lokalnie, bramki fałszywych płatności BLIK i robiła to na kanale Telegram. Tu też mamy bardzo dużo osób, które były na granicy odpowiedzialności karnej, jeśli chodzi o Kodeks karny – część z nich to byli nieletni, część ledwo co się załapała, żeby odpowiadać karne przed normalnymi sądami powszechnymi, a nie w postępowaniach dla nieletnich. 29 osób policjanci z Białegostoku zatrzymali, 17 osób zostało tymczasowo aresztowanych, oczywiście są wśród nich tacy, którzy już mieli odpowiedni wiek – to była młodzież, która postanowiła sobie zrobić biznes.

Jeśli chodzi o kryptowaluty, to jeszcze taki slajd. Bardzo istotna część, jeżeli chodzi o Policję. My te szkolenia robimy dla policjantów również innych komórek, bo jeśli chodzi o kryptowaluty, to one się pojawiają nie tylko w cyberprzestępcstwach. Kryptowaluty to jest element prania pieniędzy w różnych przestępcstwach. Gdy pracowałem w innym biurze, spotkałem się z kryptowalutami przy uprowadzeniach. Wiadomo, że to wszystko robione jest po to, żeby pozostać anonimowym.

Następny slajd poproszę. Ponieważ zagadnień w biurze jest dużo i tematyka jest bardzo trudna, a poziom naszych policjantów też jest różny, bo wiadomo, że każdy z nich posiada inne wykształcenie, każdy ma inne doświadczenie, to stworzyliśmy zespół szkoleniowy, który jest odpowiedzialny za przygotowanie programu szkoleń dla reszty polskich policjantów. Ale szkolimy się też sami wewnętrznie, policjanci szkolą się za granicą, w policyjnej akademii norweskiej, współpracujemy ze wszystkimi ważnymi służbami, które zajmują się ściganiem cyberprzestępców na świecie i wiem, że to jest słuszny kierunek, bo inaczej nie rozwijalibyśmy się ani nie byłibyśmy skuteczni w wielu obszarach, bo sprawcy zostawiają czasami drobne tropy, ale w wielu miejscach na świecie, i wielkim sukcesem jest połączyć te puzzle w jedną całość, w jeden obraz.

Trochę liczb, jeśli chodzi o szkolenia, o których wspomniał pan komendant Michułka, bo działalność szkoleniowa ma wiele aspektów. Oprócz tego, że szkolimy policjantów, robimy szkolenia wspólnie z prokuratorami, jak państwo widzicie, w tym roku przeszkoliliśmy 1884 policjantów z komend powiatowych, miejskich. Mamy algorytmy, jak postępować przy różnego rodzaju postępowaniach, ale oprócz tego prowadzimy szkolenia – i uznajemy ten kierunek za niezmiernie ważny – dla różnych grup, poczynając od małych dzieci w szkołach, gdzie mamy specjalnie przygotowaną prezentację, która jest przez nie przyswajana, a tematyka jest do nich dostosowana, przez uczniów klas V–VIII, zahaczając nawet o początek szkoły średniej, więc dla osób starszych. I nie będę odkrywcy, jak

powiem, że te treści edukacyjne są dostosowane do zagrożeń w danych grupach wiekowych – mówimy o hejcie, o tym, jak niebezpieczne jest publikowanie takich wiadomości, mówimy o seksualnym wykorzystywaniu, a w przypadku osób starszych mówimy o oszustwach. Zatem ten przekrój jest bardzo duży, ale staramy się wszystkich uczulać na cyberhigienę, bo bez tego tych spraw byłoby tyle, że żadna policja na świecie nie byłaby w stanie przerobić tych postępowań, gdyby nie odpowiednie zachowanie. Podczas tych spotkań, szczególnie z młodzieżą w szkołach średnich i na wyższych uczelniach – a wiemy z doświadczenia, że to jest słuszny kierunek rekrutacji do nas i być może stąd ta liczba podań, bo mamy już podpisanych trochę porozumień ze szkołami średnimi i wyższymi w każdym regionie w kraju, przeszkoliliśmy ponad 25 tys. osób – ale podczas tych szkoleń mówimy też o biurze. Zachęcamy, żeby do nas wstępować, oferujemy przy tym całkiem przyzwoite zarobki, jeśli chodzi o rynek IT. Informatyka śledcza to taka dziedzina, która jest trochę sercem naszej pracy, bo wszystkie ślady cyfrowe zabezpieczone na nośnikach mają istotne znaczenie. Może być trochę problem z czasem przeanalizowania ich, bo tego jest bardzo dużo, ale posiadamy narzędzia, które faktycznie są skuteczne. Większość działalności przestępczej i śladów zostawionych jest na nośnikach małych, czyli telefonach, smartfonach, których używamy na co dzień. Jak państwo widziecie, liczba badanych urządzeń rośnie – nośników, telefonów, komputerów – także to oprogramowanie z pewnością już na siebie zarobiło, bo gdybyśmy mieli oddawać to biegłym, na rynek zewnętrzny, to koszty byłyby duże, a poza tym byłoby to trochę nielogiczne.

Jeśli chodzi o wsparcie jednostek Policji – poproszę następny slajd – jeśli chodzi o urządzenia mobilne, telefony, to około 40% naszych badań to jest pomoc jednostkom terenowym Policji. Jeśli chodzi o komputery, kopie binarne, to 20%. 193 razy policjanci brali udział w realizacjach – mam na myśli wyjazd z policjantami z komend powiatowych, miejskich na miejsce jakiegoś zdarzenia – robili kopie binarne albo pomagali w innych czynnościach informatycznych na miejscu.

Dziękuję. Pewnie jeszcze wielu rzeczy nie powiedziałem, ale zakładam, że będzie dużo pytań.

Przewodniczący poseł Konrad Fryszak (KO):

Bardzo dziękuję, panie generale. Otwieram listę mówców. Pan poseł Gosek, bardzo proszę.

Poseł Mariusz Gosek (PiS):

Chciałem podziękować jako sprawozdawca projektu o powołaniu CBZC w zeszłej kadencji polskiej Policji, ministrom, także panu ministrowi Zielińskiemu, panu ministrowi Kamińskiemu, panu ministrowi Wąsikowi, panu ministrowi Pawłowi Szefernakerowi, a państwu chcę pogratulować tych sukcesów.

Naprawdę pięknie to się rozwinęło, rozwija, ten progres jest zauważalny, natomiast jeżeli mogę, bo jestem ze świętokrzyskiego i jako żywo jestem zainteresowany rozwojem tego województwa, mam jedno pytanie: co z Kielcami? Wiem, że tam też była planowana rozbudowa czy przebudowa obiektu, który miał służyć CBZC, ale jeżeli pan generał mógłby uzupełnić, to bardzo proszę.

Komendant CBZC nadinsp. Adam Cieślak:

Dziękuję, panie pośle. Jeśli chodzi o Kielce, to progres jest bardzo duży, bo tam jest budowa o charakterze modułowym, czyli tak zaprojektowana, że się skleja z poszczególnych elementów budynek, i wydaje mi się, że wysokość maksymalna została już osiągnięta. Mam zdjęcia przesłane przez naczelnika, może w przerwie pokazałbym panu. Wygląda to obiecująco i myślę, że niedługo będzie otwarcie. Mam na myśli przyszły rok oczywiście, bo jeszcze trzeba to pomieszczenie uzbroić, akredytować, ale wygląda to naprawdę super.

Przewodniczący poseł Konrad Fryszak (KO):

Pan poseł Bogucki.

Poseł Zbigniew Bogucki (PiS):

Ja króciutko. Panie generale, wspomniał pan o Szczecinie. Czy mógłby pan przybliżyć, jak tam kwestia inwestycji wygląda?

Komendant CBZC nadinsp. Adam Cieślak:

Być może Szczecin mam na zdjęciach?

Posel Zbigniew Bogucki (PiS):

Wymieniał pan Szczecin...

Komendant CBZC nadinsp. Adam Cieślak:

Moglibyśmy się cofnąć do zdjęć z budow?

Posel Zbigniew Bogucki (PiS):

Chodzi o to, jakie tam są plany? Na kiedy jest planowane zakończenie?

Komendant CBZC nadinsp. Adam Cieślak:

W przyszłym roku.

Posel Zbigniew Bogucki (PiS):

Dziękuję bardzo.

Posel Mariusz Gosek (PiS):

Przepraszam, panie generale...

Przewodniczący poseł Konrad Fryształ (KO):

Panie pośle, przypominam, że prowadzimy obrady, to nie wolna amerykanka.

Posel Mariusz Gosek (PiS):

Przepraszam, panie przewodniczący, oczywiście.

Przewodniczący poseł Konrad Fryształ (KO):

Proszę, udzielam panu głosu.

Posel Mariusz Gosek (PiS):

Panie generale, kwota, o której pan mówił, 700..., ile to było milionów? Ile było przewidziane, a ile brakuje?

Komendant CBZC nadinsp. Adam Cieślak:

Już mówię. Zgodnie z oceną skutków regulacji było przewidzianych 450 mln zł na budowę sieci, z tym że jeszcze pod innymi pozycjami, jak sprzęt specjalistyczny, też są pieniądze, a budowa taka często jest zakończona z pełnym wyposażeniem, więc jest trochę więcej przewidzianych niż 450 mln zł. Natomiast my szacujemy, że około 740 mln zł, z tym że te szacunki bywają zmienne, będzie potrzeba, żeby zamknąć wszystko to, co planujemy. Będziemy na pewno wnioskować o te pieniądze w takiej kolejności, jak jest to niezbędne.

Posel Mariusz Gosek (PiS):

Panie przewodniczący, jeżeli mogę...

Przewodniczący poseł Konrad Fryształ (KO):

Bardzo proszę.

Posel Mariusz Gosek (PiS):

Bo to jest niezwykle ważne, żebyśmy zauważyli też te potrzeby CBZC, bo wiem, jak dobrą robotę – przepraszam, że tak powiem – robi biuro. Ta przestępczość przeniosła się w sposób niebywały do Internetu, to jest oczywiste, dlatego myślę, że trzeba się pochylić wspólnie, powinno nam na tym zależeć, żeby te środki się znalazły. Dziękuję.

Przewodniczący poseł Konrad Fryształ (KO):

Bardzo dziękuję. Pan poseł Tuduj.

Posel Krzysztof Tuduj (Konfederacja):

Bardzo dziękuję, panie przewodniczący. Bardzo przepraszam, bo nie uczestniczyłem od samego początku w posiedzeniu Komisji, być może ta informacja padła, ale chciałbym zapytać, czy współpracują państwo na bieżąco z CSIRT-ami MON, NASK i ABW?

Komendant CBZC nadinsp. Adam Cieślak:

Tak, oczywiście, co tydzień się spotykamy z przedstawicielami CSIRT-ów na cotygodniowych posiedzeniach w RCB, gdzie wymieniamy się informacjami o zagrożeniach.

Zdarza się także, że mamy informacje wyprzedzające, wynikające chociażby z naszej pracy operacyjnej. Posiadamy też czasami, bo to nie jest główny przedmiot naszej działalności, informacje o nieszczelności pewnych systemów w różnych podmiotach, instytucjach i te informacje też przekazujemy. Tak że odpowiedź brzmi: tak.

Przewodniczący poseł Konrad Fryszak (KO):

Bardzo dziękuję, panie generale. Ponieważ posłowie zwracają uwagę, że nie otrzymali odpowiedzi na pytania, które padły po pierwszej części, to bardzo bym prosił o udzielenie tych odpowiedzi. Ale skoro jesteśmy jeszcze przy kwestii prezentacji i przedstawienia informacji przez pana generała, to mam pytanie, czy my możemy otrzymać tę prezentację? Mamy ją? Rozumiem, że sekretariat może nam tę prezentację rozesłać, żeby została w naszych służbowych skrzynkach.

I druga rzecz. Pani posłanka Nowogórska prosiła mnie, żebym w jej imieniu to pytanie zgłosił: czy macie państwo po tych 2,5 roku, od momentu powstania ustawy – przypominam, że przyjęliśmy ją ponad politycznymi podziałami, w ramach jednomysłności, że musi się tym zająć wyspecjalizowana jednostka – jakieś przemyślenia co do funkcjonowania w ramach nakreślonych ram prawnych? Czy pojawiają się jakieś potrzeby zmian ustawowych, doprecyzowania czy gdzieś tam może rozluźnienia przepisów? Czy takie wnioski państwo ewentualnie macie?

I trzecia kwestia. Widziałem mój ukochany Radom, siedziba komendy wojewódzkiej garnizonu mazowieckiego, ale widziałem tam tylko kafelek „Radom”, bez żadnego zdjęcia... Uśmiech pana gen. Michułki też dużo mówi, więc siłą rzeczy, skoro koledzy pytają o swoje małe ojczyzny, to ja też chcę się dowiedzieć, czy jakaś rozbudowa w Radomiu będzie miała miejsce, zwłaszcza że terenu wokół komendy jeszcze trochę mamy do wykorzystania. W latach słusznie minionych była tam nawet chyba jakaś szkoła policji; przez jakiś czas byłem wiceprezydentem, zarządzałem w imieniu Skarbu Państwa gruntami i pamiętam, że trochę terenu jeszcze tam mamy.

Komendant CBZC nadinsp. Adam Cieślak:

Jeśli chodzi o Radom, to jesteśmy już na dobrej drodze, bo na dniach będzie ogłoszony przetarg na plan inwestycji, zrobienie dokumentów, więc myślę, że po tym już roboty pójdą. Tam jest zaplanowana inwestycja, 85 policjantów docelowo ma pełnić służbę. Mamy to w szacunkach – daj Boże – na 2028 r.

Chciałem jeszcze powiedzieć jedną ważną rzecz, że my jesteśmy przy tych wszystkich inwestycjach i bierzemy aktywny udział, bo ciężko projektować dom, w którym nie wiadomo, co się będzie działo, natomiast wszystkie inwestycje są realizowane przez komendy wojewódzkie Policji, tam są odpowiednie wydziały, które się tym zajmują. Jeśli chodzi o pieniądze, to wiadomo, pieniądze budżetowe i to, co mamy zaplanowane, to mamy zaplanowane, ale nam też zależy na tym, żeby to biuro faktycznie miało to, co powinno mieć. Dziękuję.

Przewodniczący poseł Konrad Fryszak (KO):

Na Radom mamy środki zabezpieczone?

Komendant CBZC nadinsp. Adam Cieślak:

Mamy zabezpieczone środki na sporządzenie dokumentacji...

Przewodniczący poseł Konrad Fryszak (KO):

A na budowę?

Komendant CBZC nadinsp. Adam Cieślak:

Aż tak nie planujemy budżetu, panie pośle, w perspektywie długoletniej.

Przewodniczący poseł Konrad Fryszak (KO):

OK, rozumiem. Jakiś szacunkowy koszt wyjdzie z dokumentacji projektowej.

Komendant CBZC nadinsp. Adam Cieślak:

Kwestię logistyki zostawiłem na barkach mojego zastępcy, który jest świetny. Mam tu pięknie napisane, że około 38 mln zł planujemy na budowę.

Przewodniczący poseł Konrad Fryszak (KO):

Bardzo dziękuję za wyczerpującą odpowiedź. A odnośnie do ustrojowych zmian?

Zastępca komendanta głównego Policji nadinsp. Tomasz Michułka:

Szanowny panie przewodniczący, szanowni państwo, inwestycji w Radomiu będę pilnował, także deklaruję... Ale odnośnie do zapytania pani poseł, to póki co żadnych inicjatyw legislacyjnych nie podejmujemy z panem generałem, natomiast chciałbym powiedzieć, że jesteśmy na etapie prac, zadaliśmy sobie – jak myślę – bardzo trudne zadanie, aby dokonać klasyfikacji cyberprzestępstw. Powołałem specjalny zespół, który ma doprecyzować, które kategorie przestępstw będziemy traktować jako cyberprzestępstwa. Oczywiście jest to niezmiernie trudne, ponieważ niektóre przestępstwa, jak na przykład oszustwo, może być przestępstwem kryminalnym, gospodarczym i cyberprzestępstwem, ale poprzez analizę modus operandi sprawców chcemy je stypizować w jakiś sposób, żebyśmy już na przyszłość mieli możliwość odniesienia się, czy ta przestępczość cyberowa wzrasta i żeby obserwować tendencje. Myślę, że już na początku roku będziemy mieli taki katalog przestępstw, które zakwalifikujemy jako przestępstwa o charakterze cyberprzestępstw. Także jest taka inicjatywa i zakończenie prac zespołu szacujemy na koniec stycznia. Dziękuję bardzo.

Przewodniczący poseł Konrad Fryszak (KO):

Bardzo dziękuję i proszę o odpowiedź na pytania głównie posła Ściebiorowskiego. Bardzo proszę. Panie pośle, króciutko proszę o przypomnienie.

Poseł Łukasz Ściebiorowski (KO):

Dziękuję. Pytałem o kraje, z których ataki do nas docierają. Nie wiem, czy państwo chcą, czy mogą w tej chwili konkretne kraje podać, gdzie – poza tymi naszymi wewnętrznymi – się kumulują te ataki? Jedno państwo przychodzi nam pewnie wszystkim na myśl, ale czy są jeszcze inne, zwłaszcza te spoza unii?

Komendant CBZC nadinsp. Adam Cieślak:

Jeśli chodzi o wektor ataków, to nie zawsze da się go określić, dlatego że ten ruch często przechodzi przez różnego rodzaju VPN-y, gdzie są tzw. przystanki. Czasami są to kraje, które nie współpracują z żadnymi organami ścigania i tam to zapytanie gdzieś grzeźnie. Jeśli chodzi o grupy ransomware, to my przynajmniej tak je odczytujemy, że one mogą być rozsiane po całym świecie, a osoby odpowiedzialne za poszczególne etapy tego przestępstwa mogą na różnych półkulach nawet pracować. Stąd oprócz tych, co do których mamy podejrzenia, skąd pochodzą, jest jeszcze cała masa tych funkcjonujących w celach typowo zarobkowych, czyli wyłudzenia okupu. Odpowiedź na to pytanie jest więc taka, że nie zawsze da się ustalić wektor ataku.

Zastępca dyrektora departamentu w MC Marcin Wysocki:

Panie przewodniczący, wynotowałem pytania, będą bardzo zwięzłe odpowiedzi. Pierwsze z pytań pani poseł dotyczyło faktycznej liczby incydentów, jeżeli chodzi o infrastrukturę krytyczną. Sięgnę do raportu o stanie cyberprzestrzeni RP w 2023 r. – to jest raport przygotowany przez CSIRT GOV, przez zespół odpowiadający za bezpieczeństwo przede wszystkim komputerowe i infrastruktury krytycznej w wymiarze cywilnym, administracji państwowej, rządowej najwyższego szczebla. Jak możemy przeczytać w raporcie, w roku 2023 CSIRT GOV zarejestrował łącznie 322 656 zgłoszeń o potencjalnym wystąpieniu incydentu teleinformatycznego w swoim obszarze kompetencyjnym, spośród których 43 785 zostało zakwalifikowanych jako faktyczne incydenty bezpieczeństwa informatycznego. Wskazana statystyka zawiera zgłoszenia rejestrowane automatycznie w systemie ARAKIS, jak również zgłoszenia obsługiwane w ramach bieżącej pracy zespołu CSIRT GOV. Na co jeszcze zwraca uwagę ABW w stosunku do systemu ARAKIS? Wzrost liczby wygenerowanych przez system incydentów przy jednoczesnym spadku liczby zdarzeń zarejestrowanych jako zagrożenia dla infrastruktury teleinformatycznej podmiotów w 2020 r. w porównaniu do 2022, na co wpływ mają także zmiany w zakresie detekcji. Ponadto zespół CSIRT GOV odnotował 19 888 zgłoszeń, na podstawie których zarejestrowano 4676 incydentów w rozumieniu ustawy o krajowym systemie cyberbezpieczeństwa.

Było też pytanie pani poseł, podpytanie o wektory ataku, przede wszystkim o kraje, z których jesteście atakowani. Na to pytanie już odpowiedział pan generał, ja tylko

powiem, że jeżeli chodzi o atrybucję grup APT, te wyspecjalizowane, zorganizowane to przede wszystkim Rosja. Natomiast jeżeli chodzi o przepływ ruchu, to rozwinięcie wyjaśnienia pana generała jest dokładnie opisane między innymi w raporcie ABW przywołanym przeze mnie.

Co do drugiego pytania o rekomendacje pełnomocnika dotyczące platform biuletynów informacji publicznej, z których nie warto korzystać, to oczywiście poprzez narzędzie skanujące zespół CSIRT NASK sprawdził, że z takich podatnych platform korzysta wiele instytucji publicznych. Dlatego w rekomendacjach zostało wskazane, że może wystąpić tzw. incydent krytyczny, czyli mający najdalsze skutki incydent kwalifikowany z ustawą o krajowym systemie cyberbezpieczeństwa. Przedmiotem rekomendacji jest stosowanie systemów udostępnionych przez Centralny Ośrodek Informatyki. Konkretniej liczby nie wskażę, natomiast skala tego zjawiska, tych podatnych BIP-ów była na tyle duża, że jak najbardziej warto było takie rekomendacje wydać. To co istotne to przede wszystkim możliwość publikowania w takim biuletynie informacji publicznej na przykład w sposób skoordynowany fałszywych informacji, dezinformacji, więc jest to bardzo ważne.

Trzecie pytanie: czy wynagrodzenia w sektorze publicznym i sektorze prywatnym zostały zrównane? W zakresie szczegółowego porównania, w oparciu o raporty powszechnie dostępne, oczywiście możemy przesłać Wysokiej Komisji takie wyjaśnienia na piśmie. Ja tylko wskażę, że ze sprawozdania ministra cyfryzacji z 2022 r. wynika, że między innymi Ministerstwo Infrastruktury, Ministerstwo Finansów wskazywało na to, że udało się utrzymać personel, pozyskać nowy personel, że jesteśmy konkurencyjni. Natomiast to, co należy zaznaczyć, to fakt, że nie każdy podmiot publiczny może być beneficjentem Funduszu Cyberbezpieczeństwa, czyli nie wszyscy eksperci pracujący w administracji publicznej, jedynie podmioty szczebla rządowego, CSIRT-y poziomu krajowego szczególnie istotne dla bezpieczeństwa teleinformatycznego, wskazane w ustawie. Natomiast oczywiście projektujemy i rozważamy rozszerzenie tego katalogu podmiotowego beneficjentów między innymi o Państwową Straż Pożarną.

Kolejne pytanie panów posłów – walka z dezinformacją. Chciałbym powiedzieć przede wszystkim o kampanii ogólnopolskiej prowadzonej przez MC – trzy spoty radiowe, trzy telewizyjne, materiały graficzne z wizerunkiem trolli. Każdy z nich odpowiadał na inny cel dezinformacji – wywoływanie paniki i strachu, polaryzacja społeczna, podważanie zaufania do instytucji publicznych. Walka z taką dezinformacją skupia się na unikaniu rozpowszechniania nieprawdziwych treści, weryfikacji źródeł informacji. Ja też zachęcam do tego, żeby zgłaszać dezinformacje i zapamiętać taką stronę internetową: www.nask.pl/dezinfo. W mojej ocenie jest to najlepsza kampania, jeśli chodzi o dezinformację, jaka została przeprowadzona przez podmiot publiczny. Mam nadzieję, że przynajmniej do części z państwa ona dotarła.

Kolejne pytanie dotyczyło ochrony małoletnich. Superważne zadania zostały opisane przez panów generałów, jakie realizują policjanci i policjantki z CBZC. Zostało też wskazane, jak ważna jest profilaktyka w tym zakresie, zwiększanie wiedzy, ściganie sprawców tych przestępstw. Ja tylko tytułem uzupełnienia: w ramach CSIRT NASK funkcjonuje zespół Dyżurnet, z kolei Dyżurnet można znaleźć między innymi pod adresem: dyzurnet.pl i można tam zgłaszać nielegalne treści. I co jeszcze istotne w kontekście ochrony małoletnich, to również minister cyfryzacji przedstawił niedawno założenia do projektu ustawy o ochronie małoletnich przed dostępem do treści szkodliwych w Internecie. Ten projekt jest na etapie wnioskowania o wpis do wykazu prac Rady Ministrów.

Pytanie pani poseł dotyczyło również liczby ataków, wycieku danych wrażliwych. Z raportu CSIRT GOV przenoszę się do raportu CSIRT NASK. Cytując: łącznie w 2023 r. zgłoszono około 185 000 podatności do błędnych konfiguracji, w tym około 3500 przypadków, gdy wrażliwe dane takie jak kopie zapasowe, kod źródłowy, zrzuty bazy danych czy dzienniki zdarzeń serwera były dostępne publicznie. O tym, jak działają między innymi funkcjonariusze Policji w Darknecie, jakie są skutki tego, jeżeli wyciekną nasze dane, to znaczy informacje superważne, żeby zadbać o to, żeby do tego incydentu nie doszło, bo w przypadku wycieku takich danych z VIP WEB-u informacje już nie znikają, ale oczywiście można podjąć pewne działania mitygujące te zagrożenia, między innymi zastrzec numer PESEL.

Było też pytanie dotyczące dbania o bezpieczeństwo w relacjach z dostawcami. To jest temat szalenie złożony, ale mogę powiedzieć, że podmioty publiczne są zobowiązane do wprowadzania wielu rozwiązań z zakresu systemu zarządzania bezpieczeństwem informacji, co wynika z rozporządzenia o krajowych ramach interoperacyjności, tzw. rozporządzenia KRI. Co z tego wynika? Oszacowanie ryzyka, wskazanie zagrożeń, zaadresowanie ich m.in. w umowach z dostawcami – tu będą takie postanowienia, które gwarantują kontrolę nad przetwarzaniem danych, zgodność z polityką bezpieczeństwa informacji podmiotów. W przypadku, jeśli korzystamy z usług chmurowych, należy jeszcze wykorzystać standardy chmury obliczeniowej, które są kompatybilne z projektem wspólnej infrastruktury państwa, o którym wspominałem wcześniej, czyli możliwość korzystania z chmury rządowej, ale również bezpiecznej chmury świadczonej przez podmioty komercyjne.

Mam nadzieję, panie przewodniczący, że udało mi się zwięźle odnieść do pytań, które zidentyfikowałem.

Przewodniczący poseł Konrad Fryszak (KO):

Bardzo dziękuję. O głos prosił jeszcze pan dyrektor.

Dyrektor departamentu w MSWiA Dariusz Nowak-Nova:

Odpowiedź na ostatnie pytanie może być trochę krótsza. Świadczenia bezpieczeństwa przemysłowego, poświadczenia dla pracowników, instrukcje bezpieczeństwa, które opisują konkretny system. Systemy klasyfikujemy i rzeczywiście tego rodzaju dokumentacji wymagamy. Dziękuję.

Przewodniczący poseł Konrad Fryszak (KO):

Bardzo dziękuję. W związku z wyczerpaniem porządku obrad i wyczerpaniem listy mówców zamykam posiedzenie Komisji.