PREZES
NAJWYŻSZEJ IZBY KONTROLI
Marian Banaś

KPB.410.007.04.2021

Pan Janusz Antoni Cieszyński
Pełnomocnik Rządu do Spraw Cyberbezpieczeństwa
Kancelaria Prezesa Rady Ministrów
ul. Królewska 27, 00-060 Warszawa

WYSTĄPIENIE POKONTROLNE

zmienione zgodnie z treścią uchwały nr 48/2022 Kolegium Najwyższej Izby Kontroli z dnia 28 września 2022 r.

P/21/042 „Działania państwa w zakresie zapobiegania i zwalczania skutków wybranych przestępstw internetowych, w tym kradzieży tożsamości".

NAJWYŻSZA IZBA KONTROLI
ul. Filtrowa 57, 02-056 Warszawa
T +48 22 444 50 00, F +48 22 444 57 93
nik@nik.gov.pl
Adres korespondencyjny: Skr. poczt. P-14, 00-950 Warszawa

I. Dane identyfikacyjne

Jednostka kontrolowana	Kancelaria Prezesa Rady Ministrów[1], ul. Królewska 27, 00-060 Warszawa[2]
Kierownik jednostki kontrolowanej	Janusz Cieszyński, Pełnomocnik Rządu do Spraw Cyberbezpieczeństwa[3], powołany na stanowisko z dniem 8 czerwca 2021 r. W okresie objętym kontrolą funkcję kierownika jednostki poprzednio pełnili: ▪ Marek Zagórski, Pełnomocnik Rządu do Spraw Cyberbezpieczeństwa, od 27 kwietnia 2020 r. do 7 czerwca 2021 r.; ▪ Karol Okoński, Pełnomocnik Rządu do Spraw Cyberbezpieczeństwa, od 7 grudnia 2018 r. do 16 grudnia 2019 r.
Zakres przedmiotowy kontroli	▪ szacowanie ryzyk i monitoring zagrożeń w obszarze przestępstw internetowych; ▪ koordynacja działań w obszarze zapobiegania i minimalizowania skutków przestępstw internetowych; ▪ efekty działań w obszarze zapobiegania i minimalizowania skutków przestępstw internetowych; ▪ przygotowanie kadrowe, logistyczne i organizacyjne do zapobiegania i zwalczania skutków przestępstw internetowych; ▪ wydawanie wytycznych oraz rekomendacji podnoszących poziom bezpieczeństwa użytkowników Internetu i zapobiegających przestępstwom internetowym; ▪ działania edukacyjne skierowane do obywateli (użytkowników Internetu) służące upowszechnianiu wiedzy na temat przestępstw internetowych.
Okres objęty kontrolą	1 stycznia 2019 r. – 31 grudnia 2021 r.
Podstawa prawna podjęcia kontroli	Art. 2 ust. 1 ustawy z dnia 23 grudnia 1994 r. o Najwyższej Izbie Kontroli[4]
Jednostka przeprowadzająca kontrolę	Najwyższa Izba Kontroli Departament Porządku i Bezpieczeństwa Wewnętrznego
Kontrolerzy	1. Paweł Gibuła, doradca ekonomiczny, upoważnienie do kontroli nr KPB/77/2021 z 10 listopada 2021 r. 2. Adam Zakrzewski, główny specjalista kontroli państwowej, upoważnienie do kontroli nr KPB/78/2021 z 10 listopada 2021 r. 3. Daniel Michalecki, główny specjalista kontroli państwowej, upoważnienie do kontroli nr KPB/79/2021 z 10 listopada 2021 r. 4. Adriana Surwiło, specjalista kontroli państwowej, upoważnienie do kontroli nr KPB/80/2021 z 10 listopada 2021 r. (akta kontroli str.1-8)

1 Zwana dalej: KPRM lub Kancelarią.

2 Na podstawie rozporządzenia Rady Ministrów z dnia 7 października 2020 r. (Dz. U. poz. 1730) w sprawie zniesienia Ministerstwa Cyfryzacji, z dniem 7 października 2020 r. zniesione zostało Ministerstwo Cyfryzacji, a pracownicy tego Ministerstwa obsługujący sprawy działu informatyzacja zostali włączeni do KPRM.

3 Minister Cyfryzacji upoważnił Pana Janusza Cieszyńskiego, sekretarza stanu w KPRM (a wcześniej Pana Marka Zagórskiego) do wykonywania zadań Ministra Cyfryzacji oraz do sprawowania nadzoru nad Naukową i Akademicką Siecią Komputerową – Państwowym Instytutem Badawczym (dalej: NASK-PIB).

4 Dz. U. z 2022 r. poz. 623., dalej: ustawa o NIK.

II. Ocena ogólna[5] kontrolowanej działalności

OCENA OGÓLNA

W ocenie NIK, Pełnomocnik Rządu do Spraw Cyberbezpieczeństwa[6] (wykonujący również obowiązki Ministra Cyfryzacji[7]) nie podjął w badanym okresie adekwatnych (do skali występujących w tym zakresie incydentów) działań, mających na celu zapobieganie oraz ograniczanie skutków przestępstw internetowych, zagrażających indywidualnym użytkownikom Internetu.

Uzasadnienie oceny ogólnej

Pełnomocnik Rządu podejmował liczne aktywności mające na celu wdrożenie mechanizmów koordynacji polityki rządu w zakresie zapewnienia cyberbezpieczeństwa RP. Prowadzone działania były ukierunkowane na ochronę systemów uznawanych za kluczowe dla funkcjonowania państwa i koncentrowały się na budowie dedykowanych temu zadaniu struktur organizacyjnych. Realizując te istotne zadania, nie zwracano w wystarczającym stopniu uwagi na fakt, że w badanym okresie dominującą i dotykającą wszystkich obywateli kategorią incydentów były oszustwa komputerowe i phishing. Pomimo dysponowania danymi ukazującymi skalę i rodzaj takich zdarzeń, Pełnomocnik nie określił w sposób rzetelny ram strategicznych działań państwa w zakresie ochrony indywidualnych użytkowników Internetu przed przestępczością internetową. Nie podjął również skutecznych działań mających na celu edukowanie i ostrzeganie obywateli na temat niebezpieczeństw grożących im ze strony sprawców przestępstw internetowych, w tym trwających kampanii phishingowych, do czego był zobligowany m.in. na podstawie art. 62 ust. 1 pkt 4 oraz art. 62 ust. 2 pkt 3 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa[8].

---

5 Najwyższa Izba Kontroli formułuje ocenę ogólną jako ocenę pozytywną, ocenę negatywną albo ocenę w formie opisowej.

6 Zwany dalej „Pełnomocnikiem Rządu" lub „Pełnomocnikiem".

7 W okresie objętym kontrolą obsługa merytoryczna zadań ministra właściwego do spraw informatyzacji oraz Pełnomocnika Rządu do Spraw Cyberbezpieczeństwa, 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 do Spraw Cyberbezpieczeństwa. W związku z powyższym, w przedstawionej ocenie ogólnej oraz w ramach poszczególnych opisanych w wystąpieniu pokontrolnym 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. (...)".

8 Dz. U. z 2020 r. poz. 1369, ze zm.

III. Opis ustalonego stanu faktycznego oraz oceny cząstkowe[9] kontrolowanej działalności

OBSZAR

1. System zapobiegania i minimalizowania skutków przestępstw internetowych[10]

1.1 Szacowanie ryzyk i monitoring zagrożeń w obszarze przestępstw internetowych

Opis stanu faktycznego

W okresie objętym kontrolą w komórkach organizacyjnych KPRM obsługujących Pełnomocnika nie prowadzono odrębnej analizy ryzyka w obszarze przestępczości internetowej. Pozyskiwano natomiast, od podmiotów krajowego systemu cyberbezpieczeństwa[11], 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 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[12] przez CSIRT GOV[13], m.in. w oparciu o dane z systemu wczesnego ostrzegania ARAKIS.GOV.

(akta kontroli str. 9-40,163)

W raporcie rocznym Cert Polska[14] 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 phising[15], który stanowił około 54,2% wszystkich incydentów.

W 2020 r.[16] odnotowano 10420 incydentów cyberbezpieczeństwa, z czego najpopularniejszym typem incydentu był ponownie phishing. Ataki tego rodzaju

---

9 Oceny cząstkowe to oceny działalności w poszczególnych obszarach badań kontrolnych. Ocena cząstkowa może być sformułowana jako ocena pozytywna, ocena negatywna albo ocena w formie opisowej.

10 Na gruncie polskiego prawa karnego brak jest legalnej definicji takich pojęć, jak: przestępczość komputerowa, przestępczość internetowa, czy cyberprzestępczość. Definicja taka ukształtowana została jednak na gruncie doktryny i literatury przedmiotu. W ich świetle „przestępstwa internetowe" to grupa czynów zabronionych polegających na posługiwaniu się elektronicznymi systemami przetwarzania informacji do naruszania dóbr chronionych przez prawo karne. Na potrzeby niniejszej kontroli, jako dodatkowe kryterium definiujące tego rodzaju przestępstwa przyjęto ich integralny związek ze środowiskiem, w którym są one popełniane, tj. Internetem. Oznacza to, że badania kontrolne dotyczyły przestępstw, które przebiegają zasadniczo w środowisku cyberprzestrzeni i nie stanowią wyłącznie elementu klasycznego przestępstwa, gdzie użycie cyberprzestrzeni jest jedynie uzupełnieniem głównej przestępczej kombinacji. 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, Dz. U. z 2021 r. poz. 2345, ze zm.), 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.

11 System ten został zdefiniowany w ustawie o krajowym systemie cyberbezpieczeństwa, zwanej dalej ustawą o KSC.

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

13 Prowadzony przez Agencję Bezpieczeństwa Wewnętrznego.

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

15 Metoda ataku polegająca na przesyłaniu smsów lub e-maili, których nadawcy podszywają się pod różne podmioty (np. firmy kurierskie, organy publiczne, dostawców usług) w celu wyłudzenia danych (np. numeru kart płatniczych, danych umożliwiających logowanie do bankowości elektronicznej) i w efekcie kradzieży środków finansowych.

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

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[17].

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

- w styczniu 2021 r. zarejestrowano 1154 incydenty[18], 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;

---

[17] 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.

[18] 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.

- 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 4186 incydentów, w tym jeden poważny. Spośród wszystkich obsłużonych incydentów 75% stanowiły oszustwa komputerowe, w tym phishing.

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

(akta kontroli str.164-166)

W badanym okresie Pełnomocnik Rządu przeprowadzał analizę ryzyka w obszarze bezpieczeństwa cyberprzestrzeni, w związku z realizacją obowiązków nałożonych na niego na podstawie art. 5a ust. 2 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym[19]. Przygotował, w oparciu o raporty cząstkowe przekazywane przez ministrów kierujących działami administracji rządowej, kierowników urzędów

[19] Dz. U z 2022 r. poz. 261, ze zm.

centralnych oraz wojewodów, „Raport o zagrożeniach bezpieczeństwa narodowego w części dotyczącej zagrożeń cyberbezpieczeństwa mogących doprowadzić do sytuacji kryzysowej", którego wnioski, zgodnie z ww. ustawą, powinny stanowić element Krajowego Planu Zarządzania Kryzysowego oraz zostać uwzględnione w planach zarządzania kryzysowego[20].

W Raporcie wskazano, że w związku z brakiem jasnych kryteriów przygotowywania raportów cząstkowych[21], jak również nieokreśleniem jednolitego systemu definicyjnego nie udało się zagregować otrzymanych danych i w konsekwencji wypracować spójnych wniosków w obszarze zagrożeń cyberbezpieczeństwa[22]. Podkreślono natomiast wyraźną tendencję wzrostową w zakresie liczby zgłaszanych incydentów oraz fakt, że „Najbardziej wyróżniającą się (pod względem liczby) kategorią na tle pozostałych ataków był phishing."

(akta kontroli str. 9-40, 162, 196)

Minister Cyfryzacji oraz Pełnomocnik Rządu wskazywali, że jednym z narzędzi wykorzystywanych do sprawowania nadzoru nad procesem zarządzania ryzykiem krajowego sytemu cyberbezpieczeństwa jest tzw. system S46, utworzony na podstawie art. 46 ustawy o krajowym systemie cyberbezpieczeństwa. Zgodnie z ww. przepisem system ten powinien zapewniać:

- współpracę podmiotów wchodzących w skład krajowego systemu cyberbezpieczeństwa;
- generowanie i przekazywanie rekomendacji dotyczących działań podnoszących poziom cyberbezpieczeństwa;
- zgłaszanie i obsługę incydentów;
- szacowanie ryzyka na poziomie krajowym;
- ostrzeganie o zagrożeniach cyberbezpieczeństwa.

Produkcyjne uruchomienie systemu S46 nastąpiło w styczniu 2021 r. W wyniku przeprowadzonych oględzin[23] ustalono, że na dzień dokonania tej czynności brak było możliwości praktycznego wykorzystania tego systemu przez Pełnomocnika Rządu, w tym w kontekście szacowania ryzyka cyberbezpieczeństwa na poziomie krajowym. Ustalono w szczególności, że:

- w systemie, z poziomu użytkownika KPRM, brak było informacji o zgłoszonych incydentach, a z poziomu użytkownika CSIRT NASK widoczny był jeden zaewidencjonowany incydent (dotyczący NASK S.A.);
- w systemie, z poziomu użytkownika KPRM, znajdowały się informacje o usługach dwóch podmiotów: NASK-PIB oraz NASK S.A. (razem cztery usługi kluczowe i cyfrowe) widocznych z poziomu ministra właściwego do spraw informatyzacji, jako organu właściwego dla sektora infrastruktura cyfrowa oraz organu właściwego dla dostawców usług cyfrowych. Brak było natomiast informacji z innych sektorów kluczowych, które powinny być widoczne z poziomu Pełnomocnika Rządu do Spraw Cyberbezpieczeństwa, co jak wyjaśniono mogło

---

[20] Aktualny „Raport o zagrożeniach bezpieczeństwa narodowego" z 2020 r. został przyjęty uchwałą Rady Ministrów z dnia 11 marca 2021 r.

[21] Przepisy nakładające obowiązek opracowania „Raportu o zagrożeniach bezpieczeństwa narodowego w części dotyczącej zagrożeń cyberbezpieczeństwa mogących doprowadzić do sytuacji kryzysowej" weszły w życie w dniu 28 sierpnia 2018 r., w związku z czym był to pierwszy Raport przygotowany w tym zakresie przez Pełnomocnika Rządu.

[22] Tematyka zarządzania kryzysowego, w tym przygotowania i praktycznego zastosowania raportów o zagrożeniach bezpieczeństwa narodowego oraz Krajowych Planów Zarządzania Kryzysowego była przedmiotem licznych, odrębnych kontroli NIK m.in. nr P/17/039 pt. „Ochrona ludności w ramach zarządzania kryzysowego i obrony cywilnej".

[23] Oględziny 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).

wnikać z niskiej dojrzałości systemu i braku dodania na chwilę oględzin w systemie możliwości podglądu przez Pełnomocnika;

- 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. W przypadku użytkownika CSIRT NASK w arkuszu „analiza ryzyka" brak było zgłoszonych ryzyk;
- w przypadku użytkownika CSIRT NASK arkusz „zdarzenia", który powinien zawierać obserwowane zdarzenia, które nie zostały zaklasyfikowane jak incydenty nie zawierał żadnych zdarzeń. W arkuszu „ostrzeżenia" znajdowało się sześć ostrzeżeń, a w arkuszu „rekomendacje" brak było dotychczas wydanych rekomendacji, co jak wyjaśniono wynikało z faktu przekazywania rekomendacji innymi kanałami informacyjnymi;
- na dzień oględzin KPRM dysponował tylko jednym terminalem do obsługi systemu S46 użyczonym przez NASK-PIB, a jedynym użytkownikiem tego systemu w Kancelarii[24] był Pan Łukasz Wojewoda, Dyrektor Departamentu Cyberbezpieczeństwa.

Wg stanu na dzień 14 grudnia 2021 r. łączna liczba podmiotów krajowego systemu cyberbezpieczeństwa podłączonych do systemu S46 wyniosła 12 i objęła ona: KPRM; CSIRTy NASK, ABW i MON; Ministra Obrony Narodowej (jako organ właściwy); PKP PLK; PERN, Urząd Komunikacji Elektronicznej (dalej: UKE); Ministerstwo Infrastruktury; Ministerstwo Kultury i Dziedzictwa Narodowego; Komisję Nadzoru Finansowego; NASK S.A. Wg stanu na 16 marca 2022 r. do systemu podłączonych było 14 z około 350 podmiotów, które w założeniu mają być jego podstawowymi użytkownikami[25].

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.

(akta kontroli str. 9-40, 88-118)

Pełnomocnik Rządu 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.

Wskazał również, że szacowanie ryzyka, które w przyszłości ma być prowadzone za pomocą sytemu S46 dotyczy przede wszystkim ryzyk dla świadczenia usług kluczowych, cyfrowych oraz publicznych. „System S46 nie służy zatem do prowadzenia „oceny ryzyka i aktualnych zagrożeń ze strony sprawców przestępstw internetowych", gdyż sama ustawa o KSC, w zakresie przedmiotowym, nie dotyczy zwalczania i przeciwdziałania „przestępstw internetowych".

(akta kontroli str. 9-40, 169-195)

NIK zwraca uwagę, że ponad rok po produkcyjnym uruchomieniu systemu S46, realne możliwości wykorzystania tego narzędzia w celu podnoszenia poziomu cyberbezpieczeństwa są bardzo ograniczone. Wynika to z małej liczby podłączonych podmiotów, znikomej liczby danych wprowadzonych dotychczas do systemu oraz

---

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

[25] KPRM zakłada przede wszystkim konieczność podłączenia do systemu wszystkich 170 operatorów usług kluczowych oraz 71 zdefiniowanych dostawców usług cyfrowych.

z braku przygotowania poszczególnych użytkowników, w tym KPRM, do jego obsługi (m.in. brak uprawnionych użytkowników). Uwzględniając znaczne nakłady poniesione dotychczas oraz planowane w kolejnych latach na budowę i utrzymanie tego systemu stwarza to ryzyko niegospodarnego wykorzystania znacznych środków publicznych. W celu zapewnienia praktycznego wykorzystania tego narzędzia do podnoszenia poziomu cyberbezpieczeństwa niezbędne jest zatem nie tylko zakończenie prowadzonych prac legislacyjnych nakładających obowiązek przyłączenia do niego wybranych kategorii podmiotów, ale również przekonanie użytkowników o realnej wartości jego wykorzystania, w tym bieżącego zasilania systemu aktualnymi danymi.

1.2 Koordynacja działań w obszarze zapobiegania i minimalizowania skutków przestępstw internetowych

Opis stanu faktycznego

Obowiązującym w badanym okresie dokumentem wyznaczającym cele i priorytety państwa w obszarze cyberbezpieczeństwa była Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019-2024 (zwana dalej „Strategią")[26], której koordynację Rada Ministrów powierzyła ministrowi właściwemu ds. informatyzacji. Głównym celem tego dokumentu było „Podniesienie poziomu odporności na cyberzagrożenia oraz zwiększenie poziomu ochrony informacji w sektorze publicznym, militarnym, prywatnym oraz promowanie wiedzy i dobrych praktyk umożliwiających obywatelom lepszą ochronę ich informacji." W celach szczegółowych Strategii wskazano liczne działania państwa, które powinny zostać podjęte lub zintensyfikowane w celu lepszego zapobiegania i zwalczania przestępczości internetowej, w tym w szczególności:

- prawidłowe zabezpieczanie dowodów cyfrowych[27];
- 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[28];
- transgraniczną współpracę organów ścigania i podmiotów typu CERT/CSIRT oraz stworzenie sprawnych i zaufanych kanałów wymiany informacji między organami ścigania różnych państw[29];
- wprowadzenie przepisów umożliwiających przetwarzanie dokumentów procesowych w postaci elektronicznej i przesyłanie ich w takiej postaci[30];
- rozwijanie badań naukowych w obszarze zwalczania cyberprzestępczości, których wyniki zapewnią wsparcie dla organów ścigania[31];
- wskazanie sposobów postępowania dla osób dotkniętych przestępstwem[32];
- opracowanie programów badawczych mających na celu wypracowanie metod wykrywania i analizy nowych typów cyberprzestępstw, cyberterroryzmu i cyberszpiegostwa[33];
- wzmocnienie systemu szkoleń dla wszystkich pracowników podmiotów istotnych dla cyberbezpieczeństwa oraz dla przedstawicieli organów ścigania i wymiaru sprawiedliwości, przez wdrożenie dedykowanego programu edukacyjnego

---

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

27 Cel szczegółowy nr 1 – rozwój krajowego systemu cyberbezpieczeństwa, pkt 5.6. „Zwiększanie zdolności do zwalczania cyberprzestępczości, w tym cyberszpiegostwa i zdarzeń o charakterze terrorystycznym", akapit nr 1.

28 Cel szczegółowy nr 1, pkt 5.6., akapit nr 2.

29 Cel szczegółowy nr 1, pkt 5.6., akapit nr 3.

30 Cel szczegółowy nr 1, pkt 5.6., akapit nr 4.

31 Cel szczegółowy nr 1, pkt 5.6., akapit nr 5.

32 Cel szczegółowy nr 1, pkt 5.6., akapit nr 5.

33 Cel szczegółowy nr 3 - Zwiększenie potencjału narodowego w zakresie technologii cyberbezpieczeństwa, pkt 7.3. „Stymulowanie badań i rozwoju w obszarze cyberbezpieczeństwa", ppkt 3).

zawierającego zarówno szkolenia teoretyczne, jak i praktyczne na realnych przykładach zagrożeń[34];

- włączanie się rządu w działania na rzecz skutecznego zwalczania cyberprzestępczości w wymiarze międzynarodowym[35].

Minister Cyfryzacji, działając na podstawie pkt 10 Strategii, opracował projekt dokumentu wykonawczego – „Planu działań na rzecz wdrożenia Strategii Cyberbezpieczeństwa" (zwanego dalej: „Planem działań"), który został przyjęty w trybie konsultacji międzyresortowych. W Planie działań, w ramach celu szczegółowego Strategii nr 1 – rozwój krajowego systemu cyberbezpieczeństwa, pkt 1.6 „Zwiększanie zdolności do zwalczania cyberprzestępczości, w tym cyberszpiegostwa i zdarzeń o charakterze terrorystycznym" zawarto trzy następujące zadania w sposób bezpośredni związane z tematyką zwalczania cyberprzestępczości:

- zadanie 1.6.1 – „współpraca z krajowymi i międzynarodowymi podmiotami, w tym szczególnie z operatorami telekomunikacyjnymi, platformami społecznościowymi w kontekście przeciwdziałania i zapobeganiu cyberprzestępczości", przewidziane do realizacji przez KPRM we współpracy z innymi podmiotami, w okresie I kwartał 2020 r. - IV kwartał 2024 r. Efektem realizacji zadania miało być zacieśnienie współpracy w kontekście zapobiegania oraz przeciwdziałania szkodliwym i nielegalnym aktywnościom w cyberprzestrzeni.
- zadanie 1.6.2 – „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. Efektem realizacji zadania miało być stałe podnoszenie kompetencji, wiedzy oraz umiejętności kadr Policji, prokuratury oraz sędziów zajmujących się wykrywaniem, ściganiem oraz karaniem sprawców cyberprzestępstw.
- 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. Efektem realizacji zadania miało być prowadzenie kampanii społecznych o charakterze profilaktycznym w kontekście cyberzagrożeń.

Pozostałe, ujęte w Planie działań zadania, związane z tematyką przestępczości internetowej dotyczyły:

- zadanie 4.2.4 – rozbudowy i modernizacji Dyżurnet.pl poprzez prowadzenie działań zwiększających bezpieczeństwo dzieci w Internecie w ramach programu Safer Internet oraz wsparcie rozwoju działań Zespołu Dyżurnet.pl. Jako podmiot wiodący dla zadania, które miało być realizowane w całym okresie wdrażania Strategii, został wyznaczony NASK-PIB.
- działanie 4.3.1.1 – prowadzenia kampanii informacyjnych skierowanych do różnych grup interesariuszy[36]. Jako podmiot wiodący dla zadania, które miało być realizowane w całym okresie wdrażania Strategii, został wyznaczony KPRM.

(akta kontroli str. 9-40, 164, 169-195)

---

34 Cel szczegółowy nr 4 - Budowanie świadomości i kompetencji społecznych w zakresie cyberbezpieczeństwa, pkt 8.1. „Zwiększanie kompetencji kadry podmiotów istotnych dla cyberbezpieczeństwa Rzeczypospolitej Polskiej", akapit nr 2.

35 Cel szczegółowy nr 5 - Zbudowanie silnej pozycji międzynarodowej Rzeczypospolitej Polskiej w obszarze cyberbezpieczeństwa, pkt 9.1. „Aktywna współpraca międzynarodowa na poziomie strategiczno-politycznym", akapit nr 4.

36 Działanie w ramach zadania 4.3.1. „Rozwój działań edukacyjno-informacyjnych poprzez podniesienie świadomości społecznej w zakresie zagrożeń płynących z obszaru cyberbezpieczeństwa".

W przedstawionych Radzie Ministrów sprawozdaniach z realizacji Strategii[37], poza jednym działaniem[38], nie wskazano zadań zrealizowanych w okresie sprawozdawczym przez KPRM w ramach celu szczegółowego nr 1 Strategii, pkt 1.6 „Zwiększanie zdolności do zwalczania cyberprzestępczości, w tym cyberszpiegostwa i zdarzeń o charakterze terrorystycznym". Podmioty współdziałające z KPRM przy realizacji tego zadania deklarowały przede wszystkim prowadzenie bieżącej współpracy w tym obszarze, w tym z organami ścigania i wymiaru sprawiedliwości.

W ramach realizacji celu szczegółowego nr 4 Strategii, pkt 4.3 „Rozwijanie świadomości społecznej w kierunku bezpiecznego korzystania z cyberprzestrzeni" wykazano w szczególności kampanie społeczne kierowane do rodziców, seniorów i dzieci oraz „bazę wiedzy" z zakresu cyberbezpieczeństwa prowadzone przez KPRM[39], a także serwisy internetowe oraz wydarzenia podnoszące świadomość w zakresie cyberbezpieczeństwa, dla których podmiotem prowadzącym (organizatorem) były NASK-PIB oraz UKE.

(akta kontroli str. 9-40, 164-166, 169-195)

W sprawozdaniach z działalności Pełnomocnika Rządu za 2019 i 2020 r., przedkładanych Radzie Ministrów na podstawie art. 63 ust. 1 ustawy o KSC, wśród najważniejszych obszarów aktywności Pełnomocnika wymieniono w szczególności:

- identyfikowanie i monitorowanie procesu wyznaczania operatorów usług kluczowych oraz dostawców usług cyfrowych;
- wspieranie tworzenia sektorowych zespołów cyberbezpieczeństwa oraz Centrów Wymiany i Analizy Informacji;
- budowę systemu teleinformatycznego S46;
- przeprowadzanie międzysektorowych ćwiczeń cyberbezpieczeństwa;
- prowadzenie szkoleń z zakresu cyberbezpieczeństwa dla pracowników podmiotów publicznych, w tym w szczególności samorządu terytorialnego;
- wydawanie rekomendacji cyberbezpieczeństwa;
- rozbudowywanie „bazy wiedzy" z zakresu cyberbezpieczeństwa[40];

W badanym okresie w komórkach organizacyjnych KPRM obsługujących Pełnomocnika przygotowano również założenia do nowelizacji ustawy o KSC[41]. 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. Założono wprowadzenie obowiązku korzystania z systemu S46 m.in. przez operatorów usług kluczowych. 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

---

37 Sprawozdania z dnia 2 lipca 2020 r. oraz 23 marca 2021 r. przedstawione na podstawie § 3 i § 4 uchwały nr 125 Rady Ministrów w sprawie Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019-2024.

38 Podpisanie „Deklaracji Współpracy na rzecz Bezpieczeństwa Dzieci w Sieci".

39 Opisano szczegółowo w pkt. III.3. wystąpienia pokontrolnego.

40 Opisano szczegółowo w pkt III.3. wystąpienia pokontrolnego.

41 Projekt ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz ustawy – Prawo telekomunikacyjne (nr UD68) znajduje się obecnie na etapie prac w Stałym Komitecie Radzie Ministrów.

krajowego systemu cyberbezpieczeństwa[42]. 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[43].

(akta kontroli str. 9-40, 163-166, 169-195)

Stwierdzone nieprawidłowości

W działalności kontrolowanej jednostki w przedstawionym wyżej zakresie stwierdzono następującą nieprawidłowość:

Pełnomocnik Rządu (wykonujący również obowiązki Ministra Cyfryzacji) nie realizował w sposób rzetelny przypisanych mu zadań (wynikających w szczególności z art. 60 ustawy o KSC), dotyczących koordynowania działań w zakresie zapewnienia cyberbezpieczeństwa RP, w istotnym obszarze tego bezpieczeństwa obejmującym ochronę obywateli przed przestępczością internetową. Koordynowany przez Pełnomocnika system cyberbezpieczeństwa oraz zdecydowana większość działań realizowanych w badanym okresie przez KPRM koncentrowały się na innych aspektach bezpieczeństwa, takich jak ochrona usług kluczowych i obsługa incydentów poważnych oraz budowa dedykowanych temu zadaniu struktur organizacyjnych (zespoły CSIRT, system S46). Realizując te istotne zadania, nie zwracano w wystarczającym stopniu uwagi na fakt, że z dostępnych Pełnomocnikowi i prezentowanych w oficjalnych dokumentach danych wynikało, że w badanym okresie dominującą i dotykającą w praktyce wszystkich obywateli kategorią incydentów były oszustwa komputerowe i phishing.

Pomimo dysponowania ww. informacjami Pełnomocnik nie określił ram strategicznych aktywności organów państwa w zakresie zapobiegania i minimalizowania skutków przestępstw internetowych. W opracowanym w KPRM Planie działań nie ujęto większości działań wskazanych w Strategii Cyberbezpieczeństwa RP, mających służyć zwalczaniu cyberprzestępczości[44], a w przypadku zadań (działania) przewidzianych w Planie (nr: 1.6.1, 1.6.2, 1.6.3, 4.3.1.1) brak było lub nie określono konkretnych mierników ich realizacji[45]. W rezultacie brak było możliwości sprawowania rzetelnej koordynacji działań organów państwa w tym obszarze, a informacje przekazywane Radzie Ministrów przez Pełnomocnika na temat postępów we wdrażaniu Strategii polegały zasadniczo na agregowaniu nieporównywalnych danych przekazywanych przez różne podmioty na temat ich bieżącej działalności.

W wyjaśnieniach udzielanych w toku kontroli Minister Cyfryzacji oraz Pełnomocnik Rządu wskazywali, że zagadnienia związane z przestępczością internetową w praktyce nie wchodzą w zakres ich kompetencji. Dowodzili przy tym, że zadania związane z zapobieganiem i zwalczaniem skutków przestępczości internetowej nie są literalnie wymienione wśród zadań Ministra/Pełnomocnika wskazanych w ustawie

---

42 Podmioty te byłyby zobowiązane uwzględniać te rekomendacje podczas procesu zarządzania ryzykiem.

43 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 czerwca 2019 r. str. 15.

44 Działania wymienione w tiretach na str. 9-10 wystąpienia pokontrolnego.

45 W przypadku zadania 1.6.1 brak było w ogóle miernika, a dla zadań 1.6.2 oraz 1.6.3 określono mierniki w postaci liczby przeszkolonych osób/funkcjonariuszy oraz liczby przeprowadzonych kampanii społecznych – bez wskazania jaką liczbę szkoleń i kampanii oraz dla kogo zamierzano przeprowadzić. Analogiczna sytuacja miała miejsce w przypadku działania 4.3.1.1.

o KSC, a zawarta w tej ustawie definicja legalna „cyberbezpieczeństwa"[46] nie obejmuje ścigania sprawców przestępstw internetowych. Pełnomocnik zanegował nawet fakt koordynowania przez podległe mu struktury wdrażania Strategii i dowodził, że odpowiedzialność za nierzetelne przygotowanie Planu działań spoczywa na innych organach, które mają w swojej właściwości zwalczanie cyberprzestępczości. Wskazał m.in.: „Realizacja poszczególnych zadań Strategii opisana w Planie działań leży w gestii organów właściwych odpowiedzialnych za dany obszar – organem właściwym w kwestii cyberprzestępczości jest minister właściwy ds. sprawiedliwości oraz organy ścigania. Brak wskazania w Planie działań konkretnych zadań wynika z decyzji poszczególnych organów właściwych. (...)"

W ocenie NIK przedstawiona argumentacja nie zasługuje na uwzględnienie. Prowadziłaby ona do wniosku, że w obowiązującym obecnie porządku prawnym istnieje istotna luka i żaden z organów państwa nie ma przypisanych zadań w zakresie ochrony obywateli przed cyberprzestępczością, w szczególności w obszarze dominującej kategorii zagrożeń, jakimi są oszustwa komputerowe. Należy przy tym wyraźnie rozgraniczyć zadania związane ze ściganiem sprawców przestępstw komputerowych od obowiązków związanych z edukowaniem użytkowników Internetu na temat grożących im niebezpieczeństw oraz upowszechniania dobrych praktyk, mających na celu przeciwdziałanie takim zdarzeniom i minimalizowanie ich skutków. Zadania w zakresie podnoszenia „cyberświadomości" społeczeństwa zostały przypisane Ministrowi Cyfryzacji (art. 45 ust. 1 pkt 4 ustawy o KSC) oraz Pełnomocnikowi Rządu (m.in. art. 62 ust. 1 pkt 4 oraz art. 62 ust. 2 pkt 3 ww. ustawy). Należy również podkreślić, że na podstawie art. 12a ust. 1 ustawy z dnia 4 września 1997 r. o działach administracji rządowej[47] Minister Cyfryzacji odpowiada za bezpieczeństwo cyberprzestrzeni w wymiarze cywilnym. Dodatkowo sprawuje on nadzór nad NASK-PiB[48], który jako jedyny podmiot krajowego systemu bezpieczeństwa ma bezpośrednio przypisane zadania (art. 30 ust. 1 ustawy o KSC) w zakresie wsparcia indywidulanych użytkowników Internetu (osób fizycznych).

(akta kontroli str. 9-40, 163-166, 169-195)

OCENA CZĄSTKOWA

W okresie objętym kontrolą Pełnomocnik podejmował aktywne działania w ramach koordynacji działań i polityki rządu w zakresie zapewnienia cyberbezpieczeństwa RP. Prowadzone działania były ukierunkowane na ochronę systemów uznawanych za kluczowe dla funkcjonowania państwa. W niewystarczającym stopniu, pomimo dysponowania danymi ukazującymi skalę i rodzaj dominujących incydentów, uwzględniały zagrożenia dla indywidulanych użytkowników Internetu za strony sprawców przestępstw internetowych. Nie określono w sposób rzetelny ram strategicznych działalności państwa w kontekście tych zagrożeń, co m.in. wpłynęło na brak skuteczności działań edukacyjnych skierowanych do obywateli[49].

OBSZAR

2. Przygotowanie kadrowe i organizacyjne do zapobiegania oraz zwalczania skutków przestępstw internetowych

Opis stanu faktycznego

W okresie objętym kontrolą obsługa merytoryczna zadań ministra właściwego do spraw informatyzacji oraz Pełnomocnika Rządu, wynikających z ustawy o KSC, była prowadzona przez Departament Cyberbezpieczeństwa KPRM. Dodatkowo,

---

[46] W art. 2 pkt 4 ustawy wskazano, że „cyberbezpieczeństwo" oznacza odporność systemów informacyjnych na działania naruszające poufność, integralność, dostępność i autentyczność przetwarzanych danych lub związanych z nimi usług oferowanych przez te systemy.

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

[48] Obwieszczenie Ministra Cyfryzacji z dnia 15 maja 2019 r. w sprawie wykazu jednostek organizacyjnych podległych Ministrowi Cyfryzacji lub przez niego nadzorowanych (M. P. poz. 462).

[49] Opisanych w pkt III.3. wystąpienia pokontrolnego.

z dniem 16 lipca 2021 r., utworzone zostało Biuro Pełnomocnika Rządu do Spraw Cyberbezpieczeństwa – komórka organizacyjna, do której obowiązków należały przede wszystkim: obsługa kancelaryjna Pełnomocnika, obsługa posiedzeń Rady do Spraw Cyfryzacji oraz Kolegium do Spraw Cyberbezpieczeństwa, koordynowanie współpracy z parlamentem, a także inicjowanie, koordynowanie i realizacja wybranych kampanii społecznych i działań informacyjno-promocyjnych z obszaru polityki cyfrowej.

W okresie od 1 stycznia 2019 r. do 31 grudnia 2021 r. w Departamencie Cyberbezpieczeństwa (dalej: Departament lub DC) zatrudnionych było łącznie 34 pracowników realizujących zadania merytoryczne[50]. Na dzień 31 grudnia 2021 r. zatrudnionych było 26 osób, spośród których dwie znajdowały się w okresie wypowiedzenia stosunku pracy, dwie były oddelegowane do innych instytucji, a jedna była długotrwale nieobecna[51]. Spośród wszystkich pracowników zatrudnionych w badanym okresie w Departamencie, 20 rozpoczęło pracę w DC w 2019 r. lub później. W przypadku 10 pracowników, którzy w kontrolowanym okresie zakończyli stosunek pracy lub znajdowali się w okresie wypowiedzenia staż pracy w Departamencie wyniósł: 20 dni (jedna osoba), dwa miesiące (jedna osoba), około jednego roku (cztery osoby) oraz około 3-4 lat (cztery osoby).

Spośród 34 pracowników zatrudnionych w badanym okresie w DC, 21 odbyło szkolenia informatyczne, bądź z zakresu cyberbezpieczeństwa, albo posiadało wykształcenie informatyczne (magisterskie, inżynierskie, podyplomowe) i/lub doświadczenie zawodowe w tym zakresie. Pozostałych 13 osób nie posiadało specjalistycznego wykształcenia w dziedzinie informatyki lub cyberbezpieczeństwa, ani nie odbyło żadnych szkoleń w tym zakresie. Spośród tej grupy jedna osoba była oddelegowana do pracy w innej instytucji, cztery zakończyły zatrudnienie w DC, a w przypadku dwóch osób zatwierdzono ich udział w szkoleniach specjalistycznych dotyczących bezpieczeństwa informacyjnego, z zakresu IT oraz cyberbezpieczeństwa.

(akta kontroli str. 119-123, 130-134, 141)

Wg stanu na dzień 31 grudnia 2021 r. w Biurze Pełnomocnika Rządu do Spraw Cyberbezpieczeństwa zatrudnionych było 13 pracowników merytorycznych[52], w tym dziewięciu w Wydziale do spraw Informacji w Obszarze Cyfryzacji[53] oraz po jednej osobie w Wydziale Promocji Polityki Cyfrowej[54] oraz na Samodzielnym Stanowisku do spraw realizacji kampanii edukacyjno-informacyjnych. Jedna osoba (Zastępca Dyrektora Biura) znajdowała się w okresie wypowiedzenia stosunku pracy.

Żadna z osób zatrudnionych w Biurze Pełnomocnika nie posiadała wykształcenia specjalistycznego w zakresie informatyki, czy cyberbezpieczeństwa. Jedynie dwie osoby (w tym jedna znajdująca się w okresie wypowiedzenia) odbyły szkolenia z zakresu cyberbezpieczeństwa prowadzone przez instruktora z CSIRT GOV, a dwie kolejne szkolenia wewnętrzne z zakresu ochrony danych osobowych i bezpieczeństwa teleinformatycznego oraz dla administratorów bezpieczeństwa.

(akta kontroli str. 124-129, 135-141)

NIK zwraca uwagę na znaczną fluktuację pracowników oraz istotne ograniczenia kadrowe Departamentu Cyberbezpieczeństwa, które w świetle dużej liczby oraz znacznego stopnia złożoności realizowanych zadań mogły wpływać na jakość

---

50 W Departamencie zatrudniona była jeszcze jedna osoba odpowiedzialna za obsługę sekretariatu.

51 Od 17 października 2020 r. do 17 stycznia 2022 r.

52 W Biurze zatrudnione były jeszcze cztery osoby odpowiedzialne za obsługę sekretariatów.

53 Do którego zadań należała m.in. obsługa kancelaryjna Pełnomocnika, obsługa posiedzeń Rady do Spraw Cyfryzacji oraz Kolegium do Spraw Cyberbezpieczeństwa, koordynowanie współpracy z parlamentem.

54 Do zadań Wydziału należało m.in. inicjowanie, koordynowanie i realizacja wybranych kampanii społecznych i działań informacyjno-promocyjnych z obszaru polityki cyfrowej, w tym w ramach kampanii edukacyjno-informacyjnych na temat wykorzystywania technologii cyfrowych.

podejmowanych działań. Należy przy czym odnotować podjęte m.in. w tym zakresie działania legislacyjne dotyczące przyjęcia ustawy[55] oraz rozporządzenia wykonawczego[56] zapewniających możliwość otrzymywania dodatków przez pracowników realizujących zadania związane z bezpieczeństwem cyberprzestrzeni. W ocenie NIK, realizacja tych działań powinna ułatwić pozyskiwanie pracowników posiadających odpowiednie kwalifikacje do realizacji zadań w obszarze cyberbezpieczeństwa.

W opisanym powyżej kontekście ograniczonych zasobów Departamentu Cyberbezpieczeństwa, NIK zwraca również uwagę na wątpliwości dotyczące celowości funkcjonowania odrębnej, rozbudowanej (zatrudniającej kilkanaście osób) komórki organizacyjnej sprawującej m.in. obsługę kancelaryjną Pełnomocnika. Wątpliwości te potęguje także fakt braku specjalistycznego wykształcenia pracowników Biura w obszarach, w których mają oni stanowić wsparcie Pełnomocnika Rządu.

Stwierdzone nieprawidłowości

W działalności kontrolowanej jednostki w przedstawionym wyżej zakresie nie stwierdzono nieprawidłowości.

OCENA CZĄSTKOWA

Kontrola wykazała, że w KPRM funkcjonowały struktury organizacyjne mające zapewniać realizację zadań Ministra Cyfryzacji oraz Pełnomocnika Rządu związanych z bezpieczeństwem cyberprzestrzeni. NIK zwróciła jednak uwagę na ograniczenia kadrowe komórki organizacyjnej odpowiedzialnej za funkcjonowanie krajowego systemu cyberbezpieczeństwa.

3. Działania edukacyjne skierowane do obywateli służące upowszechnianiu wiedzy na temat przestępstw internetowych oraz wydawanie wytycznych i rekomendacji podnoszących poziom bezpieczeństwa użytkowników Internetu

Opis stanu faktycznego

W dniu 29 października 2019 r. Departament Cyberbezpieczeństwa upublicznił na portalu gov.pl „bazę wiedzy", stanowiącą repozytorium ostrzeżeń, zaleceń oraz dobrych praktyk z zakresu bezpieczeństwa informatycznego. Wg stanu na dzień 14 stycznia 2022 r.[57] 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".

Dostęp do „bazy wiedzy" następował z poziomu głównej strony portalu gov.pl, poprzez rozwijalne menu po lewej stronie ekranu, przez link „baza wiedzy"[58], który prowadził do trzech zakładek tematycznych: „Cyberbezpieczeństwo", „Dostępność cyfrowa", „Społeczna Odpowiedzialność Administracji". Po wejściu w temat: „Cyberbezpieczeństwo" wyświetlała się „baza wiedzy" z zakresu cyberbezpieczeństwa. Pracownicy Departamentu Cyberbezpieczeństwa, wyjaśniali, że zamieszczony na portalu gov.pl link „baza wiedzy" nie został uzupełniony o termin „cyberbezpieczeństwa", ponieważ, baza ta jest dedykowana różnym obszarom tematycznym. Wskazali, że w związku z architekturą i koncepcją portalu gov.pl, który obejmuje strony wielu podmiotów publicznych brak było również możliwości

[55] Ustawa z dnia 2 grudnia 2021 r. o szczególnych zasadach wynagradzania osób realizujących zadania z zakresu cyberbezpieczeństwa (Dz. U. poz. 2333).

[56] Rozporządzenie Rady Ministrów z dnia 19 stycznia 2022 r. w sprawie wysokości świadczenia teleinformatycznego dla osób realizujących zadania z zakresu cyberbezpieczeństwa (Dz. U. poz. 131).

[57] Tj. na dzień oględzin „bazy wiedzy" przez kontrolerów NIK.

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

wyodrębnienia na głównej stronie portalu gov.pl linka dedykowanego wyłącznie „bazie 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").

Wg stanu na 14 stycznia 2022 r. w „bazie wiedzy" brak było dedykowanej wyszukiwarki, a ta dostępna z poziomu całego portalu gov.pl przeszukując strony internetowe wszystkich podmiotów publicznych obecnych na tym portalu realnie uniemożliwiała (lub znacząco utrudniała) korzystanie z „bazy wiedzy"[59]. Pracownicy Departamentu Cyberbezpieczeństwa wyjaśnili, że w momencie tworzenia bazy, w toku konsultacji z komórką organizacyjną KPRM będącą architektem portalu gov.pl, ustalono, że brak jest możliwości umieszczenia wydzielonej wyszukiwarki bezpośrednio w „bazie wiedzy" z zakresu cyberbezpieczeństwa.

(akta kontroli str. 142-159)

W Departamencie Cyberbezpieczeństwa prowadzono monitoring liczby odsłon materiałów publikowanych w „bazie wiedzy", uzyskując dane statystyczne z Google Analytics[60], prezentujące w ujęciu kwartalnym[61] ogólną liczbę wejść na poszczególne zakładki bazy. Z przedstawionych danych wynikało, że od momentu upublicznienia „bazy wiedzy"[62] największą liczbę wejść odnotowano w zakładkach:

- „Dla każdego - cyberhigiena" – 34218 wejść łącznie, przy czym największą liczba wejść miała miejsce w okresie 31 marca - 30 czerwca 2020 r. (8159), natomiast w ostatnim kwartale 2021 r. wyniosła ona 2286;
- „Aktualności" - 22050 wejść łącznie, przy czym największą 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) oraz „Najczęściej zadawane pytania" (1136 w całym okresie funkcjonowania tej zakładki).

(akta kontroli str. 41-87, 160-161, 167-195)

W związku z prowadzoną kontrolą NIK, w Departamencie Cyberbezpieczeństwa, przeprowadzono analizę danych z Google Analytics prezentujących: kanały pozyskiwania ruchu na stronach „bazy wiedzy", najczęściej czytane artykuły w trzech zakładkach bazy oraz osiem dobranych celowo przez kontrolujących publikacji ostrzegających przed różnymi metodami działania przestępców internetowych. Ustalono, że:

- Największy ruch w „bazie wiedzy" generowany był przez zewnętrzne wyszukiwarki google i bing (łącznie 162187 sesji, w tym 155136 przez google). 36665 sesji zostało wygenerowanych poprzez bezpośrednie wejście na stronę „bazy wiedzy" lub poszczególnych artykułów.
- Najczęściej odwiedzanym artykułem w zakładce „Dla każdego - cyberhigiena" był artykuł dotyczący phishingu[63], który miał 52129 odsłon ogółem, w tym 41841 unikalnych[64]. Cztery artykuły dotyczące m.in. zasad korzystania z urządzeń

---

59 W toku oględzin podjęto próbę wyszukania haseł: „kampanie phishingowe", „phishing", „kradzież tożsamości".

60 Z komórki organizacyjnej KPRM zarządzającej portalem gov.pl.

61 Z udzielonych wyjaśnień wynika, że dane na temat liczby wejść są incydentalnie (w miarę potrzeb) uzyskiwane dla wybranych artykułów zamieszczonych w „bazie wiedzy".

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

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

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

mobilnych, tworzenia bezpiecznych haseł, e-bankowości oraz rozpoznawania nieprawdziwych informacji odnotowały od 18629 do 10132 odsłon. W przypadku czterech kolejnych publikacji liczba odsłon nie przekroczyła 10000.

- W zakładce „Aktualności" najczęściej odwiedzanym artykułem było opracowanie ENISA dotyczące 15 głównych cyberzagrożeń, które osiągnęło 3132 odsłon, w tym 2515 unikalnych. Kolejne trzy artykuły odnotowały między 3029 a 1433 odsłon, a sześć kolejnych poniżej 1000 odsłon.
- W zakładce „Dla profesjonalistów" – jeden artykuł dotyczący pracy zdalnej[65] odnotował 7129 odsłon, w tym 4591 unikalnych. Z pozostałych dziewięciu najczęściej czytanych publikacji tylko jedna osiągnęła powyżej 1000 odsłon.

W przypadku poszczególnych, dobranych do badania artykułów liczba odsłon, w tym unikalnych wyniosła:

- „Szykujesz się na Black Friday? Sprawdź, jak nie stać się ofiarą internetowych oszustów[66] – 342/293;
- „UWAGA – CSIRT NASK ostrzega!!![67] – 343/279;
- „Rejestracja na szczepienie – zachowaj czujność!!!"[68] – 375/327;
- „Black Friday 2020 – jak kupować, żeby nie żałować"[69] – 874/419;
- „UWAGA – CSIRT NASK ostrzega przed kolejnymi oszustwami związanymi z pandemią COVID-19"[70] – 221/208;
- „UWAGA! CSIRT NASK ostrzega – trwa zmasowana kampania SMS-owa celująca w użytkowników telefonów z systemem Android!"[71] – 892/766;
- „Black Friday i bezpieczne zakupy w Internecie. Jak nie dać się oszukać?"[72] – 79/48;
- „CSIRT NASK ostrzega - przedświąteczny okres zakupowy to wzmożony czas działalności przestępców w internecie"[73] – 145/122.

(akta kontroli str. 41-87, 160-161, 169-195)

W poszczególnych sekcjach tematycznych „bazy wiedzy" publikowane były zalecenia i rekomendacje, mające na celu zwiększenie poziomu bezpieczeństwa, w tym zapobieganie przestępstwom internetowym. Zalecenia i rekomendacje obejmowały:

- zalecenia na poziomie podstawowym kierowane przede wszystkim do indywidulanych użytkowników Internetu, zamieszczone w zakładce „Dla każdego - cyberhigiena";
- uniwersalne poradniki kierowane do różnych grup użytkowników Internetu[74];
- poradniki „branżowe" skierowane do nauczycieli[75] oraz podmiotów ochrony zdrowia[76];
- liczne rekomendacje adresowane do profesjonalistów dotyczące w szczególności zabezpieczeń sieci i systemów informatycznych, opublikowane w zakładce „Narodowe Standardy Cyberbezpieczeństwa";

---

65 www.gov.pl/web/baza-wiedzy/praca-zdalna---razem-ale-osobno
66 Opublikowano w „bazie wiedzy" 28 listopada 2019 r.
67 Opublikowano 7 października 2020 r.
68 Opublikowano 15 stycznia 2021 r.
69 Opublikowano 23 listopada 2020 r.
70 Opublikowano 26 sierpnia 2021 r.
71 Opublikowano 24 września 2021 r.
72 Opublikowano 25 listopada 2021 r.
73 Opublikowano 20 grudnia 2021 r.
74 Poradnik „Jak chronić się przed cyberatakami? Praktyczne wskazówki dla parlamentarzystów i nie tylko.", styczeń 2021 r.
75 „Poradnik dla nauczycieli PR-EDU-01 – bezpieczne korzystanie z platform do edukacji zdalnej", kwiecień 2020 r.
76 „Zgłaszanie incydentów cyberbezpieczeństwa przez podmioty sektora ochrony zdrowia", kwiecień 2020 r.

- rekomendacje „branżowe" cyberbezpieczeństwa dla sektora wodno-kanalizacyjnego oraz ochrony zdrowia;
- rekomendacje partnerów technologicznych (firm CISCO, DELL, Microsoft).

Analiza danych ze zintegrowanego środowiska programistycznego[77] wykazała, że spośród 38 zamieszczonych w „bazie wiedzy" poradników i rekomendacji tylko dwa zostały pobrane ze strony gov.pl więcej niż 1000 razy. W przypadku poradników, których treść mogła być wykorzystywana przez indywidulanych użytkowników Internetu liczba pobrań wyniosła odpowiednio: 350[78], 172[79] oraz 132[80].

(akta kontroli str. 9-40, 56-87)

W pierwszej połowie 2020 r. w „bazie wiedzy" uruchomiona została usługa subskrypcji wiadomości z zakresu cyberbezpieczeństwa, która zgodnie z wyjaśnieniami Pełnomocnika, jest dostępna dla każdej zainteresowanej osoby.

Przeprowadzona analiza wszystkich 809 adresów e-mail należących do zarejestrowanych subskrybentów[81] wykazała, że zdecydowana większość z nich (co najmniej 700) należała do podmiotów sektora finansów publicznych (administracji rządowej, samorządowej, państwowych i samorządowych jednostek organizacyjnych), w tym sześć adresów należało do pracowników Departamentu Cyberbezpieczeństwa KPRM. W grupie subskrybentów można było również wyróżnić domeny należące do 25 firm świadczących szeroko pojęte usługi informatyczne (w tym również szkolenia z zakresu informatyki i bezpieczeństwa). Przeprowadzona analiza wykazała tylko dwa adresy w domenie gmail.com, które mogły należeć do osób fizycznych, tj. subskrybentów niepowiązanych z żadną instytucją.

Pełnomocnik wyjaśnił, że usługa subskrypcji „cyberwiadomości" została utworzona z myślą o instytucjach publicznych, w szczególności jednostkach samorządu terytorialnego, a dopiero w kolejnym etapie udostępniono ją innym podmiotom. Nie wskazał żadnych działań podjętych dotychczas w celu upowszechnienia tej usługi wśród osób fizycznych.

(akta kontroli str. 41-87,169-195)

W dniu 20 grudnia 2021 r. w zakładce „Aktualności" została zamieszczona ankieta ewaluacyjna „bazy wiedzy" oraz wystosowano do subskrybentów „cyberwiadomości" prośbę o jej wypełnienie. Wg stanu na dzień 31 grudnia 2021 r. ankietę wypełniły 154 osoby, z których większość stanowili przedstawiciele administracji publicznej, w tym samorządowej (126 osób) oraz dodatkowo dziewięć osób fizycznych, nie reprezentujących żadnego podmiotu. W raporcie z badania ewaluacyjnego wskazano m.in., że respondenci potwierdzili przydatność materiałów publikowanych w „bazie wiedzy", w tym „Narodowych Standardów Cyberbezpieczeństwa" i poinformowali o skali ich wdrożenia w swoich jednostkach organizacyjnych.

(akta kontroli str. 56-87,169-195)

W okresie objętym kontrolą KPRM realizowała lub współpracowała (w szczególności z NASK-PIB) przy realizacji następujących kampanii i akcji edukacyjnych dotyczących korzystania z Internetu i związanych z tym zagrożeń:

1. Realizowana w latach 2019-2020 kampania „e-polak potrafi!" obejmowała cztery obszary tematyczne: „jakość życia", „e-usługi publiczne", „bezpieczeństwo w sieci", „programowanie". Wiodącym elementem całej kampanii było zachęcanie

---

77 Dane za okres 1 czerwca 2021 r. – 31 grudnia 2021 r.

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 Wg stanu na dzień 11 stycznia 2022 r.

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.

W trakcie kontroli, prowadzony był przetarg na kontynuację, w okresie do 2023 r., kampanii „e-polak potrafi!". Pełnomocnik wyjaśnił, 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).

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.

(akta kontroli str. 9-87, 167-168)

Szczegółowym badaniem w zakresie skuteczności działań edukacyjnych skierowanych do obywateli, wydawanych ostrzeżeń i rekomendacji podnoszących poziom bezpieczeństwa objęto szczęść dobranych celowo kampanii phishingowych (opisywanych m.in. w raportach rocznych z działalności Cert Polska oraz w raportach miesięcznych CSIRT NASK dla Pełnomocnika Rządu):

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. Trwająca w okresie styczeń - sierpień 2020 r. kampania mająca 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. Prowadzona od 2020 r. kampania dotycząca fałszywych zawiadomień o skierowaniu na kwarantannę.
5. Trwająca od grudnia 2021 r. aktywna kampania polegająca na dostarczaniu fałszywych wiadomości SMS na temat przesyłek.
6. Trwająca, co najmniej od połowy 2020 r., kampania ukierunkowana na wyłudzenia danych od użytkowników serwisu OLX, prowadzona m.in. z wykorzystaniem komunikatora WhatsApp.

Kontrolującym nie przekazano dokumentacji potwierdzającej działania KPRM podjęte w bezpośrednim związku oraz skorelowane czasowo z kampaniami opisanymi w pkt 1-3 oraz w pkt 6. Jako działania informujące użytkowników Internetu o konkretnej prowadzonej kampanii wskazywano m.in. ogólne publikacje na temat złośliwego

oprogramowania zamieszczone w „bazie wiedzy"[82]. Odwołano się również do czterech, powiązanych tematycznie z ww. kampaniami artykułów z „bazy wiedzy", w przypadku których liczba odsłon wyniosła odpowiednio: 892[83], 375[84], 221[85] oraz 145[86]. Wskazywano także na korespondencję e-mail z ostrzeżeniami przekazywaną subskrybentom „cyberwiadomości" oraz zamieszczoną w „bazie wiedzy" instrukcję zgłaszania incydentów do Cert Polska.

(akta kontroli str. 56-87)

W Departamencie Cyberbezpieczeństwa opracowana została koncepcja działań promujących wiedzę o cyberbezpieczeństwie w 2022 r. W dokumencie tym przewidziano m.in. dalsze rozbudowywanie „bazy wiedzy" na portalu gov.pl oraz uruchomienie kont Departamentu w mediach społecznościowych.

(akta kontroli str. 192-195)

Stwierdzone nieprawidłowości

W działalności kontrolowanej jednostki w przedstawionym wyżej zakresie stwierdzono następującą nieprawidłowość:

Kontrola wykazała, że budowana od 2019 r. „baza wiedzy" nie spełniała swojego zadania, jakim było stworzenie jednolitego i łatwo dostępnego dla obywateli oraz różnych instytucji repozytorium ostrzeżeń, zaleceń oraz dobrych praktyk z zakresu cyberbezpieczeństwa. Utworzona baza podlegała istotnym ograniczeniom w zakresie dostępności i łatwości wyszukiwania informacji, co wynikało m.in. z jej umieszczenia na portalu gov.pl. Brak było w szczególności bezpośredniej i wyraźnie oznaczonej „ścieżki dostępu" do bazy, co mogło ograniczać dostępność i rozpoznawalność zawartych tam treści.

Przeprowadzone w związku z kontrolą NIK analizy wykazały niewielką skalę wykorzystania informacji opublikowanych w bazie, których odsłony (w przypadku całych zakładek tematycznych) nie przekraczały w skali kwartału kilku tysięcy, lub nawet tylko kilkuset wejść. W przypadku poszczególnych artykułów i poradników pojedyncze z nich odnotowały istotną liczbę odsłon, a zdecydowana większość, w tym dobrane do badania opracowania dotyczące oszustw komputerowych i phishingu, osiągnęły nie więcej niż kilkaset wejść. Nie zostały również podjęte działania mające na celu bezpośrednie dotarcie z informacjami na temat cyberzagrożeń do indywidulanych użytkowników Internetu, m.in. poprzez upowszechnienie wśród osób fizycznych korzystania z subskrypcji „cyberwiadomości" KPRM.

Prowadzony w tym zakresie monitoring ograniczał się zasadniczo do uzyskiwania danych prezentujących, w ujęciu kwartalnym, łączną liczbę wejść na poszczególne zakładki bazy, a szczegółowe badania, pod kątem liczby odsłon wybranych artykułów, przeprowadzono dopiero w związku z kontrolą NIK. 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.

Pełnomocnik Rządu nie przedstawił kontrolującym żadnych materiałów potwierdzających podejmowane przez niego działania, które miałyby na celu zwiększenie liczby odsłon materiałów i artykułów publikowanych w „bazie wiedzy". Nie wypracował również z kierownictwem nadzorowanej przez siebie jednostki (NASK-PIB) jednolitego stanowiska odnośnie optymalnego modelu edukowania obywateli o zagrożeniach cyberbezpieczeństwa. W rezultacie, w badanym okresie,

---

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

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

84 „Rejestracja na szczepienie – zachowaj czujność!!!"

85 „UWAGA – CSIRT NASK ostrzega przed kolejnymi oszustwami związanymi z pandemią COVID-19"

86 „CSIRT NASK ostrzega - przedświąteczny okres zakupowy to wzmożony czas działalności przestępców w internecie"

funkcjonowały w tym obszarze dwa modele komunikacyjne – scentralizowany („baza wiedzy" KPRM) oraz rozproszony (wdrażany przez NASK-PIB) w postaci różnych specjalizowanych lub przeznaczonych dla wybranych grup użytkowników stron i serwisów informacyjnych[87].

Zidentyfikowane nieprawidłowości w zakresie funkcjonowania „bazy wiedzy" nie były kompensowane poprzez prowadzone przez KPRM kampanie edukacyjne z zakresu cyberbezpieczeństwa. Działania te w niewielkim stopniu odnosiły się dotychczas do tematyki 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.

Powyższe nieprawidłowości powodowały, co potwierdziła m.in. zbadana próba kampanii phishingowych, że indywidualni użytkownicy Internetu byli pozbawieni aktualnych i pochodzących od Pełnomocnika Rządu informacji na temat grożących im zagrożeń cyberbezpieczeństwa.

(akta kontroli str. 9-87, 142-161, 167-195)

OCENA CZĄSTKOWA

W okresie objętym kontrolą Pełnomocnik Rządu nie wypracował skutecznego modelu edukowania i informowania obywateli na temat niebezpieczeństw grożących im ze strony sprawców przestępstw internetowych. Pomimo podjęcia aktywnych działań obejmujących budowę „bazy wiedzy" z zakresu cyberbezpieczeństwa, jak również organizację kampanii edukacyjnych, indywidualni użytkownicy Internetu byli w znacznej mierze pozbawieni aktualnych i pochodzących od instytucji publicznych informacji na temat istniejących w tym obszarze zagrożeń.

IV. Uwagi i wnioski

W związku ze stwierdzonymi nieprawidłowościami, Najwyższa Izba Kontroli, na podstawie art. 53 ust. 1 pkt 5 ustawy o NIK, przedstawia następujące uwagi i wnioski:

Uwagi

1. NIK zwraca uwagę, że prowadzona przez KPRM „baza wiedzy" z zakresu cyberbezpieczeństwa podlegała istotnym ograniczeniom w zakresie dostępności i łatwości wyszukiwania informacji, co wynikało m.in. z jej umieszczenia w ramach rozległego serwisu internetowego, jakim jest portal gov.pl. Pomimo, że większość odsłon materiałów bazy generowana jest z poziomu wyszukiwarek internetowych, w ocenie NIK, pożądane byłoby stworzenie jednego, rozpoznawalnego, oficjalnego, państwowego serwisu, zawierającego łatwo dostępne informacje na temat zagrożeń cyberbezpieczeństwa, trwających obecnie kampanii, a także zaleceń i dobrych praktyk z zakresu „cyberhigieny". Uwzględniając ograniczenia związane z prowadzaniem takiej bazy na portalu gov.pl. zasadne byłoby rozważenie zlecenia innemu podmiotowi (np. NASK-PIB, który niewątpliwie dysponuje zasobami do realizacji takiego zadania) utworzenia i dalszego aktualizowania jednego repozytorium wiedzy z zakresu cyberbezpieczeństwa.

Wnioski

1. Dokonanie modyfikacji Strategii Cyberbezpieczeństwa RP oraz Planu działań poprzez uwzględnienie w treści tych dokumentów wyników analizy ryzyka wskazujących na dominującą skalę zagrożeń ze strony oszustw komputerowych oraz zdefiniowanie porównywalnych mierników stopnia realizacji zadań służących zapobieganiu i minimalizowaniu tego rodzaju zagrożeń.

---

[87] Szczegółowo opisano w wystąpieniu pokontrolnym znak: KPB. 410.007.03.2021 przekazanym do Dyrektora NASK-PIB.

2. Wypracowanie i wdrożenie, we współpracy z NASK-PIB, jednolitych założeń stosowanego modelu edukowania oraz ostrzegania obywateli na temat zagrożeń cyberbezpieczeństwa.
3. Wdrożenie mechanizmów ewaluacji efektów prowadzonych działań edukacyjnych z zakresu cyberbezpieczeństwa.

V. Pozostałe informacje i pouczenia

Wystąpienie pokontrolne zostało sporządzone w dwóch egzemplarzach; jeden dla kierownika jednostki kontrolowanej, drugi do akt kontroli.

Prawo zgłoszenia zastrzeżeń

Zgodnie z art. 54 ustawy o NIK kierownikowi jednostki kontrolowanej przysługuje prawo zgłoszenia na piśmie umotywowanych zastrzeżeń do wystąpienia pokontrolnego, w terminie 21 dni od dnia jego przekazania. Zastrzeżenia zgłasza się do Prezesa NIK. Prawo zgłaszania zastrzeżeń, zgodnie z art. 61b ust. 2 ustawy o NIK, nie przysługuje do wystąpienia pokontrolnego zmienionego zgodnie z treścią uchwały w sprawie zastrzeżeń.

Obowiązek poinformowania NIK o sposobie wykorzystania uwag i wykonania wniosków

Zgodnie z art. 62 ustawy o NIK należy poinformować Najwyższą Izbę Kontroli, w terminie 21 od otrzymania wystąpienia pokontrolnego, o sposobie wykorzystania uwag i wykonania wniosków pokontrolnych oraz o podjętych działaniach lub przyczynach niepodjęcia tych działań.

W przypadku wniesienia zastrzeżeń do wystąpienia pokontrolnego, termin przedstawienia informacji liczy się od dnia otrzymania uchwały o oddaleniu zastrzeżeń w całości lub zmienionego wystąpienia pokontrolnego.

Warszawa, dnia 27 kwietnia 2022 r.

Prezes
Najwyższa Izba Kontroli
Marian Banaś
/-/

Zmian w wystąpieniu pokontrolnym dokonał:

Tomasz Sordyl
p.o. Dyrektor Departamentu
Porządku i Bezpieczeństwa Wewnętrznego

.....

podpis