PREZES
NAJWYŻSZEJ IZBY KONTROLI
Marian Banaś

KPB. 411.004.01.2022

Pan
Mateusz Morawiecki
Minister Cyfryzacji
Kancelaria Prezesa Rady Ministrów
ul. Królewska 27, 00-060 Warszawa

WYSTĄPIENIE POKONTROLNE

I/22/003/KPB - Funkcjonowanie Krajowego Węzła Identyfikacji Elektronicznej

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, ul. Królewska 27, 00-060 Warszawa[1]
Kierownik jednostki kontrolowanej	Mateusz Morawiecki, Minister Cyfryzacji od dnia 6 października 2020 r.[2] (dalej także: Minister) W okresie objętym kontrolą funkcję kierownika jednostki poprzednio pełnili: Anna Streżyńska, Minister Cyfryzacji, od 16 listopada 2015 r. do 9 stycznia 2018 r. Marek Zagórski, Minister Cyfryzacji, od 17 kwietnia 2018 r. do 6 października 2020 r.
Zakres przedmiotowy kontroli	1. funkcjonowanie Krajowego Węzła Identyfikacji Elektronicznej (dalej także: KWIE, Węzeł, WK); 2. organizacja Krajowego Schematu Identyfikacji Elektronicznej; 3. poziom bezpieczeństwa systemów identyfikacja elektronicznej podłączonych do KWIE – w tym incydenty bezpieczeństwa; 4. nadzór nad KWIE; 5. nadzór nad środkami identyfikacji elektroniczne podłączonymi do KWIE; 6. proces notyfikacji w UE krajowych środków identyfikacji elektronicznej podłączonych do KWIE.
Okres objęty kontrolą	1 stycznia 2016 r. – 31 października 2022 r., z wykorzystaniem dokumentów sporządzonych przed tym okresem lub po nim, o ile mają one związek z kontrolowaną działalnością
Podstawa prawna podjęcia kontroli	Art. 2 ust. 1 ustawy z dnia 23 grudnia 1994 r. o Najwyższej Izbie Kontroli[3]
Jednostka przeprowadzająca kontrolę	Najwyższa Izba Kontroli Departament Porządku i Bezpieczeństwa Wewnętrznego
Kontrolerzy	Adam Zakrzewski, główny specjalista kontroli państwowej, upoważnienie do kontroli nr KPB/125/2022 z 24 listopada 2022 r. Daniel Michalecki, główny specjalista kontroli państwowej, upoważnienie do kontroli nr KPB/126/2022 z 24 listopada 2022 r. (akta kontroli str. (akta kontroli str. 1-4)

[1] 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 Kancelarii Prezesa Rady Ministrów.

[2] Postanowienie Prezydenta Rzeczypospolitej Polskiej z dnia 6 października 2020 r. nr 1131.27.2020 o zmianie w składzie Rady Ministrów (M. P. poz. 896).

[3] Dz. U. z 2022 r. poz. 623, dalej: ustawa o NIK.

II. Ocena ogólna[4] kontrolowanej działalności

OCENA OGÓLNA

Minister Cyfryzacji rzetelnie opracował koncepcję Krajowego Węzła Identyfikacji Elektronicznej i na jej podstawie wdrożył rozwiązanie, które w jednym narzędziu zintegrowało Dostawców usług oraz Dostawców Środków Identyfikacji[5]. Wybrany model Węzła sprzyjał realizacji głównego celu projektu, tj. upowszechnieniu w Polsce usług online wymagających uwierzytelnienia. Minister opracował i opublikował procedury integracji z KWIE, które zapewniły zarówno transparentność, jak i standaryzację tego procesu. Rzetelnie wywiązywał się z obowiązku nadzoru nad przyłączaniem do Węzła Dostawców Środków Identyfikacji, a sam WK poddawany był zewnętrznym audytom i testom bezpieczeństwa.

Kontrola NIK wykazała jednak, że Minister po etapie przyłączenia do Węzła nie kontynuował kontroli w ramach systemu identyfikacji elektronicznej eID[6], ograniczając się do przeprowadzania badań ankietowych. Z kolei sposób realizacji wybranych do kontroli wymagań Polityki Bezpieczeństwa Informacji Węzła Krajowego, jej polityk szczegółowych i procedur zwiększył w ocenie NIK ryzyko wystąpienia incydentów bezpieczeństwa informacji. W wyniku kontroli stwierdzono bowiem nieprawidłowości związane z: procesem zarządzania ryzykiem, przeglądami bezpieczeństwa informacji, procesem informowania ministra właściwego do spraw cyfryzacji o stanie bezpieczeństwa WK, wewnętrznymi audytami bezpieczeństwa WK, publikacją treści Polityki Bezpieczeństwa WK oraz zasadami uprawnionego dostępu do WK. W trakcie kontroli, która ze względu na swój doraźny charakter miała ograniczony zakres, nie ustalono bezpośredniego związku pomiędzy stwierdzonymi nieprawidłowościami, a konkretnymi zidentyfikowanymi incydentami bezpieczeństwa informacji, należy jednak liczyć się z możliwością, że takie naruszenia bezpieczeństwa mają miejsce, ale nie zostały jeszcze wykryte.

III. Opis ustalonego stanu faktycznego

Opis stanu faktycznego

Przed uruchomieniem Krajowego Węzła Identyfikacji Elektronicznej brak było możliwości łączenia w ujednolicony sposób Dostawców Tożsamości z Dostawcami Usług. Poszczególne systemy informatyczne administracji publicznej wykorzystywały w procesie identyfikacji elektronicznej użytkowników głównie wewnętrzne mechanizmy[7]. Wymagało to od każdego systemu odrębnej integracji z dostępnymi dostawcami środków identyfikacji elektronicznej. Z kolei użytkownik e-usług zmuszony był do zakładania wielu kont, aby mieć dostęp do systemów świadczących określone usługi. Ponieważ usługodawcy stosowali na ogół zabezpieczenia adekwatne do świadczonych przez siebie usług (innych zabezpieczeń mógł wymagać bank, a innych instytucja administracji publicznej), użytkownik zobligowany był do uczenia się i zapamiętywania różnych sposobów identyfikowania się w wielu systemach zarządzanych przez poszczególnych dostawców usług.

(akta kontroli str. akta kontroli str. 7-20, pliki 001, 029)

---

[4] Najwyższa Izba Kontroli formułuje ocenę ogólną jako ocenę pozytywną, ocenę negatywną albo ocenę w formie opisowej.

[5] Dostawca usług - podmiot lub system oferujący usługi online (inne niż identyfikacja i uwierzytelnienie). Dostawcą usługi może być podmiot publiczny lub prywatny, np. ePUAP świadczący usługę wydania dowodu osobistego. Dostawca tożsamości (lub Dostawca środków identyfikacji elektronicznej, DŚI) - podmiot odpowiedzialny za rejestrację osób i wydawanie im środków identyfikacji elektronicznej (eID). Wydaje środki identyfikacji na określonych poziomach bezpieczeństwa (zaufania), np. Ministerstwo Cyfryzacji wydające obywatelom Profil Zaufany, czy też bank wydający środki identyfikacji swoim klientom.

[6] System eID (mojeID) – system identyfikacji elektronicznej przyłączony do WK (obok Publicznego Systemu Identyfikacji Elektronicznej). W jego ramach funkcjonują poszczególne środki identyfikacji wydawane przez banki. W momencie zakończenia kontroli liczba takich „bankowych środków" wynosiła 526.

[7] Funkcjonujący mechanizm Profilu Zaufanego był wykorzystywany w niezadowalającym stopniu, co powodowało konieczność rozwijania wewnętrznych systemów identyfikujących użytkowników u każdego usługodawcy.

KWIE zaplanowano jako odpowiedź na powyższe problemy. Powszechny system identyfikacji elektronicznej i uwierzytelniania miał zdjąć odpowiedzialność za te mechanizmy z usługodawców, zintegrować w jednym rozwiązaniu dostawców usług, atrybutów[8] i środków identyfikacji, dynamicznie zarządzać wymaganym poziomem zabezpieczeń oraz chronić użytkowników m.in. poprzez automatyczne powiadamianie o każdym użyciu ich e-tożsamości w ramach Węzła. Wytworzony w trakcie przygotowań do utworzenia KWIE *Opis założeń projektu informatycznego: Budowa Krajowego Węzła Identyfikacji Elektronicznej* (pełniący rolę tzw. fiszki projektowej), definiował jako cel nadrzędny dla WK stworzenie warunków i narzędzia umożliwiającego upowszechnienie usług online wymagających uwierzytelnienia. Wdrożenie tego rozwiązania miało także zwiększyć bezpieczeństwo usług cyfrowych, m.in. poprzez ujednolicenie standardu integracji, stworzenie przejrzystego modelu identyfikacji elektronicznej oraz wprowadzenie wspólnego standardu dla interfejsów zgodnego z wymaganiami Rozporządzenia Parlamentu Europejskiego i Rady (UE) NR 910/2014 z dnia 23 lipca 2014 r., w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylającego dyrektywę 1999/93/WE[9], zwanego także Rozporządzeniem eIDAS.

(akta kontroli str. 7-20, pliki 029, 030)

W styczniu 2017 r. podpisana została umowa na utworzenie KWIE z Centralnym Ośrodkiem Informatyki. Do maja 2017 r. przeprowadzono analizę biznesowo-techniczną, w wyniku której powstał Projekt Techniczny WK[10]. Historia zmian tego dokumentu wskazuje na dokonywane w nim aktualizacje między marcem 2017 r. a lutym 2018 r.[11] Wersja produkcyjna systemu uruchomiona została we wrześniu 2018 r., tj. trzynaście miesięcy po zaplanowanym pierwotnie terminie jego wdrożenia (początkowo zakładano uruchomienie WK w sierpniu 2017 r.). Główną przyczyną opóźnienia były przedłużające się uzgodnienia międzyresortowe w obszarze zmian prawnych towarzyszących KWIE oraz fluktuacje personelu w zespole projektowym (w tym na stanowisku Kierownika Projektu po stronie Wykonawcy).

(akta kontroli str. 7-20, pliki 038, 178)

Rozwiązania przyjęte w KWIE opierały się na tzw. modelu federacyjnym, tj. funkcjonowały one w oparciu o wiele środków identyfikacji elektronicznej wydawanych przez różne podmioty. Złożyło się na to zarówno to, jakie rozwiązania stosowano w Polsce przed wdrożeniem Węzła (m.in. istniejąca już możliwość potwierdzania Profilu Zaufanego za pomocą poświadczeń bankowych), jak i wnioski wypływające z analizy porównującej rozwiązania regulujące problematykę eID[12] w Austrii i Szwecji. Wynikało z niej, że rozwój rynku eID, a co za tym idzie usług realizowanych drogą elektroniczną, w tym e-gov, jest łatwiejszy do osiągnięcia przy modelu federacyjnym, tak jak miało to miejsce w Szwecji[13]. Przyjęcie tego modelu

---

[8] Dostawca atrybutów – to podmiot odpowiedzialny za uzupełnianie danych identyfikacyjnych przekazanych od Dostawców Tożsamości o dodatkowe atrybuty. Dostawcami Atrybutów są np. rejestry państwowe.

[9] Dz. Urz. UE. L. 257 z 28.08.2014, str. 73.

[10] Pn.: Krajowy Węzeł Identyfikacji Elektronicznej - Projekt Techniczny.

[11] Dokumentacja techniczna nie była po tym okresie aktualizowana, jednak w ramach kolejnych modyfikacji systemu wykonywane były opisy zmian, które Ministerstwo otrzymywało wraz z odbiorem zleceń.

[12] Identyfikacja elektroniczna, identyfikacja w usługach online.

[13] W Austrii przyjęto model centralny funkcjonujący w oparciu o uznawany przez państwo powszechny środek identyfikacji elektronicznej. Szwecja była przykładem państwa, które zdecydowało się na model federacyjny, istniejący w oparciu o wiele środków identyfikacji elektronicznej wydawanych przez różne podmioty. Model szwedzki osiągnął znacznie lepsze rezultaty niż austriacki – środki identyfikacji elektronicznej były tam znacznie częściej wykorzystywane. Złożyło się na to m.in. to, że model centralny ograniczony jest rozwojem centralnej infrastruktury, przez co posiada znacznie większą bezwładność. Dodatkowo infrastruktura techniczna w Austrii uznawana była za skomplikowaną i ograniczającą rozwój e-usług. W Szwecji, która przyjęła model otwarty, firmy działały bez uzależnienia od instytucji państwowych w zakresie tworzenia i integracji rozwiązań. Realizacje obu

było więc zbieżne z głównym celem projektu budowy Węzła, tj. upowszechnianiem w Polsce usług online wymagających uwierzytelnienia.

(akta kontroli str. 7-20, plik 029, 038)

WK wykorzystywał dwa ośrodki przetwarzania danych, którymi zarządzał Centralny Ośrodek Informatyki na podstawie umowy utrzymaniowej. Za bezpieczeństwo fizyczne tych ośrodków odpowiadała Komenda Główna Policji[14] oraz konsorcjum NASK PIB i NASK S.A. Planowane jest utworzenie trzeciego, zapasowego ośrodka przetwarzania danych[15] w ramach realizacji projektu Krajowego Centrum Przetwarzania Danych, który – według wyjaśnień Dyrektor Departamentu Tożsamości Cyfrowej KPRM – ma zostać sfinansowany z Krajowego Planu Odbudowy i Zwiększania Odporności (KPO) i powstać do połowy 2026 r.

(akta kontroli str. 7-20, pliki 178, 182)

Na podstawie aktualnych na dzień 22 grudnia 2022 r. wskaźników należy stwierdzić, że cele i korzyści wynikające z wdrożenia projektu KWIE zostały w znacznej mierze osiągnięte (raport zamykający projekt wskazuje na osiągnięcie wszystkich celów, z wyjątkiem jednego, od realizacji którego odstąpiono). Z WK zintegrowanych zostało 524 dostawców środków identyfikacji oraz 1203 dostawców usług. Wypracowano standard integracji z Węzłem dla dostawców środków identyfikacji (DŚI) i dostawców usług (DU). Liczba logowań do Węzła Krajowego wzrastała z roku na rok: w 2018 r. wyniosła 2 802 139, w 2019 r. 26 686 787, w 2020 r. 125 270 986, a w 2021 r. osiągnęła 328 492 369. Liczba unikatowych użytkowników z wydanymi narzędziami eID wzrosła z 1 324 438 w 2017 r. do 13 426 360 w roku 2021.

(akta kontroli str. 5-6, 7-20, pliki 039, 046, 054, 194-195, 199)

Minister monitorował cele związane z KWIE. W Planach działalności Ministra Cyfryzacji w kolejnych latach określano cel polegający na zwiększeniu liczby podmiotów realizujących zadania publiczne dysponujących możliwością komunikowania się drogą elektroniczną. Miernikiem określającym stopień realizacji tego celu była liczba podmiotów przyłączonych do Węzła Krajowego. Przykładowo w planie na 2021 r. założono przyłączenie stu nowych podmiotów. Według sprawozdania z wykonania planu działalności do 31 grudnia 2021 r. przyłączono takich podmiotów 407[16]. Dokonano także całościowego podsumowania celów i korzyści[17] wraz z zamknięciem projektu budowy Węzła. NIK zwróciła jednak uwagę, że prognozy i założenia dotyczące korzystania w kolejnych latach z publicznych e-usług – na podstawie których określono wymagania dla infrastruktury środowiska produkcyjnego WK – okazały się w części trudne do zweryfikowania. Ministerstwo nie potrafiło przedstawić aktualnych danych odnoszących się do szacowanej średniej aktywności użytkowników, którzy zarejestrowali Profil Zaufany w latach poprzednich w relacji do wyliczanego, szacowanego procentu aktywnych użytkowników logujących się w celu sprawdzenia konta miesięcznie, poziomu cyfryzacji społeczeństwa (tj. udziału usług wykonywanych za pośrednictwem mediów elektronicznych), a także szacowanego rocznego wzrostu wykorzystania usług publicznych w stosunku do roku 2015 czy 2016.

(akta kontroli str. 7-20, pliki 029, 054, 195-195, 199)

---

modeli mają swoje zalety i wady. Przykładowo w Austrii państwo zapewniało kompletną infrastrukturę i ponosiło ciężar inwestycji i utrzymania schematu eID, ale za to oferowane w jego ramach usługi były darmowe.

[14] Na podstawie Porozumienia zawartego w dniu 15 marca 2022 r.

[15] Pierwotny projekt budowy Węzła zakładał powstanie w przyszłości dodatkowego, zapasowego ośrodka przetwarzania danych.

[16] (odczyt w dn. 9 stycznia 2023 r.); https://www.gov.pl/web/premier/sprawozdanie-z-wykonania-planu-dzialalnosci-za-rok-2021-z-dzialu-administracji-rzadowej-informatyzacja.

[17] Określonych w Opisie założeń projektu.

KWIE poddany został dwóm audytom bezpieczeństwa. Pierwszy wykonany został przez ABW w 2019 r., a drugi przez Centralny Ośrodek Informatyki (dalej także: COI) w 2021 r. Z kolei środki identyfikacji w ramach Publicznego Systemu Identyfikacji Elektronicznej poddane zostały następującym badaniom: dowód osobisty z warstwą elektroniczną został kompleksowo oceniony przez NASK oraz Instytut Łączności - Państwowy Instytut Badawczy, natomiast w przypadku Profilu Zaufanego zespół audytu wewnętrznego KPRM dokonał na przełomie 2021 i 2022 r. oceny zgodności tego środka z wymogami Rozporządzenia Wykonawczego Komisji (UE) 2015/1502 z dnia 8 września 2015 r.

(akta kontroli str. 7-20, pliki 047, 043-044)

W związku z decyzjami wydawanymi na podstawie art. 21b ustawy o usługach zaufania oraz identyfikacji elektronicznej[18] (dalej także: ustawa o usługach zaufania) Minister opracował i opublikował procedury integracji z KWIE dla Dostawców Usług i Dostawców Środków Identyfikacji[19]. Procedury te spełniały założone w projekcie warunki zarówno transparentności, jak i standaryzacji dla procesu integracji z Węzłem. Badanie dokumentacji z przyłączenia pięciu losowo wybranych DŚI potwierdziło, że procedura opracowana przez Ministra była przestrzegana, a jej poszczególne etapy (w tym testy integracyjne i weryfikujące deklarowany poziom bezpieczeństwa) zostały zrealizowane w każdym z badanych przypadków. W celu realizacji obowiązku wynikającego z art. 39b ust. 1 pkt 1 lit. a ww. ustawy, tj. nadzoru na DŚI już przyłączonymi do Węzła, Minister prowadził badania ankietowe[20]. Pozwalały one na wyodrębnienie słabych i mocnych stron podłączonych do Węzła podmiotów. NIK docenia tę inicjatywę i uważa za wartościową, zwraca jednak uwagę, że wyniki takich ankiet mają charakter deklaratywny i mogą być elementem jedynie komplementarnym wobec działań kontrolnych, do których zobowiązuje Ministra ww. ustawa (więcej o tym w sekcji *Stwierdzone nieprawidłowości*).

(akta kontroli str. 7-20, pliki 046, 109-175, 196-198)

W przypadku przyłączonych do Węzła Krajowego systemów teleinformatycznych udostępniających usługi online Minister zgodnie z art. 39b ust. 1 pkt 1 lit. b ustawy o usługach zaufania przeprowadził w latach 2019-2020 sześć kontroli[21] w zakresie spełniania przez przyłączone systemy wymagań, o których mowa w art. 21t ust. 1 tej regulacji. Działania te Minister wzmocnił dodatkowo opisanymi wyżej badaniami ankietowymi.

(akta kontroli str. 7-20, plik 046, str. 22, pliki 1-7)

Połączenie polskiego Publicznego Systemu Identyfikacji Elektronicznej z systemami innych krajów UE możliwe będzie po dokonaniu jego notyfikacji Komisji Europejskiej. Dla zapewnienia odpowiedniego poziomu bezpieczeństwa logowania przyjęto bowiem, że do systemu logowania transgranicznego dopuszczone są jedynie notyfikowane, czyli sprawdzone pod względem bezpieczeństwa i zaakceptowane przez kraje UE, systemy logowania państw członkowskich[22]. Pierwotnie Minister Cyfryzacji planował notyfikację wyłącznie profilu zaufanego (na średnim poziomie bezpieczeństwa). Prace przygotowawcze do notyfikacji tego środka identyfikacji rozpoczęły się w 2017 roku. Były one jednak przerywane lub wstrzymywane

[18] Z dnia 5 września 2016 r. (Dz. U. 2021 r. poz. 1797).

[19] Link do strony: https://mc.bip.gov.pl/interoperacyjnosc-mc/wezel-krajowy-dokumentacja-dotyczaca-integracji-z-wezlem-krajowym.html

[20] W latach 2021-2022 badaniami ankietowymi objęto łącznie 229 podmiotów przyłączonych do Węzła, w tym podmiot odpowiedzialny za system identyfikacji elektronicznej mojeID.

[21] Kontrolą objęto: Starostwo Powiatu Warszawskiego Zachodniego, Urząd Transportu Kolejowego, Stowarzyszenie Notariuszy Rzeczypospolitej Polskiej w Warszawie, Urząd Gminy Gniezno, Urząd Miasta Ostrołęki, Urząd Miasta i Gminy Góra Kalwaria.

[22] https://www.gov.pl/web/cyfryzacja/budowa-i-wdrozenie-wezla-transgranicznego

w związku ze zmieniającą się koncepcją rozwoju środków identyfikacji, pandemią oraz przybyciem do Polski znacznej liczby obywateli Ukrainy wywołanym konfliktem zbrojnym na terytorium tego kraju. Prace nad notyfikacją zostały początkowo wstrzymane z powodu planów dotyczących wprowadzenia dowodu osobistego z warstwą elektroniczną[23]. Wprowadzenie e-dowodu wpłynęłoby na mechanizmy uwierzytelniania w profilu zaufanym i stanowiłoby podstawę do jednoczesnej notyfikacji tego środka na wysokim poziomie bezpieczeństwa. Zdecydowano więc o łącznej notyfikacji obu środków[24]. Kolejną przyczyną opóźniającą rozpoczęcie procesu notyfikacji było planowane wprowadzenie możliwości potwierdzania profilu zaufanego przez lekarza, pielęgniarkę lub położną podstawowej opieki zdrowotnej[25]. W związku z epidemią COVID-19 wprowadzono z kolei możliwość potwierdzenia tożsamości (poprzedzającej wydanie profilu zaufanego) podczas rejestrowanej transmisji audiowizualnej. Wreszcie wybuch wojny w Ukrainie – a w konsekwencji fala uchodźców chroniących się na terytorium RP – wymusiły wprowadzenie kolejnych zmian związanych z potwierdzeniem profilu zaufanego dla obywateli Ukrainy. W związku z tym, że – zgodnie z wyjaśnieniami Dyrektor DTC – „każda modyfikacja w notyfikowanym systemie identyfikacji również wymaga notyfikacji[26], a proces ten trwa około sześciu miesięcy" i wiąże się z określonymi nakładami, zdecydowano, że rozpocznie się on po utrwaleniu powyższych zmian.

(akta kontroli str. 7-20, 046)

Ostatecznie w ramach współpracy z NASK wytworzono niezbędną do notyfikacji dokumentację[27]. W okresie grudzień 2021 - styczeń 2022 przeprowadzono pod kierunkiem Koordynatora Zespołu Audytu Wewnętrznego KPRM badanie zgodności profilu zaufanego z wymogami rozporządzenia wykonawczego KE w sprawie ustanowienia minimalnych specyfikacji technicznych i procedur dotyczących poziomów zaufania w zakresie środków identyfikacji elektronicznej[28]. W dniu 14 czerwca 2022 r. strona polska poinformowała KE o rozpoczęciu procesu notyfikacji[29] oraz przekazała stosowną dokumentację (tj. wniosek notyfikacyjny[30], załączniki opisujące zgodność notyfikowanych środków identyfikacji z wymogami prawa oraz tzw. *whitepaper* z dodatkowymi wyjaśnieniami nieujętymi w pozostałych dokumentach). Publiczny System Identyfikacji Elektronicznej zaprezentowany został stronie unijnej 27 czerwca 2022 r. podczas spotkaniu Grupy Sieci Współpracy. Następnie utworzony został tzw. zespół oceniający, w skład którego weszli przedstawiciele wybranych państw członkowskich UE[31]. Proces oceny, w którym

---

[23] Zrealizowane ustawą z dnia z dnia 6 grudnia 2018 r. o zmianie ustawy o dowodach osobistych oraz niektórych innych ustaw (Dz.U. z 2019 r. poz. 60).

[24] Warto zauważyć, że ówcześnie wszystkie państwa członkowskie (z wyjątkiem Danii), które poddały się notyfikacji, dysponowały środkiem identyfikacji elektronicznej o wysokim stopniu bezpieczeństwa.

[25] Zrealizowane ustawą z dnia 19 lipca 2019 r. o zmianie niektórych ustaw w związku z wdrażaniem rozwiązań w obszarze e-zdrowia (Dz.U. z 2019 r. poz. 1590).

[26] Wynika to z art. 9 ust. 1 Rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 z dnia 23 lipca 2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylającego dyrektywę 1999/93/WE.

[27] Prace związane z notyfikacją Publicznego Systemu Identyfikacji Elektronicznej realizowane były we współpracy z NASK od kwietnia 2020 r.

[28] Rozporządzenie Wykonawcze Komisji (UE) 2015/1502 z dnia 8 września 2015 r. w sprawie ustanowienia minimalnych specyfikacji technicznych i procedur dotyczących poziomów zaufania w zakresie środków identyfikacji elektronicznej na podstawie art. 8 ust. 3 rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym (Dz. Urz. L 235 z 9.09.2015, str.7, ze zm.).

[29] Ten etap określa się etapem prenotyfikacji.

[30] Wniosek był zgodny z wymogami określonymi w decyzji wykonawczej Komisji (UE) 2015/1984 z dnia 3 listopada 2015 r. w sprawie określenia okoliczności, formatów i procedur notyfikacji zgodnie z art. 9 ust. 5 rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym.

[31] W skład zespołu oceniającego weszły: Estonia jako państwo koordynujące, Niemcy i Słowenia jako państwa raportujące oraz Belgia, Finlandia, Francja, Austria.

aktywną rolę odgrywała strona polska, rozpoczął się 9 sierpnia 2022 r. Łącznie udzielono odpowiedzi na 64 szczegółowe pytania. Ocena wykazała, że w ramach Publicznego Systemu Identyfikacji Elektronicznej dwa elementy wymagają poprawy[32]. Na spotkaniu Grupy Sieci Współpracy w dniach 12-13 grudnia 2022 r. zespół oceniający przedstawił wyniki przeprowadzonego badania zgodności. Potwierdzono, że wydawane w ramach Publicznego Schematu Identyfikacji Elektronicznej środki: Profil Zaufany i Profil Osobisty[33], spełniają wymagania Rozporządzenia eIDAS odnośnie do poziomu wysokiego dla Profilu Osobistego oraz poziomu średniego dla Profilu Zaufanego. Opinia ta jest w procesie notyfikacyjnym podstawą do wydania decyzji o notyfikacji przez Komisję Europejską.

(akta kontroli str. 7-20, pliki 046, 055-086, 182)

Dla Systemu Węzła Krajowego opracowano i wdrożono w styczniu 2020 r. Politykę Bezpieczeństwa Informacji. Zawierała ona zalecenia i regulacje dotyczące obszaru bezpieczeństwa informacji opracowane w oparciu o międzynarodową normę PN ISO/IEC 27001, których spełnienie pozwalało na zapewnienie odpowiedniego poziomu bezpieczeństwa dla całej organizacji (Ministerstwa Cyfryzacji, KPRM) ze szczególnym uwzględnieniem systemu informatycznego Węzła Krajowego. Obejmowała ona całościowo obszar IT podlegający regulacji: opisywała obszar działania i wpływu organizacji (kontekst organizacji), użytkowników danego systemu (Interesariuszy), wprowadziła ciągłą ocenę ryzyka funkcjonowania systemu informatycznego Węzła Krajowego, opisano w niej proces zapewnienia wymaganych zasobów i kompetencji. Określiła także explicite sposoby zapewnienia bezpieczeństwa informatycznego Węzła Krajowego poprzez wskazanie ścisłych zasad, zaleceń oraz procedur działania dla wszystkich uczestniczących stron.

(akta kontroli str. 7-20, pliki 37)

Realizacja Polityki bezpieczeństwa informacji dla Węzła Krajowego (PBI WK) napotkała w kontrolowanym okresie szereg trudności, których szczegółowy opis zawarto poniżej, w sekcji *Stwierdzone nieprawidłowości.*

Od czasu, kiedy zarządzanie bezpieczeństwem informacji systemu WK powierzono Departamentowi Tożsamości Cyfrowej KPRM (DTC), tj. od 11 lutego 2022 r. podjęte zostały działania mające na celu zapewnienie odpowiedniego zaplecza kadrowego dla realizacji zadań związanych z aktualizacją dokumentacji dotyczącej bezpieczeństwa informacji. Z dniem 1 kwietnia 2022 r. nowo pozyskanemu pracownikowi zostało wydane polecenie służbowe dot. przeglądu i aktualizacji kluczowego dokumentu z obszaru bezpieczeństwa informacji Węzła Krajowego, tj. PBI WK. Pierwszym efektem tych działań było wytworzenie 15 kwietnia 2022 r. dokumentu, który zawierał wstępne uwagi do PBI WK. Kolejne, pogłębione prace nad tym dokumentem zaowocowały wytworzeniem nowej wersji PBI WK, która została przekazana do wewnętrznego zaopiniowania w KPRM. Do momentu zakończenia kontroli nowa wersja PBI WK nie została zatwierdzona.

(akta kontroli str. 7-20, pliki 37, 55)

Stwierdzone nieprawidłowości

W działalności kontrolowanej jednostki w przedstawionym wyżej zakresie stwierdzono następujące nieprawidłowości:

1. Minister nie prowadził kontroli, do których zobowiązuje go art. 39b ust. 1 pkt 1 lit. a ustawy o usługach zaufania. Przeprowadzał co prawda badania ankietowe,

[32] Uwagi dotyczyły dwóch zagadnień związanych odpowiednio ze zdalnym potwierdzaniem tożsamości przed wydaniem profilu zaufanego oraz potwierdzaniem profilu zaufanego za pomocą profilu osobistego.

[33] Profil osobisty powiązany jest z dowodem osobistym z warstwą elektroniczną – dowód taki pozwala na identyfikację elektroniczną.

które pozwalały na wyodrębnienie słabych i mocnych stron podłączonych do Węzła podmiotów, jednak miały one charakter deklaratywny i zdaniem NIK nie mogły zastąpić przewidzianych prawem działań kontrolnych. NIK zwróciła szczególną uwagę, że Minister nie kontrolował, czy w ramach systemu identyfikacji eID (mojeID) zachowywane są zadeklarowane poziomy bezpieczeństwa. Minister wyjaśnił, że poprawność przygotowanych przez poszczególnych dostawców tożsamości rozwiązań oraz ich zgodność z eIDAS są testowane i weryfikowane przed przyłączeniem do Węzła. Z kolei Dyrektor Departamentu Tożsamości Cyfrowej (pełniąca rolę Gestora systemu WK) wyjaśniła, że banki zgodnie z § 19 ust. 1 pkt 3 rozporządzenia Ministra Cyfryzacji z dnia 29 czerwca 2020 r. w sprawie profilu zaufanego i podpisu zaufanego[34] zobowiązane są do poddawania się niezależnemu audytowi, o którym mowa w pkt 2.4.7 załącznika do rozporządzenia wykonawczego 2015/1502, sprawdzającemu spełnianie wymagań, o których mowa w pkt 1 i 2, nie rzadziej niż raz na dwa lata, i w przypadku zmiany poziomu bezpieczeństwa wynik audytu wykazałby niezgodność. Dodatkowo sposoby logowania za pomocą bankowości oparte są o politykę ustanowioną w Banku, zgodną z PSD2[35], która wymusza na nich drugi faktor uwierzytelnienia, czyli średni poziom bezpieczeństwa.

W opinii NIK działania audytowe prywatnych podmiotów nie mogą zastąpić ustawowego nadzoru Ministra, a polityka ustanowiona w Banku powinna zgodnie z przytoczonym przepisem ustawy o usługach zaufania podlegać weryfikacji w taki sposób, w jaki podlegała przy przyłączeniu danego podmiotu do Węzła. W konsekwencji nieprzeprowadzania kontroli Minister pozbawił się wiedzy o aktualności zadeklarowanych przez dostawców tożsamości poziomów bezpieczeństwa. To z kolei mogło zwiększyć ryzyko nieutrzymania przez nich zadeklarowanego w trakcie przyłączenia do Węzła poziomu bezpieczeństwa.

(akta kontroli str. 7-20, pliki 046, 109, 183; str. 22, plik 004)

2. Kontrolujący dokonali przeglądu wybranych w oparciu o własną analizę ryzyka obszarów działania WK regulowanych przez PBI WK. Zidentyfikowano następujące nieprawidłowości:

2.1. Obszar Zarządzanie ryzykiem

Proces zarządzania ryzykiem dla systemu WK nie był dokumentowany zgodnie z wymaganiami załącznika 1.6 PBI WK, a ponadto w kontrolowanym okresie nie były prowadzone udokumentowane przeglądy ryzyka.

PBI WK wyznacza reguły postępowania z ryzykiem i wiąże się ze stosowaniem określonych reguł we wszystkich obszarach i czynnościach, które mogą być zagrożone wystąpieniem określonych słabości (podatności). Działania zmierzające do obsługi danego ryzyka powinny być prowadzone cyklicznie (np. systematyczna ocena podatności systemu wraz z analizą ryzyka), jak również, jeżeli wymaga tego sytuacja ad-hoc (np. ocena ryzyka wynikającego ze zmiany w procesie lub zmiany w oprogramowaniu). Proces identyfikacji, szacowania oraz postępowania z ryzykiem powinien być stosowany przy podejmowaniu wszystkich ważniejszych decyzji dotyczących zarówno wymiaru organizacyjnego, jak i technicznego w zakresie działania Systemu. Realizacja procesu zarządzania ryzykiem wiązała się między innymi ze sporządzaniem następujących wskazanych w załączniku 1.6 do PBI WK dokumentów:

[34] Dz.U. z 2020 r. poz. 1194, ze zm.

[35] PSD2 (ang. Payment Services Directive) to unijna dyrektywa dotycząca usług płatniczych. Jej regulacje zostały wprowadzone do polskiego porządku prawnego.

„Dokumentowanie procesu zarządzania ryzykiem", „Słabości i zabezpieczenia WK".

Kontrolującym nie przekazano żadnego z powyższych dokumentów, a jako potwierdzenie realizacji procesu zarządzania ryzykiem przedstawiono im inne opracowanie, które nie były zgodne z wymaganiami PBI WK[36].

Pan Janusz Cieszyński, Sekretarz Stanu w KPRM, w odpowiedzi udzielonej w imieniu Ministra Cyfryzacji oświadczył, że: „ocena ryzyka jest procesem ciągłym i potwierdzające to dokumenty zostały przekazane do NIK (...)" Nie odniósł się natomiast do kwestii braku zgodności tych dokumentów z PBI WK.

W pkt 5.4 załącznika 1.6 do PBI WK określono również wymóg cyklicznego dokonywania przeglądów ryzyka dotyczącego funkcjonowania Węzła. Monitoringowi powinny podlegać wszystkie czynniki, które mogą mieć wpływ na poziom zidentyfikowanego już ryzyka, a także powodować nowe zagrożenia. Powinien on obejmować zabezpieczenia, w wymiarze ich wpływu na redukcję poziomu zagrożenia (czy też redukcję możliwości wykorzystania podatności) oraz same podatności i zagrożenia. Każdy przegląd powinien być udokumentowany i odbywać się co najmniej raz do roku, jak również ad-hoc, w sytuacji istotnej zmiany związanej z otoczeniem lub funkcjonowaniem systemu.

Kontrolującym nie przedstawiono dokumentów potwierdzających dokonywanie w badanym okresie cyklicznych przeglądów zarejestrowanych ryzyk, a jedyny taki przegląd przeprowadzono dopiero w trakcie trwania kontroli NIK[37]. Wyniki tego przeglądu nie skutkowały jednak uzupełnieniem rejestru ryzyk o zaistniałe w kontrolowanym okresie zagrożenia, przedstawione w przekazanych kontrolującym wyjaśnieniach, tj.: podatność SMS w procesie uwierzytelniania, wprowadzenie stopni alarmowych CRP, niecelowość publikacji pełnej treści PBI WK, podatności Meltdown, Spectre i Apache Log4j.

Odpowiedzialność za utrzymanie, nadzór całościowy nad Węzłem Krajowym, w tym także za realizację i koordynację procesu zarządzania ryzykiem ponosił Gestor systemu WK[38].

Skutkiem stwierdzonych nieprawidłowości w zakresie zarządzania ryzykiem był w ocenie NIK brak możliwości pełnego zidentyfikowania i zwymiarowania wszystkich aktualnych zagrożeń dla bezpiecznego funkcjonowania WK, a w konsekwencji brak ich minimalizacji.

(akta kontroli str. 7-20, pliki 37, 8, 109, 202)

2.2. Obszar - przeglądy zarządzania bezpieczeństwem informacji

W kontrolowanym okresie nie prowadzono udokumentowanych przeglądów zarządzania bezpieczeństwem informacji Węzła Krajowego.

---

[36] Jako potwierdzenie realizacji procesu zarządzania ryzykiem przedstawiono kontrolującym niepodpisany plik o nazwie WK-AR-E1-DOK-170504-MBO-PPE-MSI-analiza_ryzyka.docx o tytule „analiza ryzyka WK" i adnotacji „wersja 1.0, 04.05.2017". Jego tytuł, forma i zawartość nie były zgodne z wymaganiami PBI WK dotyczącymi dokumentacji procesu zarządzania ryzykiem. Brak było w nim odniesień do „Wartościowania aktywów WK" oraz „Słabości i zabezpieczenia WK".

[37] Jako potwierdzenie przeprowadzonych cyklicznie przeglądów zarejestrowanych ryzyk przedstawiono kontrolującym niepodpisany plik o nazwie „1_Rejestr_Przegląd_Ryzyka_WK_2022.xlsx" zawierający tytuł „Dokument obszarowego przeglądu ryzyk" i datę uaktualnienia: 06.12.2022 r.

[38] Od dnia 15 września 2018 r. (data uruchomienia produkcyjnego Węzła Krajowego) rolę Gestora systemu WK pełnili kolejno dyrektorzy: Departamentu Systemów Państwowych - Piotr Gajewski, Departamentu Zarządzania Systemami - Katarzyna Kopytowska, Departamentu Rozwoju Usług – Michał Widelski /Michał Przymusiński/ Aleksander Dumański, Departamentu Rozwiązań Innowacyjnych – Anna Weber, Departamentu Tożsamości Cyfrowej – Anna Weber (do zakończenia kontroli).

Zgodnie z pkt 2 lp. 3 ppkt 6 załącznika 1.2 do PBI WK Gestor systemu przeprowadza przeglądy zarządzania bezpieczeństwem informacji, przekazuje ministrowi właściwemu do spraw informatyzacji raporty z przeglądu zarządzania bezpieczeństwem oraz informacje o stopniu realizacji celów bezpieczeństwa, stanie bezpieczeństwa systemu, wynikach audytów bezpieczeństwa, ilości, częstości i zakresie odstępstw, incydentów, niezgodności oraz podjętych działań korygujących.

Zgodnie z PBI WK przegląd zarządzania jest cyklicznym działaniem zarządczym, polegającym na: zebraniu danych dotyczących stanu bezpieczeństwa informacji i systemu oraz skuteczności wdrożonych rozwiązań organizacyjnych i technicznych bezpieczeństwa; ocenie na ich podstawie luk, niezgodności i potrzeb; podjęciu decyzji, co do realizacji niezbędnych działań dla zapewnienia wysokiego poziomu bezpieczeństwa systemu WK oraz przetwarzanych w nim danych, jak również ciągłego doskonalenia polityki bezpieczeństwa informacji. Przegląd zarządzania bezpieczeństwem informacji powinien być realizowany przez Gestora systemu WK cyklicznie, co najmniej jeden raz do roku, w pierwszym kwartale danego roku.

Przegląd zarządzania bezpieczeństwem informacji powinien uwzględniać oraz obejmować analizę i ocenę, co najmniej następujących danych:

A. czynników zewnętrznych i wewnętrznych środowiska funkcjonowania WK istotnych dla jego bezpieczeństwa i ich zmiany (w tym stan prawny i zmiany wymagań prawnych),
B. statusu i stanu działań podjętych w następstwie wcześniejszych przeglądów zarządzania bezpieczeństwem,
C. stopnia osiągnięcia ustalonego poziomu oraz celów bezpieczeństwa,
D. skuteczności funkcjonowania procesów określonych polityką bezpieczeństwa,
E. występowania, skali, zakresu oddziaływania i skutków incydentów bezpieczeństwa oraz niezgodności realizacji rozwiązań organizacyjnych i technicznych bezpieczeństwa,
F. stopnia i poziomu wdrożenia rozwiązań organizacyjnych i technicznych bezpieczeństwa u wszystkich Interesariuszy systemu oraz potrzeby ich aktualizacji,
G. wyników audytów bezpieczeństwa i stopnia realizacji zaleceń autowych,
H. informacji dotyczących zarządzania incydentami bezpieczeństwa systemu WK,
I. wyników szacowania ryzyka i stopnia realizacji decyzji, co do postępowania z ryzykiem,
J. informacji dotyczących zarejestrowanych odstępstw i wyjątków,
K. informacji od interesariuszy.

Kontrolującym nie przedstawiono raportów potwierdzających przeprowadzanie w badanym okresie przeglądów zarządzania bezpieczeństwem informacji Węzła Krajowego, ani potwierdzenia przekazywania związanych z nimi informacji, ministrowi właściwemu do spraw informatyzacji.

Zgodnie z wyjaśnieniem Dyrektor DTC: *Dla okresu objętego kontrolą nie udokumentowano w formie raportu przeglądu zarządzania bezpieczeństwem informacji w zakresie systemu zarządzania bezpieczeństwem informacji WK.*

Skutkiem opisanej powyżej nieprawidłowości, było ograniczenie możliwości wydawania zaleceń i podejmowania decyzji dotyczących: zmiany lub

zwiększenia skuteczności rozwiązań organizacyjnych i technicznych w zakresie polityki bezpieczeństwa informacji, zapewnienia adekwatnych zasobów osobowych i technicznych oraz doskonalenia skuteczności systemu zarządzania bezpieczeństwem informacji.

(akta kontroli str. 7-20, pliki 37, 54, 55, 4, 5)

2.3. Obszar Deklaracji Stosowania

Zgodnie z punktem 6.1.3 *Postępowanie z ryzykiem w bezpieczeństwie informacji* normy PN-ISO/IEC 27001 organizacja powinna opracować i wdrożyć proces postępowania z ryzykiem w bezpieczeństwie informacji w celu (...) opracowania Deklaracji Stosowania zawierającej wykaz niezbędnych zabezpieczeń oraz uzasadnienie ich wyboru (niezależnie od tego czy są wdrożone czy nie), a także uzasadnienie pominięcia zabezpieczeń z Załącznika A wyżej wspomnianej normy. Deklaracja powinna powstać w momencie wdrożenia PBI, a następnie być regularnie weryfikowana i aktualizowana.

W kontrolowanym okresie nie opracowano Deklaracji Stosowania Węzła Krajowego, której wzór stanowił załącznik nr 1.4 do PBI WK.

Odpowiedzialność za utrzymanie, nadzór całościowy nad Węzłem Krajowym, w tym także za wdrożenie i respektowanie postanowień PBI przez wszystkich interesariuszy ponosił Gestor systemu WK.

Dyrektor DTC wskazała, że podjęte dotychczas przez Departament działania mające na celu aktualizację PBI WK potwierdzają ustalenia NIK dotyczące nieopracowania Deklaracji Stosowania oraz że uzupełnienie tego dokumentu zostanie potraktowane w sposób priorytetowy.

Skutkiem powyższej nieprawidłowości było utrudnienie weryfikacji stosowania zabezpieczeń wymienionych w załączniku A normy PN-ISO/IEC 27001 w czasie prowadzonych zewnętrznych lub wewnętrznych przeglądów bezpieczeństwa systemu WK.

(akta kontroli str. 7-20, pliki 37, 6)

2.4. Obszar kontroli dostępu

W badanym okresie nie przestrzegano postanowień PBI WK określających zasady nadawania uprawnień użytkownikom tego systemu, i tak:

- przyznawano uprawnienia bezterminowego dostępu do systemu WK, co było niezgodne z wymaganiami załącznika nr 3 „Wniosek o udzielenie dostępu do systemu WK" do załącznika nr 2.9 „Polityka Kontroli Dostępu WK" do PBI WK, z którego wynika, iż niedozwolone jest nadawanie dostępu bezterminowego, a zaleca się, aby był to maksymalnie okres jednego roku lub termin, w którym odbywa się planowany audyt uprawnień;
- nie dokonywano przeglądów „listy osób uprawnionych do dostępu do systemu WK" pod kątem aktualności osób wpisanych na listę oraz spełniania przez te osoby warunków formalnych. Powyższe było niezgodne z wymaganiami pkt 5.7 „Kontrola i przegląd uprawnień" załącznika 2.9 „Polityka kontroli dostępu WK" do PBI WK, z którego wynika, że przeglądy aktualności i weryfikacja „listy osób uprawnionych do dostępu do systemu WK" powinny odbywać się nie rzadziej, niż jeden raz na pół roku;
- nie przeprowadzano audytów aktualności i adekwatności ról i uprawnień dostępu do systemu WK w stosunku do wnioskowanego zakresu tych uprawnień, co było niezgodne z wymaganiami pkt 15 do pkt 5.3.1

„Wymagania dotyczące dostępu" załącznika 2.9 do PBI WK „Polityka kontroli dostępu WK", z którego wynika, że tego rodzaju audyt powinien być przeprowadzany nie rzadziej niż raz na rok, zgodnie z zasadami audytu wewnętrznego „Polityki Bezpieczeństwa Informacji dla Węzła Krajowego";

– jeden z identyfikatorów użytkownika systemu WK o uprzywilejowanych uprawnieniach był wykorzystywany zamiennie przez trzy różne osoby[39]. Powyższe było niezgodne z zasadą wyrażoną w pkt 5.3.1 „Wymagania dotyczące dostępu" załącznika 2.9 do PBI WK „Polityka kontroli dostępu WK, zgodnie z którą praca w systemie odbywa się przy zachowaniu pełnej rozliczalności dostępu.

Dyrektor DTC nie wyjaśniła przyczyn zaniechania przeglądów i audytów dotyczących udzielonych uprawnień.

W ocenie NIK, opisane powyżej nieprawidłowości dotyczące kontroli dostępu do Węzła Krajowego stanowią poważne naruszenie zasad bezpieczeństwa tego systemu. Należy podkreślić, że wszystkie uprawnienia dostępu nadawano w zbyt szerokim zakresie oraz że nie prowadzono obowiązkowych cyklicznych audytów i przeglądów mających zweryfikować zasadność i aktualność nadanych uprawnień. Dodatkowo rozliczalność wykorzystania jednego z uprzywilejowanych identyfikatorów była ograniczona.

Odpowiedzialność za utrzymanie, nadzór całościowy nad Węzłem Krajowym, oraz podejmowanie decyzji w zakresie zapewnienia bezpieczeństwa informacji systemu ponosił Gestor systemu WK.

(akta kontroli str. 7-20, pliki 37, 28, 202, 181, 182, 176)

2.5. Obszar audytów wewnętrznych

Zgodnie z treścią pkt 5.2 „Audyt wewnętrzny" PBI WK, „audyt wewnętrzny służy potwierdzeniu zgodności systemu Węzła Krajowego z wymaganiami dotyczącymi bezpieczeństwa informacji, zarówno w kontekście przepisów prawa stanowionego jak i innych regulacji normatywnych czy wewnętrznych. (...) Audyt wewnętrzny jest procesem systematycznym - cyklicznie powtarzalnym, który musi być przeprowadzony, co najmniej 1 raz do roku."

W okresie objętym kontrolą nie prowadzono obowiązkowych, cyklicznych audytów wewnętrznych potwierdzających zgodność systemu Węzła Krajowego z wymaganiami dotyczącymi bezpieczeństwa informacji.

Dyrektor DTC poinformowała, że w badanym okresie Węzeł Krajowy został poddany następującym testom/audytom:

1. Raport ABW z oceny bezpieczeństwa systemów teleinformatycznych Ministerstwa Cyfryzacji (...)
2. Testy bezpieczeństwa systemów Węzeł Krajowy oraz Profil Zaufany po wdrożeniu zabezpieczeń sieciowych i podziale aplikacji WK zrealizowane przez Centralny Ośrodek Informatyki (...)

Wskazała również, że w jej ocenie dopuszczalne jest zamienne stosowanie określenia „Testy Bezpieczeństwa" i „Audyt" oraz że wskazane powyżej badania rekompensują brak audytów wewnętrznych wymaganych PBI WK.

NIK zauważa, że oba wymienione powyżej badania zostały przeprowadzone przez podmioty zewnętrzne i nie mogą być utożsamione z opisanymi w PBI WK

[39] W trakcie kontroli nie przekazano dokumentów upoważniających te trzy osoby do wykorzystywania tego samego identyfikatora użytkownika systemu WK.

wewnętrznymi audytami bezpieczeństwa. W PBI WK nie została również wprowadzona tożsamość określeń „Testy Bezpieczeństwa" i „Audyty".

W ocenie NIK, skutkiem braku cyklicznych audytów wewnętrznych był wzrost ryzyka, że system WK nie spełnia wymogów dotyczących bezpieczeństwa informacji. Wzrost ryzyka dotyczy również nieodpowiedniego poziomu świadomości i kompetencji użytkowników.

Odpowiedzialnym za realizację audytu wewnętrznego dotyczącego bezpieczeństwa WK był minister właściwy do spraw informatyzacji.

(akta kontroli str. 7-20, pliki 37, 202, 47)

2.6. Obszar publikacji PBI WK

Na stronie internetowej ministra właściwego ds. informatyzacji nie udostępniono Polityki Bezpieczeństwa Informacji Węzła Krajowego, a jedynie wyciąg z tego dokumentu.

Powyższe stanowiło naruszenie art. 39b ust. 1 pkt 3 ustawy z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej, zgodnie z którym właściwy minister określa i udostępnia w Biuletynie Informacji Publicznej na swojej stronie podmiotowej politykę bezpieczeństwa węzła krajowego.

Dyrektor DTC wyjaśniła, że PBI WK w wersji obecnie obowiązującej zawiera elementy, które zostały uznane za niepodlegające upublicznieniu ze względów bezpieczeństwa. Poinformowała, że trwające obecnie prace nad tym dokumentem mają doprowadzić do tego, że stanie się możliwe uczynienie zadość wymaganiom ustawy w zakresie jego upublicznienia.

NIK zauważa, że w przedstawionej dokumentacji zarządzania ryzykiem brak jest zapisów dotyczących postępowania z ryzykiem dotyczącym udostepnienia treści PBI WK. W ocenie NIK upublicznienie jedynie arbitralnie dokonanego wyciągu z Polityki pozbawiło użytkowników i potencjalnych interesariuszy tego systemu właściwej wiedzy o zapewnieniu jego bezpieczeństwa. Należy także wskazać, iż PBI WK nie jest dokumentem niejawnym w rozumieniu ustawy o ochronie informacji niejawnych[40], a także nie podlega ograniczeniu w zakresie publikacji na zasadach określonych w ustawie o dostępie do informacji publicznej[41], tj. w szczególności ze względu na prywatność osoby fizycznej lub tajemnicę przedsiębiorcy.

Osobą odpowiedzialną za publikacje PBI WK był minister właściwy do spraw informatyzacji.

(akta kontroli str. 7-20, pliki 202,109)

[40] Ustawa z dnia 5 sierpnia 2010 r. o ochronie informacji niejawnych (Dz. U. z 2019 r. poz. 742, ze zm.)
[41] Ustawa z dnia 6 września 2001 r. o dostępie do informacji publicznej (Dz. U. z 2022 r. poz. 902)

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 wnioski:

Wnioski

1. Podjęcie działań mających na celu realizowanie przez Ministra Cyfryzacji obowiązku wynikającego z art. 39b ust. 1 pkt 1 lit. a ustawy o usługach zaufania, tj. przeprowadzanie kontroli spełniania przez systemy identyfikacji elektronicznej przyłączone do Węzła Krajowego wymagań, o których mowa w art. 21b ust. 1 powołanej ww. ustawy.
2. Wdrożenie rozwiązań organizacyjnych pozwalających na pełną realizację Polityki Bezpieczeństwa Informacji WK.
3. Przeprowadzenie analizy ryzyka związanej z ewentualną zmianą PBI WK w ramach trwających prac nad modyfikacją tego dokumentu.

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.

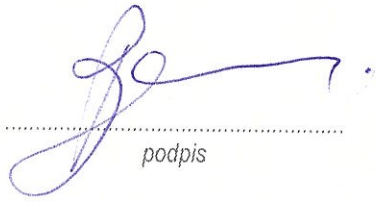
Obowiązek poinformowania NIK o sposobie wykorzystania uwag i wykonania wniosków

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 14 lutego 2023 r.

Prezes
Najwyższa Izba Kontroli
Marian Banaś



podpis