DOI: 10.53122/ISSN.0452-5027/2023.1.30 kontrola i audyt

Ustalenia kontroli NIK

Obywatele bez ochrony

Przestępstwa internetowe – zapobieganie i zwalczanie

DANIEL MICHALECKI

Dzięki wielu zaletom – łatwości komunikacji, szybkości i wygodzie zakupów, dostępowi do administracji publicznej czy bankowości elektronicznej – Internet stał się ważnym elementem naszego życia. Jest on jednak również polem działalności przestępców, których ofiarami są nie tylko instytucje, ale i obywatele. Ze względu na rosnącą skalę tego zjawiska Najwyższa Izba Kontroli sprawdziła, czy w latach 2019–2021 państwo prowadziło skuteczne działania pozwalające zidentyfikować, zapobiegać oraz ograniczać skutki przestępstw internetowych[1]. Przedmiotem kontroli były te wymierzone w indywidualnych użytkowników Internetu, niosące dla nich ryzyko strat finansowych. Sprawdzono cztery podmioty: Ministra Cyfryzacji (dalej Minister), Pełnomocnika Rządu ds. Cyberbezpieczeństwa (dalej Pełnomocnik Rządu), Komendę Główną Policji (KGP) oraz Naukową i Akademicką Sieć Komputerową – Państwowy Instytut Badawczy (NASK). Ustalenia NIK wskazują, że skoncentrowały się one na ochronie instytucji i systemów kluczowych dla funkcjonowania kraju. Jednocześnie pomijały obywateli, którzy w okresie wzmożonej działalności cyberprzestępców byli zdani tylko na siebie.

Wprowadzenie

Sieć internetowa stała się nieodłączną częścią życia prywatnego i zawodowego wielu Polaków – według badania CBOS przeprowadzonego w 2022 r.[2] regularną obecność online deklaruje ponad trzy czwarte dorosłych. W ciągu dwóch lat, na które przypadła epidemia koronawirusa odsetek internautów wzrósł o dziewięć punktów procentowych. Niemal dwie trzecie Polaków twierdzi, że kupiło coś przez Internet. Wzrosła także popularność sprzedawania rzeczy w ten sposób. Z kolei badanie opinii publicznej przeprowadzone na zlecenie NIK wykazało, że 71% ankietowanych korzystało z usług e-administracji[3].

[1] Artykuł opracowano na podstawie Informacji z kontroli NIK: *Działania państwa w zakresie zapobiegania i zwalczania skutków wybranych przestępstw internetowych, w tym kradzieży tożsamości*, nr. ewid. 125/2022/P/21/042/KPB.

[2] CBOS, *Korzystanie z Internetu w 2022 r.*, komunikat z badań nr 77/2022: <https://www.cbos.pl/SPISKOM.POL/2022/K_077_22.PDF>.

[3] Badanie przeprowadzono w okresie 20-28.4.2022.

Lawinowo rosnąca liczba ataków hakerskich, kradzieży tożsamości, *phishingu*[4] czy szantażu opartego na oprogramowaniu *ransomware*[5] sprawia, że kwestia cyberzagrożeń i cyberbezpieczeństwa stała się problemem społecznym. Z tego powodu NIK skoncentrowała się na przestępstwach wymierzonych w indywidualnych użytkowników Internetu[6], związanych z ryzykiem utraty przez nich środków finansowych (nie zajmowała się zatem pedofilią czy tzw. mową nienawiści, ale przestępstwami polegającymi najczęściej na oszustwie lub szantażu).

Dostrzeżenie problemu

Podmioty objęte kontrolą dostrzegały problem narastającej fali przestępczości internetowej. Analizy prowadzone zarówno przez Policję, NASK czy jednostki Kancelarii Prezesa Rady Ministrów obsługujące Ministra Cyfryzacji i Pełnomocnika Rządu wskazywały na gwałtowny wzrost liczby incydentów komputerowych wymierzonych w indywidualnych użytkowników Internetu, zwłaszcza kampanii *phishingowych*. Statystyki Policji wykazywały bezprecedensowy w stosunku do poprzednich lat wzrost zgłoszeń dotyczących cyberprzestępstw:

- w 2019 r. – 67 822, w tym 48 127 internetowych,
- w 2020 r. – 68 633, w tym 49 435 internetowych,
- w 2021 r. (tylko do października) – 59 273, w tym 37 786 internetowych.

Z kolei inna policyjna statystyka, tj. liczba stwierdzonych przestępstw wynosiła:

- 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. (tylko do października) – 64 139, w tym 47 408 oszustw internetowych.

Policja odnotowała w okresie pandemii COVID-19 wzrost liczby domen internetowych służących m.in. do rejestracji fałszywych sklepów internetowych, dystrybucji złośliwego oprogramowania oraz kradzieży danych osobowych. W przeprowadzonej w 2020 r. diagnozie Policja wskazywała, że *phishing*, oszustwa przy wykorzystaniu portali aukcyjnych oraz sklepów internetowych, a także ataki typu *ransomware* wyznaczają główne obszary ryzyka

[4] *Phishing* to rodzaj oszustwa wykorzystującego techniki inżynierii społecznej, polegającego na podszyciu się pod inną osobę lub instytucję w celu wyłudzenia poufnych lub wrażliwych informacji lub zainfekowania komputera ofiary złośliwym oprogramowaniem. Może przybrać np. postać wiadomości e-mail od rzekomo naszego banku, podczas gdy tak naprawdę e-mail ten został spreparowany przez oszustów.

[5] Oprogramowanie to zaprojektowane jest tak, by pozbawić użytkownika dostępu do komputera, na którym zostało zainstalowane. *Ransomware* używa w tym celu najczęściej technik szyfrowania. Przestępcy po zainfekowaniu komputera ofiary (w tym przypadku najczęściej organizacji), żądają okupu (ang. *ransom*) za udostępnienie klucza deszyfrującego, który umożliwi ponowny dostęp do zablokowanych zasobów.

[6] W polskim prawie karnym nie istnieje definicja takich pojęć, jak: przestępczość komputerowa, przestępczość internetowa czy cyberprzestępczość. Definicja taka ukształtowana została jednak na gruncie doktryny i literatury przedmiotu. Kontrolerzy wykorzystali określenie „przestępstwo internetowe", zdefiniowane jako grupa czynów zabronionych 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.

związanego z rozwojem cyberprzestępczości. W zdecydowanej większości przestępstwa te dotyczyły właśnie indywidualnych użytkowników Internetu.

Z kolei prowadzona przez CSIRT NASK[7] analiza zgłoszeń i incydentów, przekazywana regularnie Pełnomocnikowi Rządu, pozwoliła na wskazanie występujących w 2021 r. przestępczych trendów w Internecie. Były to:

- kampanie oszustów wykorzystujących popularność serwisu ogłoszeniowego OLX;
- wyłudzenia danych uwierzytelniających do kont w serwisach społecznościowych, głównie do serwisu Facebook;
- kampanie *phishingowe* polegające na podszywaniu się pod firmy kurierskie oraz dostawców energii elektrycznej;
- kampanie SMS, w których oszuści wykorzystywali sytuację związaną z trwającą pandemią COVID-19 (np. przez nawiązywanie do loterii towarzyszącej Narodowemu programowi szczepień przeciw COVID-19).

Także w tych wypadkach były to przestępstwa w zdecydowanej większości skierowane przeciwko „zwykłym", nie zaś instytucjonalnym użytkownikom Internetu. Dlaczego więc dysponując taką wiedzą, państwo – pomimo wysiłku poszczególnych instytucji, urzędników i funkcjonariuszy – nie zadbało o bezpieczeństwo obywateli? Z Informacji o wynikach kontroli NIK wyłaniają się cztery główne przyczyny.

Przyczyny niezapewnienia ochrony

Brak zasobów

Zapewnienie cyberbezpieczeństwa cyfrowego wymaga wysokich nakładów finansowych. Specjaliści z tej branży, zwani cyberbezpiecznikami, są obecnie – obok fachowców od *Big Data*[8] – najlepiej opłacanymi pracownikami IT. W dodatku jest ich niewielu w stosunku do potrzeb rynku – w Polsce brakuje ok. 18 tys. takich ekspertów[9]. Nie jest to zresztą tylko nasz problem – ich niedobór odczuwa wiele krajów[10]. Ze względu na małe możliwości płacowe instytucje publiczne mają trudności z pozyskaniem wykwalifikowanych pracowników. Nie było więc zaskoczeniem, że w wypadku dwóch z trzech zbadanych podmiotów (Policja oraz urząd obsługujący Ministra Cyfryzacji i Pełnomocnika Rządu) kontrola wykazała braki kadrowe.

W policyjnym pionie do walki z cyberprzestępczością w okresie objętym kontrolą zatrudniano faktycznie 305 funkcjonariuszy (a uwzględniając pracowników cywilnych – 338 osób). Stanowiły tylko 0,33% wszystkich etatów w Policji (103 309).

---

[7] W polskim systemie cyberbezpieczeństwa działają trzy zespoły CSIRT (zespoły reagowania na incydenty komputerowe, ang. *Computer Security Incident Response Team*), odpowiedzialne za poszczególne obszary funkcjonowania państwa. CSIRT GOV zbiera informacje o incydentach w jednostkach administracji rządowej, CSIRT MON w podmiotach podległych Ministerstwu Obrony Narodowej, a CSIRT NASK przyjmuje zgłoszenia m.in. od operatorów usług kluczowych, samorządów i obywateli.

[8] Analitycy *Big Data* zajmują się wydobywaniem informacji z rozległych zbiorów danych, w celu uzyskania rekomendacji i wskazówek przydatnych np. do dalszego prowadzenia biznesu.

[9] <https://resilia.pl/blog/cyberbezpieczenstwo-w-firmie-a-brak-specjalistow-na-rynku/>

[10] <https://serwisy.gazetaprawna.pl/nowe-technologie/artykuly/8415381,na-calym-swiecie-brakuje-specjalistow-od-cyberbezpieczenstwa.html>

W Departamencie Cyberbezpieczeństwa KPRM, prowadzącym obsługę merytoryczną Ministra Cyfryzacji i Pełnomocnika Rządu, według stanu na koniec 2021 r., efektywne zatrudnienie wyniosło tylko 21 osób. Dodatkowym problemem była tzw. „karuzela kadrowa". W połączeniu z ograniczonymi zasobami finansowymi i sprzętowymi, musiało to wpłynąć na jakość zadań związanych ze zwalczaniem i ograniczaniem skutków przestępczości internetowej. Sam Pełnomocnik przyznał, że utrudniało to lub wręcz uniemożliwiało rzetelne wykonywanie przypisanych mu zadań związanych z koordynacją i realizacją polityki rządu dotyczącej cyberbezpieczeństwa RP[11].

Ograniczone zasoby Policji osłabiła też nieefektywna struktura. Funkcjonujące w komendach wojewódzkich wydziały do walki z cyberprzestępczością podlegały właściwym miejscowo komendantom wojewódzkim i były w praktyce niezależne od Biura do Walki z Cyberprzestępczością Komendy Głównej Policji. Choć Biuro podejmowało działania koordynujące i zlecało tym wydziałom określone czynności, w praktyce ich realizacja była uzależniona od posiadanych przez dany wydział sił i środków oraz określanych lokalnie priorytetów. W tym miejscu warto wspomnieć o specyfice działań cyberprzestępców, dla których granice terytorialne nie są żadną przeszkodą. Efektywna struktura do walki z nimi powinna być więc spójna, tj. działać ponad takimi granicami.

Jeszcze w toku czynności kontrolnych Policja rozpoczęła wdrażanie nowej struktury do walki z cyberprzestępczością, opartej na Centralnym Biurze Zwalczania Cyberprzestępczości (CBZC) – wyspecjalizowanej jednostce organizacyjnej Policji, powołanej na mocy ustawy z 17 grudnia 2021 r.[12] Zaplanowano w niej m.in. środki w wysokości 4,4 mld zł na powstanie nowej służby, utworzenie spójnej struktury (CBZC będzie działać na wzór Centralnego Biura Śledczego), dodatkowe 1,8 tys. etatów niezbędnych do uruchomienia jednostki. Uregulowano także wymagania stawiane kandydatom do służby w CBZC oraz zagwarantowano podwyższone uposażenie, dzięki któremu do służby mają trafić wykwalifikowani specjaliści ds. cyberbezpieczeństwa. Zainicjowane przez Policję działania były zbieżne z przygotowywanym przez NIK wnioskiem. Choć nakłady przeznaczone na utworzenie CBZC mogą wydawać się bardzo wysokie, warto zadać sobie pytanie, czy stać nas na oszczędności w dziedzinie cyberbezpieczeństwa. Sektor prywatny coraz częściej dochodzi do wniosku, że tym, na co go nie stać, są koszty wynikające z udanego cyberataku[13]. W 2021 r. organizacje na całym świecie straciły średnio ponad pięć mln dolarów w wyniku jednego tylko wariantu ataku *phishingowego* znanego jako BEC (*Business Email Compromise* – specyfika tego ataku

[11] Informacja o wynikach kontroli NIK: *Działania państwa w zakresie zapobiegania*…, op.cit., s. 28.
[12] Ustawa z 17.12.2021 o zmianie niektórych ustaw w związku z powołaniem Centralnego Biura Zwalczania Cyberprzestępczości (Dz. U. poz. 2447).
[13] <https://www.gmv.com/pl-pl/media/blog/cyberbezpieczenstwo/cyberbezpieczenstwo-jest-drogie-w-porownaniu-z-czym>

polega na podszywaniu się przez hakerów pod konkretne osoby zatrudnione w firmie lub kontrahentów i wysyłaniu w ich imieniu fałszywych wiadomości do osób odpowiedzialnych za finanse z prośbą – przykładowo – o zmianę numeru rachunku do przelewu lub uregulowanie płatności na wskazany adres)[14]. Jeśli więc NIK wskazała na zagrożenia związane z powstaniem CBZC, to polegały one przede wszystkim na trudnościach w pozyskaniu w założonym terminie (do końca 2025 r.) 1,8 tys. odpowiedniej klasy specjalistów. Z danych udostępnionych przez zastępcę komendanta CBZC insp. Michała Pudłę podczas posiedzenia sejmowej Komisji do spraw Kontroli Państwowej wynika, że do 25 maja 2023 r. liczba wakatów w Biurze (które rozpoczęło swoją działalność 12 lipca 2022 r.) utrzymywała się na poziomie bliskim 40% (800 zaplanowanych etatów, 317 wakatów)[15]. Rekrutacja trwa, należy więc wstrzymać się z wyciąganiem pochopnych wniosków. NIK zwróciła jednak uwagę na konieczność objęcia procesu powstawania CBZC bezpośrednim nadzorem ze strony Komendanta Głównego Policji[16].

Brak spójnego modelu edukacji

Podstawowym warunkiem poprawy cyberbezpieczeństwa jest edukowanie obywateli oraz ostrzeganie ich przed zagrożeniami związanymi z funkcjonowaniem Internetu. W tym obszarze w kontrolowanym przez NIK okresie państwo zawiodło – pomimo niezwykłej aktywności niektórych instytucji i ich pracowników. W ocenie Izby zabrakło przede wszystkim jednolitego modelu edukowania i ostrzegania oraz ewaluacji prowadzonych w tym obszarze działań (takiej, która umożliwiłaby zwiększenie ich skuteczności). Słowem każda z instytucji podejmowała własne działania, przyjmując różne koncepcje i rozwiązania, przy czym żadna nie sprawdzała, czy przynoszą zamierzony efekt.

Minister Cyfryzacji oraz Pełnomocnik Rządu doprowadzili do utworzenia na portalu gov.pl bazy wiedzy (zawierającej ostrzeżenia, zalecenia oraz dobre praktyki) dotyczącej cyberbezpieczeństwa. Została ona oddana do użytku obywateli i instytucji w październiku 2019 r. Podlegała jednak istotnym ograniczeniom związanym z dostępnością i łatwością wyszukiwania informacji. Wynikały one zarówno z braku odpowiedniej wyszukiwarki, jak i umiejscowienia bazy w ramach serwisu portal.gov. Koncepcja funkcjonowania tego portalu, który dotyczy działalności wielu publicznych podmiotów, a przez to jest poświęcony zróżnicowanej tematyce, utrudnia wyeksponowanie treści dotyczących cyberbezpieczeństwa. Zdaniem

[14] <https://pieniadze.rp.pl/finanse-firmy/art36817681-najkosztowniejsze-cyberataki-dla-firm-straty-ida-w-miliony>

[15] Posiedzenie Komisji do spraw Kontroli Państwowej z 25.5.2023 poświęcone rozpatrzeniu Informacji o wynikach kontroli NIK sprawdzającej działania państwa dotyczące zapobieganiu i zwalczaniu skutków wybranych przestępstw internetowych, w tym kradzieży tożsamości.

[16] NIK przewidywała już w toku kontroli, że trudniejszy będzie drugi etap pozyskania specjalistów do CBZC. W pierwszym Policja posiłkowała się rekrutacją wewnętrzną, tj. pozyskiwała do nowego Biura funkcjonariuszy, którzy w ramach innych jednostek Policji mieli do czynienia ze zwalczaniem cyberprzestępczości. Znacznie trudniejsze może okazać się pozyskanie takich specjalistów z rynku cywilnego.

kontrolerów baza wiedzy sprawiała wrażenie wręcz ukrytej[17]. W konsekwencji zarówno prowadzony w KPRM monitoring kwartalnej liczby odsłon poszczególnych zakładek tematycznych bazy wiedzy, jak i szczegółowe analizy zlecone przez kontrolerów NIK potwierdziły niewielką skalę wykorzystania opublikowanych tam informacji, komunikatów oraz rekomendacji. Wybrane przez kontrolerów metodą celową publikacje dotyczące metod działania przestępców internetowych miały liczbę unikalnych odsłon od 48 do maksymalnie 766. W wypadku poradników przeznaczonych dla indywidualnych użytkowników Internetu liczba ich pobrań wyniosła odpowiednio: 350, 172 oraz 132. W bazie wiedzy pojedyncze artykuły cieszyły się większą popularnością[18], lecz w dalszym ciągu nie była to skala, która pozwoliłaby mówić o skutecznym dotarciu z przekazem do obywateli.

Zabrakło także ewaluacji efektów utworzonej bazy wiedzy. Monitoring KPRM ograniczał się do agregowania mało użytecznych danych prezentujących w ujęciu kwartalnym łączną liczbę wejść w poszczególne zakładki bazy. Natomiast nie prowadzono szczegółowych badań dotyczących faktycznej liczby odsłon wybranych artykułów (analizy wykonano dopiero na wniosek kontrolerów NIK). Bez takiej wiedzy niemożliwe było dostosowanie materiałów publikowanych w bazie do potrzeb odbiorców i zwiększenie w ten sposób zasięgu i oddziaływania.

O ile Minister i Pełnomocnik Rządu zdecydowali się na jeden serwis informacyjny dotyczący cyberbezpieczeństwa, o tyle NASK-PIB przyjął model rozproszony w postaci różnych wyspecjalizowanych i sprofilowanych serwisów, wzmocnionych publikacjami w mediach społecznościowych. Poziom aktywności Instytutu w obszarze informacyjno-edukacyjnym oceniono bardzo wysoko. Prowadzone działania objęły liczne kampanie i akcje edukacyjne realizowane samodzielnie oraz we współpracy z partnerami krajowymi i zagranicznymi. Mimo to, jak ustaliła NIK, „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"[19].

Podobny problem dotyczył działań edukacyjnych i prewencyjnych prowadzonych

[17] Dostęp do niej następował z poziomu głównej strony portalu gov.pl, przez rozwijalne menu po lewej stronie ekranu, a następnie odnośnik „baza wiedzy" (brakowało 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").

[18] Najczęściej odwiedzanym artykułem w zakładce „Dla każdego – cyberhigiena" był artykuł dotyczący *phishingu*, który miał 41 841 unikalnych odsłon. 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.

[19] Informacja o wynikach kontroli NIK: *Działania państwa w zakresie zapobiegania*…, op.cit., s. 38.

przez Policję. Pomimo dużej aktywności w tej dziedzinie jej przekaz był osłabiony z powodu rozproszenia treści. Policja publikowała komunikaty dotyczące cyberbezpieczeństwa i cyberzagrożeń w różnych serwisach internetowych, tradycyjnych mediach, a także starała się przekazywać je podczas bezpośrednich spotkań z mieszkańcami. Ponadto miały one charakter doraźny, materiały internetowe publikowano w zakładce „Aktualności", co wobec dużej liczby zamieszczanych tam informacji znacząco utrudniało dotarcie do poszczególnych ostrzeżeń lub rekomendacji. Podobnie jak w przypadku KPRM oraz NASK-PIB, żadna z właściwych komórek organizacyjnych KGP nie dokonywała ewaluacji publikowanych materiałów.

W ocenie NIK „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"[20].

Przygotowanie skutecznej kampanii społecznej wymaga połączenia wielu elementów: zdefiniowania problemu, określenia celu i reakcji jakiej oczekujemy, wybrania grupy docelowej, dopasowania języka i formy komunikatu oraz rzetelnej i bieżącej ewaluacji. Warto więc rozważyć włączenie w proces budowania społecznej świadomości dotyczącej cyberbezpieczeństwa specjalistów ds. marketingu społecznego. 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"[21]. Wzorem dla takiego serwisu mogłaby być witryna prowadzona przez Narodowe Centrum Cyberbezpieczeństwa Wielkiej Brytanii[22]: w jej projektowaniu brali udział zarówno specjaliści w tej dziedzinie, jak i komunikacji społecznej czy UX i UI (*User Experience* i *User Interface*)[23]. To dobry przykład tego, jak skutecznie komunikować się z obywatelami i podnosić ich świadomość.

Problem z procedurą zgłaszania przestępstw

Ofiary przestępstw internetowych w zdecydowanej większości zgłaszają się po pomoc do Policji[24]. Służba ta nie wypracowała jednak instrukcji i procedur zapewniających efektywną obsługę tych zgłoszeń. Elementy instrukcji zostały co prawda zawarte w materiałach prasowych publikowanych na portalu Policja.pl, ale ich użyteczność okazała

[20] Ibid., s. 40.
[21] Tamże., s. 40.
[22] <https://www.ncsc.gov.uk/>
[23] Chodzi o specjalistów, którzy tak projektują wizualną stronę witryny lub aplikacji, by była ona funkcjonalna, intuicyjna, estetyczna, a w konsekwencji dobrze oceniana przez użytkowników i chętnie przez nich wykorzystywana.
[24] 81% respondentów badania opinii publicznej zleconego przez NIK wskazało Policję jako instytucję, do której mogą się zgłosić po pomoc, gdy staną się celem ataku przestępców internetowych.

się znikoma, ponieważ nie były w trwały sposób wyszczególnione. Tymczasem specyficzny charakter cyberprzestępstw sprawia, że efektywne poszukiwanie sprawcy oraz samo udokumentowanie przestępstwa wymaga zebrania i zabezpieczenia odpowiednich informacji, począwszy od użytkownika komputera lub urządzenia mobilnego. Poszkodowani zgłaszający się do Policji zazwyczaj nie mieli tej wiedzy.

W KGP opracowano natomiast analogiczną instrukcję dla policjantów – „Algorytmy działania Policji w odniesieniu do różnych typów działań przestępczych", którą przekazano terenowym jednostkom Policji i miała być praktyczną pomocą dla funkcjonariuszy nieposiadających wiedzy specjalistycznej. Ustalenia kontroli wykazały jednak, że dokument był obarczony istotnymi wadami. Instrukcja nie była jednoznaczna i spójna, wymagała od zgłaszającego bardzo dużej ilości informacji, a od przyjmującego zgłoszenie specjalistycznej wiedzy informatycznej potrzebnej do oceny materiału dowodowego (a przecież została stworzona jako pomoc dla funkcjonariuszy bez takiej wiedzy). Nie była też aktualizowana ani poddawana ewaluacji. Sam pomysł stworzenia „Algorytmów" NIK oceniła wysoko, jednak nie jego realizację. W połączeniu z brakiem analogicznej instrukcji adresowanej do ofiar cyberprzestępczości mogło to stanowić istotną barierę dla obywateli, którzy chcieliby zgłosić przestępstwo internetowe.

Powyższe ustalenia są zbieżne z wynikami Ogólnopolskiego Badania Wiktymizacyjnego, przeprowadzonego w 2020 r. przez Instytut Wymiaru Sprawiedliwości[25]. Pokazały one, że faktyczna skala oszustw internetowych może być znacznie wyższa niż ta, która wynika z policyjnych statystyk, ponieważ były one najrzadziej zgłaszane.

W przypadku NASK-PIB, który również zajmował się przyjmowaniem zgłoszeń i obsługą incydentów, opracowane procedury były spójne i zostały pozytywie ocenione przez NIK. Jednak tylko 1%. respondentów zleconego przez Izbę badania opinii publicznej posiadał wiedzę na temat możliwości wsparcia ze strony Instytutu. Użyteczność procedur stosowanych w NASK-PIB dla ofiar cyberprzestępstw była w okresie objętym kontrolą ograniczona z powodu niskiej rozpoznawalności tego podmiotu wśród obywateli.

Liczne zaniechania

Negatywnie NIK oceniła nieprzyjmowanie odpowiedzialności przez Ministra Cyfryzacji oraz Pełnomocnika Rządu ds. Cyberbezpieczeństwa za ochronę indywidualnych użytkowników Internetu. Oba podmioty zanegowały przypisane sobie obowiązki w tym zakresie. Pomimo że w latach 2019–2021 dominującą i gwałtownie zwiększającą się kategorią incydentów były te wymierzone w obywateli, oba podmioty nie podjęły działań legislacyjnych i organizacyjnych, które zapewniłyby im ochronę. Na tym

[25] <https://iws.gov.pl/wp-content/uploads/2021/05/IWS_-Wlodarczyk-Madejska-J.-i-in._Ogolnopolskie-Badanie-Wiktymizacyjne-2020.-Raport-z-badania.pdf>

polu powstał spór prawny między Izbą a Ministrem i Pełnomocnikiem Rządu: „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, 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”[26].

Obywatele mają prawo oczekiwać aktywnych działań od centralnych organów władzy państwowej w celu zapewnienia im ochrony przed przestępcami, także tymi działającymi w Internecie. Powinny one odpowiadać aktualnym zagrożeniom, a także być zaplanowane w postaci konkretnych zadań, z przypisanymi im wykonawcami oraz miernikami realizacji. W wypadku dwóch strategicznych dokumentów Rady Ministrów, wyznaczających cele i priorytety państwa w obszarze bezpieczeństwa internetowego, tj. „Strategii cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019–2024” oraz „Planu działań na rzecz wdrożenia strategii cyberbezpieczeństwa” – za koordynację których odpowiada Minister Cyfryzacji i Pełnomocnik Rządu – tych elementów zabrakło. W Planie, będącym dokumentem wykonawczym do Strategii, zabrakło wielu wymienionych w niej elementów związanych ze zwalczaniem cyberprzestępczości, a te, które się tam znalazły, nie zawierały mierników realizacji. W ten sposób te dokumenty stały się kolejnymi przyjmowanymi przez polski rząd w tym obszarze („Polityka ochrony cyberprzestrzeni RP”, „Krajowe ramy polityki cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017–2022”)[27], niezawierającymi konkretów, tj. precyzyjnie wskazanych zadań, terminów realizacji,

[26] Informacja o wynikach kontroli NIK: *Działania państwa*…, op.cit. s. 25.
[27] Zob. m.in. wyniki kontroli NIK *Realizacja przez podmioty państwowe zadań w zakresie ochrony cyberprzestrzeni RP*, nr. ewid. 42/2015/p/14/043/KPB.

osób odpowiedzialnych i przede wszystkim – kalkulacji kosztów oraz wskazania źródeł finansowania. Bez tych elementów nie sposób podejmować strategicznych działań, prowadzących do zapewnienia bezpieczeństwa indywidualnym użytkownikom Internetu. Zabrakło ich po stronie Ministra Cyfryzacji i Pełnomocnika Rządu.

Oba podmioty pozostały także bezczynne wobec masowo podejmowanych kampanii *phishingowych*. Komunikaty NASK i Policji były z kolei rozproszone, często spóźnione i nie docierały do adresatów. W rezultacie obywatele byli pozbawieni aktualnych i pochodzących z oficjalnych źródeł informacji na temat zagrożeń ze strony przestępców komputerowych oraz rekomendowanych środków ochrony.

Te przeszkody i zaniechania złożyły się na sytuację, w której w okresie wzmożonego działania cyberprzestępców, przypadającego na okres pandemii COVID-19 (praca zdalna i nauka przez Internet), obywatele byli narażeni na falę fałszywych e-maili, SMS-ów, prób wyłudzeń tożsamości w mediach społecznościowych, a państwo wydawało się wobec nich bierne i bezradne. Zlecone przez NIK badanie sondażowe[28] potwierdziło, że osoby fizyczne nie wiedziały, co robić ani gdzie się zgłosić w wypadku ataku oszustów komputerowych. Z kolei spośród osób, które mimo wszystko zgłosiło takie przestępstwo, aż 85% odpowiedziało, że ich sprawa nie została wyjaśniona i zakończyła się umorzeniem postępowania lub utratą środków finansowych bądź danych. Tylko 2% spraw zakończyło się wykryciem sprawcy lub odzyskaniem środków[29].

Podsumowanie

Kontrola NIK wykazała, że w latach 2019–2021 najważniejsze organy w Polsce skoncentrowały się na ochronie instytucji i systemów kluczowych dla funkcjonowania kraju. Jednocześnie pomijały obywateli, którzy w okresie wzmożonej działalności cyberprzestępców byli zdani wyłącznie na siebie. Izba nie zakwestionowała szczególnego wsparcia państwa dla instytucjonalnych interesariuszy krajowego systemu cyberbezpieczeństwa. Państwo musi chronić przede wszystkim swoje systemy krytyczne. Jednak pominięcie w działaniach Ministra Cyfryzacji i Pełnomocnika Rządu ds. Cyberbezpieczeństwa ochrony indywidualnych użytkowników sieci było błędem – i to z co najmniej trzech powodów. Po pierwsze, skoro państwo zachęca obywateli, by korzystali z usług e-administracji, a częściowo już od nich tego wymaga, to powinno wziąć współodpowiedzialność za ich bezpieczeństwo w wirtualnej przestrzeni (analogicznie

[28] Badanie przeprowadzono w okresie 20-28 kwietnia 2022 r. z wykorzystaniem metody telefonicznych, standaryzowanych wywiadów kwestionariuszowych wspomaganych komputerowo (CATI) na reprezentatywnej próbie 1000 pełnoletnich mieszkańców Polski. Jego szczegółowe wyniki znajdują się w Informacji o wynikach kontroli NIK: *Działania państwa w zakresie zapobiegania*…, op.cit., s. 40-48.

[29] W wypadku pozostałych spraw respondenci odpowiedzieli, że sprawa jest w toku lub nie mają na jej temat żadnej wiedzy.

do tego, jak wygląda to w przestrzeni fizycznej). Po drugie, wycofanie się państwa z jakiegoś obszaru zachęca przestępców do aktywności, a wzrastająca przez to liczba nielegalnych działań prowadzi do społecznego poczucia bezradności instytucji państwowych i skutkuje brakiem wiary w ich skuteczność, co faktycznie miało miejsce, jak wykazało badanie ankietowe przeprowadzone na zlecenie NIK. Po trzecie, jeśli państwo chce skutecznie chronić swoje kluczowe systemy oraz instytucje nie powinno zapominać, że za ich obsługę odpowiadają ci sami obywatele, którzy – jako osoby prywatne – zostali pominięci w systemie cyberbezpieczeństwa.

Wnioski pokontrolne

Główne wnioski sformułowane przez NIK po zakończeniu kontroli odnosiły się do opisanych wyżej kwestii. Izba rekomendowała m.in.:

- uregulowanie w ustawie o krajowym systemie cyberbezpieczeństwa kwestii ochrony indywidualnych użytkowników Internetu;
- przygotowanie i przedstawienie Radzie Ministrów projektów modyfikacji „Strategii cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019–2024" oraz „Planu działań na rzecz wdrożenia Strategii cyberbezpieczeństwa";
- wdrożenie jednolitego modelu edukowania obywateli na temat bezpieczeństwa w sieci oraz stworzenie rozpoznawalnego, oficjalnego, państwowego serwisu, zawierającego łatwo dostępne informacje na temat cyberzagrożeń, trwających kampanii, a także zaleceń i dobrych praktyk z zakresu cyberhigieny;
- usprawnienie procesu przyjmowania zgłoszeń obywateli w sprawie przestępstw internetowych.

Minister nie zgodził się w wielu kwestiach z ustaleniami NIK. Mimo to nastąpiły już pierwsze zmiany zbieżne z wnioskami Izby. Przede wszystkim widoczny jest zwrot w podejściu Ministra i Pełnomocnika do odpowiedzialności za bezpieczeństwo osób fizycznych. W konsekwencji przygotowano dwa projekty ustaw. Pierwszy ma związek z zapobieganiem kradzieży tożsamości (istotą rozwiązań ujętych w projekcie jest umożliwienie osobie, której dane dotyczą, zastrzeżenia lub cofnięcia zastrzeżenia numeru PESEL za pomocą usługi elektronicznej w specjalnym rejestrze). Drugi dotyczy zwalczania nadużyć w komunikacji elektronicznej (w szczególności polegających na podszywaniu się pod różnego rodzaju instytucje za pomocą połączeń głosowych bądź z wykorzystaniem SMS-ów).

To dopiero pierwszy krok służący wzmocnieniu ochrony. Konieczne są dalsze działania.

W maju 2023 r. Ministerstwo Cyfryzacji przedstawiło wyniki badania świadomości Polaków dotyczące cyberbezpieczeństwa, które wykazało, że o *phishingu* słyszało 47% ankietowanych, o ataku DDoS 21%, a o *ransomware* zaledwie 16%. Są to dane zbieżne z ustaleniami Najwyższej Izby Kontroli.

DANIEL MICHALECKI
główny specjalista kontroli państwowej,
Departament Porządku
i Bezpieczeństwa Wewnętrznego NIK

Słowa kluczowe: zwalczanie przestępstw internetowych, cyberbezpieczeństwo, cyberatak, przestępczość internetowa

Bibliografia:

1. Klimczak J., Siemiaszko A.: *Nękani, oszukiwani, hakowani. Nowe i tradycyjne wymiary wiktymizacji*, Warszawa 2021.
2. *Korzystanie z internetu w 2022 roku*, komunikat nr 77/2022 z badań CBOS, czerwiec 2022.
3. Perlroth N.: *Cyberbroń i wyścig zbrojeń*, MT Biznes, Warszawa 2022.
4. Sanger D.: *Cyberbroń – broń doskonała*, Helion, Gliwice 2021.
5. *Ogólnopolskie Badanie Wiktymizacyjne 2020*, Instytut Wymiaru Sprawiedliwości, Warszawa 2020.

ABSTRACT

Prevention and Combating Internet Crime – Citizens Without Protection

Due to its numerous advantages such as easy communication, speed and comfortable shopping, access to public administration or electronic banking – the internet has become an important element of our lives. It is, however, also an area for criminals, whose victims are both institutions and citizens. Taking into account the growing scale of this phenomenon, the Supreme Audit Office examined whether in the years 2019–2021 the State took effective measures that would allow to identify, prevent or reduce the consequences of internet crime. The audit covered the crimes targeted at individual users of the internet, which may bring financial loss risks. Four entities were audited: the Minister of Digitalisation, the Government Proxy for Cybersecurity, the Police Headquarters and the Scientific and Academic Computer Network – the State Research Institute. The findings of the NIK audit show that these entities focused on protection of the systems of key importance for the State. Simultaneously, they ignored citizens who, at the time of increased activities of cybercriminals, were left alone.

Daniel Michalecki, senior public audit expert, Department of Public Order & Internal Security of NIK

Key words: combating internet crime, cybersecurity, cyberattack, internet crime