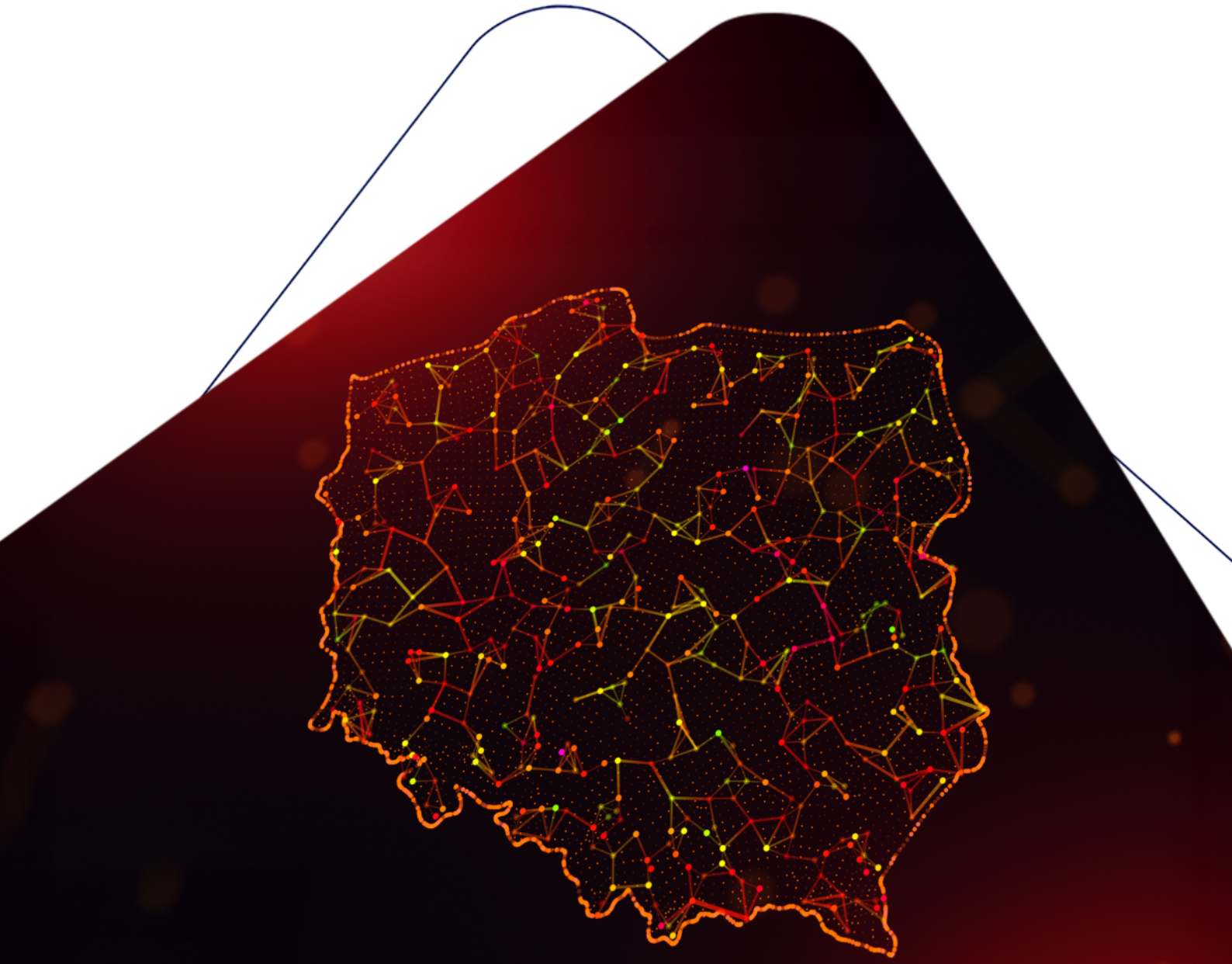
NAJWYŻSZA IZBA KONTROLI

Informacja o wynikach kontroli

Cyberbezpieczeństwo wybranych usług kluczowych



MISJA NAJWYŻSZEJ IZBY KONTROLI

Niezależna, profesjonalna kontrola zadań publicznych w interesie obywateli i państwa

P/25/083

Nr ewid. 45/2026/P/25/083/DZS

Zachodniopomorska Delegatura NIK w Szczecinie

p.o. Dyrektora Zachodniopomorskiej Delegatury Najwyższej Izby Kontroli w Szczecinie

Jarosław Pułka
/podpisano elektronicznie/

Wiceprezes Najwyższej Izby Kontroli

Jacek Kozłowski
/podpisano elektronicznie/

Prezes Najwyższej Izby Kontroli

Mariusz Haładyj
/podpisano elektronicznie/

lipiec 2026 r.

Zespół koordynujący kontrolę:
Adam Milczarek, specjalista kontroli państwowej
Bogumiła Mędrzak, doradca ekonomiczny

SPIS TREŚCI

1. KLUCZOWE FAKTY I LICZBY

Sieci i systemy informatyczne oraz sieci i usługi łączności elektronicznej odgrywają kluczową rolę w społeczeństwie i stały się podstawą wzrostu gospodarczego. Zakłócenie ich działania może prowadzić do przerw w dostawach energii i wody, ograniczenia funkcjonowania transportu, strat gospodarczych, a także zagrożenia bezpieczeństwa ludzi. Dodatkowo Polska, jako członek Unii Europejskiej[1] i NATO, mierzy się z zagrożeniami ze strony grup cyberprzestępczych, grup hakerskich, czy grup sponsorowanych przez obce państwa.

Skala zagrożeń cybernetycznych systematycznie rośnie. W 2025 r. zespoły CSIRT poziomu krajowego[2] obsłużyły niemal 273 tys. incydentów cyberbezpieczeństwa[3], o 144,4% więcej niż rok wcześniej, co oznacza, że statystycznie incydent w polskiej cyberprzestrzeni następuje średnio co 2 minuty. Szczególne znaczenie mają incydenty dotyczące systemów wykorzystywanych do świadczenia usług kluczowych[4], ponieważ ich skutki mogą wykraczać poza sferę cyfrową i wpływać bezpośrednio na przebieg procesów fizycznych oraz ciągłość świadczenia usług.

W latach objętych (2021–2025) kontrolą krajowy system cyberbezpieczeństwa funkcjonował na podstawie ustawy o krajowym systemie cyberbezpieczeństwa[5], która wdrożyła w Polsce dyrektywę NIS1[6]. System określał m.in. zadania organów państwa oraz operatorów usług kluczowych. Do obowiązków tych należało m.in. zarządzanie ryzykiem, stosowanie odpowiednich zabezpieczeń, obsługa i zgłaszanie incydentów, a po stronie właściwych organów – identyfikacja operatorów, monitorowanie wykonywania obowiązków, nadzór i egzekwowanie wymagań.

Celem kontroli było zbadanie, czy organy państwa oraz dostawcy i operatorzy wybranych usług kluczowych podejmowali prawidłowe i skuteczne działania w celu zapewnienia odpowiedniego poziomu cyberbezpieczeństwa. Kontrola obejmowała organizację warunków funkcjonowania krajowego systemu cyberbezpieczeństwa, działania podejmowane przez operatorów usług kluczowych, obsługę incydentów oraz wykonywanie przez właściwe organy zadań monitorujących, nadzorczych i egzekucyjnych.

---

1 Dalej: UE.

2 Sprawozdanie Pełnomocnika Rządu ds. Cyberbezpieczeństwa za 2025 r. – https://www.gov.pl/attachment/73507c5b-eab8-432d-ac3a-890061346e31.

3 Zdarzenie, które ma lub może mieć niekorzystny wpływ na cyberbezpieczeństwo (np. systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej.

4 Usług, które mają kluczowe znaczenie dla utrzymania krytycznej działalności społecznej lub gospodarczej – wymienionych w wykazie usług kluczowych – stanowiących załączniku nr 1 do ustawy o KSC.

5 Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa zmieniona ustawą z dnia 23 stycznia 2026 r. o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw.

6 Dyrektywa Parlamentu Europejskiego i Rady (UE) 2016/1148 w sprawie środków na rzecz wysokiego wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii Europejskiej.

Badaniem objęto wybrane podmioty z sektorów energii, zaopatrzenia w wodę pitną oraz transportu kolejowego i wodnego. Sektory te mają istotne znaczenie dla funkcjonowania państwa i zaspokajania podstawowych potrzeb ludności, są w wysokim stopniu zależne od systemów IT i OT[7], a zakłócenia ich działania mogą powodować skutki kaskadowe.

Kontrola dotyczyła funkcjonowania systemu w modelu opartym na dyrektywie NIS1. W końcowym okresie kontroli uchwalona została nowelizacja ustawy o KSC wdrażająca dyrektywę NIS2[8], która znacząco rozszerzyła liczbę podmiotów zobowiązanych do zapewnienia cyberbezpieczeństwa[9] z 397 do ponad 38 tys., z czego najliczniejszą grupę będzie stanowiła administracja publiczna (ok. 28 tys.). Wyniki kontroli mogą zatem zostać wykorzystane przy wdrażaniu nowego modelu oraz ograniczaniu ryzyka powtórzenia zidentyfikowanych problemów w znacznie większej grupie podmiotów.

7 Przemysłowe systemy sterowania.

8 Dyrektywa Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium UE, zmieniająca rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylająca dyrektywę (UE) 2016/1148.

9 Odporność systemów informacyjnych na działania naruszające poufność, integralność, dostępność i autentyczność przetwarzanych danych lub związanych z nimi usług oferowanych przez te systemy.

2. OCENA I WNIOSKI

Działania wybranych operatorów usług kluczowych w sektorach energii, transportu i wody pitnej[10] oraz organów państwa[11] w okresie 2021–2025 były niewystarczające dla zapewnienia skutecznej realizacji zadań i obowiązków w ramach krajowego systemu cyberbezpieczeństwa. Skutkowało to tym, że stosowane środki bezpieczeństwa były nieadekwatne do obecnego charakteru i skali zagrożeń w cyberprzestrzeni.

Wyniki kontroli NIK u ośmiu operatorów, uzupełnione analizą 44 sprawozdań z audytów dotyczących wybranych operatorów nadzorowanych przez kontrolowanych ministrów, wskazują na powtarzające się i istotne słabości zarządzania cyberbezpieczeństwem oraz nadzoru w objętych badaniem sektorach. Mechanizmy krajowego systemu cyberbezpieczeństwa nie zapewniły skutecznego identyfikowania i egzekwowania realizacji obowiązków operatorów. Słabości te, wobec znacznego rozszerzenia liczby podmiotów objętych ustawą o KSC, tworzą istotne ryzyko dla sprawnego wdrożenia nowych wymagań wynikających z dyrektywy NIS2.

Operatorzy usług kluczowych nieprawidłowo szacowali ryzyka lub nie wdrażali wymaganych i proporcjonalnych do oszacowanego ryzyka procedur i zabezpieczeń w celu:

- utrzymania i bezpiecznej eksploatacji systemów informacyjnych. W szczególności nieprawidłowo zarządzali podatnościami poprzez wykorzystywanie oprogramowania lub urządzeń nieposiadających wparcia producenta lub posiadające znane podatności CVE[12];
- zabezpieczenia fizycznego i środowiskowego (np. przed pożarem lub zalaniem). Nieprawidłowości polegały m.in. na: niestosowaniu dwustopniowego uwierzytelniania, które chroni przed atakami phishingowymi stanowiącymi 60% ataków w UE[13]; niewykorzystywaniu w godzinach pracy systemu alarmowego, niespełnianiu przez budynek klasy odporności pożarowej[14]; niestosowaniu drzwi o wymaganej klasie[15]; składowaniu w serwerowniach materiałów łatwopalnych, pozostawiania otwartych i niezabezpieczonych szaf serwerowych;

---

10 Kontrolą objęto ośmiu operatorów, w tym: czterech w sektorze transport, trzech w sektorze energia i jeden w sektorze zaopatrzenia w wodę pitną i jej dystrybucji (operatorzy lub OUK).

11 Minister Cyfryzacji jako minister właściwy ds. informatyzacji; Minister Energii jako organ właściwy ds. cyberbezpieczeństwa w sektorze energii oraz Minister Infrastruktury jako organ właściwy ds. cyberbezpieczeństwa w sektorze zaopatrzenia w wodę pitną i jej dystrybucji oraz sektorze transportu, w tym w podsektorze transportu wodnego (ministrowie).

12 Common Vulnerabilities and Exposures – publiczna lista znanych luk w zabezpieczeniach oprogramowania i sprzętu.

13 ENISA Threat Landscape 2025 – https://www.enisa.europa.eu/publications/enisa-threat-landscape-2025.

14 Wymagana dla budynku klasa odporności to nie niższa niż B.

15 Drzwi do pomieszczenia lub zespołu pomieszczeń spełniające co najmniej wymagania klasy 2 określone w Polskiej Normie PN-EN 1627, wyposażone w zamek spełniający co najmniej wymagania klasy 4 określone w Polskiej Normie PN-EN 12209 – rozporządzenie Ministra Cyfryzacji z dnia 4 grudnia 2019 r. w sprawie warunków organizacyjnych i technicznych dla podmiotów świadczących usługi z zakresu cyberbezpieczeństwa oraz wewnętrznych struktur organizacyjnych operatorów usług kluczowych odpowiedzialnych za cyberbezpieczeństwo.

- monitorowania w trybie ciągłym systemów informacyjnych wykorzystywanych do świadczenia usług kluczowych. W szczególności ignorowano alerty generowane przez te systemy i nie zapewniano ich obsługi, a w skrajnych przypadkach – nie podejmowano w ogóle realizacji obowiązku ich monitorowania. Powyższe mogło skutkować brakiem wiedzy operatorów o potencjalnych incydentach.

Operatorzy nie tworzyli albo nie utrzymywali również aktualnej i kompletnej dokumentacji niezbędnej do zapewnienia cyberbezpieczeństwa świadczonych usług oraz nie w każdym przypadku – terminowo przeprowadzali okresowe audyty bezpieczeństwa systemu informacyjnego.

Operatorzy nie wdrożyli ponadto prawidłowego systemu zarządzania bezpieczeństwem w systemach informacyjnych wykorzystywanych do świadczenia usługi kluczowej spełniającego wymogi określone w ustawie o KSC i normach ISO[16], a stosowane środki bezpieczeństwa w badanych sektorach były nieadekwatne do aktualnego charakteru i skali zagrożeń w cyberprzestrzeni.

Organy państwa właściwe ds. cyberbezpieczeństwa w kontrolowanych sektorach[17] nie wykonywały wobec żadnego z objętych analizą NIK operatorów[18] działań nadzorczych polegających na wszczęciu kontroli lub postępowań w sprawie nałożenia kary pieniężnej, pomimo posiadania informacji o zaniechaniu wykonania przez OUK istotnych obowiązków w zakresie przeciwdziałania cyberzagrożeniom. Ministrowie nie wszczynali również postępowań w sprawie nałożenia kar pieniężnych za nieprzeprowadzenie terminowo audytów przez OUK. Nieprawidłowości te wynikały z niezapewnienia odpowiednich zasobów kadrowych do ich realizacji. Kary pieniężne za naruszenie obowiązków określonych w ustawie o KSC stanowią przychód Funduszu Cyberbezpieczeństwa, którego celem jest wsparcie działań zmierzających do zapewnienia bezpieczeństwa systemów teleinformatycznych przed cyberzagrożeniami.

Minister Cyfryzacji, wykonując zadania ministra właściwego ds. informatyzacji określone w ustawie o KSC[19], nie przeprowadzili żadnego z dwóch wymaganych przepisami przeglądów i ocen skuteczności Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019-2024, jak i z opóźnieniem przedłożył projekt nowej strategii do wykazu prac

---

16 1. Norma PN/EN ISO/IEC 27001:2017-06 Technika informatyczna – Techniki bezpieczeństwa – Systemy zarządzania bezpieczeństwem informacji – Wymagania – od 8 maja 2017 r. do 16 maja 2023 r.
2. Norma PN-EN ISO/IEC 27001:2023-08 Bezpieczeństwo informacji, cyberbezpieczeństwo i ochrona prywatności – System zarządzania bezpieczeństwem informacji – Wymagania – od 17 sierpnia 2023 r.
3. Norma PN-EN ISO 22301:2020-04 Bezpieczeństwo, i odporność – System zarządzania ciągłością działania – Wymagania.

17 Tj. Minister Energii jako organ właściwy ds. cyberbezpieczeństwa w sektorze energii oraz Minister Infrastruktury jako organ właściwy ds. cyberbezpieczeństwa w sektorze zaopatrzenia w wodę pitną i jej dystrybucji oraz sektorze transportu (w tym w podsektorze transportu wodnego).

18 Tj. 27 ze 103 operatorów nadzorowanych przez tych ministrów, z tego: 13 OUK (z 32) nadzorowanych przez Ministra Infrastruktury oraz 14 OUK (z 71) nadzorowanych przez Ministra Energii.

19 Art. 45-50 ustawy o KSC.

legislacyjnych i programowych Rady Ministrów. Finalnie, Rada Ministrów podjęła uchwałę o przyjęciu nowej strategii dopiero – 10 marca 2026 r.[20], tj. 434 dni po upływie okresu obowiązywania poprzedniej. Ponadto Minister z opóźnieniem przygotował projekt ustawy wdrażającej Dyrektywę NIS2, w wyniku czego dopiero od 3 kwietnia 2026 r.[21], tj. 532 dni po terminie, około 38 tys. podmiotów zostało objętych obowiązkami zapewnienia odpowiednio wysokiego poziomu cyberbezpieczeństwa świadczonych usług.

WNIOSKI:

OPERATORZY USŁUG KLUCZOWYCH:

Podkreślając istotność i znaczenie stwierdzonych nieprawidłowości, dotyczących niezapewnienia przez OUK cyberbezpieczeństwa świadczonych usług oraz zwracając uwagę na nowe wyzwania, wynikające z nowelizacji ustawy o KSC, Najwyższa Izba Kontroli wnosi o:

1. Dostosowanie do wymagań określonych w ustawie o KSC funkcjonujących u operatorów systemów zarządzania bezpieczeństwem informacji w procesach wpływających na świadczenie usług, w szczególności zapewnienie:

- systematycznego identyfikowania i szacowania ryzyka wystąpienia incydentu oraz zarządzania tym ryzykiem;
- wdrożenia odpowiednich i proporcjonalnych do oszacowanego ryzyka środków (zabezpieczeń) technicznych i organizacyjnych, w tym uwzględniających bezpieczeństwo fizyczne i środowiskowe;
- monitorowania i bezzwłocznego reagowania na alerty bezpieczeństwa.

Realizacja powyższych działań ma na celu utrzymanie odpowiedniego poziomu cyberbezpieczeństwa systemów informacyjnych służących do zapewnienia niezakłóconego świadczenia usług przez te podmioty.

2. Zapewnienie kompletnej (tj. zawierającej wszystkie elementy wymagane ustawą o KSC) i aktualnej dokumentacji dotyczącej cyberbezpieczeństwa systemów informacyjnych wykorzystywanych do świadczenia usług.

Uregulowania ujęte w dokumentacji powinny określać podstawy funkcjonowania ww. systemów, stwarzając warunki do utrzymania ciągłości działania obsługiwanych przez nie usług, przy jednoczesnym zapewnieniu poufności, integralności, dostępności i autentyczności przetwarzanych danych.

MINISTER ENERGII i MINISTER INFRASTRUKTURY – ORGANY WŁAŚCIWE DS. CYBERBEZPIECZEŃSTWA:

Uwzględniając ustalenia przedstawione powyżej Najwyższa Izba Kontroli wnosi o:

[20] https://monitorpolski.gov.pl/M2026000030901.pdf.
[21] Wejście w życie znowelizowanej ustawy o KSC.

1. Zapewnienie kompleksowego monitorowania i nadzoru nad stosowaniem przez podmioty ważne i kluczowe przepisów ustawy o KSC.

2**.** Podjęcie bez zbędnej zwłoki wobec dotychczas nadzorowanych operatorów usług kluczowych postępowań administracyjnych w sprawie nałożenia kar pieniężnych, w celu zdyscyplinowania tych podmiotów do realizacji obowiązków określonych w ustawie o KSC przed nowelizacją.

Hipotezą art. 35 ustawy z dnia 23 stycznia 2026 r. o zmianie ustawy o KSC nie są objęte czyny (delikty administracyjne) popełnione przed dniem wejścia w życie tej ustawy, a zatem nie dotyczy ich dwuletni okres, w którym przepis ten wyłącza możliwość nałożenia kary pieniężnej. Ratio legis tego przepisu polega na wprowadzeniu swoistego „okresu przejściowego", w którym nie będą nakładane kary za nowowprowadzane przez nowelizację delikty administracyjne. Nie obejmuje ono jednak wyłączenia w stosunku do deliktów popełnionych w świetle przepisów obowiązujących przed dniem wejścia w życie ustawy, których dopuścić się mogli operatorzy usług kluczowych.

3. KLUCZOWE USTALENIA

Ustawa o KSC utworzyła podstawy prawno-instytucjonalne dla cyberbezpieczeństwa na poziomie krajowym i określiła zadania i obowiązki podmiotów wchodzących w skład krajowego systemu cyberbezpieczeństwa. W szczególności wyznaczyła zadania i obowiązki OUK w celu zapewnienia odpowiednio wysokiego poziomu cyberbezpieczeństwa systemów informacyjnych w sektorach usług mających kluczowe znaczenie dla utrzymania krytycznej działalności społecznej lub gospodarczej, jak również zadania organów właściwych ds. cyberbezpieczeństwa w zakresie nadzoru nad nimi.

3.1. OPERATORZY USŁUG KLUCZOWYCH

Zapewnienie cyberbezpieczeństwa przez operatorów usług kluczowych jest fundamentalne, ponieważ informacja[22] oraz wspierające zarządzanie organizacją procesy i systemy teleinformatyczne stanowią obecnie ich najważniejsze aktywa biznesowe. Odpowiedni poziom ochrony tych zasobów jest warunkiem koniecznym do zachowania ciągłości i bezpieczeństwa świadczonych usług, a także zapewnienia poufności, integralności, dostępności i autentyczności informacji[23].

Infografika nr 1. Atrybuty informacji

Źródło: opracowanie własne NIK.

Współczesne organizacje operują w środowiskach narażonych na niezwykle zróżnicowane zagrożenia – od pospolitego wandalizmu, przez wyrafinowane szpiegostwo i sabotaż, aż po skutki kataklizmów naturalnych. W obliczu rosnącej powszechności technicznie zaawansowanych metod ataku, takich jak złośliwe oprogramowanie, czy blokady dostępu,

[22] Za informację należy uznać tylko taki zestaw znaków, któremu można przypisać określone znaczenie, rozumiane jako wskazywany przez nie sens – Postanowienie Sądu Najwyższego z dnia 5 marca 2019 r. sygn. akt II KK 208/18.

[23] K. Chałubińska-Jentkiewicz [w:] W. Kitler, J. Taczkowska-Olszewska, F. Radoniewicz (red.), Ustawa o krajowym systemie cyberbezpieczeństwa. Komentarz, wyd. 1, 2019, art. 8, Nb 2.

utrzymywanie i ciągłe doskonalenie standardów bezpieczeństwa przestaje być jedynie kwestią techniczną. Staje się ono niezbędnym elementem zgodności z wymogami prawnymi oraz wyrazem odpowiedzialności za stabilność całego systemu, w którym działalność jednego podmiotu bezpośrednio wpływa na funkcjonowanie innych uczestników rynku i konsumentów[24]. W obliczu napięć geopolitycznych i ekonomicznych kluczowe staje się również identyfikowanie nawet marginalnych zagrożeń w zakresie cyberbezpieczeństwa[25].

Wszyscy spośród ośmiu skontrolowanych operatorów usług kluczowych[26], pomimo uznania świadczonych przez nich usług za kluczowe od 2019 r. i nałożenia na nich obowiązków w zakresie zapewnienia ciągłości ich świadczenia[27], nie zapewnili odpowiedniego poziomu cyberbezpieczeństwa systemów informacyjnych służących do świadczenia usługi kluczowej.

3.1.1. Niezarządzanie, nieprawidłowe zarządzanie ryzykiem w bezpieczeństwie informacji

Zgodnie z normą dotyczącą zarządzania ryzykiem w bezpieczeństwie informacji (PN-ISO/IEC 27005:2014-01) – *w celu określenia potrzeb organizacji w odniesieniu do wymagań związanych z bezpieczeństwem informacji oraz utworzenia skutecznego systemu zarządzania bezpieczeństwem informacji (SZBI) potrzebne jest systematyczne podejście do zarządzania ryzykiem w bezpieczeństwie informacji (...) zaleca się, aby zarządzanie ryzykiem w bezpieczeństwie informacji było integralną częścią wszystkich działań związanych z zarządzaniem bezpieczeństwem informacji oraz zostało zastosowane zarówno do wdrożenia, jak i w ciągłej eksploatacji SZBI. Zaleca się, aby zarządzanie ryzykiem w bezpieczeństwie informacji było procesem ciągłym. Zaleca się, aby w procesie tym ustanowiono kontekst zewnętrzny i wewnętrzny, oszacowano ryzyko oraz postąpiono z ryzykiem zgodnie z planem postępowania z ryzykiem, w celu wdrożenia zaleceń i decyzji. W ramach zarządzania ryzykiem analizuje się, co może się zdarzyć i jakie mogą być możliwe następstwa, a następnie decyduje się, co i kiedy należy wykonać, aby zredukować ryzyko do akceptowalnego poziomu*[28].

Powyższe podejście do zarządzania bezpieczeństwem informacji poprzez ryzyko (risk-based approach) zostało określone w art. 8 pkt 1 ustawy o KSC oraz wynikała wprost z Dyrektywy NIS1[29] i normy ISO 27001[30]. Przepisy ustawy o KSC nakładają obowiązek, aby OUK prowadziły systematyczne szacowanie ryzyka wystąpienia incydentu oraz zarządzały tym ryzykiem.

---

[24] Franciszek Wesołowski, Janusz Zawiła-Niedźwiecki, Bezpieczeństwo systemów informacyjnych. Praktyczny przewodnik zgodny z normami polskimi i międzynarodowymi. Wyd. Edu-Libri, Kraków-Warszawa 2012, str. 17.

[25] Np. wektor ataku na farmy odnawialnych źródeł energii https://cert.pl/posts/2026/01/raport-incydent-sektor-energii-2025/.

[26] Ośmiu, w tym: czterech w sektorze transport, trzech w sektorze energia i jeden w sektorze zaopatrzenia w wodę pitną i jej dystrybucji.

[27] Podmioty objęte kontrolą zostały uznane za OUK w rozumieniu ustawy o KSC w 2019 r.

[28] PN-ISO/IEC 27005:2014-01 – Zarządzanie ryzykiem w bezpieczeństwie informacji.

[29] Jak również w znowelizowanej ustawie o KSC na podstawie Dyrektywy NIS2.

[30] Norma PN/EN ISO/IEC 27001:2017-06 Technika informatyczna – Techniki bezpieczeństwa – Systemy zarządzania bezpieczeństwem informacji – Wymagania – od 8 maja 2017 r. do 16 maja 2023 r. Norma PN-EN ISO/IEC 27001:2023-08 Bezpieczeństwo informacji, cyberbezpieczeństwo i ochrona prywatności – System zarządzania bezpieczeństwem informacji – Wymagania – od 17 sierpnia 2023 r.

Dopiero prawidłowe określenie kontekstu organizacji, w tym czynników zewnętrznych i wewnętrznych istotnych z punktu widzenia osiągania jej celów, a następnie określenie ryzyk i ocenienie ich wpływu na te cele, stanowi podstawę do podjęcia przez organizację niezbędnych działań. *Szacowanie ryzyka pozwala określić, jaki cel powinny realizować zabezpieczenia, ale również pozwala na utrzymanie skuteczności zastosowanych zabezpieczeń*[31].

Sześć z ośmiu kontrolowanych OUK nie stosowało prawidłowego podejścia do zarządzania ryzykiem, w szczególności poprzez: nieszacowanie systematycznie tego ryzyka[32], brak jednoznacznych kryteriów oceny prawdopodobieństwa/skutku wystąpienia ryzyka oraz niesporządzenie planów postępowania z ryzykiem.

Przykład

Jeden z kontrolowanych OUK:

- nie zapewnił powtarzalności procesu szacowania ryzyka i porównywalności wyników wskutek braku zdefiniowania mierzalnych kryteriów poziomu prawdopodobieństwa i konsekwencji oraz określenia obszaru wpływu ryzka na prowadzoną działalność;
- nie udokumentował planu postępowania z ryzykiem i oceny skuteczności podjętych działań;
- nie przeprowadził w ogóle w latach 2023–2025 analizy ryzyka.

W oparciu o przeprowadzoną analizę ryzyka organizacja powinna doprowadzić do jego ograniczenia do akceptowalnego poziomu, tzn. takiego, przy którym organizacja może prowadzić swoją działalność pomimo urzeczywistnienia się niekorzystnych zjawisk[33]. Służyć temu ma opracowanie i wdrożenie procesu postępowania z ryzykiem w bezpieczeństwie informacji, w ramach którego jednostka musi wybrać odpowiednie opcje postępowania z ryzykiem, określić wszystkie zabezpieczenia niezbędne do jej wdrożenia[34]. Nieprawidłowe szacowanie ryzyka i określenie postępowania z ryzykiem w bezpieczeństwie informacji uniemożliwia wdrożenie odpowiednich i proporcjonalnych środków technicznych i organizacyjnych.

3.1.2. Niewdrożenie odpowiednich i proporcjonalnych do oszacowanego ryzyka środków technicznych i organizacyjnych

Obowiązek wdrożenia odpowiednich i proporcjonalnych do oszacowanego ryzyka środków technicznych i organizacyjnych, uwzględniających najnowszy stan wiedzy został określony w art. 8 pkt 2 ustawy o KSC. Realizacja tego obowiązku przez OUK powinna polegała m.in. na:

- utrzymaniu i bezpiecznej eksploatacji systemów informacyjnych;

---

31 K. Gałaj-Emiliańczyk, w: Wdrożenie systemu zarządzania bezpieczeństwem informacji zgodnie z normą ISO/IEC 27001:2019, str. 121, Gdańsk 2021.

32 Przynajmniej raz na 12 miesięcy.

33 Franciszek Wesołowski, Janusz Zawiła-Niedźwiecki, Bezpieczeństwo systemów informacyjnych. Praktyczny przewodnik zgodny z normami polskimi i międzynarodowymi, str. 43–44.

34 Norma ISO 27001 pkt 6.1.3. lit. a i b.

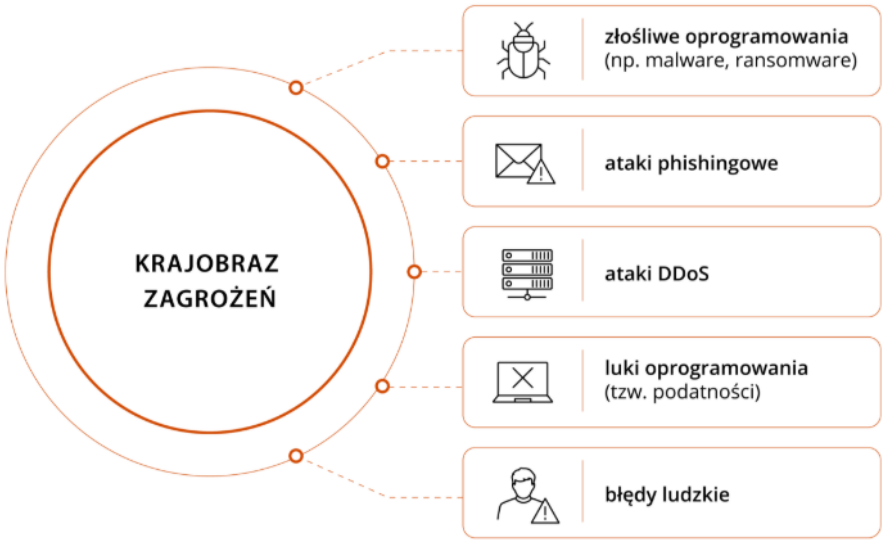
- zapewnieniu bezpieczeństwa fizycznego i środowiskowego, uwzględniającego kontrolę dostępu;
- zapewnieniu bezpieczeństwa i ciągłości dostaw usług, od których zależało świadczenie usługi kluczowej;
- wdrażaniu, dokumentowaniu i utrzymywaniu planów działania umożliwiających ciągłe i niezakłócone świadczenie usługi kluczowej oraz zapewniających poufność, integralność, dostępność i autentyczność informacji;
- objęciu systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej systemem monitorowania w trybie ciągłym.

Powyższe obowiązki pozostają aktualne w znowelizowanej[35] ustawie o KSC, a żaden z kontrolowanych operatorów nie zrealizował wszystkich wskazanych powyżej wymagań.

Brak realizacji obowiązku utrzymania i bezpiecznej eksploatacji systemu informacyjnego

Bezpieczeństwo systemów informacyjnych definiuje się jako odporność systemów na działania naruszające poufność, integralność, dostępność przetwarzanych danych lub związanych z nimi usług oferowanych przez te systemy. Zagrożeniami dla tego bezpieczeństwa są m.in.: złośliwe oprogramowania (np. malware, ransomware), ataki phishingowe, ataki DDoS[36], luki oprogramowania (tzw. podatności) oraz błędy ludzkie.

Infografika nr 2. Krajobraz zagrożeń



Źródło: opracowanie własne NIK.

Żaden z kontrolowanych operatorów nie zapewnił utrzymania i bezpiecznej eksploatacji tych systemów poprzez zapewnienie odporności systemów informacyjnych na działania naruszające poufność, integralność, dostępność i autentyczność przetwarzanych danych lub

[35] Na podstawie Dyrektywy NIS2.

[36] Rozproszona odmowa usługi, której celem jest zablokowanie dostępu do serwera, strony internetowej lub sieci poprzez ich przeciążenie sztucznie generowanym ruchem.

związanych z nimi usług oferowanych przez te systemy. Do najczęstszych nieprawidłowości należało: nieprawidłowe zarządzanie dostępami do systemów, błędy w konfiguracji systemów bezpieczeństwa i dziedzinowych, brak wdrożenia systemów DLP[37], brak wykorzystywania uwierzytelniania wieloskładnikowego, wykorzystywanie oprogramowania o statusie EOL/EOS[38] lub posiadających znane podatności CVE[39].

Przykład

Jeden z kontrolowanych OUK:

- wdrożył urządzenia produkcyjne z istniejącymi podatnościami – polegało to na uruchomieniu urządzenia w środowisku produkcyjnym (tj. świadczonej usługi kluczowej) z wersją oprogramowania ze zidentyfikowaną podatnością o wysokim stopniu krytyczności. W wyjaśnieniach organizacji wskazano, że zainstalowana wersja była w momencie wdrożenia rekomendowana przez producenta, a opóźnienie w instalacji nowszej poprawki wynikało z konieczności planowania okien serwisowych. OUK nie przedstawił jednak formalnego harmonogramu ani uzgodnień z dostawcą, które gwarantowałyby jak najszybszą możliwą reakcję na tego typu incydenty w przyszłości;
- utrzymywał podatności krytyczne w oprogramowaniu macierzy dyskowych, tj. działały one w oparciu o wersję oprogramowania obarczoną podatnościami ocenianymi na 9.8–10 w skali CVSS[40].

Utrzymywanie podatnego (nieaktualnego lub niewspieranego) oprogramowania stanowi jedno z najpoważniejszych zagrożeń dla bezpieczeństwa teleinformatycznego[41], będąc głównym wektorem inicjującym ataki. Według raportów CSIRT-ów[42], atakujący potrafią wykorzystać nowo odkryte luki w ciągu zaledwie kilku godzin lub dni od ich publicznego ujawnienia[43]. Powyższe pozostaje szczególnie istotne w zakresie systemów informacyjnych wykorzystywanych do świadczenia usługi kluczowej lub systemów z nią powiązanych, w celu zapewnienia niezakłóconego świadczenia tej usługi.

---

37 Data lost prevention - zestaw narzędzi i strategii mających na celu zapobieganie wyciekom danych.

38 Bez wsparcia producenta i aktualizacji.

39 Common Vulnerabilities and Exposures – publiczna lista znanych luk w zabezpieczeniach oprogramowania i sprzętu.

40 Zgodnie ze skalą Common Vulnerability Scoring System podatności ocenione od 9.0 do 10.0 są krytyczne, tj. są niezwykle niebezpieczne i wymagają natychmiastowego załatania lub podjęcia działań ograniczających jej skutki (https://www.first.org/cvss/v4.0/user-guide).

41 W 2025 r. stanowił wektor 21,3% ataków w UE – ENISA Threat Landscape 2025 – https://www.enisa.europa.eu/sites/default/files/2026-01/ENISA%20Threat%20Landscape%202025_v1.2.pdf.

42 Tj. Zespoły Reagowania na Incydenty Bezpieczeństwa Komputerowego działający na poziomie krajowym prowadzone przez: Szefa Agencji Bezpieczeństwa Wewnętrznego (CSIRT GOV), Ministra Obrony Narodowej (CSIRT MON), Naukową i Akademicką Sieć Komputerową - Państwowy Instytut Badawczy (CSIRT NASK).

43 https://cert.pl/uploads/docs/CERT_Polska_Poradnik_ransomware.pdf i https://csirt.gov.pl/cer/publikacje/raporty-o-stanie-bezpi/983,Raport-o-stanie-bezpieczenstwa-cyberprzestrzeni-RP-w-2024-roku.html.

Brak reakcji na alerty cyberbezpieczeństwa

Sześciu z ośmiu skontrolowanych operatorów systemowo nie zapewniało monitorowania i reagowania na alerty dotyczące podatności lub zagrożeń cyberbezpieczeństwa. W szczególności ignorowane były generowane przez systemy bezpieczeństwa komunikaty dotyczące potencjalnych incydentów cyberbezpieczeństwa, skompromitowanych stacji roboczych[44], braku aktualizacji systemu antywirusowego, czy podatnościach zainstalowanego oprogramowania. Brak reagowania na alerty cyberbezpieczeństwa uniemożliwia szybką reakcję na pojawiające się cyberzagrożenia dla systemów informacyjnych, co może prowadzić do eskalacji incydentu i zakłócenia świadczenia usługi kluczowej.

Przykłady:

- przez ponad 426 dni utrzymywano kluczowy system bezpieczeństwa, w tym urządzenie brzegowe sieci OT[45], z oprogramowaniem, które nie było już wspierane przez producenta;
- przez ponad 578 dni ignorowano alerty z systemów bezpieczeństwa dotyczących braku łączności z elementami infrastruktury IT;
- zidentyfikowano wyciek poświadczeń (hasło użytkownika) pracownika stanowiący krytyczny incydent bezpieczeństwa, który nie został obsłużony.

Brak zapewnienia bezpieczeństwa fizycznego i środowiskowego

Bezpieczeństwo środowiskowe powinno przeciwdziałać czynnikom środowiskowym (np. takim jak pożar lub zalanie), które mogą uszkodzić m.in. infrastrukturę informatyczną.
Celem bezpieczeństwa fizycznego jest zaprojektowanie zabezpieczeń, które uniemożliwiają nieupoważnionym osobom dostęp do budynku, pomieszczenia lub do zasobu, w którym przechowywane lub przetwarzane są informacje, jak również uniemożliwiają tym osobom wrogie działania. Służy temu również kontrola dostępu, której celem jest nadzorowanie tego kto ma dostęp do danego zasobu (rozliczalność)[46]. *Zasoby informatyczne, ze względu na swoją wartość oraz wartość zgormadzonych w nich danych, powinny być przechowywane w sposób gwarantujący adekwatne do wartości zabezpieczenia przed czynnikami środowiskowymi oraz zniszczeniem lub kradzieżą*[47].

Tylko jeden z kontrolowanych operatorów zapewnił bezpieczeństwo fizyczne i środowiskowe, uwzględniające kontrolę dostępu. W pozostałych przypadkach stwierdzono w tym zakresie nieprawidłowości, które dotyczyły m.in.: braku wykorzystywania w godzinach pracy systemu alarmowego, niespełniania przez budynek klasy odporności pożarowej[48], niestosowania drzwi

---

44 Komputer lub inne urządzenie końcowe, którego zabezpieczenia zostały przełamane przez niepowołaną osobę trzecią lub złośliwe oprogramowanie.
45 Systemy wykorzystywane do monitorowania i sterowania procesami przemysłowymi oraz infrastrukturą fizyczną.
46 WGITA – IDI Handbook on IT audit for supreme audit instituton (v. 2022), str. 75-76.
47 Mirosław Forystek, Audyt Informatyczny, wyd. 1, Warszawa 2005 r., str. 108.
48 Wymagana dla budynku klasa odporności to nie niższa niż B.

o wymaganej klasie[49] (np. drzwi przeszklonych lub ze sklejki), składowania w serwerowniach materiałów łatwopalnych, pozostawiania otwartych szaf serwerowych (rack).

Przykłady

Niezapewnienia bezpieczeństwa środowiskowego i fizycznego:

- fizyczne połączenie elementów dwuskładnikowego uwierzytelniania wejścia do serwerowni OT (tj. karty i klucza), co eliminowało dodatkową warstwę zabezpieczeń i czyniło ten mechanizm bezużytecznym;
- składowanie w serwerowniach oraz pomieszczeniach technicznych UPS[50] łatwopalnych materiałów (np. kartonów i folii);
- nieuzbrajanie w godzinach pracy organizacji systemu sygnalizacji napadu i włamania w serwerowni IT oraz w pomieszczeniach z UPS;
- nieprzeprowadzanie przeglądów oraz nieweryfikowanie zabezpieczeń wejścia awaryjnego (śluzy);
- niewykorzystywanie systemu sygnalizacji pojawienia się wody w celu zabezpieczenia serwerowni oraz pomieszczenia z UPS przed zalaniem;
- pozostawianie otwartych szaf serwerowych (rack) w serwerowni;
- brak możliwości zidentyfikowania/ustalenia miejsca lokalizacji i posiadacza karty „master", służącej do systemu kontroli dostępu (dającej dostęp do wszystkich serwerowni);
- nieusunięcie z systemu kontroli dostępu uszkodzonych kart dostępu – zidentyfikowano przypadki, w których uszkodzone karty dostępu były nadal aktywne;
- nieposiadanie atestowanych drzwi i zamka do głównej serwerowni.

Niezapewnienie bezpieczeństwa środowiskowego i fizycznego tworzy dodatkową powierzchnię ataków, która może zostać wykorzystana nawet przy zapewnieniu bezpiecznej eksploatacji systemów informacyjnych, w tym tych wykorzystywanych do świadczenia usługi kluczowej. Nawet najlepsze systemy informatyczne nie zabezpieczą organizacji przed fizycznym zniszczeniem ich infrastruktury informatycznej i produkcyjnej.

Brak wdrożenia, dokumentowania i utrzymywania planów ciągłości działania

Dostępność i prawidłowe działanie systemów informatycznych ma zasadnicze znaczenie dla zdolności OUK do świadczenia przez nich usług kluczowych. Systemy te odgrywają ważną rolę

[49] Drzwi do pomieszczenia lub zespołu pomieszczeń spełniające co najmniej wymagania klasy 2 określone w Polskiej Normie PN-EN 1627, wyposażone w zamek spełniający co najmniej wymagania klasy 4 określone w Polskiej Normie PN-EN 12209 - rozporządzenie Ministra Cyfryzacji z dnia 4 grudnia 2019 r. w sprawie warunków organizacyjnych i technicznych dla podmiotów świadczących usługi z zakresu cyberbezpieczeństwa oraz wewnętrznych struktur organizacyjnych operatorów usług kluczowych odpowiedzialnych za cyberbezpieczeństwo.

[50] Zasilacz awaryjny.

w tak różnorodnych działaniach tych jednostek, a w rzeczywistości wiele działań nie może być skutecznie realizowanych bez ich wsparcia. W celu ograniczenia zakłóceń i przestojów w działaniu tych systemów, organizacje powinny opracować strategię planowania ciągłości działania oraz związane z nią procedury.

Pięciu kontrolowanych operatorów nie zapewniło wdrożenia zgodnych z normą ISO 22301[51] planów ciągłości działania usługi kluczowej, w tym odtworzenia systemów informacyjnych po awariach. Dokumentacja w tym zakresie była niekompletna, tj. nie zawierała zakresu, szczegółowych procedur odtworzeniowych, nie określono takich parametrów jak RTO[52] (maksymalny dopuszczalny czas przywrócenia) oraz RPO[53] (maksymalny akceptowalny poziom utraty danych), nie testowano planów ciągłości działania.

Przykłady

Nieokreślenie w dokumentacji dotyczącej cyberbezpieczeństwa systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej – procedur lub zasad dotyczących ciągłości działania usługi kluczowej, w tym:

- parametrów odtworzeniowych RTO i RPO dla poszczególnych systemów IT i OT;
- planów działania dla skomplikowanych scenariuszy, takich jak np.: jednoczesny atak ransomware i nagła niedostępność kluczowego personelu;
- sposobu dokumentowania przeprowadzenia testów, ćwiczeń czy symulacji planów ciągłości działania (tj. dowodów testowania planów ciągłości działania);
- zastępowalności osób kluczowych dla działania tych planów – uzależnienia działania planu ciągłości działania od pojedynczych osób;
- szczegółowych, technicznych procedur odtworzeniowych (krok po kroku) oraz planu komunikacji kryzysowej;
- procedur weryfikacji stabilności systemu po usunięciu awarii i zamknięcia incydentu;
- opisu aktywów niezbędnych do realizacji działania w planach ciągłości działania – poprzez nieokreślnie precyzyjnych informacji o lokalizacji dokumentacji technicznej, danych dostępowych czy wymaganym oprogramowaniu;
- kompletnych i szczegółowych procedur odzyskiwania danych.

Brak określenia, testowania i doskonalenia procedur ciągłości działania może skutkować niepodjęciem skutecznych i adekwatnych działań w obliczu pojawienia się sytuacji zagrażającej niezakłóconemu świadczeniu usługi kluczowej. W efekcie dojść może do przerwania świadczenia tej usługi, jak i wydłużenia czasu potrzebnego do przywrócenia pełnego działania systemów informacyjnych.

---

[51] Norma PN-EN ISO 22301:2020-04 Bezpieczeństwo, i odporność – System zarządzania ciągłością działania – Wymagania.

[52] Recovery Time Objective.

[53] Recovery Point Objective.

3.1.3. NIEPRAWIDŁOWA DOKUMENTACJA DOTYCZĄCA CYBERBEZPIECZEŃSTWA

Dokumentacja opracowana przez połowę skontrolowanych operatorów nie spełniała wymogów określonych w rozporządzeniu Rady Ministrów z dnia 16 października 2018 r. w sprawie rodzajów dokumentacji dotyczącej cyberbezpieczeństwa systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej, w szczególności nieprawidłowo ją opracowano lub aktualizowano, w tym w zakresie zgodności z wymaganiami normy ISO 27001, a w kontekście ciągłości działania – normy ISO 22301. W jednym przypadku podmiot przez sześć lat od otrzymania decyzji o uznaniu za OUK nie opracował takiej dokumentacji, mimo obowiązku opracowania jej w terminie sześciu miesięcy od otrzymania takiej decyzji. W pozostałych trzech przypadkach, pomimo zgodności dokumentacji z ww. normą, procedury w niej określone nie były prawidłowo realizowane, co niweczyło skuteczność zabezpieczeń w niej wskazanych.

Przykłady

Dokumentacja cyberbezpieczeństwa systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej nie określała:

- mierzalnych celów bezpieczeństwa informacji oraz procesów oceny i doskonalenia;
- zasad przyznawania, przeglądu i odbierania uprawnień administracyjnych oraz stosowania kont do zadań administracyjnych;
- wymogów zapewniających bezpieczeństwo informacji podczas pracy zdalnej, do której użytkownicy wykorzystywali sprzęt prywatny;
- ról i odpowiedzialności (w tym za rejestrację i informowanie o ryzykach);
- kryteriów klasyfikacji i nadawania priorytetu incydentom, formalnego wymogu prowadzenia rejestru incydentów, zasad identyfikacji i zabezpieczenia dowodów oraz wykorzystywania wiedzy związanej z incydentami do wzmocnienia i poprawy zabezpieczeń informacji;
- polityk (procedur) w sprawie wymagań środków organizacyjnych i technicznych zapobiegających wyciekowi informacji, w tym informacji wrażliwych;
- zasad zarządzania bezpieczeństwem w: relacjach z dostawcami usług informatycznych (wymogów weryfikacji dostawców i monitorowania ich działań) i procesów nabywania, rozwoju i wycofywania oprogramowania, aplikacji i systemów informacyjnych;
- zasad zarządzania podatnościami (kryteriów oceny i kwalifikacji, wymaganych czasów reakcji i zasad zarządzania wyjątkami) i konfiguracją (minimalnych wymagań bezpieczeństwa, zasad utwardzania systemów i urządzeń sieciowych, zarządzania regułami na zaporze sieciowej i segmentacji sieci);
- wykazu oprogramowania dopuszczonego do używania; zinwentaryzowanych informacji przechowywanych i przetwarzanych w systemach informacyjnych; wzorców konfiguracyjnych dla kluczowych systemów bezpieczeństwa, określających akceptowany przez OUK sposób ich skonfigurowania.

Nieprawidłowe opracowanie lub nieaktualizowanie dokumentacji, dotyczącej cyberbezpieczeństwa[54] uniemożliwia podjęcie przez organizację odpowiednich działań operacyjnych (procesów) celem zapewnienia cyberbezpieczeństwa usługi kluczowej.

3.1.4. NIETERMINOWE PRZEPROWADZANIE AUDYTÓW BEZPIECZEŃSTWA

Audyt bezpieczeństwa systemu informacyjnego to systematyczny, niezależny i udokumentowany proces badania infrastruktury informatycznej, oprogramowania, procedur i zasad w celu uzyskania obiektywnych dowodów ich zgodności z wymaganiami prawnymi i celami biznesowymi. Audyt obejmuje szczegółową analizę systemów i mechanizmów kontroli dokonywaną w celu upewnienia się, że zabezpieczają one aktywa informacyjne, zapewniają integralność danych oraz chronią prywatność bez narażania organizacji na nieuzasadnione koszty. Kluczowym celem audytu jest identyfikacja wszelkich odstępstw od ustalonych kryteriów (np. normy ISO 27001) oraz wykrycie podatności, które mogłyby zostać wykorzystane przez cyberzagrożenia[55].

Operatorzy, na podstawie art. 15 ust. 1 ustawy o KSC, byli zobowiązani do przeprowadzenia, co najmniej raz na 2 lata audytu bezpieczeństwa systemu informacyjnego. Powyższy przepis stanowił realizację art. 15 ust. 2 lit. b Dyrektywy NIS1, który wymaga od operatorów usług kluczowych przekazywania właściwym organom krajowym dowodów na skuteczną realizację polityki w zakresie bezpieczeństwa[56]. Z poziomu organizacji nieprzeprowadzenie audytów skutkuje brakiem aktualnych informacji na poziomie kierownictwa organizacji na temat stanu cyberbezpieczeństwa świadczonej usługi kluczowej, co w konsekwencji uniemożliwia podjęcie odpowiednich działań naprawczych w zakresie stwierdzonych w ramach audytu błędów i niezgodności. Połowa kontrolowanych OUK nie realizowała w terminie tego obowiązku, a przekroczenia w tym zakresie wynosiły od czterech dni do czterech lat.

3.2. ORGANY WŁAŚCIWE DS. CYBERBEZPIECZEŃSTWA[57]

W okresie objętym kontrolą organem właściwym ds. cyberbezpieczeństwa w sektorze energii[58] był minister właściwy ds. energii, a organem właściwym ds. cyberbezpieczeństwa w sektorach: zaopatrzenia w wodę pitną i jej dystrybucji oraz transportu (w tym podsektorze transportu wodnego) – Minister Infrastruktury.

---

54 Systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej.

55 WGITA – IDI Handbook on IT audit for supreme audit instituton (v. 2022), str. 7.

56 M. Nowikowska [w:] W. Kitler, J. Taczkowska-Olszewska, F. Radoniewicz (red.), Ustawa o krajowym systemie cyberbezpieczeństwa. Komentarz, wyd. 1, 2019, art. 15.

57 Organami właściwymi ds. cyberbezpieczeństwa są podmioty wymienione w art. 41 ustawy o KSC, właściwe dla poszczególnych sektorów, m.in.: dla sektora energii – minister właściwy ds. energii; dla sektora transportu z wyłączeniem podsektora transportu wodnego – minister właściwy ds. transportu; dla podsektora transportu wodnego - minister właściwy do spraw gospodarki morskiej i minister właściwy do spraw żeglugi śródlądowej; dla sektora zaopatrzenia w wodę pitną i jej dystrybucji – minister właściwy ds. gospodarki wodnej.

58 W okresie objętym kontrolą organem właściwymi ds. cyberbezpieczeństwa w sektorze energii był do 23 lipca 2025 r. Minister Klimatu i Środowiska, a od 24 lipca 2025 r. – Minister Energii.

3.2.1. REALIZACJA ZADAŃ PRZEZ ORGANY WŁAŚCIWE DS. CYBERBEZPIECZEŃSTWA

Ministrowie Energii oraz Infrastruktury, w ramach uprawnień i obowiązków określonych w art. 42 i 43 ustawy o KSC, prowadzili bieżącą analizę podmiotów pod kątem uznania ich za OUK. Jednak Minister Infrastruktury aż w połowie analizowanych przez NIK postępowań w sprawie uznania podmiotu za OUK oraz wygaśnięcia decyzji o uznaniu za OUK[59] nie zapewnił stronom czynnego udziału w postępowaniu i terminowego załatwiania sprawy. Ponadto ministrowie nieterminowo powiadamiali Ministra Cyfryzacji (łącznie w 38,5% objętych analizą przypadków[60]) o konieczności dokonania wpisów, wykreśleń i zmian danych w wykazie OUK, tj. z opóźnieniem od 17 do 609 dni.

Ministrowie prawidłowo korzystali z uproszczonych procedur identyfikowania OUK oraz niezwłocznie informowali operatorów o stwierdzonych przez CSIRT-y podatnościach w celu przeciwdziałania wystąpieniu incydentów. Współpracowali z organami państw członkowskich UE oraz z organami ścigania w zakresie realizowanych zadań.

Minister właściwy ds. energii opracował dwie rekomendacje dotyczące działań mających na celu wzmocnienie cyberbezpieczeństwa[61], ale nie skorzystał z uprawnienia ustanowienia sektorowych zespołów cyberbezpieczeństwa (art. 44 ust. 1 ww. ustawy). Minister Infrastruktury we współpracy z innymi podmiotami opracował dwa raporty[62], m.in. w celu ustalenia poziomu dojrzałości w obszarze cyberbezpieczeństwa w nadzorowanych sektorach w odniesieniu do obowiązującej ustawy o KSC oraz przygotowania do jej nowelizacji w związku z wdrożeniem Dyrektywy NIS2, a także podjął działania w celu utworzenia sektorowego zespołu cyberbezpieczeństwa dla podmiotów nadzorowanych przez Ministra.

3.2.2. NIEPRAWIDŁOWY I NIESKUTECZNY NADZÓR ORGANÓW WŁAŚCIWYCH DS. CYBERBEZPIECZEŃSTWA NAD OUK

Ministrowie Energii oraz Infrastruktury, mimo obowiązków określonych w art. 53 ust. 1 pkt 2 lit. a i ust. 2 ustawy o KSC[63], nie podejmowali odpowiednich działań nadzorczych wobec OUK, realizowanych poprzez wszczynanie kontroli lub postępowań w sprawie nałożenia kary pieniężnej, w przypadkach niewykonania przez operatorów obowiązków określonych w ustawie o KSC, aktach wykonawczych do ww. ustawy oraz normach ISO 27001 i 22301.

---

59 NIK objęła analizą 10 postępowań administracyjnych przeprowadzonych przez Ministra Infrastruktury w przedmiocie wydania decyzji o uznaniu za OUK, stwierdzenia wygaśnięcia decyzji oraz zmiany danych w wykazie OUK prowadzonym przez Ministra Cyfryzacji.

60 Tj. łącznie w 15 przypadkach z 39 objętych analizą przez NIK.

61 W sektorze energii oraz wytyczne sektorowe dotyczące zgłaszania incydentów (opracowane przez pracowników Ministerstwa) oraz dotyczące cyberbezpieczeństwa dla prosumentów OZE (wydane wspólnie z Ministerstwem Cyfryzacji, CERT Polska - zespołem działającym w strukturach CSIRT NASK, Polskimi Sieciami Elektroenergetycznymi w tym CERT PSE (Zespołem Reagowania na Incydenty w spółce Polskie Sieci Elektroenergetyczne S.A.).

62 Pn.: Raport dojrzałości w obszarze cyberbezpieczeństwa sektora transportu w Polsce (we współpracy z CSIRT NASK oraz podmiotem prywatnym) oraz Raport dojrzałości w obszarze cyberbezpieczeństwa dla sektora zaopatrzenia w wodę pitną i jej dystrybucji (we współpracy z Agencją Unii Europejskiej ds. Cyberbezpieczeństwa – ENISA).

63 W brzmieniu sprzed nowelizacji ustawy.

Ministrowie – po przeprowadzeniu analizy sprawozdań z audytów[64] – pomimo, iż posiadali informacje o niezapewnianiu przez operatorów cyberbezpieczeństwa usług kluczowych to nie zaplanowali przeprowadzenia kontroli lub wszczęcia postępowania w sprawie nałożenia kary pieniężnej na operatorów.

We wszystkich analizowanych przez NIK sprawozdaniach z audytów[65], audytorzy sformułowali rekomendacje, obserwacje lub stwierdzili nieprawidłowości (w tym o priorytecie wysokim i średnim), które dotyczyły zaniechania przez operatorów wykonania istotnych obowiązków w zakresie przeciwdziałania zagrożeniom cyberbezpieczeństwa, określonych w ustawie o KSC, aktach wykonawczych do tej ustawy oraz ww. normach ISO[66]. Informacje zawarte w sprawozdaniach z audytów świadczyły o tym, że podmioty, które zostały uznane przez ministrów za OUK w latach 2019–2023[67], w kolejnych latach wciąż nie wykonały obowiązków dotyczących przeciwdziałania cyberzagrożeniom i nie wdrożyły systemu zarządzania bezpieczeństwem w systemie informacyjnym wykorzystywanym do świadczenia usługi kluczowej. Zatem operatorzy nie zapewnili odpowiednio wysokiego poziomu cyberbezpieczeństwa systemów informacyjnych, stosowanych do świadczenia usług kluczowych.

Niepodjęcie przez ministrów działań nadzorczych nad operatorami, mimo posiadanych informacji o niespełnieniu przez nich wymogów dotyczących przeciwdziałania zagrożeniom cyberbezpieczeństwa, stanowiło naruszenie obowiązków organu ds. cyberbezpieczeństwa określonych w art. 53 ust. 1 pkt 2 lit. a i ust. 2 ustawy o KSC oraz zasad określonych również w wewnętrznych procedurach obu Ministerstw.

Minister Infrastruktury co prawda skontrolował 14 OUK (43,8%)[68], przeprowadzając od jednej do pięciu kontroli rocznie, a na trzy OUK (tj. 9,3%) nałożył karę pieniężną za niewykonanie w terminie zaleceń pokontrolnych i niespełnienie wymogów określonych w ustawie o KSC, ale nie podjął działań nadzorczych wobec pozostałych OUK (w tym tych objętych analizą przez NIK), którzy przekazali sprawozdania z audytów, w których audytorzy stwierdzili zaniechanie

---

64 NIK objęła szczegółową analizą 44 sprawozdania (ze 178) otrzymane przez ministrów, z tego: 23 sprawozdania z audytów ze 136 przekazanych przez OUK ministrowi właściwemu ds. energii i 21 sprawozdań z 42 przekazanych – Ministrowi Infrastruktury.

65 Otrzymanych od 27 ze 103 operatorów nadzorowanych przez ministrów (z tego: 71 nadzorowanych przez Ministra Energii i 32 nadzorowanych przez Ministra Infrastruktury).

66 Dotyczących, np.: nieprzeprowadzenia lub nieprawidłowego szacowania ryzyka, w tym braku udokumentowanej analizy Bussines Impact Analysis; niezapewnienia wymaganych szkoleń pracowników; nieweryfikowania „utrzymania" systemów informacyjnych wykorzystywanych do świadczenia usługi kluczowej; niepowołania wewnętrznej struktury organizacyjnej ds. cyberbezpieczeństwa lub niepowierzenia tych zadań podmiotowi świadczącemu te usługi (w ramach usługi Security Operations Center); niezapewnienia wymaganych warunków technicznych i organizacyjnych pracownikom realizującym zadania zakresu cyberbezpieczeństwa; nieopracowania planów ciągłości działania systemów IT i OT, w tym procesu ciągłości dostaw; niezapewnienia utrzymania bezpiecznej eksploatacji systemów informacyjnych wykorzystywanych do świadczenia usługi kluczowej; niewdrożenia narzędzi do skanowania podatności systemów informacyjnych wykorzystywanych do świadczenia usługi kluczowej; wykorzystywania nieaktualnych aplikacji i systemów podatnych na zagrożenia; nieustanowienia lub niewłaściwego ustanowienia procesu zarządzania incydentami, itp.

67 W 2019 r. – 21 podmiotów; w 2022 r. – jeden podmiot i w 2023 r. – pięć podmiotów.

68 Z 32 OUK (w tym dwa podmioty dwukrotnie).

realizacji obowiązków określonych w ustawie o KSC. Nadto Minister po przeprowadzeniu pięciu kontroli (z sześciu, w których stwierdził nieprawidłowości) nie sformułował zaleceń pokontrolnych oraz nie nałożył kary pieniężnej, co stanowiło naruszenie wymogów określonych w art. 59 ust. 1 oraz art. 73 ust. 1 w związku z art. 74 ust. 1 ustawy o KSC.

3.2.3. NIEPODEJMOWANIE DZIAŁAŃ NADZORCZYCH WOBEC OUK, KTÓRZY NIE PRZEPROWADZALI TERMINOWO AUDYTÓW

O niepodejmowaniu działań nadzorczych przez ministrów wobec OUK świadczyły także wyniki dodatkowego badania analitycznego przeprowadzonego przez NIK, dotyczącego wszczynania postępowań w sprawie nałożenia kar pieniężnych za nieprzeprowadzanie terminowo audytów.

Analiza terminów i częstotliwości przeprowadzenia audytów przez wszystkich OUK w latach 2021-2025 wykazała, że w 80 przypadkach[69] operatorzy nie wywiązali się z obowiązku przeprowadzenia pierwszego audytu (na podstawie art. 16 pkt 3 ustawy o KSC) oraz kolejnych audytów[70] (na podstawie art. 15 ust. 1 ww. ustawy).

Ministrowie nie podjęli jednak stosownych działań nadzorczych, w tym nie wszczęli postępowań w sprawie nałożenia kary pieniężnej, na podstawie art. 74 ust. 1 w związku z art. 73 ust. 1 pkt 11, ust. 3 pkt 10 i ust. 4 pkt 3 ustawy o KSC, mimo że posiadali wiedzę o niewywiązaniu się przez OUK z ww. obowiązków. Dopiero w trakcie kontroli NIK Minister Infrastruktury wszczął jedno postępowanie, a minister właściwy ds. energii – cztery postępowania. Szacowana łączna wartość kar pieniężnych za nieprzeprowadzenie w terminie pierwszego i kolejnych audytów wyniosłaby łącznie 3 718,9 tys. zł (odpowiednio: 1 790,5 tys. zł i 1 928,4 tys. zł)[71]. Określone w ustawie o KSC kary pieniężne są narzędziem dyscyplinującym podmioty do realizacji obowiązków określonych w ustawie o KSC i stanowią należności Skarbu Państwa. Organ właściwy ds. cyberbezpieczeństwa był zobowiązany nałożyć na OUK kary w przypadkach wskazanych w art. 73 ust. 1 ustawy o KSC. Mając na uwadze obowiązki jednostki sektora finansów publicznych wskazane w art. 42 ust. 5 ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych, nieuprawnione było niepodjęcie działań w celu zweryfikowania zasadności nałożenia kary pieniężnej określonej w art. 73 ust. 1 ustawy o KSC i ustalenia kwoty należności Skarbu Państwa w przypadkach wskazanych w ww. przepisie, w tym za nieprzeprowadzenia przez OUK audytu (art. 73 ust. 1 pkt 11 ww. ustawy).

---

69 Z tego: w 57 przypadkach OUK nadzorowanych przez ministra właściwego ds. energii oraz w 23 przypadkach OUK nadzorowanych przez Ministra Infrastruktury.

70 Tj. co najmniej raz na dwa lata.

71 Oszacowanych przez ministrów Infrastruktury i Energii – na podstawie art. 73 ust. 3 pkt 10 i ust. 4 pkt 3 ustawy o KSC.

3.2.4. NIEPRAWIDŁOWE I NIESKUTECZNE DZIAŁANIA ORGANIZUJĄCE REALIZACJĘ ZADAŃ ORGANÓW DS. CYBERBEZPIECZEŃSTWA.

Stwierdzone przez NIK nieprawidłowości dotyczące realizacji zadań organu ds. cyberbezpieczeństwa, w szczególności nieprawidłowego i nieskutecznego nadzoru nad OUK, wynikały z niezapewnienia odpowiednich zasobów kadrowych (liczby etatów) do ich realizacji.

Ministrowie Energii oraz Infrastruktury nie podejmowali prawidłowych i wystarczająco skutecznych działań organizujących warunki w celu zapewnienia cyberbezpieczeństwa usług kluczowych w podległych sektorach[72]. Ministrowie, mimo utworzenia w strukturze organizacyjnej komórek organizacyjnych odpowiedzialnych za realizację zadań tych organów, nie zapewnili odpowiednich zasobów kadrowych (liczby etatów) do ich realizacji.

Stan zatrudnienia w Ministerstwie Infrastruktury na koniec każdego roku w latach 2021–2024 wynosił od czterech do siedmiu etatów, mimo że planowana liczba etatów do realizacji zadań tego organu wynosiła łącznie 12 etatów[73]. Zadania ministra właściwego ds. energii jako organu ds. cyberbezpieczeństwa do końca 2024 r. realizowało dziewięciu pracowników zatrudnionych na łącznie osiem etatów, ale w 2025 r. zmniejszono liczbę etatów o dwa (tj. do sześciu), mimo że w kalkulacji limitów wydatków ww. ministra, określonych w art. 93 ust. 6 ustawy o KSC przewidziano osiem etatów do realizacji jego zadań, jako organu ds. cyberbezpieczeństwa.

W trakcie kontroli NIK, dyrektorzy generalni kontrolowanych ministerstw oraz kierownicy/zastępcy kierowników komórek organizacyjnych odpowiedzialnych za realizację zadań ministrów jako organów ds. cyberbezpieczeństwa, w udzielonych wyjaśnieniach wielokrotnie powoływali się na problemy dotyczące niewystarczającej liczby zasobów kadrowych do realizacji tych zadań. Ministrowie, pomimo posiadanych informacji o niewystarczających zasobach kadrowych, nie podjęli adekwatnych działań zaradczych w celu zapewnienia prawidłowej, rzetelnej i skutecznej realizacji zadań ministrów jako organów ds. cyberbezpieczeństwa, w szczególności w zakresie sprawowania nadzoru nad OUK.

Minister Infrastruktury nie podjął działań w celu zapewnienia zasobów kadrowych odpowiadających liczbie etatów, przewidzianej na etapie tworzenia ustawy o KSC do realizacji zadań ww. organu i nie wykorzystał limitów wydatków przeznaczonych na wynagrodzenia osób realizujących te zadania[74]. Ponadto nie monitorował i nie oceniał wykonania ww. limitów, co stanowiło naruszenie wymogów określonych w art. 93 ust. 16, 17 i 19 ustawy o KSC. Minister właściwy ds. energii wykorzystał określony ustawowo limit wydatków na

---

[72] Minister Energii jako organ właściwy ds. cyberbezpieczeństwa w sektorze energii oraz Minister Infrastruktury jako organ właściwy ds. cyberbezpieczeństwa w sektorze zaopatrzenia w wodę pitną i jej dystrybucji oraz sektorze transportu (w tym w podsektorze transportu wodnego).

[73] Planowana liczba etatów Ministra Infrastruktury jako organu ds. cyberbezpieczeństwa, określonych w art. 93 ust. 1–2 i 4 ustawy o KSC – z tego: ministra właściwego ds. transportu – cztery etaty; ministra właściwego ds. gospodarki morskiej – cztery etaty, ministra właściwego ds. gospodarki wodnej – cztery etaty.

[74] W latach 2021–2025 roczny limit wydatków z budżetu państwa, określony w art. 93 ust. 6 ustawy o KSC, wyniósł w każdym roku po 404 tys. zł w część budżetowej 21 – Gospodarka morska; 22 – Gospodarka wodna i 39 – Transport.

wynagrodzenia osób realizujących zadania organu ds. cyberbezpieczeństwa[75], przy czym znaczną część wydatków z tytułu należnych wynagrodzeń (33,2%[76]) w latach 2021-2024 dodatkowo sfinansowano ze środków budżetowych Ministerstwa. Minister właściwy ds. energii, mimo że w 2020 r. (przed okresem objętym kontrolą NIK) podjął działania w zakresie zwiększenia zatrudnienia o dodatkowe etaty i środki finansowe przeznaczone do realizacji zadań organu ds. cyberbezpieczeństwa, zaniechał tych działań w okresie pięciu kolejnych lat (objętych kontrolą przez NIK).

3.3. Minister Cyfryzacji

Minister Cyfryzacji pełni kluczową rolę w ramach ustawy o KSC, będąc głównym organem odpowiedzialnym za politykę cyberbezpieczeństwa państwa. Odpowiada m.in. za nadzór nad Strategią Cyberbezpieczeństwa RP, prowadzenie wykazu podmiotów kluczowych i ważnych oraz wdrażanie dyrektywy NIS2.

3.3.1. Niezapewnienie funkcjonowania Strategii Cyberbezpieczeństwa RP

Strategia Cyberbezpieczeństwa RP jest jednym z najważniejszych dokumentów obowiązujących w ramach krajowego systemu cyberbezpieczeństwa., To w niej określa się cele strategiczne oraz odpowiednie środki polityczne i regulacyjne, mające na celu osiągnięcie i utrzymanie wysokiego poziomu cyberbezpieczeństwa. Istotne jest, aby dokument ten zachowywał swoją aktualność względem zmieniających się cyberzagrożeń.

Minister z opóźnieniem opracował projekt *Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej* na lata 2025–2029, co uniemożliwiło Radzie Ministrów uchwalenie dokumentu strategicznego na kolejne pięć lat[77] przed wygaśnięciem okresu obowiązywania poprzedniej. Dokument ten został przekazany z wnioskiem o wpis do *Wykazu prac legislacyjnych i programowych Rady Ministrów* dopiero 20 maja 2025 r[78]., co przyczyniło się do tego, że Rada Ministrów podjęła uchwałę o przyjęciu nowej strategii dopiero– 10 marca 2026 r.[79] (tj. po zakończeniu czynności kontrolnych NIK), tj. 434 dni po upływie okresu obowiązywania poprzedniej.

Minister Cyfryzacji nie realizował również określonych w art. 71 ustawy o KSC obowiązków przeprowadzenia przeglądów *Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019–2024*[80], które powinny być przeprowadzone co 2 lata, tj. w 2021 r. i 2023 r. Minister w 2021 r., choć wystąpił do interesariuszy[81] o przesłanie uwag do Strategii, jednak mimo ich otrzymania nie dokonał formalnego przeglądu i oceny oddziaływania Strategii, której efektem powinno

---

75 W latach 2021–2025 roczny limit wydatków z budżetu państwa, określony w art. 93 ust. 6 ustawy o KSC, wyniósł w każdym roku po 789 tys. zł.
76 Tj. 1 048,8 tys. zł.
77 Art. 68 ust. 1 ustawy o KSC.
78 Wpis nastąpił 23 czerwca 2025 r. (ID131).
79 Uchwała nr 92 Rady Ministrów z dnia 10 marca 2026 r. (M. P. poz. 309).
80 Uchwała Rady Ministrów nr 125 z dnia 22 października 2019 r. (M. P. poz. 1037), wygasła z końcem dnia 31 grudnia 2024 r.
81 Pełnomocnika ds. cyberbezpieczeństwa, ministrów i właściwych kierowników urzędów centralnych.

być opracowanie ewentualnych działań korygujących. Tym samym, w całym okresie obowiązywania nie była ona aktualizowana, w tym również w obliczu zmiany w 2022 r. sytuacji geopolitycznej związanej z wojną na Ukrainie, która podniosła faktyczny poziom zagrożenia bezpieczeństwa cyberprzestrzeni Rzeczypospolitej Polskiej[82], w wyniku którego ogłoszono na terenie RP trzeci stopień alarmowy CHARLIE-CRP[83].

3.3.2. Opóźnienia związane z wdrożeniem Dyrektywy NIS2

Uchwalona Dyrektywa NIS2 zastąpiła Dyrektywę NIS1 na podstawie, której funkcjonował dotychczasowy krajowy system cyberbezpieczeństwa. Dyrektywa NIS2 utworzyła nowe ramy systemu zapewnienia cyberbezpieczeństwa w UE. Wprowadziła nowe zadania państw członkowskich UE w tym obszarze oraz rozszerzyła zakres podmiotów objętych obowiązkami w zakresie cyberbezpieczeństwa. Ponadto rozszerzeniu uległ katalog sektorów objętych dyrektywą i zmieniono podział z operatorów usług kluczowych i dostawców usług cyfrowych określony w NIS1, na podmioty kluczowe i podmioty ważne. W konsekwencji większa liczba podmiotów (z 397 na ok. 38 tys.) została zobowiązana m.in. do stosowania odpowiednich i proporcjonalnych środków technicznych, operacyjnych i organizacyjnych w celu zarządzania ryzykiem dla bezpieczeństwa sieci i systemów informatycznych wykorzystywanych przez te podmioty do prowadzenia działalności lub świadczenia usług. Zmiany te zostały wprowadzone w związku z szybko postępującą transformacją cyfrową i siecią wzajemnych połączeń w społeczeństwie, w tym w kontekście wymiany transgranicznej, sieci i systemy informatyczne stały się zasadniczym elementem codziennego życia. Zmiana ta doprowadziła do ewolucji krajobrazu cyberzagrożeń, przynosząc nowe wyzwania, które wymagają dostosowanych, skoordynowanych i innowacyjnych reakcji we wszystkich państwach członkowskich. Liczba, skala, zaawansowanie, częstotliwość oraz wpływ incydentów stają się coraz większe i stanowią poważne zagrożenie dla funkcjonowania sieci i systemów informatycznych. W rezultacie incydenty mogą utrudniać prowadzenie działalności gospodarczej na rynku wewnętrznym, powodować straty finansowe, podważać zaufanie użytkowników oraz powodować poważne szkody dla gospodarki i społeczeństw[84].

Prowadzony przez Ministra Cyfryzacji proces legislacyjny dotyczący *projektu ustawy o zmianie ustawy o KSC oraz niektórych innych ustaw* skutkował opóźnieniem we wdrożeniu Dyrektywy NIS2. Termin implementacji przedmiotowej dyrektywy został określony na dzień 17 października 2024 r. Do dnia przedłożenia Radzie Ministrów projektu ustawy, tj. 8 października 2025 r. opóźnienie wynosiło 356 dni[85], a na dzień podpisania ustawy przez Prezydenta RP, tj. 19 lutego 2026 r.[86], opóźnienie wynosiło 490 dni i mogło spowodować

---

82 Raport o stanie bezpieczeństwa cyberprzestrzeni RP w roku 2022 - https://csirt.gov.pl/download/3/214/RaportostaniebezpieczenstwacyberprzestrzeniRPw2022.pdf.

83 Zarządzenie Prezesa Rady Ministrów nr 40 z dnia 21 lutego 2022 roku w sprawie zmiany stopnia alarmowego CRP – III stopnień alarmowy CRP, który obowiązywał do 29 lutego 2024 r.

84 https://orka.sejm.gov.pl/Druki10ka.nsf/0/EAE89BDA7AEC8DECC1258D450063FA62/%24File/1955-uzasadnienie.docx.

85 Tj. do dnia przedłożenia Radzie Ministrów projektu ustawy – 8 października 2025 r.

86 https://www.prezydent.pl/prawo/ustawy-podpisane/ustawy-podpisane-w-lutym-2026-r,114968.

nałożenie przez Trybunał Sprawiedliwości UE kary w wysokości 27 264 554,79 zł[87]. Opóźnienie we wdrożeniu dyrektywy skutkowało brakiem obowiązku stosowania odpowiednich i proporcjonalnych środków technicznych, operacyjnych i organizacyjnych w celu zarządzania ryzykiem dla bezpieczeństwa sieci i systemów informatycznych wykorzystywanych do prowadzenia działalności lub świadczenia usług dla około 38 tys.[88] nowych podmiotów, które zostaną objęte nowelizacją ustawy o KSC. Opóźnienie przesunęło również w czasie osiągnięcie celu Dyrektywy NIS2 jakim było wyeliminowanie rozbieżności pomiędzy państwami członkowskimi UE, wynikającymi z wdrożenia różnych rozwiązań ujętych w Dyrektywach NIS1 i NIS2, co mogło skutkować większą podatnością na cyberzagrożenia i wywołać reperkusje dla całej Unii[89].

3.3.3. NIEPODEJMOWANIE ODPOWIEDNICH DZIAŁAŃ NADZORCZYCH NAD PODMIOTAMI KRAJOWEGO SYSTEMU CYBERBEZPIECZEŃSTWA

Minister Cyfryzacji w latach 2021–2025 nie podejmował odpowiednich działań nadzorczych wobec podmiotów świadczących usługi z zakresu cyberbezpieczeństwa oraz dostawców usług cyfrowych, w zakresie realizowanych przez nich obowiązków określonych w ustawie o KSC. Ponadto w 2022 r. nie przeprowadził żadnej kontroli operatorów (w sektorze infrastruktury cyfrowej), w zakresie realizacji przez nich obowiązków dotyczących przeciwdziałania cyberzagrożeniom i zgłaszania incydentów poważnych. Powyższe zaniechania wynikały z niedostosowania zasobów kadrowych Ministerstwa pozwalających na skuteczną i efektywną realizację ww. zadań.

[87] 6 458 445 euro przeliczonych po kursie NBP z dnia 19 lutego 2026 r. – 4,2220 zł.
[88] Na podstawie szacunków wskazanych w OSR z 7 października 2025 r.
[89] Motyw 5. do Dyrektywy NIS2.

4. ZAŁĄCZNIKI

4.1. METODYKA KONTROLI

Uzasadnienie podjęcia kontroli

W ostatnich latach odnotowuje się coraz większą liczbę ataków mogących mieć istotny skutek polegający na zakłóceniu świadczenia usługi kluczowej (tj. usługi istotnej dla utrzymania krytycznej działalności społecznej lub gospodarczej). Jednocześnie coraz więcej doniesień medialnych wskazuje, iż ataki te mogą być wynikiem tzw. wojny cybernetycznej lub hybrydowej.

W okresie objętym kontrolą, w ustawie o KSC zostały określone zadania i obwiązki różnych podmiotów w ramach krajowego systemu cyberbezpieczeństwa, które mają zapewnić odpowiednio wysoki poziom cyberbezpieczeństwa systemów informacyjnych wykorzystywanych do świadczenia m.in. usług kluczowych. W ramach tego Systemu organem odpowiedzialnym za organizację cyberbezpieczeństwa usług kluczowych w wymiarze cywilnym, jest minister właściwy ds. informatyzacji. Organizacja ta odnosiła się do wdrożenia obowiązków państw członkowskich określonych w Dyrektywie NIS1. Podmiotem zobowiązanym do zapewnienia bezpieczeństwa systemu informacyjnego wykorzystywanego do świadczenia usługi kluczowej i prawidłowej obsługi incydentów – jest operator usługi kluczowej. Jego identyfikację w wymiarze krajowym oraz nadzór nad przestrzeganiem przez niego obowiązków dotyczących przeciwdziałania zagrożeniom cyberbezpieczeństwa i obsługi incydentów sprawują właściwe organy ds. cyberbezpieczeństwa (m.in. ministrowie kierujący określonym działem administracji rządowej dla danego sektora gospodarki).

Przeprowadzenie przedmiotowej kontroli miało na celu zweryfikowanie stanu zapewnienia cyberbezpieczeństwa usług kluczowych przed wdrożeniem Dyrektywy NIS2, która zaostrzyła wymagania w zakresie cyberbezpieczeństwa, jak i zwiększyła liczbę podmiotów objętych obowiązkami związanymi z cyberbezpieczeństwem.

Pytanie definiujące cel główny kontroli

Czy organy państwa i dostawcy lub operatorzy wybranych usług kluczowych podejmowali prawidłowe i skuteczne działania w celu zapewnienia cyberbezpieczeństwa?

Pytania definiujące cele szczegółowe kontroli

1. Czy organy państwa podejmowały prawidłowe i skuteczne działania organizujące warunki w celu zapewnienia cyberbezpieczeństwa?
2. Czy dostawcy/operatorzy usług kluczowych podejmowali prawidłowe i skuteczne działania w celu zapewniania prawidłowego funkcjonowania i doskonalenia cyberbezpieczeństwa?
3. Czy podejmowano prawidłowe i skuteczne działania związane z obsługą incydentów?
4. Czy organy państwa prawidłowo monitorowały, nadzorowały i egzekwowały wymagania w zakresie cyberbezpieczeństwa?

Okres objęty kontrolą

Od 1 stycznia 2021 r. do 16 lutego 2026 r. (dla realizacji celów kontroli były wykorzystywane dowody sporządzone w okresach wcześniejszych, związane z przedmiotem kontroli). Czynności kontrolne w jednostkach przeprowadzono w okresie 6 maja 2025 r. do 16 lutego 2026 r.

4.2. STAN REALIZACJI WNIOSKÓW POKONTROLNYCH

Najwyższa Izba Kontroli, w związku ze stwierdzonymi nieprawidłowościami sformułowała łącznie 46 wniosków w 11 wystąpieniach pokontrolnych skierowanych do: Ministra Cyfryzacji, Ministra Energii, Ministra Infrastruktury i wszystkich ośmiu kontrolowanych operatorów usług kluczowych. Zrealizowano 15 wniosków, a 31 pozostaje w trakcie realizacji.

4.3. OPIS ELEMENTÓW POZATEKSTOWYCH ZAWARTYCH W INFORMACJI

4.3.1. INFOGRAFIKA NR 1 – ATRYBUTY INFORMACJI

- Poufność – zapewnienie, że informacja nie jest udostępniana lub wyjawiana nieupoważnionym osobom, podmiotom lub procesom.
- Integralność – zapewnienie dokładności i kompletności informacji oraz metod jej przetwarzania.
- Dostępność – zapewnienie, że informacja jest dostępna i użyteczna na żądanie upoważnionego podmiotu.
- Autentyczność – zapewnienie, że tożsamość podmiotu lub zasobu jest taka, jak deklarowana.

Źródło: opracowanie własne NIK.

4.3.2. INFOGRAFIKA NR 2 – KRAJOBRAZ ZAGROŻEŃ

- złośliwe oprogramowania (np. malware, ransomware),
- ataki phishingowe, ataki DDoS,
- luki oprogramowania (tzw. podatności)
- błędy ludzkie.

Źródło: opracowanie własne NIK.

4.4. WYKAZ KLUCZOWYCH PODMIOTÓW, KTÓRYM PRZEKAZANO INFORMACJĘ O WYNIKACH KONTROLI

1. Prezydent Rzeczypospolitej Polskiej
2. Marszałek Sejmu Rzeczypospolitej Polskiej
3. Marszałek Senatu Rzeczypospolitej Polskiej
4. Prezes Rady Ministrów
5. Przewodniczący Komisji do Spraw Kontroli Państwowej Sejmu RP
6. Przewodniczący Komisji Cyfryzacji, Innowacyjności i Nowoczesnych Technologii Sejmu RP
7. Przewodniczący Komisji Infrastruktury Senatu RP
8. Minister do spraw Nadzoru nad Wdrażaniem Polityki Rządu
9. Minister Cyfryzacji, Pełnomocnik Rządu ds. Cyberbezpieczeństwa
10. Minister Infrastruktury
11. Minister Energii
12. Minister Zdrowia
13. Minister Obrony Narodowej
14. Minister Rozwoju i Technologii
15. Minister Rolnictwa i Rozwoju Wsi
16. Minister Klimatu i Środowiska
17. Minister Nauki i Szkolnictwa Wyższego
18. Przewodniczący Komisji Nadzoru Finansowego
19. Prezes Urzędu Komunikacji Elektronicznej
20. Dyrektor Rządowego Centrum Bezpieczeństwa
21. Dyrektor Naukowej i Akademickiej Sieci Komputerowej – Państwowego Instytutu Badawczego (CSIRT NASK)
22. Szef Agencji Bezpieczeństwa Wewnętrznego (CSIRT GOV)

Minister
Cyfryzacji

BBKN.WN.0810.11.2026
Warszawa, 06 sierpnia 2026 r.

Pan
Mariusz Haładyj
Prezes
Najwyższej Izby Kontroli

Szanowny Panie Prezesie,

w odpowiedzi na otrzymaną[1] Informację o wynikach kontroli nr *P/25/083 – Cyberbezpieczeństwo wybranych usług kluczowych*, przekazuję stanowisko do ww. Informacji pokontrolnej.

1) 3.3.1. Niezapewnienie funkcjonowania Strategii Cyberbezpieczeństwa RP

Proces opracowywania przyjętej w marcu 2026 r. Strategii Cyberbezpieczeństwa RP na lata 2025–2029 przypadł na okres zmian w środowisku bezpieczeństwa międzynarodowego, w tym pełnoskalowej agresji Rosji na Ukrainę.

Konieczność uwzględnienia w dokumencie nowych wyzwań, takich jak bezpieczeństwo łańcucha dostaw oraz niespotykane dotąd nasilenie działań hybrydowych, wymagała pogłębionych analiz merytorycznych, aby dokument nie miał charakteru jedynie formalnego, lecz realnie odpowiadał na zagrożenia. Ponadto nowa Strategia musiała zostać zsynchronizowana z pracami nad nowelizacją ustawy o krajowym systemie cyberbezpieczeństwa wdrażającą Dyrektywę NIS 2, co stanowi fundament nowego systemu.

W celu wyeliminowania ryzyka zaniechania przeglądów w przyszłości, w nowym dokumencie ustanowiono sztywny reżim kontrolny, zgodnie z którym Strategia podlega obowiązkowemu przeglądowi i ocenie efektów oddziaływania po dwóch latach od przyjęcia oraz w czwartym roku jej obowiązywania, a wyniki tych prac wraz z propozycjami działań korygujących są każdorazowo przedstawiane Radzie Ministrów.

Nowa Strategia w sposób bezpośredni naprawia brak aktualizacji względem zagrożeń zidentyfikowanych w 2022 r., uznając cyberprzestrzeń za pełnoprawną domenę działań operacyjnych na równi z lądową czy powietrzną oraz wprowadzając konkretne instrumenty odpowiedzi na działania hybrydowe.

W odpowiedzi na wskazane problemy z koordynacją i przepływem informacji nowa Strategia formalizuje funkcjonowanie Połączonego Centrum Operacyjnego Cyberbezpieczeństwa (dalej: PCOC). Docelowo PCOC zostanie przekształcone w centralną instytucję zapewniającą cyberbezpieczeństwo na poziomie krajowym, pełniącą funkcję „jednego okienka” dla podmiotów systemu i obywateli. Proces ten już się rozpoczął i jest przewidziany w harmonogramie na lata 2026–2029.

Wprowadzono mechanizm stałego monitorowania realizacji celów strategicznych poprzez nałożenie na Ministra Cyfryzacji obowiązku przedkładania Radzie Ministrów corocznych informacji o realizacji Strategii w terminie do 30 września, co przy jednoczesnym przyjęciu

[1] Z datą wpływu do MC – 24 lipca 2026 r.

telefon: +48 22 245 54 45
adres email: sekretariat.BBKN@cyfra.gov.pl
adres strony internetowej: www.gov.pl/cyfryzacja

adres: ul. Królewska 27
00-060 Warszawa

szczegółowego Planu działań z określonymi miernikami, zapewnia transparentność i ciągłość nadzoru nad systemem.

2) 3.3.2. Opóźnienia związane z wdrożeniem Dyrektywy NIS2

Prace nad projektem ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw[2], wdrażającym Dyrektywę NIS 2 w Polsce, rozpoczęły się w Ministerstwie Cyfryzacji niezwłocznie po utworzeniu rządu w 2023 r. Wcześniej toczyły się prace analityczne o charakterze wewnętrznym, mające na celu przygotowanie jak najlepszego projektu ustawy implementującej dyrektywę, dostosowanego do krajowego porządku prawnego. Prace te obejmowały zarówno analizę samej dyrektywy, jak i jej potencjalnych skutków dla sektora publicznego i prywatnego, a także gromadzenie i analizowanie informacji niezbędnych do opracowania samej treści normatywnej projektu, jak i oceny skutków regulacji.

W ocenie MC nie wydaje się być uprawnionym stwierdzenie, że opóźnienie we wdrożeniu dyrektywy skutkowało brakiem obowiązku stosowania odpowiednich i proporcjonalnych środków technicznych, operacyjnych i organizacyjnych w celu zarządzania ryzykiem dla bezpieczeństwa sieci i systemów informatycznych wykorzystywanych do prowadzenia działalności lub świadczenia usług dla około 38 tys. nowych podmiotów. Chociaż zgodzić należy się ze stwierdzeniem, że Dyrektywa NIS 2 w Polsce obejmuje co najmniej ok. 38 tys. podmiotów, to pominięty został fakt, że wiele z tych podmiotów już przed wejściem w życie ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw podlegało obowiązkom z zakresu cyberbezpieczeństwa, wynikającym z poprzedniego reżimu prawnego. Dotyczyło to m.in. podmiotów publicznych, których liczbę w OSR[3] szacowano na ok. 28 tys.

Podmioty publiczne, w tym jednostki samorządu terytorialnego, były obowiązane do zgłaszania incydentów w podmiocie publicznym oraz do zarządzania incydentami. Ponadto podmioty publiczne już poprzednio miały obowiązek wdrożenia systemu zarządzania bezpieczeństwem informacji i przeprowadzania m.in. audytów (co wynika z § 19 rozporządzenia Rady Ministrów z dnia 21 maja 2024 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych[4]). Dostosowanie się podmiotów publicznych, w tym jednostek samorządu terytorialnego, do wymogów Dyrektywy NIS 2 polega zatem w szczególności na przeglądzie już wdrożonych systemów zarządzania bezpieczeństwem informacji i uzupełnieniu dokumentacji oraz środków technicznych i organizacyjnych. Skala zmian jest zależna od obecnej dojrzałości organizacyjnej poszczególnych podmiotów publicznych.

Powyższe oznacza, że rzeczywiście w pełni nowymi obowiązkami mogło być objętych ok. 10 tys. podmiotów z sektora prywatnego, które do tej pory nie były operatorami usług kluczowych czy dostawcami usług cyfrowych. Jednocześnie podkreślenia wymaga, że prace nad Dyrektywą NIS 2, a następnie projektem ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa i niektórych innych ustaw były publiczne, co umożliwiało podmiotom zapoznanie się z treścią projektowanych przepisów i potencjalnych obowiązków, a tym samym przygotowanie organizacji na nadchodzące obowiązki. W tym celu przewidziany został także roczny okres dostosowawczy i dwuletni okres, w którym nie stosuje się administracyjnych kar pieniężnych wobec podmiotów kluczowych i podmiotów ważnych.

[2] Dz.U. z 2026 r. poz. 252.
[3] Ocena Skutków Regulacji.
[4] Dz. U. z 2024 poz. 773.

Długotrwały proces legislacyjny ww. projektu ustawy wdrażającej Dyrektywę NIS 2 to efekt wielomiesięcznych prac nie tylko Ministra Cyfryzacji, ale całego rządu, pozostałej administracji publicznej, w tym jednostek samorządu terytorialnego, Sejmu, Senatu i sektora prywatnego. Projekt podlegał szerokim konsultacjom społecznym, zgłoszonych zostało wiele uwag do projektu, a tabele uwag liczyły ponad 1000 stron. Każda z tych uwag została przez Ministra Cyfryzacji rozpatrzona i do każdej przygotowano odniesienie.

Proces legislacyjny w Polsce związany z uchwalaniem przepisów rangi ustawowej jest procesem usystematyzowanym, wymagającym wykonania ściśle określonych czynności formalnych oraz zapewnienia uczestnikom procesu legislacyjnego czasu na analizę projektowanych regulacji oraz zgłaszanie propozycji, natomiast wnioskodawcy czasu na analizę i odniesienie się do zgłaszanych propozycji oraz dokonywania na ich podstawie ewentualnych korekt projektowanych regulacji. Z uwagi na charakter aktu projekt został skierowany do rozpatrzenia przez Komisję Wspólną Rządu i Samorządu Terytorialnego oraz Komitet do Spraw Europejskich, a następnie prace toczyły się na Stałym Komitecie Rady Ministrów. Na etapie parlamentarnym projekt był rozpatrywany nie tylko na posiedzeniach Sejmu i Senatu, ale również w komisjach sejmowych i senackich. Na sejmowej Komisji Cyfryzacji, Innowacyjności i Nowych Technologii odbyło się nie tylko głosowanie nad poprawkami do projektu, ale także otwarta dyskusja, w której udział brały podmioty zewnętrzne, reprezentujące rynek prywatny. Za przebieg procesu legislacyjnego i czas jego trwania nie odpowiada zatem wyłącznie Minister Cyfryzacji. Jest to wynik współpracy wielu organów i interesariuszy, co skutkowało przyjęciem i uchwaleniem ustawy w obecnym kształcie.

Jednocześnie podkreślić należy, że Polska była w czołówce państw członkowskich UE[5] w zakresie wdrażania Dyrektywy NIS 2. Wiele państw członkowskich na początku 2026 r. było na stosunkowo wczesnym etapie procesu legislacyjnego. Niektóre państwa członkowskie rozważały także wprowadzenie dłuższego okresu dostosowawczego. Nie zachodziło zatem istotne ryzyko rozbieżności pomiędzy państwami członkowskimi UE, wynikającymi z wdrożenia różnych rozwiązań ujętych w dyrektywach NIS 1 i NIS 2, a tym samym nie doszło do zmaterializowania się większej podatności na cyberzagrożenia. Wskazać należy także, że Minister Cyfryzacji wielokrotnie w toku prac nad projektem ustawy wdrażającej podkreślał, że przyjęcie ustawy powinno być traktowane priorytetowo, a opóźnienia skutkują ryzykiem nałożenia wielomilionowych kar pieniężnych na Polskę.

3) 3.3.3. Niepodejmowanie odpowiednich działań nadzorczych nad podmiotami krajowego systemu cyberbezpieczeństwa

Do czasu wejścia w życie znowelizowanej ustawy o krajowym systemie cyberbezpieczeństwa podmiot spełniający ustawowe przesłanki uzyskiwał status dostawcy usług cyfrowych z mocy prawa, bez konieczności wydania decyzji przez organ właściwy do spraw cyberbezpieczeństwa. Jednocześnie przepisy nie przewidywały podstaw prawnych do prowadzenia przez organ samodzielnej identyfikacji takich podmiotów, a nadzór nad dostawcami usług cyfrowych miał charakter wyłącznie następczy (ex post). W związku z tym oraz brakiem informacji wskazujących na naruszenia przepisów ustawowych Minister Cyfryzacji nie prowadził w kontrolowanym okresie kontroli tej kategorii podmiotów. Były jednak prowadzone kontrole operatorów usług kluczowych, wobec których był prowadzony nadzór ex ante.

Obowiązująca obecnie ustawa o krajowym systemie cyberbezpieczeństwa, wdrażająca Dyrektywę NIS 2, wprowadziła nowy model podmiotowy systemu. Dotychczasowe kategorie operatorów usług kluczowych oraz dostawców usług cyfrowych zostały

[5] Unia Europejska.

zastąpione odpowiednio podmiotami kluczowymi i podmiotami ważnymi. Do podmiotów ważnych zaliczono m.in. dotychczasowych dostawców usług cyfrowych, natomiast dostawcy usług zarządzanych w zakresie cyberbezpieczeństwa zostali objęci kategorią podmiotów kluczowych, co odzwierciedla znaczenie świadczonych przez nich usług dla bezpieczeństwa innych uczestników systemu.

W celu usprawnienia identyfikacji podmiotów objętych ustawą wprowadzono obowiązek samodzielnej rejestracji poprzez wpis do wykazu podmiotów kluczowych i podmiotów ważnych. Organ właściwy do spraw cyberbezpieczeństwa zachował jednocześnie uprawnienie do dokonania wpisu z urzędu, a w szczególnie uzasadnionych przypadkach może, w drodze decyzji administracyjnej, uznać dany podmiot za kluczowy lub ważny.

Nadzór Ministra Cyfryzacji nad podmiotami kluczowymi i ważnymi ma obecnie charakter ciągły, sformalizowany i opiera się na analizie ryzyka. Obejmuje on w szczególności analizę zgłoszeń incydentów, obowiązkowych raportów, wyników audytów oraz informacji przekazywanych przez CSIRT-y i pozostałe podmioty krajowego systemu cyberbezpieczeństwa.

W przypadku stwierdzenia naruszeń organ może stosować zróżnicowane środki nadzorcze, począwszy od zaleceń i wezwań do usunięcia nieprawidłowości, poprzez decyzje administracyjne nakazujące wdrożenie określonych środków bezpieczeństwa, aż po kontrole prowadzone na miejscu. Ustawa przewiduje również możliwość nakładania administracyjnych kar pieniężnych, których wysokość zależy m.in. od charakteru naruszenia, jego skutków oraz statusu podmiotu jako kluczowego lub ważnego. Jednocześnie przepisy przewidują, że kary pieniężne za naruszenia wynikające z nowelizacji ustawy mogą być nakładane dopiero po upływie dwóch lat od dnia wejścia w życie ustawy.

Przyjęty model nadzoru ma zapewnić nie tylko formalne wykonywanie obowiązków przez podmioty objęte ustawą, lecz przede wszystkim skuteczne wdrażanie środków zarządzania ryzykiem w obszarze cyberbezpieczeństwa.

Rozszerzenie katalogu podmiotów objętych krajowym systemem cyberbezpieczeństwa oraz wzmocnienie kompetencji organów właściwych do spraw cyberbezpieczeństwa wiąże się ze znaczącym wzrostem zakresu realizowanych zadań nadzorczych. W obowiązującej ustawie o krajowym systemie cyberbezpieczeństwa zapewniono odpowiedni poziom finansowania działalności organów właściwych do spraw cyberbezpieczeństwa, umożliwiający dostosowanie ich potencjału organizacyjnego do nowych obowiązków. W związku z tym Minister Cyfryzacji podejmuje działania zmierzające do zwiększenia zasobów kadrowych tak, aby zapewnić odpowiednią liczbę wysoko wykwalifikowanych specjalistów niezbędnych do skutecznej i efektywnej realizacji zadań nadzorczych. Działania te obejmują również dążenie do oferowania wynagrodzeń odpowiadających realiom rynku oraz adekwatnych do wymaganych kompetencji i kwalifikacji.

Z up. Paweł Olszewski
Sekretarz Stanu
w Ministerstwie Cyfryzacji
/dokument podpisany elektronicznie/

Załącznik:
Paweł Olszewski - Sekretarz Stanu upoważnienie (4) 1.

telefon: +48 22 245 54 42
adres email: sekretariat.BM@cyfra.gov.pl
adres strony internetowej: www.gov.pl/cyfryzacja

adres: ul. Królewska 27
00-060 Warszawa

NAJWYŻSZA IZBA KONTROLI
Prezes

DZS.430.3.2026 Warszawa, 18 sierpnia 2026

Opinia

Prezesa Najwyższej Izby Kontroli do stanowiska Ministra Cyfryzacji do Informacji o wynikach kontroli „Cyberbezpieczeństwo wybranych usług kluczowych"

Na podstawie art. 64 ust. 2 *ustawy o Najwyższej Izbie Kontroli* uprzejmie przedstawiam opinię do stanowiska Ministra Cyfryzacji.

Uprzejmie dziękuję za przedstawione stanowisko do Informacji o wynikach kontroli odnoszące się w szczególności do zagadnień dotyczących zapewnienia aktualności Strategii Cyberbezpieczeństwa RP oraz podejmowania odpowiednich działań nadzorczych nad podmiotami krajowego systemu cyberbezpieczeństwa. Wskazane w stanowisku potencjalne działania, które zostaną podjęte przez podmioty krajowego systemu cyberbezpieczeństwa, w ramach znowelizowanej *ustawy o krajowym systemie cyberbezpieczeństwa*, potwierdzają prawidłowość ustaleń kontroli. Skuteczna realizacja tych działań będzie odpowiadała realizacji zaleceń skierowanych do kontrolowanych podmiotów w wyniku przeprowadzonej kontroli.

Odnosząc się do stanowiska dotyczącego skutków opóźnień związanych z wdrożeniem Dyrektywy NIS2, podtrzymujemy ustalenia i oceny zawarte w Informacji o wynikach kontroli.

Na wstępie należy zwrócić uwagę, że w zakresie objęcia 38 tys. nowych podmiotów obowiązkami wynikającymi ze znowelizowanej *ustawy o KSC*, wskazane przez Ministra regulacje dotyczące podmiotów publicznych – *rozporządzenie Rady Ministrów z 21 maja 2024 r. w sprawie Krajowych Ram Interoperacyjności* – dotyczyły w szczególności minimalnych wymagań dla systemów teleinformatycznych oraz zapewniających interoperacyjność systemów. W pewnym zakresie reguluje ono obowiązki dotyczące cyberbezpieczeństwa (§19), ale regulacje te nie stanowią pełnej i kompletnej regulacji dotyczącej zapewniania cyberbezpieczeństwa, jak ma to miejsce w przypadku ww. *ustawy*. Przykładowo, *ustawa o KSC* wymaga od podmiotów monitorowania w trybie ciągłym systemu informacyjnego wykorzystywanego do świadczenia usługi - czego *rozporządzenie KRI* nie wymaga. *Ustawa o KSC* wymaga również m.in. zarządzania ryzykiem cyberbezpieczeństwa, zgłaszania incydentów do sektorowych CSIRT, wycofywaniem produktów ICT, usług ICT i procesów ICT w przypadku uznania dostawcy za dostawcę wysokiego ryzyka, czego podmioty publiczne przed objęciem ich *ustawą o KSC* nie musiały realizować.

Regulacje wynikające ze znowelizowanej *ustawy o KSC* dla wszystkich objętych podmiotów krajowego systemu cyberbezpieczeństwa są zatem nowymi regulacjami, ale nie dla wszystkich podmiotów w tym samym zakresie. Biorąc powyższe pod uwagę uzasadnione było stwierdzenie, że *opóźnienie we wdrożeniu dyrektywy skutkowało brakiem obowiązku stosowania odpowiednich*

i proporcjonalnych środków technicznych, operacyjnych i organizacyjnych w celu zarządzania ryzykiem dla bezpieczeństwa sieci i systemów informatycznych wykorzystywanych do prowadzenia działalności lub świadczenia usług dla około 38 tys. nowych podmiotów, które zostaną objęte nowelizacją ustawy o KSC.

W zakresie zapewniania przez podmioty publiczne cyberbezpieczeństwa (w tym stosowania *rozporządzenia KRI*) wielokrotnie w ramach kontroli wskazywaliśmy na liczne systemowe nieprawidłowości, w tym również polegające na niewdrożeniu Systemu Zarządzania Bezpieczeństwa Informacji, jak i niestosowaniu wymaganych zabezpieczeń[1], braku zapewniania ciągłości działania czy zarządzania oprogramowaniem, tj. obowiązków, które zostały określone w *ustawie o KSC*. Dostosowanie się zatem przez podmioty publiczne do nowych regulacji to nie tylko przegląd istniejącej dokumentacji, ale również konieczność wdrożenia nowych rozwiązań proceduralnych i technicznych, w tym poniesienia znacznych nakładów finansowych, m.in. zaplanowanych w związku z nowelizacją *ustawy o KSC* w projektach Ministerstwa Cyfryzacji o łącznym budżecie - 771,5 mln zł[2].

Z szacunkiem
Mariusz Haładyj
/podpisano elektronicznie/

[1] P/24/004/KAP Zapewnienie bezpieczeństwa informacji oraz ciągłości działania systemów informatycznych w jednostkach samorządu terytorialnego; I/23/001/LSZ Zapewnienie bezpieczeństwa teleinformatycznego przez jednostki samorządu terytorialnego województwa zachodniopomorskiego; P/22/082 Zarządzanie oprogramowaniem komputerowym przez administrację publiczną.

[2] Projekty Ministerstwa Cyfryzacji zaplanowane w ramach nowelizacji ustawy o KSC: *Cyberbezpieczny Samorząd* – 1,474 mln zł, *Utworzenie lub rozwój Lokalnych Centrów Cyberbezpieczeństwa* – 270 ml zł; *Wsparcie finansowe na rzecz cyberbezpieczeństwa - NIS2* – 500 mln zł.