KPB.430.010.2022
Nr ewid. 125/2022/P/21/042/KPB

Informacja o wynikach kontroli

DZIAŁANIA PAŃSTWA W ZAKRESIE ZAPOBIEGANIA I ZWALCZANIA SKUTKÓW WYBRANYCH PRZESTĘPSTW INTERNETOWYCH, W TYM KRADZIEŻY TOŻSAMOŚCI

DEPARTAMENT PORZĄDKU
I BEZPIECZEŃSTWA WEWNĘTRZNEGO

MISJĄ
Najwyższej Izby Kontroli jest niezależna, profesjonalna kontrola zadań publicznych w interesie obywateli i państwa

Informacja o wynikach kontroli
Działania państwa w zakresie zapobiegania i zwalczania skutków wybranych przestępstw internetowych, w tym kradzieży tożsamości

p.o. Dyrektor Departamentu Porządku
i Bezpieczeństwa Wewnętrznego

Tomasz Sordyl

Zatwierdzam:
Prezes Najwyższej Izby Kontroli

Marian Banaś
Warszawa, dnia 24. 11. 2022

Najwyższa Izba Kontroli
ul. Filtrowa 57
02-056 Warszawa
T/F +48 22 444 50 00

www.nik.gov.pl

SPIS TREŚCI

WYKAZ STOSOWANYCH SKRÓTÓW, SKRÓTOWCÓW I POJĘĆ 4

1. WPROWADZENIE 6

2. OCENA OGÓLNA 8

3. SYNTEZA WYNIKÓW KONTROLI 10

4. WNIOSKI 13

5. WAŻNIEJSZE WYNIKI KONTROLI 15

5.1. System zapobiegania i minimalizowania skutków przestępstw internetowych 15
5.2. Przygotowanie kadrowe, logistycznie oraz organizacyjne do zapobiegania i zwalczania skutków przestępstw internetowych 26
5.3. Procedury zgłaszania przestępstw internetowych i reagowania na tego rodzaju zdarzenia 29
5.4. Działania edukacyjne zwiększające wiedzę obywateli na temat przestępczości komputerowej oraz wydawanie wytycznych podnoszących poziom bezpieczeństwa użytkowników Internetu 32
5.4.1. Wyniki badania sondażowego opinii publicznej 40
5.5. Współpraca międzynarodowa 48

6. ZAŁĄCZNIKI 50

6.1. Metodyka kontroli i informacje dodatkowe 50
6.2. Analiza stanu prawnego i uwarunkowań organizacyjno-ekonomicznych 53
6.3. Wykaz aktów prawnych dotyczących kontrolowanej działalności 56
6.4. Wykaz podmiotów, którym przekazano informację o wynikach kontroli 57
6.5. Stanowisko Ministra do informacji o wynikach kontroli 58
6.6. Opinia Prezesa NIK do stanowiska Ministra 62

Wykaz stosowanych skrótów, skrótowców i pojęć

Algorytmy	Algorytmy działania Policji w odniesieniu do różnych typów działań przestępczych;
baza wiedzy *lub* **baza**	Baza wiedzy z zakresu cyberbezpieczeństwa upubliczniona przez Ministra Cyfryzacji na portalu gov.pl;
BdWzC KGP	Biuro do Walki z Cyberprzestępczością Komendy Głównej Policji;
botnet	Sieć zainfekowanych komputerów sterowanych centralnie przez specjalne kontrolery, które są używane do różnego rodzaju wrogiej działalności, bez wiedzy ich właścicieli;
CBZC *lub* **Biuro**	Centralne Biuro Zwalczania Cyberprzestępczości;
CSIRT	Zespół ekspertów do spraw bezpieczeństwa informatycznego, których głównym zadaniem jest reagowanie na incydenty z zakresu bezpieczeństwa komputerowego. Świadczy on usługi niezbędne do rozwiązania tego typu problemów oraz umożliwienia użytkownikom wznowienia normalnej działalności. Na podstawie ustawy o krajowym systemie cyberbezpieczeństwa w Polsce funkcjonują m.in. CSIRT MON (koordynujący obsługę incydentów w jednostkach podległych Ministrowi Obrony Narodowej), CSIRT NASK (koordynujący w szczególności obsługę incydentów zgłaszanych przez jednostki sektora finansów publicznych oraz przez osoby fizyczne), CSIRT GOV (koordynujący w szczególności obsługę zgłaszanych incydentów dotyczących systemów teleinformatycznych infrastruktury krytycznej);
CSIRT NASK	Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego działający na poziomie krajowym, prowadzony przez NASK-PIB;
cyberprzestrzeń	Przestrzeń przetwarzania i wymiany informacji tworzona przez systemy teleinformatyczne wraz z powiązaniami między nimi oraz relacjami z użytkownikami;
dyrektywa NIS	Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii (Dz. Urz. UE L 194 z 19.07.2016, str. 1);
ENISA	Agencja Unii Europejskiej ds. Cyberbezpieczeństwa;
incydent	Pojedyncze zdarzenie lub seria niepożądanych lub niespodziewanych zdarzeń związanych z bezpieczeństwem informacji, które stwarzają znaczne prawdopodobieństwo zakłócenia prowadzonych działań i zagrażają bezpieczeństwu informacji;
incydent poważny	Incydent, którego wystąpienie powoduje lub może spowodować istotne obniżenie jakości lub przerwanie ciągłości świadczenia usługi, która ma kluczowe znaczenie dla utrzymania krytycznej działalności społecznej lub gospodarczej państwa;
KGP	Komenda Główna Policji;

KPRM Kancelaria Prezesa Rady Ministrów;

kradzież tożsamości Podszywanie się pod inną osobę poprzez wykorzystanie jej wizerunku, innych danych osobowych lub innych danych, za pomocą których jest ona identyfikowana (np. danych logowania do bankowości elektronicznej, mediów społecznościowych, itp.) mające z reguły na celu wyrządzenie tej osobie lub innym osobom szkody majątkowej albo osobistej;

KSC Krajowy system cyberbezpieczeństwa;

KSP Komenda Stołeczna Policji;

KWP Komenda Wojewódzka Policji;

NASK-PIB *lub* **Instytut** Naukowa i Akademicka Sieć Komputerowa – Państwowy Instytut Badawczy;

Pełnomocnik *lub* **Pełnomocnik Rządu** Pełnomocnik Rządu do Spraw Cyberbezpieczeństwa;

phishing Metoda ataku polegająca na przesyłaniu smsów lub e-maili, których nadawcy podszywają się pod różne podmioty (np. firmy kurierskie, organy publiczne, dostawców usług, osoby znajome lub bliskie adresata) w celu wyłudzenia danych (np. numeru kart płatniczych, danych umożliwiających logowanie do bankowości elektronicznej) i w efekcie kradzieży środków finansowych. (od ang. *fishing* – łowienie);

Plan działań Plan działań na rzecz wdrożenia Strategii Cyberbezpieczeństwa;

ransomware Oprogramowanie, które blokuje dostęp do systemu komputerowego lub uniemożliwia odczyt zapisanych w nim danych (najczęściej poprzez techniki szyfrujące), a następnie żąda od ofiary okupu za przywrócenie stanu pierwotnego. Programy typu ransomware należą do tzw. złośliwego oprogramowania. (od ang. *ransom* – okup);

spoofing Podszywanie się przez hackera pod inne urządzenie lub innego użytkownika w sieci, aby wykraść dane, zainstalować złośliwe oprogramowanie lub ominąć mechanizmy kontroli dostępu. Istnieją różne rodzaje spoofingu w zależności od wykorzystywanego urządzenia. Spoofing telefoniczny polega na podszyciu się pod czyjś numer telefonu (Abonent A) i wykonaniu połączenia telefonicznego do innej osoby (Abonent B). (dosł. nabieranie);

Strategia Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019–2024;

UKE Urząd Komunikacji Elektronicznej;

ustawa o KSC Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. z 2022 r. poz. 1863).

1. WPROWADZENIE

Pytanie definiujące cel główny kontroli

Czy organy państwowe prowadzą adekwatne działania w celu identyfikowania, zapobiegania oraz ograniczania skutków przestępstw internetowych?

Pytania definiujące cele szczegółowe kontroli

1. Czy został wdrożony skuteczny system zapobiegania i minimalizowania skutków przestępstw internetowych?
2. Czy objęte kontrolą podmioty są właściwie przygotowane kadrowo, logistycznie oraz organizacyjne do zapobiegania i zwalczania skutków przestępstw internetowych, ze szczególnym uwzględnieniem kradzieży tożsamości?
3. Czy objęte kontrolą podmioty formułowały, wynikające z prowadzonej analizy ryzyka, wytyczne oraz rekomendacje podnoszące poziom bezpieczeństwa użytkowników Internetu?
4. Czy zostały opracowane, podane do publicznej wiadomości i były stosowane w praktyce procedury zgłaszania przestępstw internetowych i reagowania na tego rodzaju zdarzenia?

Trwający postęp technologiczny, zmiany kulturowe i społeczne, jak również wydarzenia, takie jak pandemia COVID-19 spowodowały, że Internet stał się obecnie nieodłączną częścią naszego życia prywatnego i zawodowego. Zlecone przez NIK badanie opinii publicznej[1] wykazało, że 88% ankietowanych używa tego medium z różną częstotliwością, przy czym aż 64% spędza w Internecie więcej niż godzinę każdego dnia. Respondenci wskazywali, że codziennie lub przynajmniej kilka razy w tygodniu korzystają z poczty elektronicznej (74%), komunikatorów internetowych (70%) oraz bankowości elektronicznej (65%). Znaczny odsetek osób zadeklarował także korzystanie z platform ogłoszeniowych (76%), serwisów aukcyjnych (77%) oraz dostępnych *on-line* usług administracji publicznej[2] (71% badanych).

Niestety, ten nowy obszar życia został również dostrzeżony przez przestępców, którzy uzyskali dzięki niemu kolejne narzędzia i metody prowadzenia swojej działalności. Polegają one m.in. na nielegalnym czerpaniu zysków z oszustw komputerowych, ataków hakerskich, kradzieży tożsamości, *phishingu*, czy szantażu *ransomware*. Stosowane metody ataków zmieniają się w szybkim tempie, a kolejne kampanie wymierzone w użytkowników Internetu są coraz bardziej dopracowane i trudne do zidentyfikowania. Zapewnienie bezpieczeństwa cyfrowej tożsamości przestało więc dotyczyć jedynie specjalistów i wąskiej grupy entuzjastów. Stało się ono problemem społecznym i gospodarczym, mającym bezpośredni wpływ na bezpieczeństwo obywateli.

W ostatnich latach organy państwa podjęły szereg działań mających na celu budowę krajowego systemu cyberbezpieczeństwa[3] (wynikających przede wszystkim z konieczności implementacji do polskiego porządku prawnego regulacji UE[4]). Pojawia się jednak fundamentalne pytanie, czy budowany w ten sposób system jest wystarczający? Czy zapewnia racjonalną[5] ochronę obywateli przed przestępczością komputerową? Czy indywidulani użytkownicy Internetu są informowani na temat grożących im niebezpieczeństw, a w sytuacji, gdy staną się celem ataku, czy mogą liczyć na wsparcie właściwych instytucji państwowych?

Odnosząc się do celów i założeń merytorycznych kontroli należy także wskazać, że w polskim prawie karnym brak jest legalnej definicji takich pojęć, jak: przestępczość komputerowa, przestępczość internetowa, czy cyberprzestępczość, co utrudnia badanie i opisywanie tego zjawiska. Definicja taka ukształtowana została jednak na gruncie doktryny i literatury przedmiotu. Na potrzeby niniejszej kontroli wykorzystane zostało określenie „przestępstwo internetowe" zdefiniowane, jako grupa czynów zabro-

[1] Badanie przeprowadzono w okresie 20-28 kwietnia 2022 r. na reprezentatywnej, ogólnopolskiej próbie 1000 pełnoletnich mieszkańców Polski, z wykorzystaniem metody telefonicznych, standaryzowanych wywiadów kwestionariuszowych wspomaganych komputerowo (CATI).

[2] Np.: e-PUAP, Internetowe Konto Pacjenta, Platforma Usług Elektronicznych ZUS.

[3] Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. z 2022 r. poz. 1863), zwana dalej ustawą o KSC.

[4] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii (Dz. Urz. UE L 194 z 19.07.2016, str. 1) – tzw. dyrektywa NIS.

[5] Racjonalną, tzn. jak najbardziej efektywną w stosunku do posiadanych/możliwych do pozyskania sił i środków.

5. Czy były prowadzone skuteczne działania zwiększające wiedzę obywateli (użytkowników Internetu) na temat przestępstw internetowych oraz sposobów zapobiegania takim zdarzeniom?
6. Czy objęte kontrolą podmioty współpracują z organizacjami międzynarodowymi oraz innymi uznanymi instytucjami zagranicznymi i krajowymi w ramach zapobiegania i zwalczania skutków przestępstw internetowych, w tym kradzieży tożsamości?

Jednostki kontrolowane

KPRM (jednostka obsługująca ministra właściwego do spraw informatyzacji oraz Pełnomocnika Rządu do Spraw Cyberbezpieczeństwa);

Komenda Główna Policji;

Naukowa i Akademicka Sieć Komputerowa – Państwowy Instytut Badawczy.

Okres objęty kontrolą

1 stycznia 2019 r. –31 grudnia 2021 r.

nionych polegających na wykorzystaniu możliwości istniejących w sieci Internet, wraz z dodatkowym założeniem, że ich związek z Internetem jest silny – przebiegają one wyłącznie w środowisku cyberprzestrzeni nie będąc elementem klasycznego przestępstwa, gdzie użycie cyberprzestrzeni jest jedynie uzupełnieniem głównej metody działania przestępców. Przedmiotem kontroli nie były zatem przykładowo tzw. przestępstwa związane z treścią informacji, takie jak np. propagowanie treści faszyzmu i nawoływanie do nienawiści (art. 256 ustawy z dnia 6 czerwca 1997 r. Kodeks karny[6]), czy posiadanie treści pornograficznych z udziałem małoletniego (art. 202 § 4a kk.), w których to przypadkach Internet jest tylko jednym z mediów wykorzystywanych do przetwarzania oraz rozpowszechniania zakazanych treści. Kolejnym kryterium definiującym zakres przedmiotowy kontroli było ukierunkowanie badań na zagrożenia dotyczące indywidualnych użytkowników Internetu (osób fizycznych) oraz niosące dla tych osób ryzyko strat finansowych. Niezależnie bowiem od faktu, że przestępczość internetowa może dotknąć zarówno osób, przedsiębiorstw, podmiotów publicznych, czy organizacji społecznych, to właśnie „zwykły" obywatel wydaje się być podmiotem najbardziej narażonym na zagrożenia i to właśnie jemu najtrudniej jest podjąć skuteczne działania, które ograniczą skalę strat spowodowanych przestępstwem i zmniejszą ryzyko związane z funkcjonowaniem w Internecie.

[6] Dz. U. z 2022 r. poz. 1138, ze zm.

2. OCENA OGÓLNA

Brak działań w celu zapobiegania i minimalizowania skutków przestępstw internetowych dotykających indywidualnych użytkowników Internetu, w tym kradzieży tożsamości

Tworzony w Polsce krajowy system cyberbezpieczeństwa pomijał w praktyce najliczniejszą grupę użytkowników Internetu, którymi są osoby fizyczne, koncentrując uwagę na wzmocnieniu bezpieczeństwa systemów uznawanych za kluczowe dla funkcjonowania państwa. Powyższe miało miejsce, pomimo że prowadzona analiza ryzyka oraz monitoring zagrożeń jednoznacznie wykazywały, że w badanym okresie dominującą i gwałtownie zwiększającą się kategorią incydentów były oszustwa komputerowe, w tym *phishing* i kradzież tożsamości wymierzone w indywidualnych użytkowników sieci. Organy odpowiedzialne za bezpieczeństwo cyberprzestrzeni oraz koordynację polityki rządu w tym obszarze (Minister Cyfryzacji oraz Pełnomocnik Rządu do Spraw Cyberbezpieczeństwa[7]) nie reagowały na identyfikowane ryzyka oraz zagrożenia i nie dostosowywały do nich swoich działań organizacyjnych i informacyjnych[8]. W ocenie tych organów cały obszar bezpieczeństwa obywateli w sieci oraz zagrożeń ze strony przestępczości internetowej pozostawał poza ich odpowiedzialnością i nie widziały one konieczności podejmowania w tym zakresie jakichkolwiek działań.

Kontrola pozwoliła zidentyfikować szereg barier, które utrudniają obywatelom uzyskanie skutecznego wsparcia w sytuacji pokrzywdzenia przestępstwem. W jednostkach Policji nie wypracowano instrukcji dla obywateli zgłaszających tego rodzaju zdarzenia, a algorytmy przyjmowania zgłoszeń przygotowane dla policjantów były z kolei wadliwe i stanowiły tylko ograniczone wsparcie dla funkcjonariuszy. Procedury zgłaszania i obsługi incydentów zostały wypracowane w NASK-PIB, jednakże tylko symboliczna liczba osób posiadała wiedzę na temat możliwości uzyskania wsparcia ze strony tego podmiotu. W przypadku jednostek Policji oraz struktur podległych Ministrowi Cyfryzacji i Pełnomocnikowi Rządu odnotowano również brak zasobów (kadrowych, finansowych i sprzętowych) niezbędnych do realizacji zadań w zakresie zapobiegania oraz minimalizowania skutków przestępstw internetowych.

NIK oceniła natomiast pozytywnie fakt utworzenia z początkiem 2022 r. nowej jednostki organizacyjnej Policji wyspecjalizowanej w zwalczaniu przestępczości internetowej – Centralnego Biura Zwalczania Cyberprzestępczości. Zwróciła jednak uwagę na istotne ryzyka dotyczące procesu formowania tej jednostki, w tym trudności związane z pozyskaniem w założonym terminie 1,8 tys. odpowiedniej klasy specjalistów. Negatywną konsekwencją powołania CBZC może być z kolei odpływ do tego Biura specjalistów służących dotychczas w innych jednostkach organizacyjnych Policji, które w nowym systemie nadal mają pełnić istotną rolę w zwalczaniu przestępczości internetowej.

NIK oceniła jako nierzetelne i nieskuteczne prowadzone w badanym okresie działania mające na celu edukowanie i ostrzeganie obywateli na temat niebezpieczeństw grożących im ze strony sprawców przestępstw internetowych, w tym kradzieży tożsamości. W rezultacie, indywidualni użytkownicy Internetu byli w znacznej mierze pozbawieni aktualnych

[7] Zwany dalej Pełnomocnikiem lub Pełnomocnikiem Rządu.

[8] W okresie objętym kontrolą obsługa merytoryczna zadań ministra właściwego do spraw informatyzacji oraz Pełnomocnika Rządu, była prowadzona przez tę samą komórkę organizacyjną – Departament Cyberbezpieczeństwa KPRM. Dodatkowo, przez większą część badanego okresu, zadania Ministra Cyfryzacji były wykonywane, z upoważnienia Ministra, przez Pełnomocnika Rządu. W związku z powyższym, w przedstawionej ocenie oraz w ramach poszczególnych opisanych w informacji obszarów brak było możliwości wydzielenia i dokonania odrębnej oceny działań zrealizowanych przez Ministra oraz przez Pełnomocnika. Okoliczność ta została potwierdzona poprzez wskazanie przez oba te organy tożsamych zadań wykonanych w badanym okresie, w odpowiedzi na pierwsze pisma skierowane przez kontrolujących, w dniu 25 listopada 2021 r. Udzielając odpowiedzi Pełnomocnik wskazał m.in., że „(...) nie sposób oddzielić w tym obszarze aktywności ministra właściwego do spraw informatyzacji od działań Pełnomocnika (...)".

i pochodzących z oficjalnych źródeł państwowych informacji na temat zagrożeń ze strony przestępców komputerowych oraz rekomendowanych środków ochrony.

Ustalenia kontroli NIK zostały potwierdzone wynikami zleconego przez Izbę sondażu opinii publicznej. Badanie wykazało duży rozdźwięk pomiędzy deklarowaną przez respondentów wiedzą na temat niebezpieczeństw występujących w sieci, a ich faktycznymi działaniami. **Znaczna część z grupy 404 respondentów, którzy padli ofiarą ataków przestępców komputerowych, w tym kradzieży tożsamości nie zawiadomiła właściwych organów (Policji, Zespołu CSIRT), a niektórzy nie podjęli wręcz żadnych działań. Ankietowani wskazali również, że aż 85% cyberataków, które ich dotknęły nie zostało wyjaśnione, zakończyło się umorzeniem postępowania lub utratą środków finansowych i danych. Z kolei tylko 2% spraw znalazło finał w postaci wykrycia i skazania sprawcy lub odzyskania straconych środków**[9].

[9] Wyniki badania ankietowego opisano w pkt 5.4.1. informacji o wynikach kontroli.

3. SYNTEZA WYNIKÓW KONTROLI

Rzetelna analiza ryzyka zagrożeń występujących w cyberprzestrzeni

1. Podmioty objęte kontrolą prowadziły w sposób regularny, z wykorzystaniem różnych źródeł wiedzy, analizę ryzyka oraz aktualnych zagrożeń występujących w cyberprzestrzeni, w tym związanych z działalnością przestępców internetowych. W oparciu o wyniki tej analizy jednostki organizacyjne Policji oraz NASK-PIB podejmowały aktywne działania mające na celu zarządzanie zidentyfikowanymi ryzykami, obejmujące m.in.: bieżącą obsługę incydentów, wymianę informacji (z partnerami zewnętrznymi oraz w ramach poszczególnych instytucji), jak również działania organizacyjne i reformy strukturalne (np. opracowanie koncepcji utworzenia CBZC). [str. 15–21]

Brak reakcji Ministra Cyfryzacji i Pełnomocnika Rządu na identyfikowane ryzyka

NIK oceniła, jako nierzetelne, brak reakcji na identyfikowane ryzyka ze strony organów odpowiedzialnych za bezpieczeństwo cyberprzestrzeni oraz koordynację polityki rządu w tym obszarze, tj. Ministra Cyfryzacji i Pełnomocnika Rządu. Organy te, pomimo dysponowania danymi wskazującymi w sposób jednoznaczny, że w badanym okresie dominującą i gwałtownie zwiększającą się kategorią incydentów były oszustwa komputerowe i *phishing*, wymierzone w indywidualnych użytkowników Internetu, nie podjęły działań legislacyjnych i organizacyjnych mających na celu uwzględnienie mechanizmów ochrony tej grupy użytkowników sieci w ramach tworzonego w Polsce krajowego systemu cyberbezpieczeństwa. Minister i Pełnomocnik nie określili ram strategicznych aktywności organów państwa w zakresie zapobiegania i minimalizowania skutków przestępstw internetowych oraz nie koordynowali w tym obszarze działalności innych podmiotów publicznych. Dodatkowo, w toku kontroli oraz w złożonych przez Pełnomocnika zastrzeżeniach do wystąpienia pokontrolnego NIK, podjęli próbę dowodzenia, że cały obszar bezpieczeństwa obywateli w sieci oraz zagrożeń ze strony przestępczości internetowej pozostaje poza zakresem odpowiedzialności Ministra Cyfryzacji oraz Pełnomocnika Rządu i organy te nie są zobligowane do podejmowania w tym zakresie jakichkolwiek działań[10]. [str. 21–26]

Brak adekwatnych zasobów do zwalczania przestępczości internetowej, w tym kradzieży tożsamości

2. W dwóch z trzech objętych kontrolą podmiotów (Policja oraz Kancelaria Prezesa Rady Ministrów jako urząd obsługujący Ministra Cyfryzacji i Pełnomocnika Rządu) stwierdzono braki zasobów (kadrowych, finansowych i sprzętowych), które w zasadniczy sposób wpływały na jakość realizowanych zadań związanych ze zwalczaniem i ograniczaniem skutków przestępczości internetowej. W przypadku KPRM zidentyfikowano dodatkowo zagrożenia dla gospodarnego wykorzystania środków publicznych polegające na utworzeniu drogiego i niewykorzystywanego w praktyce systemu informatycznego S46 oraz ustanowieniu rozbudowanych struktur administracyjnych przeznaczonych do obsługi kancelaryjno-biurowej Pełnomocnika Rządu.

NIK oceniła pozytywnie zainicjowane w badanym okresie działania mające na celu wzmocnienie struktur organizacyjnych zaangażowanych w zwalczanie przestępczości internetowej, w tym w szczegól-

[10] Przedstawiona argumentacja nie znalazła uznania w oczach członków Kolegium NIK, które uchwałą nr 48/2022 z dnia 28 września 2022 r. oddaliło w tym zakresie zastrzeżenia zgłoszone przez Pełnomocnika Rządu.

ności utworzenie nowej, wyspecjalizowane jednostki organizacyjnej Policji – Centralnego Biura Zwalczania Cyberprzestępczości. Zapewnienie pełnej operacyjności Biura powinno przyczynić się do rozwiązania najistotniejszych problemów ograniczających skuteczność działań Policji w obszarze zwalczania przestępczości komputerowej. Jednocześnie jednak proces formowania tej jednostki (w szczególności perspektywa pozyskania do końca 2025 r. 1,8 tys. odpowiedniej klasy specjalistów) jest w ocenie NIK obarczony wieloma ryzykami, wymagającymi szczególnego nadzoru ze strony Kierownictwa Policji. Negatywną konsekwencją powołania CBZC może być z kolei odpływ do tego Biura specjalistów służących dotychczas w innych jednostkach organizacyjnych Policji, które w nowym systemie nadal mają pełnić istotną rolę w zwalczaniu przestępczości internetowej. [str. 26–29]

Niewypracowanie rekomendacji podnoszących poziom bezpieczeństwa indywidualnych użytkowników sieci

3. Skontrolowane przez Izbę podmioty publikowały w badanym okresie rekomendacje mające na celu podnoszenie poziomu bezpieczeństwa użytkowników sieci, w tym zapobieganie przestępstwom internetowym. W związku z ukierunkowaniem krajowego systemu cyberbezpieczeństwa na jego instytucjonalnych interesariuszy zalecenia te były jednak w pierwszej kolejności adresowane do poszczególnych sektorów gospodarki i życia społecznego (np. wykorzystujących sterowane automatycznie systemy przemysłowe, kolejowych, wodno-kanalizacyjnych i ochrony zdrowia) oraz obsługujących je specjalistów. **Tylko niewielka cześć wydawanych rekomendacji mogła stanowić realne wsparcie dla indywidualnych użytkowników Internetu. Dodatkowo, w związku z nieskutecznymi działaniami edukacyjnymi podejmowanymi przez Ministra Cyfryzacji i Pełnomocnika Rządu docierały one do znikomej liczby zainteresowanych obywateli.** [str. 32–40]

Niewłaściwie przygotowane procedury zgłaszania przestępstw internetowych, w tym kradzieży tożsamości i reagowania na tego rodzaju zdarzenia w jednostkach Policji

4. W wyniku kontroli zidentyfikowano utrudnienia w zgłaszaniu przestępstw internetowych powodujące, że obywatele w wielu przypadkach rezygnowali z zawiadamiania właściwych organów o tego rodzaju zdarzeniach.

W jednostkach Policji, które w ocenie większości respondentów[11] stanowiłyby pierwsze miejsce, w którym ofiary cyberprzestępców poszukiwałyby pomocy, nie wypracowano jednolitych, dostępnych dla obywateli instrukcji dotyczących zgłaszania tego rodzaju zdarzeń. Algorytmy przyjmowania takich zgłoszeń zostały przygotowane dla funkcjonariuszy Policji, ale były one wadliwe merytorycznie i nie dokonywano ich bieżącej aktualizacji. W rezultacie, przyjęte w tym zakresie procedury stanowiły tylko ograniczone wsparcie dla Policjantów, spośród których wielu nie dysponuje specjalistyczną wiedzą, pozwalającą na sprawne przyjmowanie zgłoszeń wskazujących na wystąpienie cyberprzestępstwa oraz skuteczne zabezpieczenie materiału dowodowego. [str. 29–31]

Procedury zgłaszania i obsługi incydentów, w tym dotyczących przestępstw komputerowych zostały wypracowane w NASK-PIB. Należy

[11] 81% respondentów badania opinii publicznej zleconego przez NIK wskazało jednostki Policji, jako podmiot, do którego mogą zgłosić się o wsparcie, w przypadku gdy staną się celem ataku przestępców internetowych.

jednak zauważyć, że tylko 1% respondentów sondażu zleconego przez NIK posiadał wiedzę na temat możliwości uzyskania wsparcia ze strony tego podmiotu. [str. 31–32]

Nierzetelne i nieskuteczne edukowanie i ostrzeganie obywateli na temat przestępstw internetowych, w tym kradzieży tożsamości

5. NIK oceniła jako nierzetelne i nieskuteczne prowadzone w badanym okresie działania, mające na celu edukowanie i ostrzeganie obywateli na temat niebezpieczeństw grożących im ze strony przestępców komputerowych.

Przeprowadzona kontrola wykazała, że Minister Cyfryzacji oraz Pełnomocnik Rządu, nie wypracowali jednolitego, efektywnego modelu informowania o zagrożeniach występujących w sieci, który pozwalałby m.in. na wykorzystanie potencjału jednostki nadzorowanej przez Ministra, tj. NASK-PIB. Działania edukacyjne prowadzone przez Ministra i Pełnomocnika były skierowane przede wszystkim do podmiotów krajowego systemu cyberbezpieczeństwa (np. samorządów, podmiotów służby zdrowia), czy też profesjonalistów odpowiadających za bezpieczeństwo IT. Pomijały one i w niewystarczającym stopniu docierały do indywidualnych użytkowników Internetu, którzy stanowią „najsłabsze ogniwo", narażone na bezpośrednie ataki przestępców komputerowych. Komunikaty oraz materiały opracowane dla tej grupy były trudno dostępne, niedostosowane do aktualnych zagrożeń i, co najważniejsze, docierały do znikomej liczby osób korzystających z sieci.

NIK oceniła pozytywnie działania NASK-PIB oraz Policji, które zrealizowały w badanym okresie liczne inicjatywy informacyjno-edukacyjne służące kształtowaniu „cyberświadomości" obywateli. Realne efekty tych działań były jednak ograniczone, co wynikało z rozproszenia przekazywanych komunikatów, a także z braku rzetelnej, bieżącej ewaluacji prowadzonych działań informacyjnych. [str. 32–40]

Ustalenia kontroli wskazujące na konieczność zintensyfikowania działań edukacyjnych skierowanych do indywidualnych użytkowników Internetu zostały potwierdzone wynikami przeprowadzonego na zlecenie NIK reprezentatywnego badania opinii publicznej. Badania te wykazały duży rozdźwięk pomiędzy deklarowaną przez respondentów wiedzą na temat niebezpieczeństw występujących w sieci, a ich faktycznymi działaniami. O ile bowiem na poziomie deklaracji wysoki odsetek badanych uważał się za osoby poinformowane o aktualnych zagrożeniach (77%) i zasadach bezpiecznego korzystania z Internetu (82%) oraz wskazywał, że ma wiedzę, gdzie szukać pomocy, to w sytuacji faktycznego oszustwa, nie przekładało się to na realne i świadome działania użytkowników sieci. [str. 40–48]

Aktywna współpraca międzynarodowa Policji oraz NASK-PIB

6. Kontrola wykazała, że w badanym okresie zarówno NASK-PIB, jak i Policja aktywnie współpracowały z podmiotami zagranicznymi w celu zapobiegania i zwalczania przestępstw internetowych. W obu przypadkach zaangażowanie we współpracę międzynarodową miało wymiar praktyczny i stanowiło odpowiedź na różnorodne inicjatywy partnerów zagranicznych w zakresie walki z cyberprzestępczością. [str. 48–49]

4. WNIOSKI

Przeprowadzona kontrola wykazała konieczność wdrożenia rozwiązań systemowych zapewniających ochronę indywidualnych użytkowników Internetu przed skutkami działalności cyberprzestępców. Niezbędne jest również podniesienie poziomu wiedzy i świadomości obywateli na temat niebezpieczeństw grożących im ze strony sprawców przestępstw internetowych, a także właściwego sposobu postępowania w sytuacji, gdy staną się ofiarą tego rodzaju przestępstw. W opinii NIK, najważniejsze działania powinny objąć:

Minister Cyfryzacji

1. **Podjęcie działań legislacyjnych celem nowelizacji ustawy o krajowym systemie cyberbezpieczeństwa,** które zapewnią uregulowanie w przepisach tej ustawy tematyki bezpieczeństwa indywidualnych użytkowników Internetu, w tym zasad udzielania wsparcia osobom fizycznym, które stały się celem lub ofiarą cyberataku oraz dookreślą obowiązki poszczególnych podmiotów odpowiedzialnych za realizację zadań w tym obszarze.
2. **Przygotowanie i przedstawienie Radzie Ministrów projektów modyfikacji Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019–2024 oraz Planu działań na rzecz wdrożenia Strategii Cyberbezpieczeństwa** uwzględniających w treści tych dokumentów wyniki analizy ryzyka wskazujące na dominującą skalę zagrożeń ze strony oszustw komputerowych oraz zdefiniowane, porównywalne mierniki stopnia realizacji zadań służących zapobieganiu i minimalizowaniu skutków tego rodzaju zagrożeń.

Minister Cyfryzacji oraz Pełnomocnik Rządu do Spraw Cyberbezpieczeństwa we współpracy z Kierownictwem NASK-PIB

1. **Wypracowanie i wdrożenie jednolitych założeń modelu edukowania oraz ostrzegania obywateli na temat zagrożeń cyberbezpieczeństwa.** W opinii NIK pożądane byłoby stworzenie jednego, rozpoznawalnego, oficjalnego, państwowego serwisu, zawierającego łatwo dostępne informacje na temat zagrożeń cyberbezpieczeństwa, trwających kampanii, a także zaleceń i dobrych praktyk z zakresu „cyberhigieny”[12]. Uwzględniając ograniczenia związane z prowadzaniem bazy wiedzy z zakresu cyberbezpieczeństwa na portalu gov.pl. zasadne byłoby zlecenie utworzenia i dalszego aktualizowania takiego repozytorium NASK-PIB (dysponującemu adekwatnymi zasobami do realizacji takiego zadania).
2. **Wdrożenie mechanizmów ewaluacji efektów prowadzonych przez KPRM oraz NASK-PIB działań edukacyjnych z zakresu cyberbezpieczeństwa,** które umożliwią zwiększenie skuteczności tych działań, w tym dopasowanie sposobów docierania z komunikatami do poszczególnych grup docelowych.

Komendant Główny Policji

1. **Usprawnienie procesu przyjmowania zgłoszeń obywateli i instytucji w sprawie przestępstw internetowych.** W tym celu nieodzowne byłoby przeprowadzenie ewaluacji wykorzystania w terenowych jednostkach Policji „Algorytmów działania Policji w odniesieniu do różnych typów działań przestępczych” i uzupełnienie zidentyfikowanych w nich braków.

[12] Dobrym przykładem takiego repozytorium może być m.in. strona internetowa prowadzona przez Narodowe Centrum Cyberbezpieczeństwa Wielkiej Brytanii: https://www.ncsc.gov.uk/.

2. **Opracowanie oraz upowszechnienie wśród obywateli i instytucji, skorelowanej z Algorytmami opracowanymi dla policjantów, instrukcji zgłaszania przestępstw internetowych.**
3. **Skuteczne zarządzanie ryzykami zagrażającymi utworzeniu Centralnego Biura Zwalczania Cyberprzestępczości i zapewnieniu jego pełnej operacyjności w ramach nadzoru nad trwającym procesem formowania tej jednostki.**

5. WAŻNIEJSZE WYNIKI KONTROLI

5.1. System zapobiegania i minimalizowania skutków przestępstw internetowych

Wszystkie podmioty objęte kontrolą prowadziły w sposób regularny, z wykorzystaniem różnych źródeł wiedzy, analizę ryzyka oraz aktualnych zagrożeń występujących w cyberprzestrzeni, w tym związanych z działalnością przestępców internetowych.

Szacowanie ryzyk i monitoring zagrożeń w obszarze bezpieczeństwa cyberprzestrzeni i przestępstw internetowych

W jednostkach organizacyjnych Policji analiza ryzyka w obszarze przestępczości internetowej była prowadzona w szczególności przez Biuro do Walki z Cyberprzestępczością Komendy Głównej Policji[13]. Analizą obejmowano dane pochodzące z Krajowego Systemu Informacyjnego Policji, bazy REGON, Krajowego Rejestru Sądowego, Systemu Wspomagania Dowodzenia Policji, Elektronicznego Rejestru Czynności Dochodzeniowo-Śledczych, otwartych źródeł informacji (w tym sieci Internet), a także dane nadesłane przez podmioty i agencje współpracujące z Policją, zarówno na poziomie krajowym, jak i międzynarodowym (Europol, Interpol). Pracownicy Biura wykonywali codzienne zestawienia ujawnionych zagrożeń, które były następnie przesyłane do Dyżurnego Kraju oraz do wydziałów do walki z cyberprzestępczością Komend Wojewódzkich (Stołecznej Policji).

W NASK-PIB monitoring bieżących trendów w zakresie zagrożeń cyberbezpieczeństwa realizowany był w sposób ciągły w Dziale CERT Polska[14]. Prowadzone analizy bazowały na wnioskach wynikających z obsługi i koordynacji zgłaszanych incydentów, jak również z proaktywnego rozpoznawania zagrożeń. Szacowanie ryzyka odbywało się metodą ekspercką, w oparciu o informacje pozyskiwane z różnych źródeł wewnętrznych i zewnętrznych. Wykorzystywane źródła danych obejmowały w szczególności:

- informacje przesyłane do zespołu CERT Polska w zgłoszeniach incydentów, analizowanych według obowiązującej w zespole „Instrukcji obsługi incydentów";
- własną pracę analityczną polegającą na wyszukiwaniu zagrożeń cyberbezpieczeństwa;
- informacje o incydentach występujących we właściwości innych zespołów CSIRT w Polsce i za granicą, w tym informacje przekazywane w ramach europejskiej sieci CSIRT;
- monitoring biuletynów branżowych w zakresie błędów i podatności bezpieczeństwa występujących w sprzęcie i oprogramowaniu;
- analizę danych pochodzących z automatycznych systemów rejestrujących zdarzenia bezpieczeństwa prowadzonych przez CERT Polska (platforma n6, MWDB[15]) oraz zewnętrznych: Virus Total Intelligence, Shodan;

[13] Zwane dalej: BdWzC KGP.

[14] CERT Polska jest funkcjonującym od 1996 r. w ramach NASK zespołem zajmującym się całodobowym nadzorowaniem ruchu internetowego i podejmowaniem akcji w razie ujawnienia zagrożeń. W skład CERT Polska wchodzą zespoły: Monitoringu i Wstępnego Rozpoznania, Analiz Bieżących Zagrożeń, Analiz Sytuacyjnych i Działań Proaktywnych, Projektów Analitycznych oraz Zespół Analiz Informatyki Śledczej.

[15] Zasady działania systemów opisano na str. 20 informacji.

- informacje medialne sugerujące zdarzenia, które mogły zagrażać cyberbezpieczeństwu albo być skutkami takich zagrożeń[16].

W jednostkach organizacyjnych KPRM[17] obsługujących Ministra Cyfryzacji i Pełnomocnika Rządu pozyskiwano od podmiotów krajowego systemu cyberbezpieczeństwa, informacje i dane statystyczne odnoszące się do różnych rodzajów zagrożeń występujących w cyberprzestrzeni, zarejestrowanych zgłoszeń oraz incydentów bezpieczeństwa, w tym przestępstw internetowych. Podstawowymi źródłami informacji wykorzystywanymi przez Ministra i Pełnomocnika były w szczególności:

- raporty roczne z działalności Cert Polska „Krajobraz bezpieczeństwa polskiego internetu", a od stycznia 2021 r. „Raporty miesięczne CSIRT NASK dla Pełnomocnika Rządu ds. Cyberbezpieczeństwa";
- raporty i opracowania sporządzane cyklicznie lub w związku z konkretnymi wydarzeniami[18] przez CSIRT GOV[19], m.in. w oparciu o dane z systemu wczesnego ostrzegania ARAKIS.GOV;
- raporty cząstkowe przekazane Pełnomocnikowi Rządu przez ministrów kierujących działami administracji rządowej, kierowników urzędów centralnych oraz wojewodów, w związku z obowiązkiem przygotowania „Raportu o zagrożeniach bezpieczeństwa narodowego w części dotyczącej zagrożeń cyberbezpieczeństwa mogących doprowadzić do sytuacji kryzysowej"[20].

Gwałtowny wzrost, w latach 2019–2021, liczby incydentów komputerowych, w tym *phishingu* i kradzieży tożsamości

Opisane powyżej, prowadzone przez poszczególne badane podmioty analizy wykazywały, że w latach 2019–2021 wystąpił gwałtowny wzrost liczby incydentów komputerowych, w tym w szczególności oszustw i kampanii *phishingowych* wymierzonych w indywidualnych użytkowników Internetu.

W poszczególnych latach ww. okresu liczba cyberprzestępstw zgłoszonych do jednostek organizacyjnych Policji wyniosła odpowiednio:

- w 2019 r . – 67 822, w tym 48 127 zgłoszeń dotyczących oszustw internetowych;
- w 2020 r. – 68 633, w tym 49 435 zgłoszeń dotyczących oszustw internetowych;

[16] W kontrolowanym okresie CSIRT NASK przeprowadził również badanie 2806 stron internetowych jednostek samorządu terytorialnego, które pozwoliło zidentyfikować i wyeliminować 23 poważne błędy bezpieczeństwa. Raport z tego badania został przekazany Pełnomocnikowi Rządu, a także pozostałym zespołom CSIRT poziomu krajowego. Analogiczne badanie 22 396 witryn internetowych placówek oświatowych, pozwoliło na zidentyfikowanie kilku tysięcy stron zawierających przynajmniej jedną istotną podatność. Informacje o ustalonych zagrożeniach przekazywano administratorom tych witryn.

[17] Na podstawie rozporządzenia Rady Ministrów z dnia 7 października 2020 r. (Dz. U. poz. 1730) w sprawie zniesienia Ministerstwa Cyfryzacji, z dniem 6 października 2020 r. zniesione zostało Ministerstwo Cyfryzacji, a pracownicy tego Ministerstwa obsługujący sprawy działu informatyzacja zostali włączeni do KPRM. Rozporządzenie weszło w życie z mocą wsteczną od dnia 6 października 2020 r.

[18] Np. raport z 16 grudnia 2019 r. dotyczący analizy zdarzeń w cyberprzestrzeni w okresie wyborów do Sejmu i Senatu RP w 2019 r.

[19] Prowadzony przez Agencję Bezpieczeństwa Wewnętrznego.

[20] Obowiązek przygotowania raportu wynikał z art. 5a ust. 2 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (Dz. U. z 2022 r. poz. 261, ze zm.). Aktualny „Raport o zagrożeniach bezpieczeństwa narodowego" z 2020 r. został przyjęty uchwałą Rady Ministrów z dnia 11 marca 2021 r.

- w 2021 r. (do października) – 59 273, w tym 37 786 zgłoszeń dotyczących oszustw internetowych.

Liczba stwierdzonych przestępstw[21] wyniosła:

- w 2019 r. – 52 634, w tym 37 327 oszustw internetowych;
- w 2020 r. – 55 038, w tym 38 808 oszustw internetowych;
- w 2021 r. (do października) – 64 139, w tym 47 408 oszustw internetowych[22].

W trakcie pandemii COVID-19 Policja odnotowała wzrost wykorzystania domen internetowych służących m.in. do rejestracji fałszywych sklepów internetowych, dystrybucji złośliwego oprogramowania, czy też kradzieży danych osobowych. W przeprowadzonej w 2020 r. diagnozie wskazano także, że *phishing*, oszustwa przy wykorzystaniu portali aukcyjnych oraz sklepów internetowych, a także ataki typu *ransomware* wyznaczają główne obszary ryzyk związanych z dalszym rozwojem cyberprzestępczości.

W raporcie rocznym Cert Polska[23] wskazano, że w 2019 r. zespół ten zarejestrował 6484 incydenty (wzrost o 73% w porównaniu z rokiem wcześniejszym), spośród których najczęściej występującym typem ataków był *phishing*, który stanowił około 54,2% wszystkich incydentów.

W 2020 r.[24] odnotowano 10 420 incydentów cyberbezpieczeństwa, z czego najpopularniejszym typem incydentu był ponownie *phishing*. Ataki tego rodzaju stanowiły aż 73% wszystkich incydentów obsłużonych w 2020 r. przez Zespół Cert Polska, a ich liczba wzrosła o 116% w ujęciu rok do roku. Najpopularniejsze scenariusze ataków phishingowych miały na celu zdobycie danych logowania do konta Facebook, numeru karty płatniczej lub danych logowania do bankowości internetowej. Oszuści komputerowi wykorzystywali w celu wyłudzenia tych danych m.in. wpisy na Facebooku z sensacyjnie wyglądającymi nagłówkami, fałszywe wiadomości SMS oraz wiadomości na komunikatorze WhatsApp. W tym samym okresie CSIRT NASK, obsłużył 32 incydenty, które zaklasyfikowano jako poważne, czyli takie, których wystąpienie powoduje lub może spowodować istotne obniżenie jakości lub przerwanie ciągłości świadczenia usługi kluczowej[25].

---

21 Tj. zgłoszonych przestępstw, zakwalifikowanych przez Policję jako przestępstwa w rozumieniu Kodeksu Karnego.

22 Podane liczby zaprezentowano na podstawie danych wprowadzonych do Krajowego Systemu Informacyjnego Policji (KSIP). Większa liczba przestępstw stwierdzonych w danym okresie od liczby przestępstw zgłoszonych może wynikać z faktu, że nie wszystkie przestępstwa stwierdzone mają związek ze zgłoszeniem. Zarejestrowanie informacji o części z nich w KSIP jest związane z realizacją zadań Policji w zakresie wykrywania przestępstw i wykroczeń oraz ścigania ich sprawców, a więc jest niezależne od zgłoszenia jakiegoś zdarzenia przez osobę fizyczną lub uprawniony do tego podmiot jako przestępstwa. Ponadto w niektórych sytuacjach pojedyncze zgłoszenie może doprowadzić do stwierdzenia zaistnienia wielu przestępstw. W zaprezentowanych danych statystycznych mogą także występować sprawy wprowadzone przed kontrolowanym okresem, a zakończone w okresie objętym kontrolą NIK (np. gdy przestępstwa zaistniały w 2018 r. ale sprawy te zostały zakończone w 2021 r.).

23 https://cert.pl/uploads/docs/Raport_CP_2019.pdf

24 https://cert.pl/uploads/docs/Raport_CP_2020.pdf

25 Definicja legalna „usługi kluczowej" została zawarta w ustawie o krajowym systemie cyberbezpieczeństwa. Terminem tym określa się usługę, która ma kluczowe znaczenie dla utrzymania krytycznej działalności społecznej lub gospodarczej, wymienioną w wykazie usług kluczowych.

W poszczególnych miesiącach 2021 r. Zespół CSIRT NASK informował Pełnomocnika Rządu o następującej liczbie i charakterystyce incydentów cyberbezpieczeństwa:

- w styczniu 2021 r. zarejestrowano 1154 incydenty[26], w tym jeden poważny. Spośród wszystkich obsłużonych incydentów 86% stanowiły oszustwa komputerowe, w tym *phishing*;
- w lutym 2021 r. zarejestrowano 1324 incydenty, w tym dwa poważne. Spośród wszystkich obsłużonych incydentów 86% stanowiły oszustwa komputerowe, w tym *phishing*;
- w marcu 2021 r. zarejestrowano 1694 incydenty, w tym dwa poważne. Spośród wszystkich obsłużonych incydentów 86% stanowiły oszustwa komputerowe, w tym *phishing*;
- w kwietniu 2021 r. zarejestrowano 2749 incydentów, w tym jeden poważny. Spośród wszystkich obsłużonych incydentów 73% stanowiły oszustwa komputerowe, w tym *phishing*;
- w maju 2021 r. zarejestrowano 1833 incydenty, w tym trzy poważne. Spośród wszystkich obsłużonych incydentów 88% stanowiły oszustwa komputerowe, w tym *phishing*;
- w czerwcu 2021 r. zarejestrowano 2112 incydentów, w tym trzy poważne. Spośród wszystkich obsłużonych incydentów 93% stanowiły oszustwa komputerowe, w tym *phishing*;
- w lipcu 2021 r. zarejestrowano 2139 incydentów, w tym jeden poważny. Spośród wszystkich obsłużonych incydentów 94% stanowiły oszustwa komputerowe, w tym *phishing*;
- w sierpniu 2021 r. zarejestrowano 3512 incydentów, w tym jeden poważny. Spośród wszystkich obsłużonych incydentów 86% stanowiły oszustwa komputerowe, w tym *phishing*;
- we wrześniu 2021 r. zarejestrowano 3765 incydentów, w tym 11 poważnych. Spośród wszystkich obsłużonych incydentów 96% stanowiły oszustwa komputerowe, w tym *phishing*;
- w październiku 2021 r. zarejestrowano 2493 incydenty, w tym pięć poważnych. Spośród wszystkich obsłużonych incydentów 95% stanowiły oszustwa komputerowe, w tym *phishing*;
- w listopadzie 2021 r. zarejestrowano 2543 incydenty, w tym trzy poważne. Spośród wszystkich obsłużonych incydentów 86% stanowiły oszustwa komputerowe, w tym *phishing*;
- w grudniu 2021 r. zarejestrowano aż 4186 incydentów, w tym jeden poważny. Spośród wszystkich obsłużonych incydentów 75% stanowiły oszustwa komputerowe, w tym *phishing*.

Metody działania przestępców komputerowych

Prowadzona przez CSIRT NASK i przekazywana Pełnomocnikowi analiza zgłoszeń i incydentów pozwoliła na zidentyfikowanie występujących w 2021 r. trendów oraz dominujących zagrożeń

[26] W miesięcznych raportach CSIRT NASK oddzielną grupę wykazywanych incydentów cyberbezpieczeństwa stanowiły zdarzenia związane z publikacją potencjalnie nielegalnych treści w Internecie, w szczególności materiały przedstawiające seksualne wykorzystywanie dzieci lub inne szkodliwe treści skierowane przeciwko bezpieczeństwu małoletnich, które były obsługiwane przez odrębny zespół NASK-PIB, tj. Dyżurnet.pl. W poszczególnych miesiącach zarejestrowano od 95 (luty 2021 r.) do 321 (listopad 2021 r.) przypadków publikowania treści przedstawiających seksualne wykorzystywanie dzieci.

(kampanii) ukierunkowanych na wyrządzanie szkód użytkownikom Internetu:

- **powtarzających się kampanii podszywających się pod serwis ogłoszeniowy OLX.** Główny schemat działania sprawców polegał w tym przypadku na kontaktowaniu się (przez komunikator WhatsApp lub mailowo) z osobami, które zamieszczały ogłoszenia na portalu OLX. Fałszywi kupujący udawali zainteresowanie zakupem, a następnie przekonywali, że opłacili już produkt i w celu odebrania środków, konieczne jest wejście pod wskazany link. W rzeczywistości link kierował do fałszywej strony, wyłudzającej dane kart płatniczych lub dane do bankowości elektronicznej. Skutkiem tych działań mogła być utrata znacznych środków finansowych;
- **incydenty dotyczące kradzieży danych uwierzytelniających do kont w serwisie Facebook.** Scenariusz działania sprawców polegał na tworzeniu stron internetowych, na których publikowane były artykuły, których treść miała przykuć uwagę użytkowników Internetu i zachęcić ich do zapoznania się z materiałem. Aby uzyskać do niego dostęp, ofiary proszone były o potwierdzenie wieku poprzez zalogowanie się do portalu Facebook i następnie były przenoszone na fałszywy panel logowania. Po podaniu danych przestępcy przejmowali konto użytkownika serwisu, które wykorzystywali do dalszego rozsyłania fałszywych wiadomości, a także do wyłudzania środków finansowych metodą „na BLIKa";
- **kampanie *phishingowe* podszywające się pod firmy kurierskie oraz dostawców energii elektrycznej.** Wspólnym mianownikiem kampanii było wysyłanie masowych ilości wiadomości SMS informujących o nierozliczonych płatnościach, trudnościach z dostarczeniem przesyłki, lub nakłaniających do śledzenia statusu przesyłki. Potencjalne ofiary były nakłanianie do podawania danych kart płatniczych, lub do instalacji złośliwego oprogramowania, które m.in. wykradało dane logowania do serwisów bankowych;
- **kampanie SMS, których tłem była pandemia COVID-19.** Potencjalne ofiary były informowane o wygraniu nagrody w ramach Loterii Narodowego Programu Szczepień, do której potwierdzenia niezbędne było wejście w otrzymany link i podanie danych do karty płatniczej lub bankowości elektronicznej. Drugim schematem działania były fałszywe powiadomienia o skierowaniu na kwarantannę. Treść komunikatów nakłaniała m.in. do aktualizacji aplikacji Adobe Flash Player, a w praktyce prowadziła do instalacji złośliwego oprogramowania wykradającego wrażliwe informacje z telefonów ofiar, w tym dane uwierzytelniające do bankowości mobilnej.

Zarządzanie ryzykami przez NASK-PIB oraz Policję

Kontrola wykazała, że Kierownictwo Policji oraz NASK-PIB podejmowało aktywne oraz wynikające z ustawowego usytuowania tych podmiotów w ramach krajowego systemu cyberbezpieczeństwa działania, mające na celu zarządzanie zidentyfikowanymi ryzykami, w tym w obszarze zapobiegania i minimalizowania skutków przestępstw internetowych.

Stosowane przez CSIRT NASK metody postępowania z identyfikowanymi ryzykami (poza bieżącą obsługą incydentów[27]) obejmowały w szczególności następujące działania techniczne i informacyjne:

- **obserwowanie podejrzanych nazw domenowych i wpisywanie domen internetowych na prowadzoną od marca 2020 r. listę ostrzeżeń przed niebezpiecznymi stronami.** Na listę wpisywane były domeny, które w całości służyły do wyłudzania danych osobowych oraz danych logowania do popularnych serwisów. Podejrzane domeny były zgłaszane przez zewnętrzne podmioty, jak i wyszukiwane przez wewnętrzne systemy NASK-PIB[28]. W pierwszym kwartale 2021 r. do listy ostrzeżeń dodanych zostało 4240 domen, w drugim kwartale 7687, a w trzecim 11 783. Liczba domen wpisywanych z poszczególnych kampanii pozwalała szacować skalę zagrożeń i podejmować odpowiednie działania minimalizujące (m.in. wyłudzanie danych osobowych) oraz zapobiegające (na przykład poprzez publikacje ostrzeżeń w mediach społecznościowych CERT Polska);
- **dystrybuowanie informacji poprzez platformę n6.** Prowadzona przez CERT Polska platforma n6 służyła do gromadzenia, przetwarzania i przekazywania informacji o zdarzeniach bezpieczeństwa w sieciach informatycznych. Dostępne zbiory danych zawierały m.in. informacje o złośliwych stronach WWW, komputerach zainfekowanych złośliwym oprogramowaniem, serwerach zarządzających botnetami oraz podatnych usługach. W ramach minimalizowania ryzyka były one udostępniane bezpłatnie administratorom poszczególnych sieci;
- **udostępnianie wyników analizy szkodliwego oprogramowania poprzez system MWDB.** System MWDB stanowił platformę służącą do przechowywania i katalogowania próbek złośliwego oprogramowania oraz informacji pozyskanych w toku ich analizy[29], w szczególności informacji o wersjach złośliwego oprogramowania i adresach serwerów nim sterującym. Dostęp do platformy był darmowy dla polskich instytucji oraz analityków bezpieczeństwa z całego świata;
- **publikowanie Raportów Rocznych CERT Polska** zawierających informacje na temat klasyfikacji obsłużonych przez ten zespół incydentów wraz z analizami dotyczącymi ich przyczyn, skutków i sposobów zapobiegania. Dodatkowo od stycznia 2021 r. na potrzeby Pełnomocnika Rządu opracowywane były raporty miesięczne na temat rodzaju obsłużonych incydentów i trendów w cyberbezpieczeństwie;
- **udostępnianie przez CSIRT NASK informacji na temat działań cyberprzestępców** wymierzonych w klientów krajowych i zagranicznych instytucji finansowych. Dane takie, pozyskiwane w wyniku automatycznej i półautomatycznej analizy szkodliwego oprogramowa-

[27] W toku kontroli nie badano sposobu obsługi poszczególnych incydentów zgłaszanych do CSIRT NASK, ani spraw prowadzonych przez Policję.

[28] Każda domena przed wpisaniem na listę była oceniana przez minimum dwóch analityków, co minimalizowało ryzyko jej omyłkowego zakwalifikowania do grupy ostrzeżeń.

[29] Automatycznej, poprzez systemy dostępne w CERT Polska oraz ręcznej, wykonywanej przez analityków.

nia, były dystrybuowane poprzez dedykowany system injects.cert.pl do podmiotów, dla których zidentyfikowano zagrożenia, bądź właściwych zespołów CSIRT;
- dystrybuowanie przez CSIRT NASK, od 27 października 2020 r., powiadomień dotyczących kont użytkowników współpracujących organizacji, które pojawiły się w monitorowanych serwisach publikujących informacje pochodzące z wycieków danych logowania;
- **liczne działania edukacyjne skierowane do obywateli** służące upowszechnianiu wiedzy na temat przestępstw internetowych oraz rekomendowanych środków ochrony[30].

W odpowiedzi na wzrost zagrożeń związanych z cyberprzestępczością oraz identyfikowane w tym obszarze bariery w działalności Policji (w szczególności powszechne wykorzystywanie przez przestępców przedpłaconych kart SIM, zarejestrowanych na nieprawdziwe dane) przedstawiciele tej formacji, w związku z procedowaniem projektu ustawy Prawo komunikacji elektronicznej[31], przedstawili propozycje przepisów umożliwiających walkę z przypadkami rejestrowania abonentów na fałszywe lub nieistniejące dane. Ponadto, funkcjonariusze BdWzC KGP uczestniczyli w pracach zespołu zainicjowanego przez Związek Banków Polskich oraz w cyklu spotkań mających na celu wypracowanie zmian w ustawie z dnia 16 lipca 2004 r. Prawo telekomunikacyjne[32] pod kątem zwalczania *phishingu* i *spoofingu*[33].

Zadania związane z usprawnieniem zwalczania cyberprzestępczości zostały uwzględnione w dokumentach strategicznych Policji – „Priorytetach Komendanta Głównego Policji" na lata 2016–2020 oraz 2021–2023, a zasadniczym wynikiem prowadzonych analiz było opracowanie opisanej w pkt 5.2. informacji, koncepcji utworzenia CBZC.

Brak reakcji na zagrożenia identyfikowane w cyberprzestrzeni ze strony Ministra Cyfryzacji i Pełnomocnika Rządu

NIK oceniła negatywnie brak reakcji na identyfikowane ryzyka oraz trendy w cyberzagrożeniach, w odniesieniu do indywidulanych użytkowników sieci, ze strony Ministra Cyfryzacji i Pełnomocnika Rządu – dwóch kluczowych podmiotów krajowego systemu cyberbezpieczeństwa odpowiadających za bezpieczeństwo cyberprzestrzeni oraz koordynację polityki rządu w tym obszarze.

W badanym okresie Minister Cyfryzacji oraz Pełnomocnik Rządu prowadzili działania związane z budową i wzmocnieniem efektywności krajowego systemu cyberbezpieczeństwa, które koncentrowały się w szczególności na:

- identyfikowaniu i monitorowaniu procesu wyznaczania operatorów usług kluczowych oraz dostawców usług cyfrowych;

[30] Opisane szczegółowo w pkt 5.4. informacji.

[31] Wdrażającej do polskiego porządku prawnego przepisy Dyrektywy Parlamentu Europejskiego i Rady (UE) 2018/1972 z dnia 11 grudnia 2018 r. ustanawiającej Europejski kodeks łączności elektronicznej (Dz. Urz. UE L 321 z 17.12.2018, str. 36, ze zm.).

[32] Dz. U. z 2022 r. poz. 1648 ze zm.

[33] Spotkania te odbyły się 14 stycznia 2022 r., 25 stycznia 2022 r., 26 stycznia 2022 r., 1 lutego 2022 r., 3 lutego 2022 r., 18 lutego 2022 r. oraz 25 lutego 2022 r. Brali w nich udział przedstawiciele Urzędu Komunikacji Elektronicznej oraz najważniejszych operatorów telekomunikacyjnych, na których spoczywa obowiązek weryfikacji danych rejestracyjnych kart SIM.

- wspieraniu tworzenia sektorowych zespołów cyberbezpieczeństwa oraz Centrów Wymiany i Analizy Informacji;
- budowie systemu teleinformatycznego S46;
- przeprowadzaniu międzysektorowych ćwiczeń cyberbezpieczeństwa;
- prowadzeniu szkoleń z zakresu cyberbezpieczeństwa dla pracowników podmiotów publicznych, w tym w szczególności samorządu terytorialnego;
- wydawaniu rekomendacji cyberbezpieczeństwa.

W badanym okresie, w KPRM, przygotowano również założenia do nowelizacji ustawy o KSC[34]. W projekcie ustawy zaproponowano m.in. rozbudowę struktury krajowego systemu cyberbezpieczeństwa poprzez: wprowadzenie obowiązku funkcjonowania zespołów sektorowych CSIRT obsługujących operatorów usług kluczowych; określenie nowych zasad działalności oraz zadań dla zespołów pełniących funkcje operacyjnych centrów bezpieczeństwa (SOC) działających na rzecz operatorów usług kluczowych; utworzenie centrów wymiany i analizy informacji na temat podatności, cyberzagrożeń i incydentów (ISAC); utworzenie zespołu CSIRT INT obsługującego Agencję Wywiadu oraz polskie placówki dyplomatyczne. Przewidziano wzmocnienie pozycji Pełnomocnika polegające m.in. na nadaniu mu uprawnienia do zlecania CSIRT NASK zapewnienia wsparcia operatorom infrastruktury krytycznej w obsłudze incydentów oraz do wydawania rekomendacji mających na celu wzmocnienie poziomu bezpieczeństwa systemów informacyjnych podmiotów krajowego systemu cyberbezpieczeństwa. Zaproponowano także ustanowienie nowych mechanizmów przeciwdziałania incydentom krytycznym poprzez umożliwienie Pełnomocnikowi wydawania ostrzeżeń o takich zdarzeniach oraz zalecania określonych zachowań, które mają zmniejszać ryzyko ich wystąpienia. W projekcie ustawy określono również organizację krajowego systemu certyfikacji cyberbezpieczeństwa, co wynikało z obowiązku wdrożenia do polskiego porządku prawnego przepisów UE[35].

Wspólnym mianownikiem wymienionych powyżej działań było wspieranie instytucjonalnych interesariuszy krajowego systemu cyberbezpieczeństwa, a także wzmacnianie ochrony systemów uznawanych za kluczowe dla funkcjonowania państwa.

NIK nie neguje zasadności tego rodzaju aktywności wskazując jednak, że w działaniach Ministra Cyfryzacji i Pełnomocnika Rządu w praktyce pominięto (poza działalnością edukacyjną[36]) zagadnienia dotyczące ochrony indywidualnych użytkowników sieci. Powyższe miało miejsce, pomimo że organy te dysponowały danymi dowo-

[34] Projekt ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw (nr UD68) znajduje się obecnie na etapie prac w Stałym Komitecie Radzie Ministrów.

[35] Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2019/881 z dnia 17 kwietnia 2019 r. w sprawie ENISA (Agencji Unii Europejskiej ds. Cyberbezpieczeństwa) oraz certyfikacji cyberbezpieczeństwa w zakresie technologii informacyjno-komunikacyjnych oraz uchylenia rozporządzenia (UE) nr 526/2013 (akt o cyberbezpieczeństwie) – Dz. Urz. UE. L 151 z 7.06.2019 r. str. 15.

[36] Efekty tej działalności były jednak niewystarczające, co opisano szczegółowo w pkt 5.4. informacji.

dzącymi w sposób jednoznaczny, że w badanym okresie dominującą i gwałtownie zwiększającą się kategorią incydentów były oszustwa komputerowe i *phishing*, wymierzone w osoby fizyczne korzystające z sieci (na co wskazywano również w oficjalnych dokumentach Rady Ministrów[37]). Oznaczało to, że Minister i Pełnomocnik koncentrowali się na wspieraniu podmiotów i organizacji posiadających wyspecjalizowane służby informatyczne, a pomijali zwykłych obywateli, którzy w obliczu działań przestępców internetowych, są co do zasady pozostawieni sami sobie.

Nierzetelne przygotowanie i koordynacja strategicznych dokumentów Rady Ministrów określających zadania w ramach cyberbezpieczeństwa RP

Zastrzeżenia NIK dotyczyły nierzetelnego przygotowania oraz braku należytej koordynacji przez Ministra Cyfryzacji i Pełnomocnika strategicznych dokumentów Rady Ministrów, wyznaczających cele i priorytety państwa w obszarze cyberbezpieczeństwa, tj. „Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019–2024[38] oraz „Planu działań na rzecz wdrożenia Strategii Cyberbezpieczeństwa".

W opracowanym w KPRM „Planie działań", stanowiącym dokument wykonawczy do „Strategii", **całkowicie pominięto wymienione poniżej działania przewidziane przez Radę Ministrów w „Strategii", mające służyć lepszemu zapobieganiu i zwalczaniu przestępczości internetowej:**

- prawidłowe zabezpieczanie dowodów cyfrowych;
- zwiększenie efektywności czynności procesowych i operacyjnych poprzez podjęcie i poszerzenie współdziałania organów ścigania z innymi podmiotami, które mogą posiadać wiedzę w zakresie ustalenia istoty przestępstwa lub mogą przyczynić się do ustalenia jego sprawcy;
- transgraniczna współpraca organów ścigania i podmiotów typu CERT/CSIRT oraz stworzenie sprawnych i zaufanych kanałów wymiany informacji między organami ścigania różnych państw;
- wprowadzenie przepisów umożliwiających przetwarzanie dokumentów procesowych w postaci elektronicznej i przesyłanie ich w takiej postaci;
- rozwijanie badań naukowych w obszarze zwalczania cyberprzestępczości, których wyniki zapewnią wsparcie dla organów ścigania;
- wskazanie sposobów postępowania dla osób dotkniętych przestępstwem;
- opracowanie programów badawczych mających na celu wypracowanie metod wykrywania i analizy nowych typów cyberprzestępstw, cyberterroryzmu i cyberszpiegostwa;
- wzmocnienie systemu szkoleń dla wszystkich pracowników podmiotów istotnych dla cyberbezpieczeństwa oraz dla przedstawicieli

[37] W opracowanym przez Pełnomocnika Rządu „Raporcie o zagrożeniach bezpieczeństwa narodowego w części dotyczącej zagrożeń cyberbezpieczeństwa mogących doprowadzić do sytuacji kryzysowej" wskazano, że w związku z brakiem jasnych kryteriów przygotowywania raportów cząstkowych, jak również nieokreśleniem jednolitego systemu definicyjnego nie udało się zagregować otrzymanych danych i w konsekwencji wypracować spójnych wniosków w obszarze zagrożeń cyberbezpieczeństwa. Podkreślono jednak wyraźną tendencję wzrostową w zakresie liczby zgłaszanych incydentów oraz fakt, że „Najbardziej wyróżniającą się (pod względem liczby) kategorią na tle pozostałych ataków był phishing."

[38] Strategia Cyberbezpieczeństwa została przyjęta uchwałą nr 125 Rady Ministrów z dnia 22 października 2019 r. (M.P. poz. 1037).

organów ścigania i wymiaru sprawiedliwości, przez wdrożenie dedykowanego programu edukacyjnego zawierającego zarówno szkolenia teoretyczne, jak i praktyczne na realnych przykładach zagrożeń;
- włączenie się rządu w działania na rzecz skutecznego zwalczania cyberprzestępczości w wymiarze międzynarodowym.

Odnośnie pojedynczych, ujętych w „Planie działań" zadań dotyczących zwalczania cyberprzestępczości stwierdzono natomiast, że zostały one przygotowane w sposób wadliwy merytorycznie, ponieważ były pozbawione konkretnych mierników realizacji[39]**.** Przykładowe zaplanowane efekty tych zadań obejmowały „stałe podnoszenie kompetencji, wiedzy oraz umiejętności kadr Policji, prokuratury oraz sędziów zajmujących się wykrywaniem, ściganiem oraz karaniem sprawców cyberprzestępstw"[40] oraz „prowadzenie kampanii społecznych o charakterze profilaktycznym w kontekście cyberzagrożeń"[41]. Pomimo, że „Plan działań" miał mieć charakter dokumentu projektowego (ukierunkowanego na konkretne produkty) w opisach tych zadań nie wskazano jednak ile osób planowano przeszkolić, ani jaka liczba kampanii profilaktycznych (bądź też inna wartość) będzie oznaczać zrealizowanie efektów danego działania.

Opisane powyżej ustalenia korespondują z wynikami wcześniejszych kontroli NIK, które wykazywały rażąco niską jakość merytoryczną kolejnych, przyjmowanych przez Radę Ministrów dokumentów mających w założeniu określać szczegółowe ramy organizacyjne aktywności państwa w zakresie podnoszenia poziomu cyberbezpieczeństwa („Polityka Ochrony Cyberprzestrzeni RP", „Krajowe Ramy Polityki Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017-2022")[42]. Opracowania te były pozbawione podstawowych cech dokumentu strategicznego, tj. w szczególności mierzalnych rezultatów działań oraz źródeł ich finansowania, co uniemożliwiało podmiotom odpowiadającym za ich wdrażanie sprawowanie realnej koordynacji działań organów państwa w obszarze cyberbezpieczeństwa. **Powyższe znalazło potwierdzenie w wynikach bieżącej kontroli, które wykazały, że tzw. koordynacja**

---

[39] Zadania nr: 1.6.1, 1.6.2, 1.6.3 oraz działanie nr 4.3.1.1 „Planu działań"

[40] Zadanie 1.6.2 „Planu działań"– „program systemowego podnoszenia wiedzy oraz kompetencji organów ścigania w zakresie ścigania cyberprzestępców (CyberCrimePOL)", przewidziane do realizacji przez KPRM we współpracy z innymi podmiotami, w okresie I kwartał 2022 r. – IV kwartał 2024 r.

[41] Zadanie 1.6.3 – „uruchomienie kampanii społecznych dedykowanych profilaktyce przeciwdziałań i reagowaniu na cyberprzestępstwa", przewidziane do realizacji przez KPRM we współpracy z innymi podmiotami w okresie I kwartał 2022 r. - IV kwartał 2024 r. oraz działanie 4.3.1.1 – prowadzenia kampanii informacyjnych skierowanych do różnych grup interesariuszy (jako podmiot wiodący dla działania, które miało być realizowane w całym okresie wdrażania Strategii, został wyznaczony KPRM).

[42] Zob. m.in. wyniki kontroli nr P/14/043 „Realizacja przez podmioty państwowe zadań w zakresie ochrony cyberprzestrzeni RP", w toku której badano m.in. proces opracowania oraz realizacji „Polityki Ochrony Cyberprzestrzeni RP", przyjętej przez Radę Ministrów w dniu 25 czerwca 2013 r. NIK oceniła, że „Polityka" była wynikiem braku porozumienia i źle rozumianego kompromisu między różnymi podmiotami publicznymi. W rezultacie, Rada Ministrów przyjęła w tym obszarze bardzo nieprecyzyjny dokument, obarczony wieloma błędami merytorycznymi oraz pozbawiony podstawowych cech strategicznego dokumentu rządowego. W związku z powyższym nie istniała możliwość wykorzystania „Polityki" w celu rzeczywistej poprawy bezpieczeństwa teleinformatycznego państwa. https://www.nik.gov.pl/kontrole/wyniki-kontroli-nik/pobierz,kpb~p_14_043_20140617104838140300211 8~01,typ,k.pdf.

„Strategii" przez Ministra Cyfryzacji ograniczała się do przedkładania Radzie Ministrów rocznych sprawozdań z realizacji tego dokumentu, które stanowiły agregację nieporównywalnych danych przekazywanych przez podmioty krajowego systemu cyberbezpieczeństwa na temat ich bieżącej działalności.

Negowanie przez Ministra Cyfryzacji oraz Pełnomocnika Rządu obowiązków w zakresie ochrony obywateli przed przestępczością internetową

NIK szczególnie negatywnie oceniła podjętą przez Ministra Cyfryzacji oraz Pełnomocnika Rządu próbę zanegowania przypisanych tym organom obowiązków w zakresie ochrony indywidualnych użytkowników Internetu przed przestępczością internetową. W toku kontroli (a następnie w zastrzeżeniach złożonych do wystąpienia pokontrolnego) prezentowali oni stanowisko, że zadania w tym zakresie nie zostały literalnie wymienione wśród zadań Ministra (Pełnomocnika) wskazanych w ustawie o KSC, a ponadto osoby fizyczne – indywidulani użytkownicy Internetu nie są w praktyce objęte krajowym systemem cyberbezpieczeństwa.

NIK stanowczo odrzuciła powyższą argumentację wskazując, że pozostaje ona w rażącej sprzeczności z art. 12a ust. 1 pkt 8, 10 i 13a ustawy z dnia 4 września 1997 r. o działach administracji rządowej[43], który konstytuuje odpowiedzialność ministra właściwego do spraw informatyzacji w sprawach kształtowania polityki państwa w zakresie ochrony danych osobowych, bezpieczeństwa cyberprzestrzeni w wymiarze cywilnym oraz identyfikacji elektronicznej. Nie uwzględnia ona również treści art. 60 i 62 ustawy o KSC, na mocy których Pełnomocnikowi powierzono koordynowanie działań i realizowanie polityki rządu w zakresie zapewnienia cyberbezpieczeństwa RP, a w tym: dokonywanie analizy i oceny funkcjonowania KSC, nadzór nad procesem zarządzania ryzykiem KSC, upowszechnianie nowych rozwiązań i inicjowanie działań w zakresie zapewnienia cyberbezpieczeństwa na poziomie krajowym. Stanowisko Ministra Cyfryzacji oraz Pełnomocnika Rządu pozostaje również w sprzeczności z celami dyrektywy NIS i ustawy o KSC, które to regulacje określając standardy świadczenia usług kluczowych i usług cyfrowych mają przede wszystkim za zadanie ochronę końcowych beneficjentów tych usług[44].

W ocenie NIK, w świetle przytoczonych przepisów, nie ulega zatem wątpliwości, że obywatele mają praw oczekiwać aktywnych działań Ministra Cyfryzacji i Pełnomocnika Rządu[45] w celu zapewnienia im szeroko pojętej ochrony przed oszustami komputerowymi. Działania takie powinny bazować na wynikach analizy ryzyka oraz

[43] Dz. U. z 2021 r. poz. 1893, ze zm.

[44] Szczegółową argumentację przedstawiono w uchwale Kolegium NIK nr 48/2022, z dnia 28 września 2022 r., na podstawie której oddalono zastrzeżenia Pełnomocnika Rządu w tym zakresie.

[45] Powyższe nie oznacza, że obowiązujące w tym zakresie regulacje prawne można uznać za kompletne i precyzyjne. W wystąpieniach pokontrolnych skierowanych do Ministra Cyfryzacji oraz Pełnomocnika Rządu, NIK sformułowała uwagę o charakterze systemowym, w której wskazała, że obowiązujące regulacje prawne określające kształt krajowego systemu cyberbezpieczeństwa, w znacznej mierze pomijają tematykę bezpieczeństwa indywidualnych użytkowników Internetu. W przepisach tych brak jest w szczególności odniesienia do zasad udzielania wsparcia osobom fizycznym, które stały się celem ataku. NIK zwróciła zatem uwagę na zasadność uwzględnienia ww. zagadnień w przepisach ustawy o KSC, w celu wypracowania kompleksowych (obejmujących wszystkich kluczowych użytkowników) ram organizacyjnych krajowego systemu cyberbezpieczeństwa.

aktualnych zagrożeń, a także zostać rzetelnie zaplanowane w postaci konkretnych zadań z przypisanymi do nich odpowiedzialnymi wykonawcami i miernikami realizacji.

5.2. Przygotowanie kadrowe, logistycznie oraz organizacyjne do zapobiegania i zwalczania skutków przestępstw internetowych

Brak adekwatnych zasobów do zwalczania przestępczości internetowej, w tym kradzieży tożsamości

Przeprowadzona kontrola, w przypadku dwóch z trzech zbadanych podmiotów[46] (jednostki organizacyjne Policji oraz urząd obsługujący Ministra Cyfryzacji i Pełnomocnika Rządu) wykazała braki zasobów (kadrowych, finansowych i sprzętowych), które w zasadniczy sposób wpływały na jakość realizowanych zadań związanych ze zwalczaniem i ograniczaniem skutków przestępczości internetowej.

W okresie objętym kontrolą policyjny pion do walki z cyberprzestępczością składał się z Biura do Walki z Cyberprzestępczością KGP (dalej: BdWzC KGP) oraz wydziałów do walki z cyberprzestępczością w komendach wojewódzkich (Stołecznej) Policji (dalej: KWP/KSP). W ramach realizacji obowiązków nałożonych przez Komendanta Głównego Policji: Biuro współdziałało z KWP/KSP w zakresie czynności operacyjno-rozpoznawczych, prowadziło takie czynności samodzielnie, współpracowało z podmiotami zewnętrznymi (w tym zagranicznymi) oraz utrzymywało całodobową służbę, której podstawowym zadaniem było identyfikowanie przestępstw internetowych, ocena związanego z nimi zagrożenia i podejmowanie adekwatnych czynności.

Ograniczenia policyjnego pionu do walki z cyberprzestępczością

Opisana powyżej struktura organizacyjna okazała się być dalece nieadekwatna wobec wzrastającej liczby przestępstw komputerowych, a jej ograniczona efektywność wynikała z trzech podstawowych czynników:

- **zbyt niskiej liczby funkcjonariuszy wyspecjalizowanych w zwalczaniu przestępczości komputerowej** – łączna liczba etatów przypisanych w badanym okresie do pionu do walki z cyberprzestępczością nie przekroczyła 370 (w tym 336 etatów policyjnych), a wg stanu na 17 grudnia 2021 r. faktycznie zatrudnionych było 305 funkcjonariuszy (338 osób, uwzględniając pracowników cywilnych). Oznacza to, że etaty przypisane funkcjonariuszom wyspecjalizowanym w ściganiu cyberprzestępców stanowiły tylko 0,33% wszystkich etatów w Policji (103 309);
- **niewystarczającego dofinansowania pionu do walki z cyberprzestępczością** – w związku z ograniczeniami finansowanymi brak było możliwości realizacji potrzebnych zakupów i inwestycji oraz rezygnowano z niektórych zadań. Przykładowo BdWzC KGP nie posiadało odpowiednich

[46] W NASK-PIB zadania związane z zapobieganiem i zwalczaniem skutków przestępstw internetowych były realizowane przede wszystkim przez CSIRT NASK. Realizacja zadań CSIRT NASK została przypisana różnym komórkom organizacyjnym Instytutu, w tym w szczególności Działowi CERT Polska. Według stanu na koniec lutego 2022 r. zadania CSIRT NASK realizowało 70 osób. Sposób funkcjonowania zespołu został formalnie opisany w postaci 11 kart procesów pracy, określających między innymi: cele, wykonawców, podprocesy i czynności, niezbędne zasoby, mierniki, dane wejściowe oraz uzyskiwane produkty.

rozwiązań serwerowych do przetwarzania „big data”[47], a do 2020 r. nie dokonano zaplanowanego zakupu sprzętu i oprogramowania dla specjalistycznego laboratorium, utworzonego w ramach Wydziału Wsparcia i Badań Biura. Z kolei w 2021 r. ze względu na ograniczone środki nie udało się w BdWzC zorganizować specjalistycznego szkolenia dla funkcjonariuszy z terenowych jednostek Policji;

- **problemów strukturalnych i organizacyjnych** – funkcjonujące w KWP/KSP wydziały do walki z cyberprzestępczością podlegały właściwym miejscowo komendantom wojewódzkim (Stołecznemu) Policji i były w praktyce niezależne od BdWzC KGP. Kierownictwo Biura podejmowało działania koordynujące i zlecało tym wydziałom określone czynności, jednakże bezpośredni nadzór nad ich realizacją sprawowali zastępcy komendantów wojewódzkich (Stołecznego) Policji do spraw kryminalnych. Wydziały te podejmowały zatem działania zależnie od posiadanych przez siebie sił i środków oraz określanych lokalnie priorytetów.

Utworzenie Centralnego Biura Zwalczania Cyberprzestępczości Policji

W reakcji na opisane powyżej problemy, w KGP opracowano koncepcję utworzenia nowej, wyspecjalizowanej jednostki organizacyjnej Policji – Centralnego Biura Zwalczania Cyberprzestępczości (zwanego dalej: CBZC). Powołująca tę służbę ustawa została przyjęta 17 grudnia 2021 r.[48] Założono w niej maksymalny limit wydatków z budżetu państwa na utworzenie CBZC w wysokości 4,4 mld zł w kolejnych 10 latach[49]. Zaplanowano również skonsolidowanie wydziałów terenowych do walki z cyberprzestępczością i wzmocnienie Policji do końca 2025 roku o 1,8 tys. etatów niezbędnych do uruchomienia nowej jednostki. Uregulowano także wymagania stawiane kandydatom do służby w CBZC, które zgodnie z przyjętymi przepisami obejmują m.in. sprawdzenie wiedzy i umiejętności z zakresu informatyki, funkcjonowania systemów informatycznych, systemów teleinformatycznych, sieci teleinformatycznych oraz znajomości języka obcego obejmującej te dziedziny[50].

W ocenie NIK, zainicjowane przez Policję zmiany strukturalne pionu do walki z cyberprzestępczością były działaniem celowym. Jednocześnie jednak Izba wskazała istotne ryzyka mogące negatywnie wpływać na proces formowania nowej jednostki, w tym w szczególności trudności związane z pozyskaniem w założonym terminie (do końca 2025 r.) 1,8 tys. odpowiedniej klasy specjalistów. NIK zwróciła zatem uwagę na konieczność objęcia tego procesu bezpośrednim nadzorem ze strony Komendanta Głównego Policji.

[47] Big data - termin odnoszący się do dużych, zmiennych i różnorodnych zbiorów danych, których analiza i samo przetwarzanie są trudne ze względu na ich wielkość, ale jednocześnie wartościowe, ponieważ mogą prowadzić do pozyskania nowej wiedzy.

[48] Ustawa z 17 grudnia 2021 r. o zmianie niektórych ustaw w związku z powołaniem Centralnego Biura Zwalczania Cyberprzestępczości (Dz. U. poz. 2447).

[49] Na budowę siedziby Centralnego Biura Zwalczania Cyberprzestępczości zaplanowano 450 mln zł, natomiast na zakupy sprzętu 250 mln zł.

[50] Dotyczy to kandydatów ubiegających się o przyjęcie do służby w CBZC na stanowisko związane z bezpośrednim rozpoznawaniem i zwalczaniem przestępstw popełnionych przy użyciu systemu informatycznego, systemu teleinformatycznego lub sieci teleinformatycznej oraz zapobieganiem tym przestępstwom, a także wykrywaniem i ściganiem sprawców tych przestępstw.

Słabość kadrowa urzędu obsługującego Ministra Cyfryzacji i Pełnomocnika Rządu

Istotne ograniczenia kadrowe oraz duża fluktuacja pracowników zostały również stwierdzone w przypadku komórki organizacyjnej KPRM prowadzącej obsługę merytoryczną zadań Ministra Cyfryzacji i Pełnomocnika Rządu wynikających z ustawy o KSC, tj. Departamentu Cyberbezpieczeństwa KPRM. Według stanu na koniec 2021 r. efektywne zatrudnienie[51] w Departamencie wyniosło tylko 21 osób, co jak przyznawał Pełnomocnik (w toku kontroli oraz w zastrzeżeniach złożonych do wystąpienia pokontrolnego) utrudniało, bądź wręcz uniemożliwiało rzetelne wykonywanie przypisanych temu organowi zadań związanych z koordynacją działań i realizacją polityki rządu w zakresie zapewnienia cyberbezpieczeństwa RP.

Ryzyka niegospodarnego wykorzystania środków publicznych

Ustalenia kontroli wykazały natomiast, że w sytuacji istotnych niedoborów kadrowych komórki merytorycznej realizującej zadania związane z cyberbezpieczeństwem RP, w KPRM zostały utworzone odrębne, rozbudowane struktury przeznaczone do obsługi kancelaryjno-biurowej Pełnomocnika (Biuro Pełnomocnika Rządu do Spraw Cyberbezpieczeństwa). NIK zgłosiła wątpliwości dotyczące celowości funkcjonowania tej komórki organizacyjnej (w której na koniec 2021 r. było zatrudnione 17 osób[52]), jak również zwróciła uwagę na fakt, że pracownicy Biura nie mieli specjalistycznego wykształcenia w obszarach, w których mieli oni stanowić wsparcie Pełnomocnika Rządu.

Kolejne zidentyfikowane ryzyka niegospodarnego wykorzystania ograniczonych zasobów KPRM dotyczyły zarządzania przez Ministra Cyfryzacji i Pełnomocnika Rządu tzw. systemem informatycznym S46.

Zgodnie z art. 46 ustawy o KSC, ww. system powinien wspierać współpracę podmiotów krajowego systemu cyberbezpieczeństwa, a także umożliwiać: zgłaszanie i obsługę incydentów, szacowanie ryzyka na poziomie krajowym, ostrzeganie o zagrożeniach cyberbezpieczeństwa.

Ustalenia kontroli wykazały natomiast, że po upływie roku od uruchomienia systemu S46[53] brak było możliwości realnego wykorzystania tego narzędzia, w celu podnoszenia poziomu cyberbezpieczeństwa. W systemie brak było informacji o zgłoszonych incydentach[54], jak również danych z poszczególnych sektorów kluczowych, które powinny być widoczne z poziomu Pełnomocnika Rządu. Znajdujące się w systemie, z poziomu użytkownika KPRM, dane w arkuszu „analiza ryzyka" bazowały wyłącznie na ankietach złożonych przez dwa podmioty – NASK S.A. i NASK-PIB oraz czterech usługach kluczowych i cyfrowych realizowanych przez te podmioty. Na dzień oględzin przeprowadzonych przez Izbę, KPRM dysponował tylko jednym terminalem do obsługi systemu S46 użyczonym przez NASK-PIB, a jedynym użytkownikiem tego systemu w Kancelarii[55]

[51] Tj. po odliczeniu osób znajdujących się w okresie wypowiedzenia stosunku pracy, osób oddelegowanych oraz długotrwale nieobecnych w pracy.

[52] Jedna osoba (Zastępca Dyrektora Biura) znajdowała się w okresie wypowiedzenia stosunku pracy.

[53] Produkcyjne uruchomienie systemu S46 nastąpiło w styczniu 2021 r., a oględziny jego funkcjonowania przeprowadzono w dniu 3 stycznia 2022 r. w KPRM oraz w dniu 16 grudnia 2021 r. z poziomu użytkownika CSIRT NASK (w siedzibie NASK-PIB).

[54] Poza jednym incydentem zaewidencjonowanym z poziomu CSIRT NASK.

[55] Poza dwoma pracownikami kończącymi na przełomie 2021 i 2022 r. zatrudnienie w KPRM.

był Dyrektor Departamentu Cyberbezpieczeństwa KPRM. Według stanu na 16 marca 2022 r. do systemu podłączonych było tylko 14 z około 350 podmiotów, które, w założeniu mają być jego podstawowymi użytkownikami. (KPRM zakładał przede wszystkim konieczność podłączenia do systemu wszystkich 170 operatorów usług kluczowych oraz 71 zdefiniowanych dostawców usług cyfrowych, natomiast nie podał oczekiwanych ram czasowych przyłączenia tych podmiotów). Pełnomocnik Rządu wskazywał na brak zainteresowania m.in. ze strony operatorów usług kluczowych podłączeniem do systemu S46 oraz na koszty związane z tym przyłączeniem. Wyjaśnił, że w celu zwiększenia liczby użytkowników systemu S46 oraz zapewnienia możliwości jego pełnego wykorzystywania KPRM „(...) aktywnie poszukiwała kandydatów do podłączenia się do systemu (...)" oraz przygotowała projekt nowelizacji ustawy o KSC, wprowadzający obowiązek korzystania z systemu S46 przez wybrane kategorie podmiotów, w tym w szczególności operatorów usług kluczowych.

Dotychczasowe wydatki związane z budową i uruchomieniem systemu S46 wyniosły 9801 tys. zł, a koszty jego utrzymania i rozwoju w 2021 r. – 6296 tys. zł. W 2022 r. na rozwój i utrzymanie systemu zaplanowano kwotę 9500 tys. zł. Analogiczne, lub nawet większe wydatki (zależenie od liczby podłączanych podmiotów) mają zostać poniesione w latach kolejnych.

Uwzględniając powyższe okoliczności, NIK oceniła, że dotychczasowe działania Ministra Cyfryzacji oraz Pełnomocnika Rządu związane z budową i rozwojem systemu S46 stworzyły ryzyko niegospodarnego wykorzystania znacznych środków publicznych.

5.3. Procedury zgłaszania przestępstw internetowych i reagowania na tego rodzaju zdarzenia

Ustalenia kontroli wykazały, że w jednostkach organizacyjnych Policji, które co do zasady stanowią pierwsze miejsce, w którym ofiary cyberprzestępców poszukiwałyby pomocy[56] nie wypracowano instrukcji i procedur zapewniających efektywną obsługę tego rodzaju zgłoszeń.

Brak instrukcji dla osób pragnących złożyć zawiadomienie o cyberprzestępstwie

W Policji nie opracowano w szczególności odrębnej instrukcji dla osób i podmiotów pragnących zgłosić przestępstwa internetowe. Elementy takiej instrukcji zostały co prawda zawarte w materiałach prasowych publikowanych na portalu Policja.pl[57], ale materiały te nie były w trwały sposób wyszczególnione. Dostęp do nich był utrudniony, ponieważ Policja nie dysponowała w swoim portalu odrębną sekcją tematyczną poświęconą cyberprzestępczości (szczegółowo opisano na str. 39–40 informacji o wynikach kontroli).

[56] Szczegółowe wyniki przeprowadzonego na zlecenie NIK badania opinii publicznej opisano w pkt 5.4.1. informacji o wynikach kontroli.

[57] Przykładowo w materiale pt. „Ostrzeżenie w sprawie oszukańczych linków w wiadomościach SMS" z 22 grudnia 2021 r. znalazła się informacja, w jaki sposób zgłaszać tego rodzaju incydenty. Z kolei w materiale pt. „Kompendium – jak nie dać się oszukać w Internecie" z 21 lutego 2021 r. znalazł się fragment pn. „Gdy doszło do oszustwa", w którym zawarto informacje dla ofiar cyberprzestępstw, zgodne z wymaganiami wobec zgłaszających przestępstwo opisanymi w „Algorytmach działania Policji w odniesieniu do różnych typów działań przestępczych".

NIK oceniła natomiast pozytywnie opracowanie w BdWzC KGP i przekazanie terenowym jednostkom Policji procedury przyjmowania zgłoszeń przestępstw internetowych pn. „Algorytmy działania Policji w odniesieniu do różnych typów działań przestępczych[58]" (dalej: Algorytmy). Algorytmy miały stanowić praktyczną wskazówkę dla funkcjonariuszy nieposiadających w przedmiotowym zakresie wiedzy specjalistycznej i umożliwić im właściwe, pod względem technicznym i procesowym, zabezpieczenie materiału dowodowego.

Wadliwe i nieaktualizowane procedury dla funkcjonariuszy Policji przyjmujących zgłoszenia przestępstw internetowych

Zastrzeżenia NIK dotyczyły niedokonywania przez KGP ewaluacji faktycznej przydatności oraz stopnia wykorzystania Algorytmów przez funkcjonariuszy terenowych jednostek Policji i ich odpowiedniej aktualizacji. **Ustalenia kontroli wykazały tymczasem, że opracowana w BdWzC KGP procedura była obarczona istotnymi wadami i brakami merytorycznymi.** Stwierdzono w szczególności:

- brak jednoznaczności[59] i spójności Algorytmów[60];
- brak analizy bezpieczeństwa odnośnie narzędzi i działań opisywanych w Algorytmach;
- wymaganie od zgłaszającego zbyt dużej ilości informacji, częściowo o specjalistycznym charakterze[61];
- wymaganie od funkcjonariusza przyjmującego zgłoszenie specjalistycznej wiedzy informatycznej, potrzebnej do oceny materiału dowodowego i przyjęcia kompletnego zawiadomienia[62].

Wymienione powyżej wady powodowały, że Algorytmy stanowiły tylko ograniczone wsparcie dla funkcjonariuszy niedysponujących specjalistyczną wiedzą w zakresie informatyki. **W połączeniu z brakiem instrukcji dla ofiar cyberprzestępczości, tworzyło to istotną barierę w procesie zgłaszania przestępstw internetowych przez obywateli.**

Przedstawione powyżej ustalenia kontroli NIK są spójne z wynikami Ogólnopolskiego Badania Wiktymizacyjnego przeprowadzonego w 2020 r. przez Instytut Wymiaru Sprawiedliwości[63], które wskazują, że faktyczna skala oszustw internetowych oraz m.in. włamań na konto mailowe/społecznościowe/aukcyjne może być znacznie wyższa niż ta, która wynika z policyj-

[58] Algorytmy zostały opracowane w ramach „Programu przeciwdziałania i zwalczania przestępczości gospodarczej na lata 2015-2020", jako realizacja zadania pn. „Wypracowanie taktyki i standardów przy zwalczaniu wybranych aspektów przestępczości gospodarczej, która zagraża bezpieczeństwu ekonomicznemu państwa lub związana jest z rozwojem nowych technologii". Dokument ten został przesłany przez Dyrektora BdWzC KGP w dniu 6 listopada 2020 r. do zastępców komendantów wojewódzkich (Stołecznego) Policji ds. kryminalnych, celem przekazania podległym jednostkom Policji, jako materiał pomocniczy do wykorzystania w wykonywanych czynnościach służbowych.

[59] Np. w części dotyczącej oszustwa internetowego nie jest jasne, czy zapisy algorytmu dotyczą oszukanego kupującego, oszukanego sprzedawcy, czy też przejęcia konta na portalu aukcyjnym, sklepie internetowym, czy jeszcze innego przypadku oszustwa.

[60] Np. algorytmy dotyczące przestępstw popełnionych wobec osób fizycznych oraz podmiotów gospodarczych są ze sobą przemieszane.

[61] Dotyczy to np. informacji pozyskiwanych w związku z przejęciem konta w portalu społecznościowym.

[62] Dotyczy to np. ataku DDoS.

[63] https://iws.gov.pl/wp-content/uploads/2021/05/IWS_-Wlodarczyk-Madejska-J.-i-in._Ogolnopolskie-Badanie-Wiktymizacyjne-2020.-Raport-z-badania.pdf (dostęp w dniu 07.09.2022 r.)

nych statystyk. Oba wymienione przestępstwa znalazły się bowiem wśród czterech czynów karalnych o najwyższym wskaźniku wiktymizacji[64] (oszustwo internetowe na pierwszym miejscu ze wskaźnikiem 11,2% badanych, a włamanie na konto mailowe/społecznościowe/aukcyjne na czwartym miejscu ze wskaźnikiem 4,9% badanych). Jednocześnie oba przestępstwa były najrzadziej zgłaszane na Policję (włamanie na konto mailowe/społecznościowe/aukcyjne znalazło się na ostatnim miejscu ze wskaźnikiem zgłoszeń na poziomie 17%, a oszustwo internetowe na przedostatnim miejscu ze wskaźnikiem zgłoszeń na poziomie 22%)[65]. **Powyższe dane świadczą m.in. o tym, że obywatele w wielu przypadkach będąc ofiarami nie zgłaszają tego rodzaju zdarzeń.**

Procedury zgłaszania i obsługi incydentów, w tym o charakterze przestępstw komputerowych zostały wypracowane w NASK-PIB.

Procedury zgłaszania i obsługi incydentów wypracowane przez NASK-PIB

Zasadniczym sposobem zgłaszania do CSIRT NASK incydentów cyberbezpieczeństwa było wykorzystanie formularza zamieszczonego pod adresem incydent.cert.pl. Pomagał on, dzięki swojej budowie, w zgromadzeniu informacji na temat zgłaszającego, a także charakteru i okoliczności zdarzenia, które były niezbędne do podjęcia dalszych działań w ramach obsługi zgłoszenia. Formularz pozwalał dodatkowo na zgłoszenie domeny internetowej podejrzewanej o wyłudzanie danych i środków finansowych.

Dalsze postępowanie związane z reakcją na zgłoszony incydent zostało zdefiniowane w dokumencie pt. „Instrukcja obsługi Incydentów". Określała ona m.in.: kolejność obsługi zdarzeń, role pracowników biorących udział w obsłudze, listę docelowych zespołów reagowania właściwych dla zgłoszeń będących poza obszarem działania CSIRT NASK, listę systemów wspomagających obsługę incydentów, sposób dokumentowania działań. Główny element instrukcji stanowiło 27 algorytmów określających reakcje na wszystkie podstawowe rodzaje zgłoszeń. W zależności od przebiegu i wyników przeprowadzanej procedury, przewidziane zostały odpowiednie działania: zapobiegające negatywnym skutkom wystąpienia zagrożeń, mające na celu wyeliminowanie zagrożenia oraz informacyjno-edukacyjne. W algorytmach określono m.in.:

- rekomendacje przekazywane zgłaszającym incydenty, dotyczące sposobu postępowania ze skutkami incydentu;
- ostrzeżenia i komunikaty publikowane na temat występujących zagrożeń cyberbezpieczeństwa;
- zasady kontaktu z usługodawcami, z których infrastruktury korzystają cyberprzestępcy oraz uzupełnienia listy złośliwych domen, do których dostęp mogą zablokować administratorzy sieci;
- zasady inicjowania działań w stosunku do nazw naruszających Regulamin Rejestru Domen Internetowych oraz administracyjnego blokowania tych nazw[66].

[64] Wskaźnik wiktymizacji to odsetek badanych, którzy padli ofiarą przynajmniej jednego przestępstwa, co najmniej raz w roku poprzedzającym badanie.

[65] Dla porównania kradzież samochodu zgłosiło 97,7% respondentów, włamanie 73%, kradzież roweru 69%, a rozbój 61%.

[66] Prowadzony przez NASK-PIB rejestr domen gromadzi i w sposób zaufany upublicznia dane

Podejmowanie niezbędnych działań będących reakcją na zgłoszone incydenty, w sytuacji gdy wykraczały one poza kompetencje Zespołu CSIRT NASK, zapewniała bezpośrednia współpraca z organami ścigania. W kontrolowanym okresie przedstawiciele NASK-PIB pozostawali w kontakcie z przedstawicielami Wydziałów do Walki z Cyberprzestępczością KWP (KSP), przekazując im informacje o wykrytych w toku działalności CSIRT NASK okolicznościach, które mogły stanowić czyn zabroniony oraz wymieniając się wiedzą uzyskaną w toku analizy działań grup bądź osób. W uzasadnionych przypadkach, CSIRT NASK przekazywał również osobom zgłaszającym incydenty, instrukcje ułatwiające złożenie zawiadomienia i dalszą współpracę z organami ścigania.

NIK oceniła pozytywnie opisane powyżej procedury i działania zwracając jednak uwagę na ich ograniczone efekty wynikające z niskiej rozpoznawalności NASK-PIB wśród obywateli. Badanie opinii publicznej, przeprowadzone na zlecenie Izby[67], wykazało bowiem, że tylko 1% respondentów posiadał wiedzę na temat możliwości uzyskania wsparcia ze strony tego podmiotu.

5.4. Działania edukacyjne zwiększające wiedzę obywateli na temat przestępczości komputerowej oraz wydawanie wytycznych podnoszących poziom bezpieczeństwa użytkowników Internetu

Utworzenie „bazy wiedzy" z zakresu cyberbezpieczeństwa na portalu gov.pl

W okresie objętym kontrolą Minister Cyfryzacji oraz Pełnomocnik Rządu zainicjowali działania mające na celu utworzenie jednolitego, przeznaczonego dla obywateli oraz różnych instytucji repozytorium ostrzeżeń, zaleceń oraz dobrych praktyk z zakresu cyberbezpieczeństwa. Tzw. „baza wiedzy" została upubliczniona w październiku 2019 r. na rządowym portalu gov.pl i w kolejnych latach podlegała modyfikacjom i rozbudowie. Wg stanu na dzień 14 stycznia 2022 r. informacje oraz rekomendacje zamieszczone w bazie były podzielone na dziewięć następujących zakładek tematycznych: „Aktualności", „Dla każdego – cyberhigiena", „Dla profesjonalistów", „#CyberbezpiecznySamorząd", „Narodowe Standardy Cyberbezpieczeństwa", „Szkolenia", „Poradniki partnerów technologicznych", „Subskrypcje cyberwiadomości", „Najczęściej zadawane pytania".

W poszczególnych sekcjach tematycznych „bazy wiedzy" publikowane były m.in. zalecenia i rekomendacje, mające na celu zwiększenie poziomu bezpieczeństwa, w tym zapobieganie przestępstwom internetowym. Obejmowały one w szczególności:

- uniwersalne poradniki kierowane do różnych grup użytkowników Internetu[68];

pozwalające na sprawne funkcjonowanie użytkowników w sieci Internet. Blokada domeny powoduje wstrzymanie upubliczniania tych danych, co skutkuje praktycznym odłączeniem użytkownika od wielu funkcjonalności sieci Internet.

67 Szczegółowe wyniki badania opisano w pkt 5.4.1. informacji o wynikach kontroli.

68 Poradnik „Jak chronić się przed cyberatakami? Praktyczne wskazówki dla parlamentarzystów i nie tylko.", styczeń 2021 r.

- poradniki „branżowe" skierowane do nauczycieli[69] oraz podmiotów ochrony zdrowia[70];
- liczne rekomendacje adresowane do profesjonalistów dotyczące w szczególności zabezpieczeń sieci i systemów informatycznych, opublikowane w zakładce „Narodowe Standardy Cyberbezpieczeństwa";
- rekomendacje „branżowe" cyberbezpieczeństwa dla sektora wodno-kanalizacyjnego oraz ochrony zdrowia;
- zalecenia na poziomie podstawowym kierowane przede wszystkim do indywidualnych użytkowników Internetu, zamieszczone w zakładce „Dla każdego – cyberhigiena";
- rekomendacje partnerów technologicznych (firm CISCO, DELL, Microsoft).

Ograniczenia funkcjonalne „bazy wiedzy"

Ustalenia kontroli wykazały, że „baza wiedzy" podlegała istotnym ograniczeniom w zakresie dostępności i łatwości wyszukiwania zawartych w niej informacji.

Przede wszystkim brak było bezpośredniej i wyraźnie oznaczonej „ścieżki dostępu" do bazy. Dostęp do niej następował z poziomu głównej strony portalu gov.pl, poprzez rozwijalne menu po lewej stronie ekranu, przez link „baza wiedzy"[71] (brak było informacji, że baza ma związek z tematyką bezpieczeństwa IT), który prowadził do trzech zakładek tematycznych: „Cyberbezpieczeństwo", „Dostępność cyfrowa", „Społeczna Odpowiedzialność Administracji". Po wejściu w temat: „Cyberbezpieczeństwo" wyświetlała się „baza wiedzy" z zakresu cyberbezpieczeństwa. Alternatywną metodą dotarcia do „bazy wiedzy" było wejście na stronę internetową ministra właściwego do spraw informatyzacji – gov.pl/web/cyfryzacja i przejście przez kolejne zakładki: „co robimy" – „cyberbezpieczeństwo" – „edukacja" – „baza wiedzy o cyberbezpieczeństwie").

Według stanu na 14 stycznia 2022 r. w „bazie wiedzy" brak było również dedykowanej wyszukiwarki. Odnalezienie poszczególnych materiałów lub zagadnień tematycznych było zatem możliwe tylko za pomocą wyszukiwarki dostępnej z poziomu całego portalu gov.pl, która przeszukuje strony internetowe wszystkich podmiotów publicznych obecnych na tym portalu. Wpływało to na wyniki wyszukiwania, które w pewnych przypadkach radykalnie odbiegały od treści wpisanego hasła[72].

Opisane powyżej ograniczenia funkcjonalne wynikały z umiejscowienia „bazy wiedzy" w ramach rozległego serwisu internetowego, jakim jest portal.gov. W związku z architekturą i koncepcją funkcjonowania tego portalu, który obejmuje strony wielu podmiotów publicznych oraz bardzo zróżnicowaną tematykę brak było możliwości lepszego wyeksponowania w tym miejscu treści z zakresu cyberbezpieczeństwa. **Powyższe w znaczący sposób utrudniało korzystanie z zasobów „bazy wiedzy" oraz, co istotne, ograniczało rozpoznawalność zawartych tam treści.**

[69] „Poradnik dla nauczycieli PR-EDU-01 – bezpieczne korzystanie z platform do edukacji zdalnej", kwiecień 2020 r.

[70] „Zgłaszanie incydentów cyberbezpieczeństwa przez podmioty sektora ochrony zdrowia", kwiecień 2020 r.

[71] Dotarcie w ten sposób do „bazy wiedzy" było możliwe z jakiejkolwiek strony internetowej otwartej na portalu gov.pl.

[72] Przykładowo, wyniki przeprowadzonego w toku oględzin „bazy wiedzy" wyszukania hasła „kampanie phishingowe" dotyczyły tematyki rolnictwa i kampanii z zakresu ochrony środowiska.

Niewielka skala wykorzystania informacji i materiałów opublikowanych w „bazie wiedzy"

Prowadzony w KPRM monitoring kwartalnej liczby odsłon poszczególnych zakładek tematycznych „bazy wiedzy" oraz szczegółowe analizy zlecone przez kontrolerów NIK potwierdziły niewielką skalę wykorzystania opublikowanych tam informacji, komunikatów oraz rekomendacji.

W okresie ponad dwóch lat od utworzenia „bazy wiedzy"[73] największą liczbę wejść odnotowano w zakładkach:

- „Dla każdego – cyberhigiena" – 34 218 wejść łącznie, przy czym największa liczba wejść miała miejsce w okresie 31 marca – 30 czerwca 2020 r. (8159), natomiast w ostatnim kwartale 2021 r. wyniosła ona tylko 2286;
- „Aktualności" – 22 050 wejść łącznie, przy czym największa liczba wejść miała miejsce w okresie 30 września 2020 r. - 31 grudnia 2020 r. (5077), natomiast w ostatnim kwartale 2021 r. wyniosła ona 4862.

Najmniejszą liczbę wejść odnotowano w przypadku zakładek „Narodowe Standardy Cyberbezpieczeństwa" (1159 przez dwa kwartały jej funkcjonowania) oraz „Najczęściej zadawane pytania" (1136 przez okres jednego roku i trzech miesięcy).

W przypadku poszczególnych artykułów i poradników tylko pojedyncze z nich odnotowały istotną liczbę odsłon, a zdecydowana większość, w tym dobrane do badania przez NIK opracowania dotyczące oszustw komputerowych i phishingu[74], osiągnęły nie więcej niż kilkaset wejść, i tak:

- Najczęściej odwiedzanym artykułem w zakładce „Dla każdego - cyberhigiena" był artykuł dotyczący phishingu[75], który miał 52 129 odsłon ogółem, w tym 41 841 unikalnych[76]. Cztery artykuły dotyczące m.in. zasad korzystania z urządzeń mobilnych, tworzenia bezpiecznych haseł, e-bankowości oraz rozpoznawania nieprawdziwych informacji odnotowały od 18 629 do 10 132 odsłon. W przypadku czterech kolejnych, najczęściej czytanych publikacji liczba odsłon nie przekroczyła 10 000.
- W zakładce „Aktualności" najczęściej odwiedzanym artykułem było opracowanie ENISA dotyczące 15 głównych cyberzagrożeń, które osiągnęło 3132 odsłon, w tym 2515 unikalnych. Kolejne trzy, najczęściej czytane artykuły odnotowały między 3029 a 1433 odsłon, a sześć kolejnych poniżej 1000 odsłon.
- W zakładce „Dla profesjonalistów" – jeden artykuł dotyczący pracy zdalnej[77] odnotował 7129 odsłon, w tym 4591 unikalnych. Z pozostałych dziewięciu najczęściej czytanych publikacji tylko jedna osiągnęła powyżej 1000 odsłon.

---

73 Od 29 października 2019 r. do 22 grudnia 2021 r.

74 Na wniosek kontrolerów NIK, w Departamencie Cyberbezpieczeństwa KPRM, przeprowadzono analizę danych z Google Analytics prezentujących: kanały pozyskiwania ruchu na stronach „bazy wiedzy", najczęściej czytane artykuły w trzech zakładkach bazy („Dla każdego – cyberhigiena", „Aktualności", „Dla profesjonalistów") oraz osiem dobranych celowo przez kontrolujących publikacji ostrzegających przed różnymi metodami działania przestępców internetowych.

75 www.gov.pl/web/baza-wiedzy/czym-jest-phishing-i-jak-nie-dac-sie-nabrac-na-podejrzane-widomosci-e-mail-oraz-sms-y

76 Unikalne odsłony obejmują wszystkie odsłony wygenerowane przez tego samego użytkownika podczas tej samej sesji.

77 www.gov.pl/web/baza-wiedzy/praca-zdalna---razem-ale-osobno

- Z łącznej liczby 38 zamieszczonych w „bazie wiedzy" poradników i rekomendacji tylko dwa zostały pobrane ze strony gov.pl więcej niż 1 000 razy. W przypadku poradników, których treść mogła być wykorzystywana przez indywidualnych użytkowników Internetu liczba pobrań wyniosła odpowiednio: 350[78], 172[79] oraz 132[80].
- **W przypadku ośmiu publikacji, dobranych celowo do badania przez kontrolujących, ostrzegających przed różnymi metodami działania przestępców internetowych liczba odsłon, w tym unikalnych wyniosła:**
  - „Szykujesz się na Black Friday? Sprawdź, jak nie stać się ofiarą internetowych oszustów[81] – 342/293;
  - „UWAGA – CSIRT NASK ostrzega!!![82] – 343/279;
  - „Rejestracja na szczepienie – zachowaj czujność!!!"[83] – 375/327;
  - „Black Friday 2020 – jak kupować, żeby nie żałować"[84] – 874/419;
  - „UWAGA – CSIRT NASK ostrzega przed kolejnymi oszustwami związanymi z pandemią COVID-19"[85] – 221/208;
  - „UWAGA! CSIRT NASK ostrzega – trwa zmasowana kampania SMS-owa celująca w użytkowników telefonów z systemem Android!"[86] – 892/766;
  - „Black Friday i bezpieczne zakupy w Internecie. Jak nie dać się oszukać?"[87] – 79/48;
  - „CSIRT NASK ostrzega - przedświąteczny okres zakupowy to wzmożony czas działalności przestępców w internecie"[88] – 145/122.

Brak ewaluacji efektów funkcjonowania „bazy wiedzy" oraz działań mających na celu zwiększenie liczby odsłon publikowanych w niej materiałów

Uwzględniając powyższe dane, NIK oceniła jako nierzetelne, brak dokonywania przez Ministra Cyfryzacji ewaluacji efektów utworzonej „bazy wiedzy". Prowadzony w tym zakresie w KPRM monitoring ograniczał się do uzyskiwania mało użytecznych danych prezentujących, w ujęciu kwartalnym, łączną liczbę wejść na poszczególne zakładki bazy[89]. Nie były natomiast prowadzone szczegółowe badania pozwalające na ustalenie faktycznej liczby odsłon (w tym unikalnych) wybranych artykułów, a analizy takie zrealizowano dopiero na wniosek kontrolerów NIK. W rezultacie, w KPRM nie dysponowano wiedzą pozwalająca na dostosowanie materia-

78 Poradnik „Jak chronić się przed cyberatakami? Praktyczne wskazówki dla parlamentarzystów i nie tylko.", styczeń 2021 r.

79 „PORADNIK – PRCyber - 01 Cyberbezpieczeństwo – jak chronić nasze informacje przed atakami w cyberprzestrzeni?", maj 2020 r.

80 „Poradnik dla nauczycieli PR-EDU-01 – bezpieczne korzystanie z platform do edukacji zdalnej", kwiecień 2020 r.

81 Opublikowano w „bazie wiedzy" 28 listopada 2019 r.

82 Opublikowano 7 października 2020 r.

83 Opublikowano 15 stycznia 2021 r.

84 Opublikowano 23 listopada 2020 r.

85 Opublikowano 26 sierpnia 2021 r.

86 Opublikowano 24 września 2021 r.

87 Opublikowano 25 listopada 2021 r.

88 Opublikowano 20 grudnia 2021 r.

89 W grudniu 2021 r., w „bazie wiedzy" została co prawda udostępniona ankieta ewaluacyjna, ale jej wyniki nie były miarodajne w związku z jej upowszechnieniem w jednorodnej grupie złożonej głównie z przedstawicieli administracji państwowej.

łów publikowanych w „bazie wiedzy" do potrzeb odbiorców i zwiększenie w ten sposób liczby odsłon oraz zasięgu oddziaływania prowadzonych działań edukacyjnych.

Brak ostrzegania o trwających kampaniach *phishingowych*

Negatywna ocena NIK dotyczyła także niepodejmowania przez Ministra i Pełnomocnika niezwłocznych, adekwatnych działań w celu ostrzegania obywateli o trwających aktualnie atakach przestępców internetowych. Weryfikacja realizowanych w tym zakresie zadań została przeprowadzona przez NIK na próbie sześciu masowych kampanii *phishingowych,* które miały miejsce w latach 2019–2021 oraz obejmowały typowe dla tego okresu metody działania przestępców internetowych[90]. Badaniem objęto następujące kampanie:

1. Trwający na przełomie stycznia i lutego 2019 r. atak na klientów portalu Otomoto.pl.
2. Powtarzające się przez cały 2020 r. kampanie nakłaniające do instalacji złośliwego oprogramowania (poprzez podszywanie się pod komunikaty firmy InPost).
3. Trwającą w okresie styczeń - sierpień 2020 r. kampanię mającą na celu skłonienie do zainstalowania złośliwego oprogramowania na urządzeniach mobilnych poprzez podszywanie się pod operatorów poczty elektronicznej (m.in. WP, Interia) informujących o konieczności zaakceptowania nowego regulaminu świadczenia usług.
4. Prowadzoną od 2020 r. kampanię dotyczącą fałszywych zawiadomień o skierowaniu na kwarantannę.
5. Trwającą od grudnia 2021 r. aktywną kampanię polegającą na dostarczaniu fałszywych wiadomości SMS na temat przesyłek.
6. Trwającą, co najmniej od połowy 2020 r., kampanię ukierunkowaną na wyłudzenia danych od użytkowników serwisu OLX, prowadzoną m.in. z wykorzystaniem komunikatora WhatsApp.

Kontrola wykazała, że Minister Cyfryzacji oraz Pełnomocnik Rządu nie podjęli działań mających na celu ostrzeżenie o trwających atakach i ich potencjalnych skutkach oraz poinformowanie obywateli o zasadach postępowania w sytuacji, gdy staną się celem ataku w przypadku czterech z sześciu ww. kampanii (wymienionych w pkt 1–3 oraz w pkt 6 powyżej). Jako działania informujące użytkowników Internetu o konkretnej prowadzonej kampanii wskazywano ogólne publikacje na temat złośliwego oprogramowania zamieszczone w „bazie wiedzy"[91]. Odwołano się również do zamieszczonych w „bazie wiedzy" artykułów, które co prawda były tematycznie powiązane z dwoma z ww. kampanii, natomiast ich zasięg oddziaływania (liczba odsłon) były raczej symboliczne i wyniosły odpowiednio: 892 osoby[92], 375 osób[93], 221 osób[94] oraz 145 osób[95]. **Powyższe**

[90] Opisane m.in. w raportach rocznych z działalności Cert Polska oraz w raportach miesięcznych CSIRT NASK dla Pełnomocnika Rządu.

[91] Artykuł „Złośliwe oprogramowanie – co to takiego, jak się chronić?" z dnia 25 sierpnia 2021 r.

[92] „UWAGA! CSIRT NASK ostrzega – trwa zmasowana kampania SMS-owa celująca w użytkowników telefonów z systemem Android!".

[93] „Rejestracja na szczepienie – zachowaj czujność!!!".

[94] „UWAGA – CSIRT NASK ostrzega przed kolejnymi oszustwami związanymi z pandemią COVID-19".

[95] „CSIRT NASK ostrzega - przedświąteczny okres zakupowy to wzmożony czas działalności

oznacza, że indywidualni użytkownicy Internetu byli pozbawieni aktualnych, pochodzących od organów państwa odpowiadających za kształtowanie „cyberświadomości", informacji na temat zagrożeń ze strony przestępczości internetowej[96]**.**

Prowadzone przez Ministra Cyfryzacji i Pełnomocnika Rządu kampanie edukacyjne dotyczące korzystania z Internetu

Zidentyfikowane przez NIK nieprawidłowości w zakresie funkcjonowania „bazy wiedzy" nie były kompensowane poprzez prowadzone przez Ministra Cyfryzacji i Pełnomocnika Rządu kampanie edukacyjne z zakresu cyberbezpieczeństwa. Tematyka zrealizowanych w badanym okresie kampanii (przygotowanych we współpracy z NASK-PIB) w niewielkim stopniu odnosiła się zagrożeń ze strony oszustw komputerowych. Priorytetem było promowanie e-usług publicznych oraz wybrane (aczkolwiek bardzo istotne) aspekty bezpieczeństwa w sieci, dotyczące przede wszystkim dzieci i młodzieży, i tak:

1. Realizowana w latach 2019–2020 kampania „e-polak potrafi!" objęła cztery obszary tematyczne: „jakość życia", „e-usługi publiczne", „bezpieczeństwo w sieci", „programowanie". Wiodącym elementem całej kampanii było zachęcanie Polaków do korzystania z e-usług publicznych. W obszarze „bezpieczeństwa w sieci" priorytetem było natomiast informowanie rodziców na temat zagrożeń internetowych dotyczących dzieci, takich jak np. sexting, publikowanie wizerunku dziecka, szkodliwe treści występujące w Internecie, czy też uzależnienie od gier komputerowych. (Zbliżona tematyka była poruszana w ramach akcji edukacyjnej „Akademia Cyfrowego Rodzica" oraz kampanii „Bądź z innej bajki".) Wybrane komunikaty kampanii „e-polak potrafi!" dotyczyły także bezpieczeństwa seniorów w sieci oraz oszustw internetowych i phishingu. W ramach kampanii wykorzystywano różne kanały komunikacyjne: telewizję (m.in. lokowanie wątków w popularnych serialach i w porannych pasmach TV), Internet (m.in. filmy edukacyjne, artykuły, webinaria), media społecznościowe, prasę oraz radio[97].
2. Kampania „e-senior potrafi!" oraz akcja edukacyjna „Seniorze, spotkajmy się w sieci" zachęcające osoby starsze do korzystania z nowych technologii i informujące o związanych z tym zagrożeniach.
3. Akcja edukacyjna „#CyberbezpiecznySamorząd", w ramach której Departament Cyberbezpieczeństwa KPRM, we współpracy m.in. z partnerami technologicznym i NASK-PIB realizował szkolenia z zakresu cyberbezpieczeństwa dla pracowników podmiotów publicznych różnych szczebli.

przestępców w internecie".

[96] W KPRM nie zostały również podjęte działania mające na celu wykorzystanie alternatywnych kanałów komunikacji umożliwiających bezpośrednie dotarcie do indywidualnych użytkowników Internetu z informacjami na temat cyberzagrożeń. Co prawda, w pierwszej połowie 2020 r. w „bazie wiedzy" uruchomiono usługę subskrypcji wiadomości z zakresu cyberbezpieczeństwa, jednak większość subskrybentów stanowili przedstawiciele administracji publicznej i nie podjęto żadnych działań w celu upowszechnienia tej usługi wśród osób fizycznych.

[97] W trakcie kontroli NIK prowadzony był przetarg na kontynuację, w okresie do 2023 r., kampanii „e-polak potrafi!". Pełnomocnik wskazywał, że w ramach kolejnej edycji kampanii planowane jest istotne wzmocnienie przekazu w obszarze „bezpieczeństwo w sieci", który ma obejmować 45% tematyki działań edukacyjnych (wobec 55% przeznaczonych na cztery pozostałe obszary kampanii).

Brak określenia jednego modelu edukowania obywateli o zagrożeniach cyberbezpieczeństwa

Przeprowadzona kontrola wykazała także, że Minister Cyfryzacji oraz Pełnomocnik Rządu, którzy podjęli próbę utworzenia jednolitego repozytorium ostrzeżeń i zaleceń z zakresu cyberbezpieczeństwa nie wypracowali we współpracy z kierownictwem nadzorowanej przez siebie jednostki (NASK-PIB) spójnego stanowiska odnośnie optymalnego modelu edukowania obywateli o zagrożeniach cyberbezpieczeństwa. W rezultacie, w badanym okresie, funkcjonowały w tym obszarze dwa modele komunikacyjne – scentralizowany (opisana powyżej „baza wiedzy" KPRM) oraz rozproszony (wdrażany w szczególności przez NASK-PIB) w postaci różnych specjalizowanych lub przeznaczonych dla wybranych grup użytkowników stron i serwisów informacyjnych.

Duża skala działań informacyjno-edukacyjnych prowadzonych przez NASK-PIB

W przypadku drugiego z wymienionych powyżej podmiotów kontrolujący zidentyfikowali bezprecedensową w polskich warunkach skalę aktywności w obszarze działań informacyjno-edukacyjnych dotyczących korzystania z Internetu i związanych z tym zagrożeń. Prowadzone działania objęły liczne kampanie i akcje edukacyjne[98] realizowane samodzielnie przez NASK oraz we współpracy z takimi partnerami, jak: Minister Cyfryzacji i Pełnomocnik Rządu[99], UNICEF Polska i Facebook[100], ENISA[101] oraz organizacje pozarządowe[102]. Były one finansowane z dotacji celowych, środków UE oraz środków własnych Instytutu. Informacje dotyczące zagrożeń były również publikowane na bieżąco na stronach:

- cert.pl;
- https://twitter.com/CERT_Polska;
- https://www.facebook.com/CERT.Polska;
- https://www.linkedin.com/showcase/cert-polska/.

W 2019 r. CERT Polska zamieścił na Facebooku ponad 100 wpisów na temat bieżących zagrożeń lub analiz. W 2020 r. było to ponad 120 postów na Facebooku oraz ponad 190 wpisów na Twitterze, a w 2021 r. ponad 45 postów na Facebooku i 55 wpisów na Twitterze. W materiałach publikowanych na stronie internetowej CERT Polska przedstawiano m.in. rekomendacje dotyczące[103]: unikania nieuczciwych sprzedawców, bezpiecznego użytkowania poczty elektronicznej i mediów społecznościowych, przeciwdziałania

[98] Szczegółowo wymienione w wystąpieniu pokontrolnym z dnia 27 kwietnia 2022 r., znak: KPB. 410.007.03.2021, przekazanym do Dyrektora NASK-PIB.

[99] M.in. kampanie: „Nie zgub dziecka w sieci" (w ramach wymienionej powyżej kampanii „e-polak potrafi!"), „Akademia Cyfrowego Rodzica", „Bądź z innej bajki", „Seniorze, spotkajmy się w sieci".

[100] Projekt edukacyjny „Przystań w sieci", którego celem było uświadomienie młodym ludziom i ich nauczycielom zagrożeń, z którymi mogą się zetknąć w Internecie oraz przedstawienie im krytycznego podejścia do treści znajdujących się w sieci.

[101] NASK corocznie od 2013 r. koordynuje w Polsce ogólnoeuropejską kampanię Europejski Miesiąc Cyberbezpieczeństwa, organizowaną przez ENISA z inicjatywy Komisji Europejskiej.

[102] We współpracy z Fundacją Dajemy Dzieciom Siłę NASK-PIB zrealizował projekt edukacyjny w ramach Polskiego Centrum Programu Safer Internet.

[103] W badanym okresie CSIRT NASK przygotował również rekomendacje cyberbezpieczeństwa przeznaczone dla: sektora zdrowia – organ właściwy ds. cyberbezpieczeństwa w sektorze zdrowia przekazał rekomendacje do 21 tys. podmiotów leczniczych; sektorów wykorzystujących przemysłowe systemy sterowania – odnoszące się do zwiększonej liczby niezabezpieczonych urządzeń przemysłowych widocznych i dostępnych do konfiguracji z Internetu; sektora wodno-kanalizacyjnego; podsektora kolejowego; dla użytkowników urządzeń Weintek cMT HMI wykorzystywanych między innymi w krajowych systemach automatyki przemysłowej; dla organizacji wykorzystujących oprogramowanie Pulse Secure VPN.

phishingowi, weryfikacji nadawcy wiadomości, korzystania z listy ostrzeżeń przed niebezpiecznymi stronami, podatności w usłudze Remote Desktop, unikania ransomware i możliwości odzyskiwania zaszyfrowanych plików.

Ograniczone efekty działalności informacyjno-edukacyjnej NASK-PIB

NIK ustaliła, że realne efekty opisanych powyżej działań NASK-PIB były znacznie ograniczone, co wynikało z rozproszenia przekazywanych komunikatów, a także z braku rzetelnej, bieżącej ewaluacji prowadzonych działań informacyjnych. Szczegółowe badanie czterech wybranych celowo kampanii edukacyjnych wykazało bowiem, że w przypadku dwóch z nich (kampanie „stojpomyslpolacz.pl" oraz „bezpiecznewybory.pl") nie dokonywano żadnych pomiarów skuteczności przekazywanych komunikatów. Odnośnie kampanii „www.saferinternet.pl" NASK dokonywał pomiarów: liczby odsłon, całkowitego zasięgu Facebooka, liczby obserwujących Facebook, liczby wyświetleń tweetów. Osiągnięte wartości wyniosły:

	2019	2020	2021
liczba odsłon	31 386	35 624	119 346
całkowity zasięg FB	110 000	70 000	brak danych
liczba obserwujących FB	2 519	2 759	2 911
liczba wyświetleń tweetów	35 136	22 136	13 400

W przypadku realizowanej na zlecenie ENISA kampanii „Europejski Miesiąc Cyberbezpieczeństwa" stwierdzono natomiast, że w poszczególnych miesiącach liczba odsłon całej „Bazy Wiedzy" (stanowiącej zbiór materiałów informacyjnych, rekomendacji i zaleceń opublikowanych podczas wszystkich dotychczasowych edycji tej kampanii) nie przekraczała 6000, a średnio dla pojedynczych artykułów nie przekraczała 40. W wielu miesiącach badanego okresu cała „Baza Wiedzy" oraz jej poszczególne strony internetowe nie zostały odwiedzone nawet przez jedną osobę!

Rozproszenie i doraźny charakter działalności informacyjnej Policji

Przeprowadzona kontrola wykazała dużą skalę aktywności Policji w docieraniu do użytkowników Internetu z informacjami dotyczącymi cyberzagrożeń i cyberprzestępczości. Komunikaty Policji w tym zakresie były przekazywane przez portal Policja.pl[104], tradycyjne media, media społecznościowe[105] oraz w toku bezpośrednich spotkań z obywatelami. **Podobnie jak w przypadku NASK-PIB stwierdzono jednak rozproszenie i brak pełnego wykorzystywania potencjału prowadzonej przez Policję polityki informacyjnej.** W ramach portalu Policja.pl, który stanowił główny kanał komunikacji z obywatelami, nie stworzono odrębnej sekcji tematycznej, która pełniłaby rolę „bazy wiedzy" na temat cyberprzestępczości. Materiały z tego zakresu były publikowane w zakładce „Aktualności", co w obliczu dużej liczby zamieszczanych tam informacji (85,1 tys. artykułów)

[104] W badanym okresie łączna liczba materiałów w kategorii „cyberprzestępczość", które ukazały się na stronie głównej portalu Policja.pl, wyniosła 104. Materiały były przygotowywane samodzielnie przez Policję oraz we współpracy z instytucjami partnerskimi (np. NASK, Europol, FinCERT.pl – Bankowe Centrum Cyberbezpieczeństwa ZBP). Miały one zróżnicowany charakter – od prostych notatek do rozbudowanych artykułów wzbogaconych infografikami i filmami – spełniających rolę wytycznych dla obywateli i mających walor edukacyjny

[105] Wg stanu na dzień 22 grudnia 2021 r. główne serwisy Policji miały następującą liczbę obserwujących użytkowników : Facebook – 402 tys., Twitter – 108,6 tys., Instagram – 27,8 tys., TikTok – 203,3 tys.

znacząco utrudniało dotarcie do poszczególnych ostrzeżeń lub rekomendacji. Istotny problem stanowiło także rozproszenie przekazu informacyjnego kierowanego przez Policję do obywateli pomiędzy Komendę Główną Policji a Komendy Wojewódzkie (Stołeczną) Policji. Konkretny materiał dotyczący przestępczości internetowej mógł się pojawić na stronie głównej portalu Policja.pl albo w zakładach lokalnych jednostek Policji (lub też w obu tych miejscach równocześnie), a miejsce jego publikacji nie wynikało z rozwiązań systemowych, ale decyzji podejmowanych przez poszczególne osoby odpowiedzialne za te kanały[106]. Żadna z odpowiedzialnych komórek organizacyjnych Komendy Głównej Policji[107] nie dokonywała również ewaluacji publikowanych materiałów[108] (nie były sprawdzane statystyki wyświetleń poszczególnych artykułów), ani nie prowadzono działań mających na celu ukierunkowanie zamieszczanych publikacji na konkretne grupy docelowe odbiorców[109].

Reasumując, w ocenie NIK, należy wskazać, że zarówno budowany przez KPRM scentralizowany model komunikacji, jak i modele rozproszone (stosowane przez NASK-PIB i Policję) nie zapewniły skutecznego informowania obywateli na temat zagrożeń cyberbezpieczeństwa oraz rekomendowanych środków ochrony. Zbadane podmioty nie prowadziły rzetelnej ewaluacji efektów swoich działań edukacyjnych i nie były w stanie udokumentować zasadności przyjęcia danego modelu komunikacyjnego. Skutkowało to również nieefektywnym wykorzystywaniem przez Ministra Cyfryzacji dużego potencjału merytorycznego nadzorowanej przez niego jednostki, tj. NASK-PIB.

5.4.1. Wyniki badania sondażowego opinii publicznej

W uzupełnieniu do zebranego w toku kontroli materiału dowodowego, NIK zleciła przeprowadzenie w pierwszym kwartale 2022 r. badania opinii publicznej na reprezentatywnej, ogólnopolskiej próbie 1000 pełnoletnich

[106] Opisany powyżej mechanizm wynikał z przepisów zarządzenia nr 1204 Komendanta Głównego Policji z dnia 12 listopada 2007 r. w sprawie form i metod działalności prasowo-informacyjnej w Policji (Dz. Urz. KGP z 2018 r. poz. 90), zgodnie z którym Komendant Główny Policji i komendanci wojewódzcy (Stołeczny) Policji byli upoważnieni do prowadzenia, za pośrednictwem rzeczników prasowych, oraz w zakresie swojej właściwości działalności prasowo-informacyjnej w Policji. W badanym okresie w KGP rozpoczęto prace legislacyjne nad nowelizacją powyższego zarządzenia, co powinno umożliwić powołanie rzecznika prasowego Komendanta CBZC oraz scentralizowanie polityki informacyjnej Policji dotyczącej cyberprzestępczości i cyberbezpieczeństwa.

[107] Ani BdWzC, ani Biuro Komunikacji Społecznej KGP.

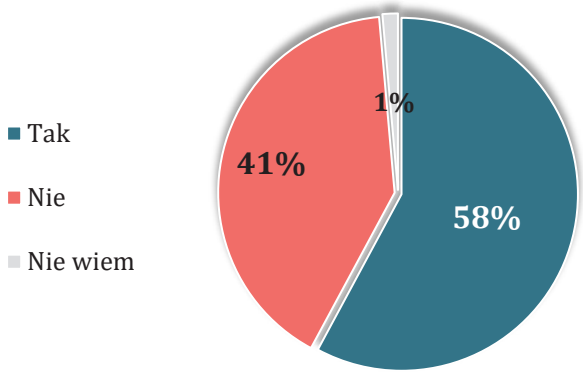
[108] Wśród zbadanych przez kontrolerów NIK 18 materiałów dotyczących cyberprzestępczości, opublikowanych na stronie głównej portalu Policja.pl, najrzadziej odwiedzany artykuł odnotował 493 unikalne odsłony, a najbardziej popularny 30 579 odsłon. Przykładowe materiały edukacyjne przygotowane przez KGP dotarły do następującej liczby użytkowników: „Kompendium – jak nie dać się oszukać w Internecie" – 9949 odsłon, „Ostrzeżenie przed próbą wyłudzenia danych" – 3608 odsłon, „Zamień swój dom w bezpieczną cybertwierdzę" – 7767 odsłon, „Uwaga na fałszywe strony udające pośredników szybkich płatności" – 21 782 odsłony. Filmy edukacyjne pn. „#Wspólnie bezpieczni" („Gdy oszukano Cię w Internecie, Co grozi za cyberprzestępstwo, Jak odzyskać skradzione pieniądze, Jak się chronić przed cyberatakami, Sukcesy w walce z cyberprzestępczością") miały łączną liczbę 11 641 odsłon. Mniejszą liczbę odsłon odnotowały materiały umieszczone w zakładkach lokalnych jednostek Policji. Wśród zbadanych 12 przykładowych artykułów dwa nie zanotowały ani jednej odsłony, dziewięć nie przekroczyło 250 odsłon, natomiast trzy miały odpowiednio 1486, 1812 i 2485 odsłon.

[109] Z nielicznymi wyjątkami, które stanowił np. materiał z okazji dnia babci i dziadka, skierowany do młodych ludzi będących wnuczkami.

mieszkańców Polski[110]. Celem badania było m.in. ustalenie deklarowanego przez respondentów stanu wiedzy na temat aktualnych zagrożeń występujących w cyberprzestrzeni oraz zweryfikowanie działań podejmowanych przez obywateli i właściwe organy państwa, w sytuacji faktycznego ataku przestępców komputerowych.

Przeprowadzone badanie wykazało, że 77% ankietowanych uważa, że przestępstwa internetowe stanowią dla nich realne zagrożenie, a sześciu na dziesięciu badanych użytkowników Internetu (58%) poszukuje informacji na temat niebezpieczeństw związanych z korzystaniem z sieci.

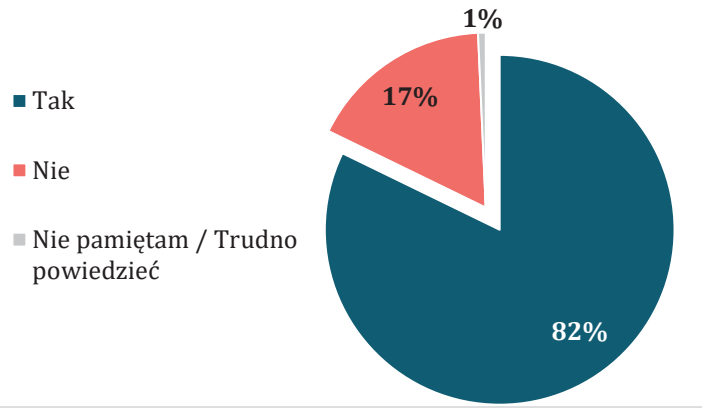
Q: Czy poszukuje lub zapoznaje się Pan/i z informacjami na temat niebezpieczeństw związanych z korzystaniem z Internetu? N=884[111]



Wysoki, deklarowany przez badanych poziom wiedzy na temat zagrożeń w Internecie oraz środków ochrony

Zdecydowana większość ankietowanych deklarowała wysoki poziom wiedzy na temat aktualnych zagrożeń występujących w Internecie oraz zasad bezpiecznego korzystania z sieci.

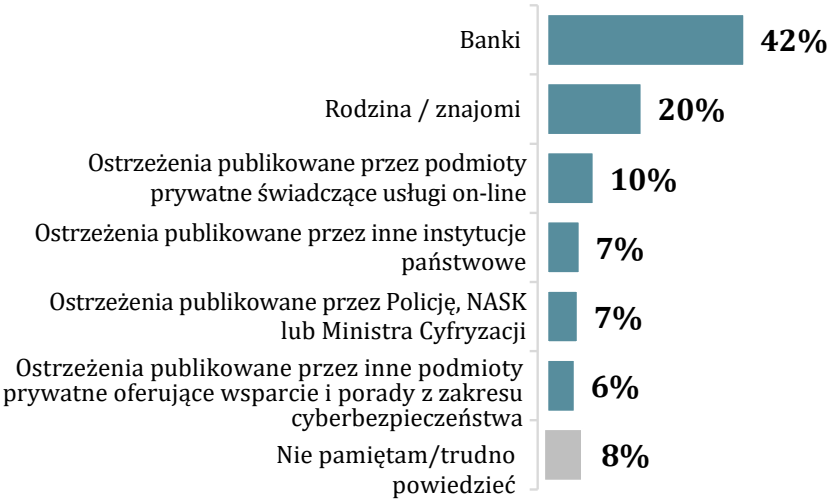
Q: Czy został(a) Pan(i) poinformowany(a) o podstawowych zasadach bezpiecznego korzystania z Internetu? (takich jak np.: zasady tworzenia bezpiecznych haseł, korzyści wynikające z instalacji programu antywirusowego, konieczność aktualizowania oprogramowania na komputerze i urządzeniach mobilnych, zasady bezpiecznego instalowania aplikacji mobilnych)? N=882



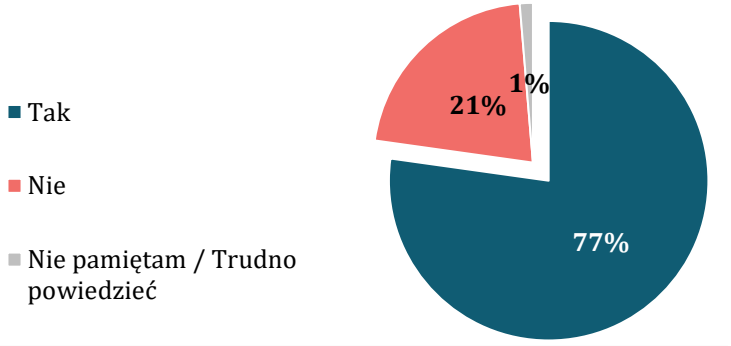
[110] Badanie przeprowadzono w okresie 20–28 kwietnia 2022 r. z wykorzystaniem metody telefonicznych, standaryzowanych wywiadów kwestionariuszowych wspomaganych komputerowo (CATI).

[111] Odpowiedzi 884 respondentów z 1000 (88%), tj. osób, które zadeklarowały korzystanie z Internetu.

Q: Przez kogo, jaką instytucję był/a Pan(i) ostrzegany(a) o aktualnych zagrożeniach i trwających kampaniach oszustów komputerowych? Odpowiedzi respondentów, którzy zostali poinformowani; N = 722

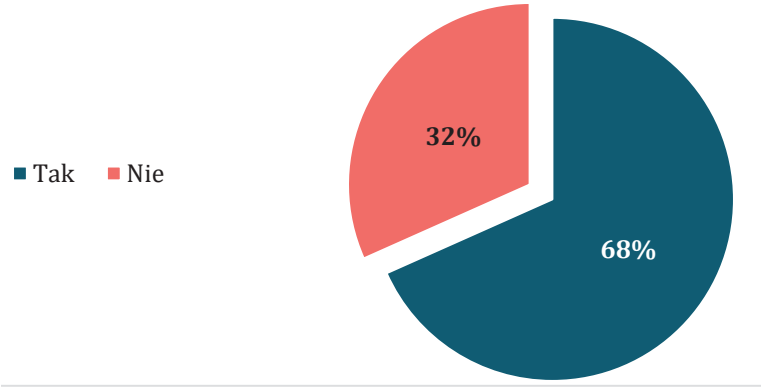


Q: Czy był(a) Pan(i) ostrzegany(a) o aktualnych zagrożeniach bezpieczeństwa w internecie, takich jak np. trwające kampanie, polegające na przesyłaniu smsów lub e-maili, których nadawcy podszywali się pod firmy kurierskie, czy też organy publiczne w celu wyłudzenia danych i kradzieży środków finansowych? N=879

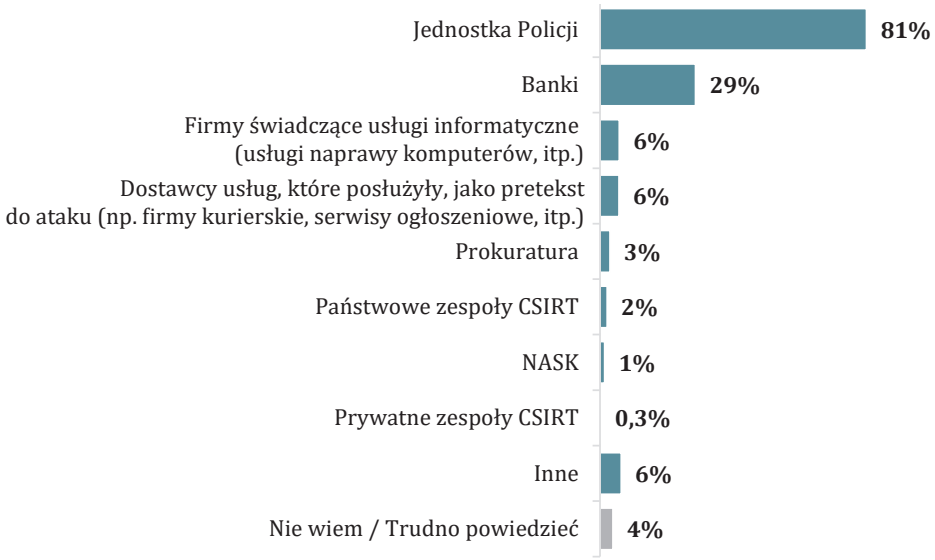


Większość badanych wskazywała także, że dysponują wiedzą, gdzie mogą szukać pomocy, w przypadku gdy staną się ofiarą ataku przestępców komputerowych. W praktyce jednak rozpoznawalność podmiotów świadczących wsparcie osobom fizycznym w sytuacji wystąpienia incydentów komputerowych była bardzo niska (NASK – 1%, państwowe zespoły CSIRT – 2%), a większość ankietowanych (81%) niejako automatycznie wskazywała na jednostki Policji, jako właściwe i kompetentne do udzielenia im pomocy.

Q: Czy potrafi Pan/i wymienić nazwy podmiotów, do których może się Pan/i zgłosić o wsparcie w przypadku, gdy stanie się Pan/i celem ataku przestępców internetowych? N=882

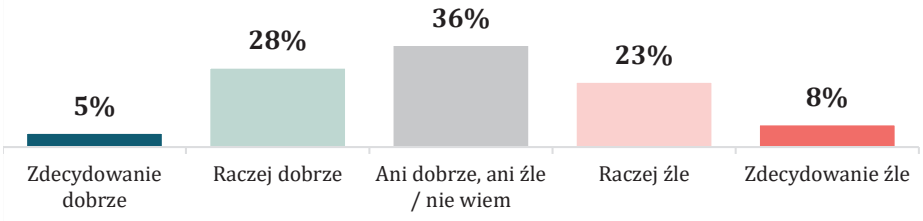


Q: Jeśli tak, to proszę wymienić nazwy tych podmiotów. N=603



Respondenci byli natomiast wyraźnie podzieleni w opiniach, jeżeli chodzi o ocenę działań państwa w zakresie informowania o zagrożeniach w sieci (odnotowano bardzo zbliżone odsetki not dobrych, złych i neutralnych).

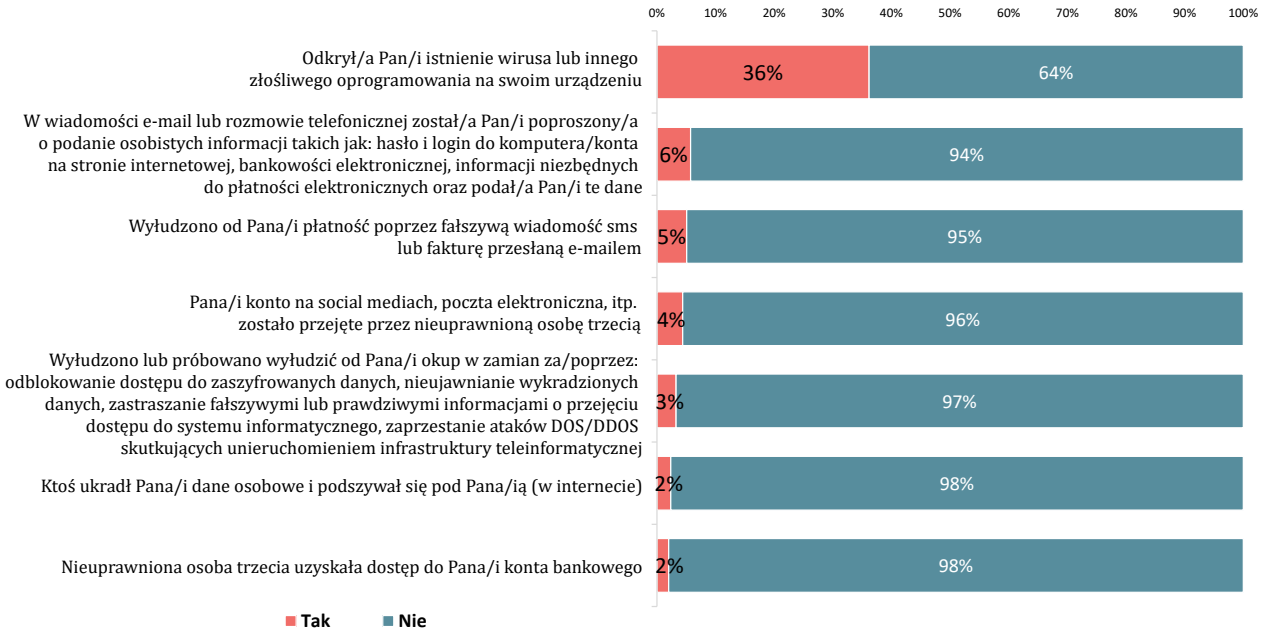
Q: Jak ocenia Pan/i działania państwa w zakresie informowania o zagrożeniach w Internecie? N=878



Przedstawione powyżej wyniki prezentujące stosunkowo pozytywną diagnozę stanu wiedzy obywateli w zakresie zagrożeń ze strony przestępczości internetowej należy poddać weryfikacji w kontekście wyników

dalszej części badania ankietowego, w toku którego odpowiedzi udzielały osoby faktycznie poszkodowane takimi przestępstwami. **Należy przy tym podkreślić, że spośród 884 badanych korzystających z Internetu, aż 404 respondentów padło ofiarą różnych form cyberataków, przy czym część z nich (21% ofiar) zostało poszkodowanych co najmniej dwukrotnie.**

Q: Czy kiedykolwiek doświadczył/a Pan/i następujących sytuacji:

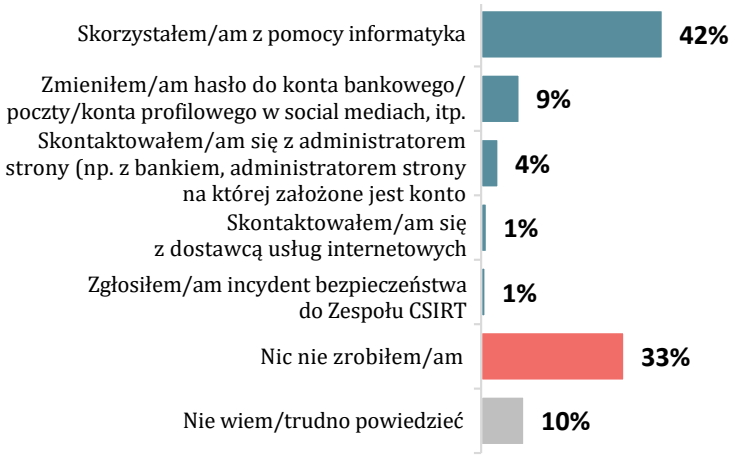


Brak wiedzy na temat adekwatnej reakcji na ataki przestępców komputerowych

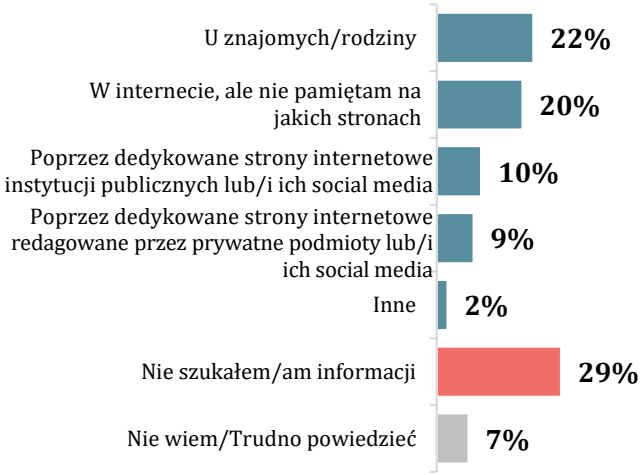
Szczegółowa analiza odpowiedzi udzielonych przez respondentów, którzy padli ofiarą ataków przestępców komputerowych wykazała, że w większości przypadków brak było z ich strony odpowiedniej reakcji na tego rodzaju zdarzenia. Nieliczni zdecydowali się zgłosić incydent na Policję, czy do zespołu CSIRT, a niektórzy nie podjęli wręcz żadnych działań (np. nie dokonali zmiany hasła do konta bankowego, czy konta w mediach społecznościowych). Powyższe uzasadniali m.in. brakiem wiedzy na temat możliwości zgłaszania tego rodzaju incydentów oraz niskim zaufaniem do skuteczności działań instytucji publicznych. Przykładowo:

Q: Czy kiedykolwiek odkrył/a Pan/i istnienie wirusa lub innego złośliwego oprogramowania na swoim urządzeniu?

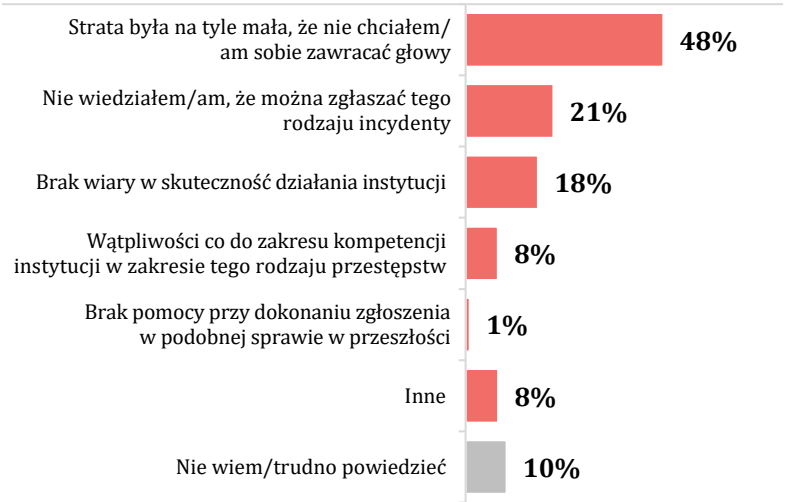
Q: Co zrobił/a Pan/i w tej sytuacji? N = 320[112]



Q: Gdzie szukał/a Pan/i informacji o możliwości podjęcia działań? N = 183[113]



Q: Dlaczego nie zawiadomił/a Pan/i właściwych organów lub instytucji? N=300[114]



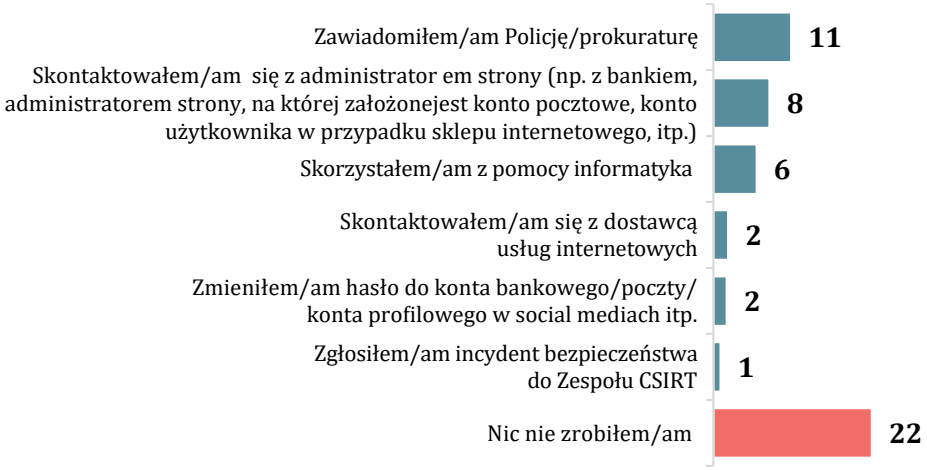
[112] Odpowiedzi respondentów, którzy doświadczyli określonej sytuacji.

[113] Odpowiedzi respondentów, którzy podjęli działania.

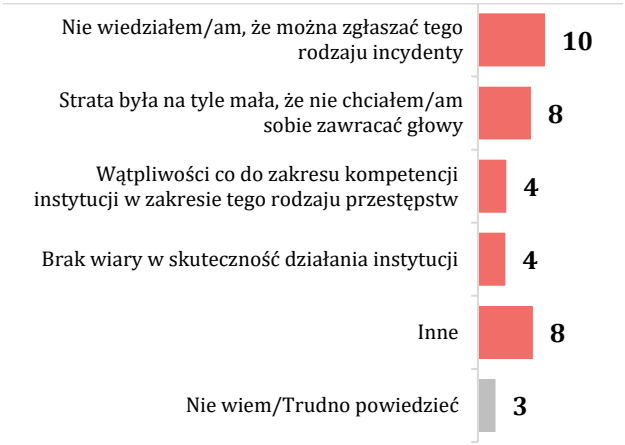
[114] Odpowiedzi respondentów, którzy nie zawiadomili właściwych organów.

Q: Czy kiedykolwiek w wiadomości e-mail lub rozmowie telefonicznej został/a Pan/i poproszony/a o podanie osobistych informacji takich jak: hasło i login do komputera/konta na stronie internetowej, bankowości elektronicznej, informacji niezbędnych do płatności elektronicznych oraz podał/a Pan/i te dane.

Q: Co zrobił/a Pan/i w tej sytuacji? N=51

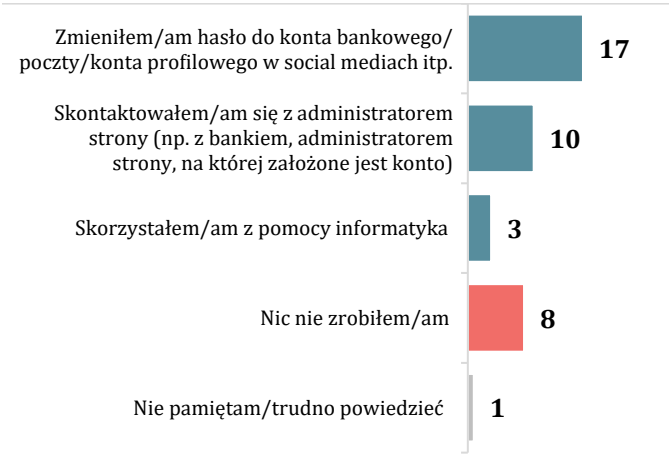


Q: Dlaczego nie zawiadomił/a Pan/i właściwych organów lub instytucji? N=30



Q: Czy kiedykolwiek Pana/i konto w social mediach, poczta elektroniczna, itp. zostało przejęte przez nieuprawnioną osobę trzecią?

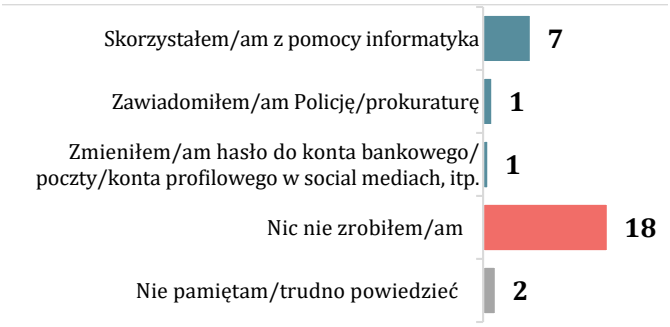
Q: Co zrobił/a Pan/i w tej sytuacji? N=39



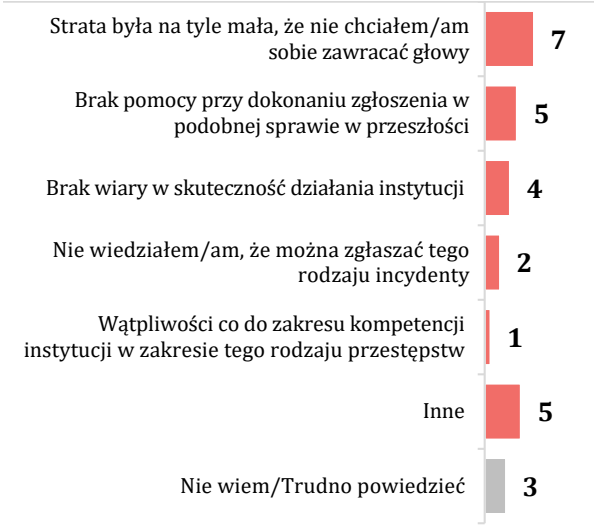
Q: Dlaczego nie zawiadomił/a Pan/i właściwych organów lub instytucji? N=29

Q: Czy kiedykolwiek wyłudzono lub próbowano wyłudzić od Pana/i okup w zamian za/poprzez: odblokowanie dostępu do zaszyfrowanych danych, nieujawnianie wykradzionych danych, zastraszanie fałszywymi lub prawdziwymi informacjami o przejęciu dostępu do systemu informatycznego, zaprzestanie ataków DOS/DDOS skutkujących unieruchomieniem infrastruktury teleinformatycznej?

Q: Co zrobił/a Pan/i w tej sytuacji? N=29

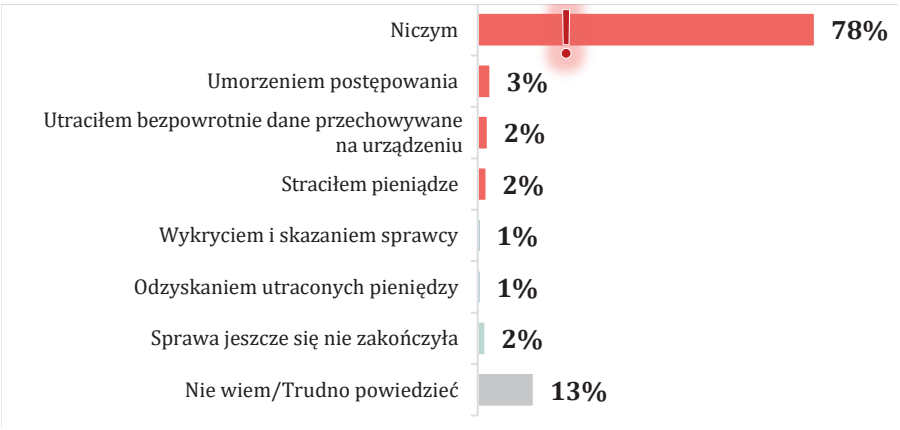


Q: Dlaczego nie zawiadomił/a Pan/i właściwych organów lub instytucji? N=27



Osoby, które padły ofiarą przestępców internetowych wskazały, że aż w 85% przypadków ich sprawy nie zostały wyjaśnione, zakończyły się umorzeniem lub utratą środków finansowych i danych. Z kolei tylko 2% spraw znalazło finał w postaci wykrycia i skazania sprawcy lub odzyskania straconych środków.

Q: Jak zakończyła się Pana/i sprawa? N=404



Przeprowadzone badanie sondażowe (w szczególności obserwowana bierność w sytuacji wystąpienia incydentów), potwierdziło w pełni ustalenia kontroli NIK wskazujące na brak skuteczności działań organów państwa w zakresie edukowania obywateli na temat cyberzagrożeń oraz zasad postępowania w sytuacji ataku przestępców komputerowych. Wykazało ono konieczność wypracowania efektywnego modelu komunikacji, a następnie zintensyfikowania prowadzonych działań informacyjno-edukacyjnych w zakresie cyberzagrożeń, w tym przestępczości internetowej.

5.5. Współpraca międzynarodowa

Inicjatywy międzynarodowe NASK-PIB i Policji

W okresie objętym kontrolą NASK-PIB współpracował z zagranicznymi organizacjami oraz brał udział w szeregu międzynarodowych przedsięwzięć dotyczących cyberbezpieczeństwa, i tak:

- realizował projekty UE organizowane przez ENISA – korzystając z pojedynczego hasła „e-Polak potrafi!", NASK stworzył tzw. kampanię parasolową, która skupiła szereg przedsięwzięć dotyczących upowszechniania bezpiecznego korzystania z cyberprzestrzeni. Pod wspólnym hasłem zrealizowano m.in. kampanie tematyczne „Nie zagub dziecka w sieci", „Bądź z innej bajki", „Seniorze spotkajmy się w sieci" oraz akcję „e-Senior potrafi!"[115];
- wziął udział w przedsięwzięciach edukacyjnych we współpracy z UNICEF Polska, Facebookiem oraz Komisją Europejską – w ten sposób zrealizował projekt „Przystań w sieci", a wraz z Fundacją „Dajemy Dzieciom Siłę" utworzył Polskie Centrum Programu Safer Internet;

[115] Opisane bardziej szczegółowo w pkt 5.4. informacji o wynikach kontroli.

- brał udział w organizacji „Szkoły Sieci Społecznościowych" – europejskiej inicjatywy non profit prowadzonej przez eduPad (europejską Inicjatywę Tworzenia Edukacyjnych Programów Antydyskryminacyjnych) w partnerstwie z European Schoolnet – celem projektu było przekazanie uczniom szkół podstawowych wiedzy na temat bezpiecznego i odpowiedzialnego korzystania z sieci społecznościowych;
- corocznie od 2013 r. koordynował w Polsce ogólnoeuropejską kampanię „Europejski Miesiąc Cyberbezpieczeństwa, organizowaną przez ENISA z inicjatywy Komisji Europejskiej. Celem kampanii była popularyzacja wiedzy, zwiększanie świadomości i upowszechnianie dobrych praktyk w obszarze cyberbezpieczeństwa wśród szerokiej grupy użytkowników Internetu, profesjonalistów oraz osób zajmujących się edukacją oraz profilaktyką dzieci i młodzieży. Przez cały październik we wszystkich krajach członkowskich organizowane są wydarzenia, które mają popularyzować wiedzę na temat bezpieczeństwa w sieci oraz nowoczesnych technologii.

Współpraca z instytucjami międzynarodowymi (Europol i ENISA) była również jednym z narzędzi wykorzystywanych przez jednostki organizacyjne Policji przy realizacji działań profilaktycznych i edukacyjnych w obszarze cyberbezpieczeństwa.

W latach objętych kontrolą BdWzC KGP uczestniczyło w międzynarodowej wymianie informacji pełniąc funkcję Krajowego Punktu Interpolu do walki z Cyberprzestępczością. Funkcjonariusze Biura brali również udział w pracach międzynarodowego stowarzyszenia *non-profit* ECTEG (Europejska Grupa ds. Szkolenia i Edukacji w zakresie Cyberprzestępczości) oraz uczestniczyli w laboratorium innowacyjności Europolu. Biuro zaangażowane było także w zainicjowane przez UE opracowanie przepisów unijnych dotyczących funkcjonowania Sztucznej Inteligencji.

6. ZAŁĄCZNIKI

6.1. Metodyka kontroli i informacje dodatkowe

Cel główny kontroli

Celem głównym kontroli było sprawdzenie, czy organy państwowe prowadzą adekwatne działania w celu identyfikowania, zapobiegania oraz ograniczania skutków przestępstw internetowych.

Cele szczegółowe

Założono, że badania kontrolne umożliwią udzielenie odpowiedzi na następujące pytania szczegółowe:

1. Czy został wdrożony skuteczny system zapobiegania i minimalizowania skutków przestępstw internetowych?
2. Czy objęte kontrolą podmioty są właściwie przygotowane kadrowo, logistycznie oraz organizacyjne do zapobiegania i zwalczania skutków przestępstw internetowych, ze szczególnym uwzględnieniem kradzieży tożsamości?
3. Czy objęte kontrolą podmioty formułowały, wynikające z prowadzonej analizy ryzyka, wytyczne oraz rekomendacje podnoszące poziom bezpieczeństwa użytkowników Internetu?
4. Czy zostały opracowane, podane do publicznej wiadomości i były stosowane w praktyce procedury zgłaszania przestępstw internetowych i reagowania na tego rodzaju zdarzenia?
5. Czy były prowadzone skuteczne działania zwiększające wiedzę obywateli (użytkowników Internetu) na temat przestępstw internetowych oraz sposobów zapobiegania takim zdarzeniom?
6. Czy objęte kontrolą podmioty współpracują z organizacjami międzynarodowymi oraz innymi uznanymi instytucjami zagranicznymi i krajowymi w ramach zapobiegania i zwalczania skutków przestępstw internetowych, w tym kradzieży tożsamości?

Zakres podmiotowy

Kontrolą zostały objęte trzy podmioty: Kancelaria Prezesa Rady Ministrów (jako jednostka obsługująca ministra właściwego do spraw informatyzacji oraz jednostka obsługująca Pełnomocnika Rządu do Spraw Cyberbezpieczeństwa), Komenda Główna Policji oraz Naukowa i Akademicka Sieć Komputerowa – Państwowy Instytut Badawczy.

Kryteria kontroli

Podstawą prawną podjęcia kontroli był art. 2 ust. 1 ustawy o NIK. Kontrola została przeprowadzona z uwzględnieniem kryteriów określonych w art. 5 ust. 1 tej ustawy, tj. legalności, gospodarności, celowości i rzetelności.

Okres objęty kontrolą

Kontrolą objęto lata 2019-2021. Czynności kontrolne przeprowadzono w okresie od dnia 15 listopada 2021 r. do dnia 27 kwietnia 2022 r.

Pozostałe informacje

Wyniki kontroli przedstawiono w czterech wystąpieniach pokontrolnych (skierowanych do Ministra Cyfryzacji, Pełnomocnika Rządu, Komendanta Głównego Policji oraz Dyrektora NASK-PIB), w których sformułowano ogółem osiem wniosków pokontrolnych dotyczących w szczególności: dokonania modyfikacji Strategii Cyberbezpieczeństwa RP; wypracowania i wdrożenia jednolitych założeń stosowanego modelu edukowania oraz ostrzegania obywateli na temat zagrożeń cyberbezpieczeństwa; przeprowadzania cyklicznej ewaluacji wykorzystania Algorytmów w terenowych jednostkach Policji, tak aby możliwe było usprawnianie procesu przyjmowania zgłoszeń ws. przestępstw internetowych.

W dniu 17 maja 2022 r. Pełnomocnik Rządu do Spraw Cyberbezpieczeństwa złożył pięć zastrzeżeń do skierowanego do niego wystąpienia pokontrolnego NIK z dnia 27 kwietnia 2022 r. odnoszących się do ocen jego działalności oraz stwierdzonych nieprawidłowości. Uchwałą Nr 48/2022 z dnia 28 września 2022 r., Kolegium Najwyższej Izby Kontroli oddaliło zastrzeżenia zgłoszone przez Pełnomocnika Rządu odnośnie wyrażonej w wystąpieniu pokontrolnym oceny ogólnej kontrolowanej działalności oraz nieprawidłowości dotyczącej nierzetelnej realizacji przez Pełnomocnika zadań związanych z koordynowaniem działań w zakresie zapewnienia cyberbezpieczeństwa RP, w istotnym obszarze tego bezpieczeństwa obejmującym ochronę obywateli przed przestępczością internetową. Kolegium uwzględniło w części zastrzeżenia odnoszące się do oceny cząstkowej obszaru „Przygotowanie kadrowe i organizacyjne do zapobiegania oraz zwalczania skutków przestępstw internetowych" oraz nieprawidłowości, w której oceniono jako nierzetelne i nieskuteczne działania Pełnomocnika służące edukowaniu obywateli na temat zagrożeń ze strony przestępczości internetowej. Kolegium uwzględniło również w całości zastrzeżenie dotyczące uwagi wskazującej na zasadność uwzględnienia w przepisach ustawy o KSC tematyki bezpieczeństwa indywidualnych użytkowników cyberprzestrzeni, wskazując w szczególności, że jest to zadanie Ministra Cyfryzacji.

W uzupełnieniu do zebranego w toku kontroli materiału dowodowego, NIK zleciła przeprowadzenie badania opinii publicznej na reprezentatywnej, ogólnopolskiej próbie 1000 pełnoletnich mieszkańców Polski. Badanie przeprowadzono w okresie 20–28 kwietnia 2022 r. z wykorzystaniem metody telefonicznych, standaryzowanych wywiadów kwestionariuszowych wspomaganych komputerowo (CATI). Celem badania było m.in. ustalenie deklarowanego przez respondentów stanu wiedzy na temat aktualnych zagrożeń występujących w cyberprzestrzeni oraz zweryfikowanie działań podejmowanych przez obywateli i właściwe organy państwa, w sytuacji faktycznego ataku przestępców komputerowych.

W kontroli uczestniczył Departament Porządku i Bezpieczeństwa Wewnętrznego NIK.

Wykaz jednostek kontrolowanych

L.p.	Jednostka organizacyjna NIK przeprowadzająca kontrolę	Nazwa jednostki kontrolowanej	Imię i nazwisko kierownika jednostki kontrolowanej
1.	Departament Porządku i Bezpieczeństwa Wewnętrznego	Kancelaria Prezesa Rady Ministrów	Mateusz Morawiecki, Marek Zagórski, (Minister Cyfryzacji)
2.		Kancelaria Prezesa Rady Ministrów	Janusz Cieszyński, Marek Zagórski, Karol Okoński (Pełnomocnik Rządu do Spraw Cyberbezpieczeństwa)
3.		Komenda Główna Policji	Gen. insp. Jarosław Szymczyk
4.		Naukowa i Akademicka Sieć Komputerowa – Państwowy Instytut Badawczy	Wojciech Pawlak, Kamil Sitarski, Jacek Leśkow, Krzysztof Silicki

Wykaz głównych ustaleń w kontrolowanych jednostkach

Lp.	Nazwa jednostki kontrolowanej	Stany mające wpływ na wydaną ocenę:	
		prawidłowe	nieprawidłowe
1.	Kancelaria Prezesa Rady Ministrów	prowadzenie bieżącej analizy zagrożeń w cyberprzestrzeni	brak reakcji na identyfikowane ryzyka wskazujące na dominujące zagrożenia dla indywidualnych użytkowników Internetu, nieskuteczne działania edukacyjne z zakresu cyberbezpieczeństwa kierowane do obywateli
2.	Komenda Główna Policji	prowadzenie regularnej analizy zagrożeń ze strony przestępstw internetowych, reagowanie na ryzyka oraz opracowanie koncepcji utworzenia CBZC	doraźne i rozproszone działania edukacyjne z zakresu cyberbezpieczeństwa
3.	Naukowa i Akademicka Sieć Komputerowa – Państwowy Instytut Badawczy	prowadzenie regularnej analizy zagrożeń w cyberprzestrzeni oraz reagowanie na identyfikowane ryzyka	doraźne i rozproszone działania edukacyjne z zakresu cyberbezpieczeństwa

6.2. Analiza stanu prawnego i uwarunkowań organizacyjno-ekonomicznych

Zgodnie z rozporządzeniem Prezesa Rady Ministrów z dnia 6 października 2020 r. w sprawie szczegółowego zakresu działania Ministra Cyfryzacji[116], **Minister Cyfryzacji** kieruje działem administracji rządowej – informatyzacja, który obejmuje m.in. sprawy z zakresu ochrony danych osobowych, bezpieczeństwa cyberprzestrzeni w wymiarze cywilnym oraz identyfikacji elektronicznej[117]. Ponadto, na podstawie art. 45 ust. 1 pkt 4 ustawy o krajowym systemie cyberbezpieczeństwa **minister właściwy do spraw informatyzacji** odpowiada za prowadzenie działań informacyjnych dotyczących dobrych praktyk, programów edukacyjnych, kampanii i szkoleń na rzecz poszerzania wiedzy i budowania świadomości z zakresu cyberbezpieczeństwa, w tym bezpiecznego korzystania z Internetu przez różne kategorie użytkowników.

Funkcję Ministra Cyfryzacji pełni obecnie Prezes Rady Ministrów, a obsługę Ministra zapewnia Kancelaria Prezesa Rady Ministrów[118].

Na podstawie art. 61 ustawy o krajowym systemie cyberbezpieczeństwa powołany został **Pełnomocnik Rządu do Spraw Cyberbezpieczeństwa,** który analogicznie jak Minister Cyfryzacji, jest obsługiwany przez KPRM[119]. Pełnomocnik koordynuje działania i realizuje politykę rządu w zakresie zapewnienia cyberbezpieczeństwa w Rzeczypospolitej Polskiej (art. 60 ww. ustawy), a do jego zadań należy (art. 62 ust. 1 pkt 1–6):

- analiza i ocena funkcjonowania krajowego systemu cyberbezpieczeństwa na podstawie zagregowanych danych i wskaźników opracowanych z udziałem organów administracji publicznej, organów właściwych do spraw cyberbezpieczeństwa, CSIRT MON, CSIRT NASK i CSIRT GOV;
- nadzór nad procesem zarządzania ryzykiem krajowego systemu cyberbezpieczeństwa z wykorzystaniem zagregowanych danych i wskaźników opracowanych z udziałem organów właściwych do spraw cyberbezpieczeństwa, CSIRT MON, CSIRT NASK i CSIRT GOV;
- opiniowanie dokumentów rządowych, w tym projektów aktów prawnych, mających wpływ na realizację zadań z zakresu cyberbezpieczeństwa;
- upowszechnianie nowych rozwiązań i inicjowanie działań w zakresie zapewnienia cyberbezpieczeństwa na poziomie krajowym;
- inicjowanie krajowych ćwiczeń w zakresie cyberbezpieczeństwa;
- wydawanie rekomendacji dotyczących stosowania urządzeń informatycznych lub oprogramowania na wniosek CSIRT.

[116] Dz. U. poz. 1716.

[117] Art. 12a ust. 1 pkt 8, 10 i 13a ustawy z dnia 4 września 1997 r. o działach administracji rządowej (Dz. U. z 2021 r. poz. 1893, ze zm.).

[118] § 1 ust. 4 rozporządzenia w sprawie szczegółowego zakresu działania Ministra Cyfryzacji.

[119] § 8 ust. 1 pkt 6 i 13 zarządzenia Nr 2 Prezesa Rady Ministrów z dnia 5 stycznia 2016 r. w sprawie nadania statutu Kancelarii Prezesa Rady Ministrów (M. P. z 2022 r. poz. 871, ze zm.) oraz § 31 i § 38 zarządzenia Nr 8 Szefa Kancelarii Prezesa Rady Ministrów z dnia 4 kwietnia 2022 r. w sprawie nadania Regulaminu organizacyjnego Kancelarii Prezesa Rady Ministrów.

Do zadań Pełnomocnika wykonywanych w porozumieniu z właściwymi ministrami należy również:

- współpraca w sprawach związanych z cyberbezpieczeństwem z innymi państwami, organizacjami oraz instytucjami międzynarodowymi;
- podejmowanie działań mających na celu wspieranie badań naukowych i rozwój technologii z zakresu cyberbezpieczeństwa;
- podejmowanie działań mających na celu podnoszenie świadomości społeczeństwa w zakresie zagrożeń cyberbezpieczeństwa i bezpiecznego korzystania z Internetu (art. 62 ust. 2 pkt 1–3 ustawy o krajowym systemie cyberbezpieczeństwa).

Naukowa i Akademicka Sieć Komputerowa – Państwowy Instytut Badawczy jest podmiotem działającym na podstawie ustawy z dnia 30 kwietnia 2010 r. o instytutach badawczych[120]. Do zadań Instytutu, wykonywanych w sposób ciągły, szczególnie ważnych dla planowania i realizacji polityki państwa, których realizacja jest niezbędna do zapewnienia bezpieczeństwa publicznego należą m.in.

- realizacja zadań ustawowych przewidzianych dla NASK w ramach krajowego systemu cyberbezpieczeństwa;
- podejmowanie i wspieranie działań na rzecz rozwoju społeczeństwa informacyjnego i prowadzenie badań nad bezpieczeństwem korzystania z sieci komputerowych, szczególnie przez dzieci[121].

W ramach NASK funkcjonuje **CSIRT NASK**, którego obowiązki, zgodnie z art. 26 ustawy o krajowym systemie cyberbezpieczeństwa, obejmują m.in.:

- monitorowanie zagrożeń cyberbezpieczeństwa i incydentów na poziomie krajowym;
- szacowanie ryzyka związanego z ujawnionym zagrożeniem cyberbezpieczeństwa oraz zaistniałymi incydentami, w tym prowadzenie dynamicznej analizy ryzyka;
- przekazywanie informacji dotyczących incydentów i ryzyk podmiotom krajowego systemu cyberbezpieczeństwa;
- wydawanie komunikatów o zidentyfikowanych zagrożeniach cyberbezpieczeństwa;
- reagowanie na zgłoszone incydenty;
- koordynacja obsługi incydentów zgłaszanych przez osoby fizyczne, przy czym zgłoszenia pochodzące m.in. od osób fizycznych, mogą zostać rozpatrzone, gdy nie stanowi to nieproporcjonalnego czy nadmiernego obciążenia dla CSIRT NASK (art. 30 ust. 3 ustawy o krajowym systemie cyberbezpieczeństwa).

Organem sprawującym nadzór nad NASK jest minister właściwy do spraw informatyzacji.

Kluczowe zadania w obszarze przestępczości internetowej są również przypisane **Policji**. Ustawą z dnia 17 grudnia 2021 r. o zmianie niektórych

[120] Dz. U. z 2022 r. poz. 498.

[121] § 6 ust. 3 pkt 1 lit. b) oraz § 6 ust. 3 pkt 4 załącznika do decyzji nr 21 Ministra Cyfryzacji z dnia 21 maja 2018 r. w sprawie zatwierdzenia statutu Naukowej i Akademickiej Sieci Komputerowej – Państwowego Instytutu Badawczego (Dz. Urz. MC, poz. 13, ze zm.).

ustaw w związku z powołaniem Centralnego Biura Zwalczania Cyberprzestępczości[122] zmieniono m.in. ustawę z dnia 6 kwietnia 1990 r. o Policji[123] i powołano nową jednostkę organizacyjną Policji do spraw zwalczania cyberprzestępczości. Zgodnie z art. 5d ust. 1 pkt 1 i 2 ustawy o Policji Centralne Biuro Zwalczania Cyberprzestępczości jest jednostką organizacyjną Policji służby zwalczania cyberprzestępczości, odpowiedzialną za realizację na obszarze całego kraju zadań w zakresie:

- rozpoznawania i zwalczania przestępstw popełnionych przy użyciu systemu informatycznego, systemu teleinformatycznego lub sieci teleinformatycznej oraz zapobiegania tym przestępstwom, a także wykrywania i ścigania sprawców tych przestępstw;
- wspierania w niezbędnym zakresie jednostek organizacyjnych Policji w rozpoznawaniu, zapobieganiu i zwalczaniu przestępstw, o których mowa powyżej, a także wykrywaniu i ściganiu sprawców tych przestępstw.

Jak wskazano już wcześniej, **na gruncie polskiego kodeksu karnego brak jest legalnej definicji takich pojęć, jak: przestępczość komputerowa, przestępczość internetowa czy cyberprzestępczość.** Na potrzeby niniejszej kontroli przyjęto definicję, że „przestępstwa internetowe" to grupa czynów zabronionych polegających na posługiwaniu się elektronicznymi systemami przetwarzania informacji do naruszania dóbr prawnych chronionych przez prawo karne. Co istotne, przestępstwa takie przebiegają zasadniczo w środowisku cyberprzestrzeni i nie stanowią wyłącznie elementu klasycznego oszustwa, gdzie użycie cyberprzestrzeni jest jedynie uzupełnieniem głównej przestępczej kombinacji. Przykładami tego rodzaju przestępstw są w szczególności:

- kradzież tożsamości (art. 190a § 2 kk.),
- hacking (art. 267 § 1 oraz § 2 kk.),
- nielegalne przechwytywanie informacji (art. 267 § 3 kk.),
- ujawnienie nielegalnie uzyskanej informacji (art. 267 § 4 kk.),
- ingerencja w dane i system (art. 268a kk.),
- zakłócenie dostępu do informacji (art. 268 kk.),
- sabotaż informatyczny (art. 269 § 1 i § 2 kk.),
- wytwarzanie i obrót narzędziami hackerskimi (art. 269b kk.),
- oszustwo komputerowe (art. 287 kk.).

[122] Dz. U. poz. 2447.

[123] Dz. U. z 2021 r. poz. 1882, ze zm.

6.3. Wykaz aktów prawnych dotyczących kontrolowanej działalności

1. Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. z 2022 r. poz. 1863).
2. Ustawa z dnia 4 września 1997 r. o działach administracji rządowej (Dz. U. z 2021 r. poz. 1893, ze zm.).
3. Ustawa z dnia 30 kwietnia 2010 r. o instytutach badawczych (Dz. U. z 2022 r. poz. 498).
4. Ustawa z dnia 6 czerwca 1997 r. Kodeks karny (Dz. U. z 2022 r. poz. 1138, ze zm.).
5. Ustawa z dnia 6 kwietnia 1990 r. o Policji (Dz. U. z 2021 r. poz. 1882, ze zm.).
6. Ustawa z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym (Dz. U. z 2022 r. poz. 261, ze zm.).
7. Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii (Dz. Urz. UE L 194 z 19.07.2016, str. 1).
8. Rozporządzenie Prezesa Rady Ministrów z dnia 6 października 2020 r. w sprawie szczegółowego zakresu działania Ministra Cyfryzacji (Dz. U. poz. 1716.).
9. Uchwała nr 125 Rady Ministrów z dnia 22 października 2019 r. w sprawie Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019-2024 (M. P. poz. 1037).
10. Zarządzenie Nr 2 Prezesa Rady Ministrów z dnia 5 stycznia 2016 r. w sprawie nadania statutu Kancelarii Prezesa Rady Ministrów (M. P. z 2022 r. poz. 871, ze zm.).
11. Zarządzenie Nr 8 Szefa Kancelarii Prezesa Rady Ministrów z dnia 4 kwietnia 2022 r. w sprawie nadania Regulaminu organizacyjnego Kancelarii Prezesa Rady Ministrów.
12. Decyzja nr 21 Ministra Cyfryzacji z dnia 21 maja 2018 r. w sprawie zatwierdzenia statutu Naukowej i Akademickiej Sieci Komputerowej – Państwowego Instytutu Badawczego (Dz. Urz. MC, poz. 13, ze zm.).

6.4. Wykaz podmiotów, którym przekazano informację o wynikach kontroli

1. Prezydent Rzeczypospolitej Polskiej
2. Marszałek Sejmu Rzeczypospolitej Polskiej
3. Marszałek Senatu Rzeczypospolitej Polskiej
4. Prezes Rady Ministrów
5. Prezes Trybunału Konstytucyjnego
6. Rzecznik Praw Obywatelskich
7. Przewodniczący Sejmowej Komisji do Spraw Kontroli Państwowej
8. Przewodniczący Sejmowej Komisji Cyfryzacji, Innowacyjności i Nowoczesnych Technologii
9. Przewodniczący Sejmowej Komisji Sprawiedliwości i Praw Człowieka
10. Komendant Główny Policji
11. Pełnomocnik Rządu do Spraw Cyberbezpieczeństwa

6.5. Stanowisko Ministra do informacji o wynikach kontroli

Minister Cyfryzacji

Mateusz Morawiecki

Znak pisma DC.WFKSC.1781.1.2022
Warszawa, 16.12.2022

Pan
Marian Banaś
Prezes Najwyższej Izby Kontroli

Szanowny Panie Prezesie,

w związku z przekazaniem Informacji o wynikach kontroli Najwyższej Izby Kontroli nr P/21/042 „Działania państwa w zakresie zapobiegania i zwalczania skutków wybranych przestępstw internetowych, w tym kradzieży tożsamości" (pismo znak: KPB.430.010.2022), działając na podstawie *art. 64 ust. 2 ustawy o Najwyższej Izbie Kontroli*[1], przedstawiam stanowisko Ministra Cyfryzacji do treści przedstawionej informacji. Tożsame stanowisko w sprawie prezentuję również jako Pełnomocnik Rządu do Spraw Cyberbezpieczeństwa.

Celem *ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa*[2] (dalej: ustawa o KSC) jest zapewnienie cyberbezpieczeństwa na poziomie krajowym, w tym niezakłóconego świadczenia usług kluczowych i usług cyfrowych oraz osiągnięcie odpowiednio wysokiego poziomu bezpieczeństwa systemów teleinformatycznych służących do świadczenia tych usług, nie zaś ochrona pojedynczych użytkowników Internetu. W związku z powyższym, zakres podmiotowy krajowego systemu cyberbezpieczeństwa został również powiązany z podziałem na sektory i podsektory, które odgrywają kluczową rolę dla bezpieczeństwa oraz gospodarki Państwa.

Ponadto ustawa o KSC w zakresie swojej regulacji implementuje Dyrektywę NIS[3], której celem jest osiągnięcie wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych w Unii, a w konsekwencji – niezakłócone świadczenie usług kluczowych z punktu widzenia państwa i gospodarki, jak również usług cyfrowych. Dyrektywa NIS odnosi się do osób fizycznych jedynie w zakresie zapewnienia im dostępu do kluczowych usług oraz do zabezpieczenia danych tych osób niezbędnych do świadczenia ww. usług.

Odnosząc się do wniosku w przedmiocie przygotowania i przedstawienia Radzie Ministrów projektów modyfikacji Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019-2024

[1] t.j. Dz.U. z 2022 r. poz. 623.
[2] t.j. Dz.U. z 2022 r. poz. 1863.
[3] Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 z dnia 6 lipca 2016 r. w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii (Dz. U. UE L Nr 194).

telefon +48 22 245 59 22
adres email: sekretariat.dc@mc.gov.pl
strona www: www.gov.pl/web/cyfryzacja

adres korespondencyjny:
00-060 Warszawa
ul. Królewska 27

(dalej: Strategia) oraz Planu działań na rzecz wdrożenia Strategii Cyberbezpieczeństwa[4] pragnę poinformować, że ww. działanie zostanie wzięte pod uwagę w trakcie trwającego procesu przeglądu Strategii.

W zakresie sformułowanych wniosków dotyczących działań edukacyjnych pragnę zwrócić uwagę, że w celu ujednolicenia edukacji o cyberbezpieczeństwie, we współpracy z Naukową i Akademicką Siecią Komputerową – Państwowym Instytutem Badawczym (NASK-PIB) opracowano narzędzia wspomagające edukację w ww. obszarze. Efekty tych prac zostały opublikowane w bazie wiedzy Cyberbezpieczeństwa na portalu gov.pl w zakładce CyberEdukacja[5]. Dostępne są tam materiały utworzone w ramach projektów Bezpieczni w Sieci[6] oraz CYBER lekcje[7], które mają na celu wsparcie kadry pedagogicznej w nauczaniu o cyberbezpieczeństwie. Celem obu projektów jest wyposażenie pedagogów i uczniów w kompetencje z zakresu cyberbezpieczeństwa. Projekt Bezpieczni w Sieci jest adresowany do uczniów klas 7-8 szkół podstawowych oraz szkół ponadpodstawowych i ich nauczycieli, w ramach którego za pośrednictwem platformy e-learningowej można przeprowadzać kompleksowe lekcje z obszaru cyberbezpieczeństwa. Celem ww. projektu jest wspieranie pedagogów i młodzieży w podnoszeniu kompetencji cyfrowych z zakresu cyberbezpieczeństwa. Natomiast projekt CYBER Lekcje to gotowe scenariusze zajęć, prezentacje, infografiki oraz krótkie filmy edukacyjne, które można łatwo pobrać z sieci i wykorzystywać w ramach różnych zajęć edukacyjnych na różnych etapach edukacji. Przygotowane scenariusze pomagają pedagogom usystematyzować wiedzę z zakresu cyberbezpieczeństwa, a także umożliwiają przeprowadzenie lekcji na temat właściwego korzystania z nowych technologii.

W ramach ewaluacji efektów prowadzonych działań edukacyjnych z zakresu cyberbezpieczeństwa, co kwartał monitorowana jest liczba wejść na poszczególne strony bazy wiedzy o cyberbezpieczeństwie. Wdrożono również narzędzia badające odbiór bazy wiedzy przez jej użytkowników oraz oczekiwania co do jej zawartości i funkcjonalności. Ankieta badawcza dostępna jest w bazie wiedzy w zakładce aktualności https://www.gov.pl/web/baza-wiedzy/ankieta-ewaluacyjna-bazy-wiedzy-cyberbezpieczenstwaa. Podsumowanie wyników badania przeprowadzono po zakończeniu trzeciego kwartału br., kolejne podsumowanie zostanie przeprowadzone po zakończeniu czwartego kwartału br. Do udziału w badaniu zachęcamy poprzez publikację artykułów, dystrybucję ankiety do subskrybentów informacji z obszaru cyberbezpieczeństwa oraz w ramach organizowanych przez Cyfryzację KPRM szkoleń dla podmiotów krajowego systemu cyberbezpieczeństwa.

Ustosunkowując się do ważniejszych wyników kontroli względem systemu S46 należy zauważyć, że kontrola prowadzona była na przełomie lat 2021 – 2022. W roku 2021 System S46 był już systemem operacyjnym, jednak proces dochodzenia do jego pełnej funkcjonalności tj. takiej, w której będzie przedstawiał pełen obraz stanu cyberbezpieczeństwa kraju, jest procesem długotrwałym. Osiągnięcie zadawalającego stanu wykorzystania systemu S46 wymaga podjęcia

[4] uwzględniających wyniki analizy ryzyka wskazujące na dominującą skalę zagrożeń ze strony oszustw komputerowych oraz zdefiniowane, porównywalne mierniki stopnia realizacji zadań służących zapobieganiu i minimalizowaniu skutków tego rodzaju zagrożeń – Informacja o wynikach kontroli, wniosek nr 2, str. 13.
[5] https://www.gov.pl/web/baza-wiedzy/cyberedukacja.
[6] https://www.gov.pl/web/baza-wiedzy/bezpieczni-w-sieci.
[7] https://www.gov.pl/web/baza-wiedzy/materialy-do-cyberlekcji.

telefon +48 22 245 59 22
adres email: sekretariat.dc@mc.gov.pl
strona www: www.gov.pl/web/cyfryzacja

adres korespondencyjny:
00-060 Warszawa
ul. Królewska 27

wielu działań formalno-prawnych
i organizacyjno-technicznych, a także woli podmiotów krajowego systemu cyberbezpieczeństwa do podłączenia się do tego systemu. Przyjmując ze zrozumieniem ocenę kontroli NIK względem Systemu S46, Minister Cyfryzacji, wraz nadzorowanym NASK-PIB podjął następujące działania mające na celu uzyskanie użyteczności systemu S46:

- Prowadzona jest akcja informacyjna zachęcająca podmioty krajowego systemu cyberbezpieczeństwa do podłączenia się do systemu, ze wskazaniem korzyści, które płyną dla tych podmiotów oraz korzyści dla sprawnego zarządzania cyberbezpieczeństwem w skali kraju;
- Rozpoczęto poszukiwanie poza częścią 27 budżetu państwa środków na finansowanie podłączeń podmiotów krajowego systemu cyberbezpieczeństwa, co poskutkowało uzyskaniem tych środków w ramach programu REACT EU[8]. Dodam, że z tych środków planowane jest w ramach projektu S46-REACT podłączenie do systemu 100 podmiotów;
- Kontynuowane jest podłączanie podmiotów krajowego systemu cyberbezpieczeństwa ze środków dotacji celowej Ministra Cyfryzacji dla NASK-PIB na rozwój i utrzymanie systemu;
- Dokonano ewaluacji funkcjonalności systemu i zawartości informacji dostępnych w tym systemie i na tej podstawie nakreślono kierunek w jakim powinny pójść zmiany:
  - ✓ przekazywanie do CSIRT-ów poziomu krajowego (CSIRT GOV, MON, NASK) informacji o wszelkich incydentach w zakresie cyberbezpieczeństwa, a nie tylko informacji o incydentach istotnych i poważnych, mających miejsce w systemach operatorów usług kluczowych i dostawców usług cyfrowych, w tym zintegrowanie z systemem S46 systemów zgłoszeń (tzw. systemów ticketowych) działających w CSIRT, udostępnianych podmiotom krajowego systemu cyberbezpieczeństwa niepodłączonych do S46;
  - ✓ zwiększenie dostępności dla podmiotów krajowego systemu cyberbezpieczeństwa do informacji o podatnościach i sposobach ich mitygowania;
  - ✓ utworzenie w systemie S46 roli analityka, pozwalającej na integrowanie informacji o stanie bezpieczeństwa pochodzących z poszczególnych CSIRT-ów na poziomie zespołu analitycznego przygotowującego informacje o stanie cyberbezpieczeństwa dla Pełnomocnika Rządu do Spraw Cyberbezpieczeństwa.
  - ✓ przygotowano monitoring wykorzystania systemu przez podmioty krajowego systemu cyberbezpieczeństwa, co pozwoli na rzetelną ocenę jego wykorzystania.

Dodam również, że w art. 10 uzgodnionego tekstu Dyrektywy NIS 2[9] zostało wskazane, że każde państwo członkowskie ma zapewnić, aby każdy CSIRT miał do dyspozycji odpowiednią, bezpieczną i odporną infrastrukturę komunikacyjno-informacyjną do wymiany informacji z podmiotami krajowego systemu cyberbezpieczeństwa. Należy więc wskazać, że system S46 spełnia ten wymóg.

[8] REACT-EU (*Recovery Assistance for Cohesion and the Territories of Europe*) to plan Komisji Europejskiej w celu ograniczenia społecznych i gospodarczych skutków pandemii COVID-19.
[9] Dyrektywa Parlamentu Europejskiego i Rady w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniająca rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylająca dyrektywę (UE) 2016/1148.

telefon +48 22 245 59 22
adres email: sekretariat.dc@mc.gov.pl
strona www: www.gov.pl/web/cyfryzacja

adres korespondencyjny:
00-060 Warszawa
ul. Królewska 27

Mając na uwadze powyższe, proszę o dołączenie mojego stanowiska do Informacji o wynikach kontroli nr P/21/042 „Działania państwa w zakresie zapobiegania i zwalczania skutków wybranych przestępstw internetowych, w tym kradzieży tożsamości”.

Z poważaniem

z up. Ministra Cyfryzacji
Janusz Cieszyński
Janusz CieszyńskiSekretarz Stanu
w Kancelarii Prezesa Rady Ministrów
Pełnomocnik Rządu do Spraw Cyberbezpieczeństwa

/podpisano kwalifikowanym podpisem elektronicznym/

telefon +48 22 245 59 22
adres email: sekretariat.dc@mc.gov.pl
strona www: www.gov.pl/web/cyfryzacja

adres korespondencyjny:
00-060 Warszawa
ul. Królewska 27

6.6. Opinia Prezesa NIK do stanowiska Ministra

PREZES
NAJWYŻSZEJ IZBY KONTROLI
MARIAN BANAŚ

KPB.430.010.2022
P/21/042

Warszawa, dnia 10 stycznia 2023 r.

Opinia
Prezesa Najwyższej Izby Kontroli
do stanowiska Ministra Cyfryzacji odnośnie informacji o wynikach kontroli nr P/21/042
„Działania państwa w zakresie zapobiegania i zwalczania skutków wybranych przestępstw internetowych, w tym kradzieży tożsamości"

Przedstawione przez Ministra Cyfryzacji stanowisko do informacji „Działania państwa w zakresie zapobiegania i zwalczania skutków wybranych przestępstw internetowych, w tym kradzieży tożsamości" w praktyce potwierdza ustalenia niniejszej kontroli oraz sformułowane w jej wyniku wnioski i rekomendacje. Zgodnie ze stanowiskiem Ministra Cyfryzacji, podjął on działania w celu realizacji niektórych wniosków i uwag systemowych przedstawionych przez NIK w informacji o wynikach kontroli. Z zadowoleniem należy w szczególności odnotować deklarację dokonania przeglądu Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019-2024 oraz Planu działań na rzecz wdrożenia Strategii pod kątem przygotowania projektów modyfikacji tych dokumentów, a także działania mające celu poprawę funkcjonalności i upowszechnienie wykorzystania systemu S46.

Odnośnie niektórych kwestii opisanych w informacji o wynikach kontroli, zawarta w stanowisku argumentacja, wskazuje jednak na niepełne zrozumienie wniosków wynikających z przeprowadzonej przez Izbę kontroli. Potwierdza ona również przedstawione w wystąpieniach pokontrolnych oceny wskazujące na doraźny i fragmentaryczny charakter działań prowadzonych przez Ministra Cyfryzacji oraz Pełnomocnika Rządu do Spraw Cyberbezpieczeństwa w kontrolowanym obszarze.

Minister Cyfryzacji po raz kolejny w otwarty sposób wyraża akceptację dla istniejącego w Polsce stanu prawnego, w którym ustawa o krajowym systemie cyberbezpieczeństwa[1], zupełnie pomija tematykę bezpieczeństwa indywidulanych użytkowników cyberprzestrzeni. Stanowisko takie wyklucza najliczniejszą i najbardziej narażoną na ataki grupę użytkowników Internetu. Z tego powodu nie może ono zostać zaakceptowane przez NIK, która w pełni podtrzymuje swój wniosek dotyczący konieczności dokonania nowelizacji tej ustawy, polegającej na zdefiniowaniu zasad udzielania wsparcia osobom fizycznym, które stały się celem lub ofiarą cyberataku oraz obowiązków podmiotów odpowiadających za realizację zadań w tym obszarze.

Odnosząc się natomiast do opisanych w stanowisku Ministra działań służących edukowaniu obywateli na temat zagrożeń cyberbezpieczeństwa, NIK zauważa, że wskazano tam tylko pojedyncze

[1] Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. z 2022 r. poz. 1863, ze zm.).

inicjatywy oraz aktywności (np. kwartalny monitoring łącznej liczby wejść na poszczególne strony bazy wiedzy o cyberbezpieczeństwie), które w wyniku kontroli zostały już wcześniej ocenione jako dalece niewystarczające. Nie mogą one zostać zatem uznane, jako działania służące wykonaniu wniosków pokontrolnych NIK, które dotyczyły „wypracowania i wdrożenia jednolitych założeń modelu edukowania oraz ostrzegania obywateli na temat zagrożeń cyberbezpieczeństwa", a także „wdrożenia mechanizmów ewaluacji efektów prowadzonych przez KPRM oraz NASK-PIB działań edukacyjnych z zakresu cyberbezpieczeństwa".

Reasumując należy podkreślić, że ustalenia kontroli jednoznacznie wskazały na konieczność wdrożenia rozwiązań systemowych zapewniających ochronę indywidualnych użytkowników Internetu oraz podniesienia poziomu wiedzy i świadomości obywateli na temat niebezpieczeństw grożących im ze strony sprawców przestępstw internetowych. Wyrażam głębokie przekonanie, że szybka i pełna implementacji wniosków sformułowanych przez NIK przyczyni się do istotnej poprawy bezpieczeństwa Państwa i jego obywateli w cyberprzestrzeni.

PREZES
Najwyższej Izby Kontroli

Marian Banaś