NAJWYŻSZA IZBA KONTROLI

Departament Porządku i Bezpieczeńswa Wewnętrznego

KPB.411.1.2.2025

Radosław Nielek
Dyrektor Naukowej i Akademickiej
Sieci Komputerowej -
Państwowego
Instytutu Badawczego

Naukowa i Akademicka Sieć
Komputerowa – Państwowy
Instytut Badawczy
ul. Kolska 12,
01-045 Warszawa

WYSTĄPIENIE POKONTROLNE

I/25/001 - Realizacja celów systemu S46

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

I. Dane identyfikacyjne

Jednostka kontrolowana	Naukowa i Akademicka Sieć Komputerowa − Państwowy Instytut Badawczy[1] ul. Kolska 12, 01-045 Warszawa
Kierownik jednostki kontrolowanej	Radosław Nielek, Dyrektor NASK - PIB, od 28 grudnia 2023 r. W okresie objętym kontrolą funkcję kierownika jednostki poprzednio pełnili: Wojciech Kamieniecki, Dyrektor NASK - PIB, 24.06.2017 - 30.08.2018 Krzysztof Silicki, p.o. Dyrektor NASK - PIB , 31.08.2018 - 14.02.2019 r. Kamil Sitarski, Dyrektor NASK - PIB, 26.02.2020 - 18.11.2020 r. Wojciech Pawlak, p.o. Dyrektor NASK - PIB, 19.11.2020 - 26.09.2023 r.
Zakres przedmiotowy kontroli	1. Przygotowanie i inicjowanie projektu dotyczącego utworzenia i rozwoju Systemu S46. 2. Nadzór i realizacja projektu. 3. Funkcjonalność i bezpieczeństwo s46. 4. Efekty realizacji projektu. 5. Rozwój projektu[2].
Okres objęty kontrolą	Od 1 stycznia 2018 r. do 22 sierpnia 2025 r. (dzień zakończenia czynności kontrolnych)
Podstawa prawna podjęcia kontroli	Art. 2 ust.1, z uwzględnieniem kryteriów określonych w art. 5 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/44/2025 z 05.05.2025 r Daniel Michalecki, główny specjalista kontroli państwowej, upoważnienie do kontroli nr KPB/59/2025 z 12.05.2025 r (akta kontroli str. 1-4)

[1] Dalej: NASK-PIB.

[2] W związku ze ścisłą współpracą MC i NASK-PIB działania obu podmiotów dotyczące wytworzenia S46 będą opisywane w wystąpieniu pokontrolnym łącznie, przy jednoczesnym zróżnicowaniu oceny zgodnie z rolą i właściwością każdej ze stron.

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

II. Ocena ogólna[4] kontrolowanej działalności

OCENA OGÓLNA

System S46 został przez NASK-PIB wdrożony w terminie określonym w art. 89 ustawy o KSC[5], jednakże nie umożliwiło to osiągnięcia celu tego projektu w postaci realnego wsparcia uczestników KSC w podnoszeniu poziomu cyberbezpieczeństwa. Zadecydowały o tym błędy popełnione na etapie inicjacyjnym, w tym przede wszystkim wynikające z presji czasu zaniechanie rzetelnego rozpoznania potrzeb uczestników Systemu[6], których mimo wysokiego poziomu profesjonalizmu, kompetencji i zaangażowania wykazanego przez kierownictwo i pracowników NASK-PIB nie udało się zniwelować w trakcie realizacji projektu.

Dyrektor NASK-PIB skutecznie zorganizował realizację projektu S46, opierając go na zmodyfikowanej metodyce zarządzania PRINCE2. Role i obowiązki uczestników projektu zostały jasno określone, a dzięki zastosowanym narzędziom zarządzania projektowego prace były prowadzone w sposób uporządkowany i kontrolowany, co jednocześnie ułatwiało współpracę z Ministerstwem Cyfryzacji[7]. Trafnie wybrano podejście kaskadowe, odpowiadające sztywnemu harmonogramowi i zdefiniowanemu budżetowi. Zdecydowana większość prac została wykonana siłami NASK-PIB – podmioty zewnętrzne odpowiadały wyłącznie za realizację wyspecjalizowanych usług. System S46 został zaprojektowany zgodnie z zasadą *security by design* i wyposażony w mechanizmy skalowalności oraz utrzymania ciągłości działania, takie jak geograficzne rozproszenie ośrodków przetwarzania danych, redundancja, równoważenie obciążeń i replikacja danych. Skuteczność przyjętych rozwiązań obniżał fakt, że mechanizmy utrzymania ciągłości działania nie były poddawane cyklicznym, dedykowanym testom, co zmniejszało pewność co do ich sprawności i gotowości do użycia w sytuacjach awaryjnych. Pozytywnie należy ocenić natomiast przeprowadzenie szkoleń dla uczestników systemu oraz wytworzenie profesjonalnych materiałów dydaktycznych.

Jednocześnie stwierdzono, że błędy popełnione na etapie przygotowania i inicjowania projektu znacząco obniżyły użyteczność S46. Brak analizy potrzeb użytkowników końcowych przed wdrożeniem doprowadził do powstania systemu, w którym podstawowe mechanizmy: rekomendacji, ostrzegania i szacowania ryzyka – nie działały zgodnie z oczekiwaniami. W konsekwencji S46 pełnił funkcję pasywnego źródła informacji, a niska liczba logowań potwierdzała jego marginalne wykorzystanie operacyjne. W ocenie NIK projekt nie osiągnął celu w postaci realnego wsparcia uczestników KSC w podnoszeniu poziomu cyberbezpieczeństwa.

Po wdrożeniu wersji produkcyjnej kierownictwo projektu prawidłowo dostrzegło ograniczenia wynikające z architektury i pominięcia wymagań użytkowników końcowych, a następnie podejmowało wraz z MC działania naprawcze

---

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

[5] Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. 2024 r. poz. 1077, ze zm. Dalej: ustawa o KSC).

[6] W Systemie S46 wyróżnia się użytkowników (CSIRT-y i organy właściwe) oraz uczestników (operatorów usług kluczowych – np. szpitale, przedsiębiorstwa). Na potrzeby tego wystąpienia ci ostatni będą nazywani także niekiedy użytkownikami końcowymi.

[7] Dalej: MC.

zmierzające do poprawy funkcjonalności i użyteczności systemu. Zakres planowanych modyfikacji, obejmujący zarówno poprawę funkcjonalności, jak i rozszerzenie wartościowych treści, daje – pod warunkiem sprawnej i konsekwentnej realizacji – realną perspektywę, że system ten zacznie pełnić rolę, dla której został powołany. Po wprowadzeniu odpowiednich zmian mógłby stać się on oczekiwanym i użytecznym narzędziem, wspierającym podmioty krajowego systemu cyberbezpieczeństwa. Ma to szczególne znaczenie w obliczu planowanej nowelizacji ustawy o KSC[8], która spowoduje znaczący wzrost liczby uczestników systemu S46, jak również w kontekście dużych nakładów poniesionych dotychczas oraz planowanych w przyszłości na jego utrzymanie.

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

OBSZAR

1. 1 Przygotowanie i inicjowanie projektu

Opis stanu faktycznego

Uzasadnieniem dla rozpoczęcia realizacji projektu S46 były przepisy zawarte w art. 46 ustawy o KSC. W artykule tym ustawodawca określił, że Minister właściwy do spraw informatyzacji zapewnia rozwój lub utrzymanie systemu teleinformatycznego wspierającego:

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

W uzasadnieniu do projektu ww. ustawy określono, że system ten pozwoli na wymianę informacji o podatnościach, zagrożeniach i incydentach, jak również będzie zbierać informacje o poziomie ryzyka wystąpienia poważnego incydentu i prowadzony będzie w nim rejestr incydentów, w tym poważnych i krytycznych. System miał także wesprzeć agregację i korelację pozyskiwanych informacji w celu określenia ryzyka wystąpienia incydentu, publikowania ostrzeżeń o zaistniałych incydentach, opracowania informacji o poziomie ryzyka dla RP, jak również prognozę skutków materializacji zagrożeń cyberbezpieczeństwa.

System S46, jako przeznaczony dla ochrony cyberprzestrzeni RP, wymagał szczególnej ochrony zastosowanych rozwiązań oraz dokumentacji technicznej i projektowej. Zgodnie z przepisami ustawy o KSC Minister mógł zrealizować to zadanie jedynie za pomocą jednostek mu podległych lub przez niego nadzorowanych. S46 był więc realizowany – z niewielkimi wyjątkami – głównie własnymi siłami NASK-PIB (jednostka nadzorowana przez Ministra).

---

[8] Projekt ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw, wpisany do Wykazu Prac Legislacyjnych Rady Ministrów obowiązującego w X kadencji Sejmu RP pod numerem UC32.

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

Model współpracy między NASK-PIB a Ministerstwem opierał się na wspólnym określaniu potrzeb i kierunków rozwoju. W procesie tym Ministerstwo pełniło rolę decyzyjną, wskazując priorytety i oczekiwany zakres działań. NASK-PIB opracował propozycję wniosku dotacyjnego zbieżną z ustalonym z MC zakresem tematycznym. Po uzgodnieniu zakresu rzeczowego oraz oszacowaniu kosztów dokument został zatwierdzony, a dla zdefiniowanego zakresu podpisano stosowną umowę dotacyjną. Ten sposób współpracy powtarzano przy kolejnych umowach dotacyjnych.

(akta kontroli str. 10, 117-195)

W przekazach medialnych osób zaangażowanych w realizację projektu S46 pojawiały się informacje sugerujące, że w swojej dojrzałej postaci system ten pozwoli z dużym prawdopodobieństwem przewidzieć, w jakim obszarze kraju lub w jakich sektorach nastąpi atak typu DDoS[10], a następnie ostrzec zagrożone podmioty, które są do niego podłączone – w tym także operatorów lokalnych. To z kolei miało umożliwiać przygotowanie się na atak i obronę przed nim z pomocą innego, dedykowanego narzędzia, takiego jak ADDOS[11].

Nadrzędnym celem przy realizacji systemu S46 miała być poprawa poziomu cyberbezpieczeństwa podmiotów wchodzących w skład KSC oraz szerzej – w całym kraju. Wszystkie cele szczegółowe wskazane w art. 46 ustawy o KSC – takie jak monitorowanie zagrożeń, wymiana informacji czy reagowanie na incydenty – służyć miały zwiększeniu odporności na zagrożenia cyfrowe, natomiast generowanie i przekazywanie uczestnikom rekomendacji wprost odnosiło się do poprawy ich poziomu cyberbezpieczeństwa.

System S46 był potrzebny przede wszystkim ze względu na rosnącą skalę i złożoność cyberzagrożeń, dotykających zarówno sektor publiczny, jak i prywatny. Zespoły reagowania na incydenty (CSIRT), mimo swojej wiedzy i doświadczenia, nie były już w stanie w skuteczny sposób samodzielnie obsłużyć tak dużej liczby zgłoszeń i przeanalizować danych napływających z różnych źródeł w czasie rzeczywistym. Potrzebowały do tego narzędzi i systemu, który umożliwiałby automatyzację wielu kluczowych procesów – od wczesnego ostrzegania, przez zgłaszanie i klasyfikację incydentów, po przekazywanie rekomendacji i tworzenie jednolitego obrazu sytuacyjnego. Pozwoliłoby to nie tylko na szybszą reakcję na zagrożenia, ale również na efektywniejszą współpracę między podmiotami odpowiedzialnymi za bezpieczeństwo cyfrowe. Dodatkowo system S46 miał gromadzić wszystkie te funkcje w jednym miejscu, co byłoby wygodne i korzystne dla jego uczestników. Przed wdrożeniem systemu zadania te realizowane były za pośrednictwem rozproszonych baz wiedzy, formularzy oraz innych narzędzi informatycznych. Prowadzone działania były

[10] Ataki polegające na tym, że bardzo wiele komputerów jednocześnie „zasypuje" stronę lub serwer ogromną ilością zapytań. Przez ten sztucznie wywołany ruch serwer nie nadąża z obsługą i staje się niedostępny dla zwykłych użytkowników.

[11] Wypowiedź kierownika Działu Strategicznych Projektów Cyberbezpieczeństwa w NASK – Państwowy Instytut Badawczy (dalej: NASK PIB) opublikowana 25 kwietnia 2023 r. na łamach ISPortal: https://isportal.pl/nask-o-s46-niezawodnosc-tego-systemu-przewyzsza-inne-rozwiazania

zautomatyzowane tylko częściowo, a w dużej części prowadzono je ręcznie za pomocą CSIRT oraz innych kluczowych podmiotów KSC.

(akta kontroli str. 7-16)

Na podstawie art. 89 ustawy o KSC, która weszła w życie z dniem 28 sierpnia 2018 r., Minister właściwy do spraw informatyzacji został zobowiązany do uruchomienia systemu teleinformatycznego, o którym mowa w art. 46 ust. 1, do dnia 1 stycznia 2021 r. Biorąc pod uwagę konieczność wcześniejszego utworzenia zespołu projektowego, identyfikacji interesariuszy, pozyskania zasobów, opracowania dokumentacji projektowej i stworzenia architektury systemu, NASK-PIB miał w praktyce 18 miesięcy, by uruchomić system w terminie wymaganym ustawą.

(akta kontroli str. 117-195)

Od 2017 roku NASK-PIB realizował projekt naukowo-badawczy pn. Narodowa Platforma Cyberbezpieczeństwa (NPC) związany z opracowaniem kompleksowego, zintegrowanego systemu monitorowania, obrazowania i ostrzegania o zagrożeniach identyfikowanych w czasie zbliżonym do rzeczywistego w cyberprzestrzeni państwa[12]. Towarzyszył mu projekt NPCnet, który miał na celu zbudowanie bezpiecznej i odpornej sieci zapewniającej łączność na potrzeby Platformy.

Uwzględniając powyższe okoliczności Minister, w porozumieniu z ówczesnym kierownictwem NASK-PIB, podjął decyzję, że system S46 zostanie oparty na rozwiązaniach powstałych w ramach prac badawczo-rozwojowych (NPC i NPCnet), do których dopisywano wymagania wynikające z ustawy o KSC. Zastosowane podejście umożliwiło uruchomienie systemu w ustalonym terminie, jednak w praktyce pociągnęło za sobą szereg ograniczeń dotyczących dopasowania funkcjonalności, zbierania wymagań uczestników oraz przyjętej koncepcji technicznej podłączeń (więcej w sekcji *Stwierdzone nieprawidłowości*).

(akta kontroli str. 28-30, 93, 66-68, 117-195)

S46 realizowany był w oparciu o własną metodykę NASK bazującą na założeniach PRINCE2 i dostosowaną do potrzeb projektu. Ze względu na tryb jego realizacji (zlecenie zadania przez Ministra Cyfryzacji w ramach umowy dotacji) nie przygotowywano uzasadnienia biznesowego projektu ani wniosku o wyrażenie zgody na realizację projektu. W zamian osoby odpowiedzialne za opiniowanie i podpisanie umowy i wniosku dotacyjnego uczestniczyły w konsultacjach tych dokumentów. Ponadto ze względu na konieczność przygotowywania raportów z realizacji umowy dotacyjnej były one po akceptacji uznawane za raport końcowy z realizacji projektu. Wymienione modyfikacje metodyki pozwalały na usprawnienie procesów inicjowania i zamykania projektu. Wybór metodyki kaskadowej był zgodny z zasadami przyjętymi dla projektów o sztywnym terminie wdrożenia (uwarunkowanym wymaganiami prawnymi) oraz z góry określonym budżecie (uznaje się bowiem, że metodyki typu *waterfall* sprawdzają

[12] Projekt realizowany był przez NASK-PIB (lidera konsorcjum) oraz Politechnikę Warszawską, Instytut Łączności – Państwowy Instytut Badawczy i Narodowe Centrum Badań Jądrowych.

się w takich przypadkach najlepiej, zwiększając prawdopodobieństwo sukcesu ukończenia projektu w terminie).

(akta kontroli str.75-79, 117-195)

Na potrzebę realizacji projektu została określona struktura organizacyjna, w tym zdefiniowano i przypisano konkretnym osobom role i obowiązki. Określono także zakres odpowiedzialności w ramach poszczególnych zespołów oraz ustanowiono zasady zarządzania komunikacją. Opisano zakres prac i bazowy harmonogram realizacji. Ustalono terminy raportów okresowych, ich autorów i odbiorców. W projekcie wspomagano się m.in. narzędziem JIRA pomocnym w zarządzaniu, planowaniu i śledzeniu pracy w zespole.

(akta kontroli str. 75-78, 117-195)

Wśród głównych ryzyk projektowych wymienione zostały m.in.: brak wyników testów wydajnościowych rozwiązania NPC oraz krótki termin do uruchomienia systemu S46. Wobec braku wyników testów wydajnościowych NPC oceniono, że planowane zakupy sprzętu i zastosowana technologia wytwarzania mogą okazać się nieadekwatne do potrzeb systemu S46. Jednocześnie ze względu na późny termin wytworzenia prototypu NPC i bardzo bliski ustawowy termin wdrożenia S46 uznano, że ryzyka tego nie można odpowiednio ograniczyć. Jak się okazało, ryzyko to częściowo się zmaterializowało (więcej na str. 9 i 21-22).

(akta kontroli str. 117-195)

Produkty projektu (listy produktów) określono w ramach poszczególnych umów dotacji celowych zawieranych między Ministrem Cyfryzacji a NASK-PIB. W przypadku umów dofinansowanych przez Centrum Projektów Polska Cyfrowa (CPPC) określono również metryki ilościowe (KPI) dotyczące ilości podłączonych do S46 podmiotów. Od 2023 r. dodano wskaźnik dotyczący dostępności systemu. Wskaźniki te były mierzalne i łatwe do weryfikacji, dotyczyły jednak strony technicznej S46. Nie określono natomiast w projekcie wskaźników dotyczących celów postawionych przed systemem w ustawie o KSC (np. liczby zgłoszonych poprzez S46 incydentów, przesłanych rekomendacji czy oczekiwanego podniesienia poziomu dojrzałości uczestników systemu).

(akta kontroli str. 19-20, 117-195)

Stwierdzone nieprawidłowości

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

Brak rzetelnego zdefiniowania wymagań użytkowników końcowych oraz weryfikacji skuteczności operacyjnej NPC – wynikający z krótkiego czasu przeznaczonego na realizację projektu S46 – skutkował powstaniem istotnych ograniczeń w zakresie funkcjonalności i efektywnego wykorzystania tego Systemu.

Zgodnie z wyjaśnieniami kierownika projektu S46 jego priorytetem było przede wszystkim dotrzymanie ustawowego terminu uruchomienia Systemu, określonego w art. 89 ustawy o KSC na dzień 1 stycznia 2021 r., a ponieważ trzeba było przede wszystkim dostosować NPC do wymagań ustawy o KSC,

każde kolejne wymaganie wprowadzone do projektu byłoby zagrożeniem dla jego realizacji w założonym czasie.

W ocenie NIK prototyp NPC był jednak przede wszystkim produktem projektu naukowo-badawczego, a projekty takie charakteryzują się silnym ukierunkowaniem na aspekt teoretyczny i eksperymentalny i często pomijają kluczowe kwestie użytkowe, takie jak ergonomia interfejsu czy efektywność wdrożenia w strukturach administracyjnych i operacyjnych. W konsekwencji wymagania użytkowników końcowych systemu S46 (tzw. uczestników) zbierane były już po jego wdrożeniu (np. w formie powtarzanych ankiet). Ponadto z części przyjętych w ramach NPC, a następnie przeniesionych do S46 rozwiązań – rezygnowano w następnych latach jako nieprzydatnych lub niefunkcjonalnych. Brak zebrania wymagań użytkowników końcowych na etapie projektowania systemu informatycznego S46 był niezgodny z uznanymi standardami zarządzania IT (np. COBIT) i zarządzania projektami/systemami (BABOK, PMBOK, ITIL, Agile).

Potrzeby użytkowników końcowych (uczestników) S46 zostały w większym stopniu rozpoznane i uwzględnione dopiero na etapie rozwoju tego systemu, tj. już po wdrożeniu podstawowej wersji rozwiązania. Oznacza to, że mechanizmy identyfikacji oczekiwań zdecydowanej większości interesariuszy oraz prace nad dostosowywaniem funkcjonalności do realnych warunków operacyjnych uruchomiono *ex post*, a nie w fazie projektowania. W 2023 r. skierowano do uczestników pierwszą ankietę z wykorzystania systemu S46, która była jednocześnie próbą zbadania ich potrzeb. W kolejnych latach zbierano uwagi i wymagania uczestników oraz przygotowywano koncepcję praktycznych rozwiązań, które podniosłyby zadowolenie z wykorzystania systemu. Proces dostosowywania Systemu do oczekiwań operacyjnych trwał do końca okresu objętego kontrolą.

(akta kontroli str. 8, 19-21, 28-30, 40-45, 60-69, 84, 93, 117-195)

OCENA CZĄSTKOWA

Zapewniona przez Dyrektora NASK-PIB organizacja projektu S46 cechowała się dojrzałością i stała na wysokim poziomie. Zastosowano autorską metodykę opartą na PRINCE2, jasno określono role i obowiązki uczestników projektu, wykorzystano narzędzia zarządzania projektowego, a współpraca między NASK-PIB a Ministerstwem Cyfryzacji przebiegała w sposób uporządkowany i formalnie kontrolowany. Trafnie wybrano też podejście kaskadowe, dostosowane do sztywnego harmonogramu i zdefiniowanego budżetu.

W ocenie NIK nierzetelne było jednak nieprzeprowadzenie analizy potrzeb użytkowników końcowych przed wdrożeniem, co doprowadziło do braku funkcjonalności odpowiadających ich oczekiwaniom. Stało się tak pod presją ustawowego terminu wdrożenia oraz z powodu decyzji kierunkowej, by S46 oprzeć na rozwiązaniach naukowo-badawczych Narodowej Platformy Cyberbezpieczeństwa. W rezultacie w kolejnych latach z części z tych rozwiązań rezygnowano ze względu na stopień ich skomplikowania lub brak wymiaru praktycznego. Nie były one także przygotowane na skalę operacyjną wymaganą przez KSC, co miało potem konsekwencje w postaci okresowo obniżonej wydajności systemu S46. Koncepcja połączeń z wykorzystaniem urządzeń brzegowych – pomimo że cechująca się wysokim poziomem bezpieczeństwa – okazała się kosztowna i trudna do wdrożenia, co ograniczyło później dostępność

systemu, zwłaszcza dla podmiotów publicznych o mniejszych lub napiętych budżetach. W konsekwencji S46 nie dostarczył oczekiwanej wartości użytkowej.

Po wdrożeniu wersji produkcyjnej kierownictwo projektu prawidłowo dostrzegło ograniczenia wynikające z architektury i pominięcia wymagań użytkowników końcowych, a następnie podejmowało wraz z MC działania naprawcze zmierzające do poprawy funkcjonalności i użyteczności systemu. Proces jego dostosowywania do potrzeb operacyjnych użytkowników trwał do zakończenia kontroli.

OBSZAR

2. Realizacja projektu

Opis stanu faktycznego

W kontrolowanym okresie system S46 był budowany i utrzymywany przez NASK w ramach siedmiu zadań finansowanych w szczególności ze środków dotacji udzielonych w tym celu przez Ministra Cyfryzacji, w tym pięciu już ukończonych:

1. „System S46” - na podstawie zawartej z Ministrem Cyfryzacji umowy dotacji celowej nr 2/DC/D/2019/2019 z dnia 25 września 2019 r.

W czasie trwania projektu zrealizowano m.in.: model architektury i specyfikację interfejsów w S46, infrastrukturę sprzętową i uruchomienie środowiska Platformy Analitycznej S46, rozbudowanie środowiska prototypowego wykorzystywanego przez CSIRT NASK, Platformę Analityczną S46 (w pierwszej wersji) wraz z kompatybilnymi wersjami komponentów Klientów. Wszystkie prace w ramach poszczególnych podzadań zakończone zostały 31 grudnia 2020 r. Zgodnie z zatwierdzonym sprawozdaniem końcowym, beneficjent wykorzystał środki dotacji w wysokości 6 207 362,13 zł.

(akta kontroli str. 75-78, 109, 117-195)

2. „Utrzymanie i rozwój S46 w 2021 roku” - na podstawie zawartej z Ministrem Cyfryzacji umowy dotacji celowej nr 3/DC/D/2021 z 16 lipca 2021 r.

W ramach poszczególnych etapów zrealizowano następujące zadania: zapewniono ciągłość działania środowiska produkcyjnego, przeprowadzono migrację do środowiska CSIRT NASK oraz wdrożono portal ServiceDesk na zasobach produkcyjnych. Równolegle rozwijano i utrzymywano warstwę aplikacyjną poprzez przygotowanie materiałów instruktażowych w formie filmów, obsługę i rozwiązywanie zgłoszeń związanych z ankietowaniem i uspójnianiem danych oraz opracowanie szablonów raportów obrazu sytuacyjnego. W obszarze rozwoju technologii i aplikacji zrealizowano zmianę architektury systemu, przeprowadzono testy w środowisku uruchomieniowym i produkcyjnym, a także wdrożono nowe wydanie na środowisku produkcyjnym. Zakończenie inwestycji obejmowało przygotowanie dokumentacji SOPZ (szczegółowy opis przedmiotu zamówienia), skierowanie zapytań RFI (pytanie ofertowe typu *Request for information*) do potencjalnych wykonawców oraz finalizację procesu poprzez podpisanie umów i odbiory przedmiotu zakupu.

Zgodnie z zatwierdzonym sprawozdaniem końcowym z wykonania zadania w ramach udzielonej dotacji celowej w okresie od 1 stycznia 2021 r. do 30 listopada 2022 r. beneficjent wykorzystał środki dotacji w wysokości 7 013 466,94 zł (w roku 2021- 6 296 028,94 zł oraz ze względu na problemy

z dostawami urządzeń i przeniesienie części środków na zakup urządzeń na środki niewygasające, w roku 2022 w wysokości 717 438,00 zł).

(akta kontroli str. 75-78, 109, 117-195)

3. „Rozwój i utrzymanie systemu teleinformatycznego S46 w 2022 roku" - na podstawie zawartej z Ministrem Cyfryzacji umowy dotacji celowej nr 32/DC/D/2021 z dnia 31 grudnia 2021 r.

Zadanie realizowano równolegle w trzech obszarach, koncentrując się na utrzymaniu i rozwoju warstwy technologicznej oraz aplikacyjnej systemu S46. W ramach utrzymania infrastruktury technicznej zainstalowano i uruchomiono nowy sprzęt, prowadzono działania związane z monitorowaniem i zarządzaniem pojemnością oraz zapewnieniem ciągłości działania, a także zarządzano siecią i elementami systemu. Realizowano zadania w ramach drugiej linii wsparcia, doskonalono narzędzia i dokumentację, pozyskiwano nowych uczestników i organizowano proces ich podłączania. Zaktualizowano dokumentację eksploatacyjną oraz przeprowadzono szkolenia dla uczestników systemu. Równocześnie w obszarze aplikacyjnym zapewniano wsparcie uczestników, korygowano błędy, realizowano wnioski o zmianę, utrzymywano kontakt z użytkownikami zewnętrznymi, a także prowadzono analizy i monitorowanie obrazu sytuacyjnego na poziomie krajowym. W ramach rozwoju systemu wdrożono nowe wydanie oprogramowania, przeprowadzono analizę możliwości przetwarzania informacji do poziomu „zastrzeżone" oraz przygotowano narzędzia zwiększające efektywność, bezpieczeństwo i zasięg systemu, dostosowując go jednocześnie do potrzeb użytkowników i wymogów wynikających z nowelizacji ustawy o krajowym systemie cyberbezpieczeństwa. Zgodnie z zatwierdzonym sprawozdaniem końcowym z wykonania zadania w ramach udzielonej dotacji w okresie od 1 stycznia 2022 r. do 23 grudnia 2022 r. beneficjent wykorzystał środki dotacji w wysokości 8 204 257,85 zł.

(akta kontroli str. 75-78, 109, 117-195)

4. „Rozwój i utrzymanie systemu teleinformatycznego S46 w latach 2023-2024" - na podstawie zawartej z Ministrem Cyfryzacji umowy dotacji celowej nr 79/DC/D/2022 z dnia 28 grudnia 2022 r.

W roku 2023 w obszarze utrzymania warstwy technologicznej zapewniono podłączanie i pozyskiwanie nowych uczestników, zaktualizowano materiały szkoleniowe w formie filmów instruktażowych oraz podpisano umowy użyczenia i porozumienia z Ministrem. Zrealizowano również planowane zakupy sprzętowe, obejmujące m.in. urządzenia Systemu Brzegowego Uczestnika (to urządzenia służące do podłączania uczestników do S46), wsparcie dla serwerów i routerów. W warstwie aplikacyjnej dokonano reorganizacji pracy zespołu rozwojowego, przeprowadzono analizy i korekty błędów, a także wdrożono nową wersję oprogramowania. Równolegle przygotowano analizy dotyczące możliwości integracji systemu ze źródłami danych oraz z systemem ARAKIS[13]. W obszarze monitorowania obrazu sytuacyjnego opracowano raporty, udzielano wsparcia uczestnikom w procesie ankietowania, a także przygotowano produkty

[13] System wczesnego ostrzegania przed zagrożeniami w sieci Internet.

towarzyszące, takie jak kalendarze ćwiczeń i warsztatów, certyfikaty ze szkoleń czy materiały dydaktyczne.

W roku 2024 kontynuowano działania na rzecz utrzymania wysokiej jakości usług systemu, osiągając wskaźnik dostępności na poziomie 99%. Zaktualizowano dokumentację eksploatacyjną oraz materiały przekazywane uczestnikom, a także zrealizowano planowany zakres zakupów. Istotnym osiągnięciem było podłączenie nowych podmiotów – łącznie w latach 2023–2024 dokonano 127 podłączeń. Opracowano i wdrożono koncepcję uproszczonych metod przyłączania do systemu, przygotowano rozwiązania dostosowujące do wymagań dyrektywy NIS2 (choć nie wdrożono ich z uwagi na brak odpowiednich przepisów[14]), a także wypracowano koncepcję wsparcia w analizie raportów audytowych. Dodatkowo opracowano koncepcję modernizacji funkcjonalności analizy ryzyka, wraz z rekomendacjami dotyczącymi jej wdrożenia.

Zgodnie z zatwierdzonym sprawozdaniem końcowym z wykonania zadania w ramach udzielonej dotacji celowej w okresie od 1 stycznia 2023 r. do 31 grudnia 2024 r. beneficjent wykorzystał środki dotacji w wysokości 16 796 151,94 zł (w tym odpowiednio 6 931 084,04 zł w 2023 r. oraz 9 908 408,14 zł w 2024 r.).

(akta kontroli str. 75-78, 109, 117-195)

5. „Podłączenie podmiotów krajowego systemu Cyberbezpieczeństwa do zintegrowanego systemu zarzadzania Cyberbezpieczeństwa S46 (S46-REACT)” - na podstawie umowy nr POPC.05.01.00-00-0001/22-00 o dofinansowanie projektu w ramach Programu Operacyjnego Polska Cyfrowa na lata 2014-2020, z dnia 29 marca 2022 r.

W ramach realizacji tego zadania dostarczono, zainstalowano i uruchomiono systemy brzegowe S46 w 100 jednostkach oraz przeprowadzono szkolenia dla 200 osób. Projekt obejmował także dostawy nowej platformy wirtualizacyjnej, rozwój środowiska deweloperskiego oraz przygotowanie puli urządzeń zapasowych. Zrealizowano ponadto dostawy infrastruktury i oprogramowania obejmujące zaawansowane systemy bezpieczeństwa teleinformatycznego, narzędzia zwiększające odporność usług na sytuacje kryzysowe, rozwiązania zapewniające większą redundancję geograficzną centrów przetwarzania danych[15] oraz wyposażenie centrów monitorowania SOC/NOC[16].

Pierwotnie planowane zakończenie projektu przewidziano na 1 czerwca 2023 r., jednak faktyczna finalizacja nastąpiła 31 grudnia 2023 r. Przyczyną przesunięcia terminu były opóźnienia w podpisaniu umowy dotacyjnej, ograniczona dostępność sprzętu w okresie pandemii, długotrwały proces pozyskiwania łączy przez jednostki podłączane do S46, wynikający z braku odpowiedniej infrastruktury, a także przedłużające się uzgodnienia dotyczące lokalizacji dodatkowego centrum przetwarzania danych.

---

[14] Przepisy zostały przygotowane, jednak na dzień zakończenia kontroli projekt ustawy zmieniającej ustawę o KSC wciąż znajdował się na etapie rządowego procesu legislacyjnego.

[15] To oznacza takie rozwiązanie, w którym serwery i dane są nie w jednym, ale w kilku centrach danych, które znajdują się w różnych lokalizacjach. Dzięki temu, jeśli jedno centrum przestanie działać (np. awaria, pożar, powódź), drugie przejmie jego rolę i usługi nadal będą dostępne.

[16] Security Operations Center/Network Operations Center – to zespoły i systemy mające kluczowe znaczenie dla utrzymania sprawnej infrastruktury sieciowej oraz cyberbezpieczeństwa.

Na podstawie zatwierdzonego Raportu końcowego z realizacji projektu informatycznego beneficjent w okresie od 1 maja 2022 r. do 31 grudnia 2023 r. wydatkował 25 946 896,79 zł.

(akta kontroli str. 75-78, 109, 117-195)

Wg stanu na dzień zakończenia kontroli w trakcie realizacji pozostawały dwa zadania:

6. „Utrzymanie i rozwój systemu teleinformatycznego S46 w latach 2025-2026" - na podstawie zawartej z Ministrem Cyfryzacji umowy dotacji celowej nr 201/DC/D/2024 z 21 stycznia 2025 r. Jej celem jest eksploatacja i utrzymanie systemu w trybie ciągłym oraz zwiększenie korzyści poprzez rozwój funkcjonalny systemu. Planowany koszt zadania to 16 135 000 zł.

(akta kontroli str. 75-78, 109, 117-195)

7. „Podłączenie 385 nowych podmiotów krajowego systemu Cyberbezpieczeństwa do zintegrowanego systemu zarzadzania Cyberbezpieczeństwa (system S46) oraz dalszy rozwój tego systemu" - na podstawie Porozumienia ze Skarbem Państwa o objęcie Przedsięwzięcia wsparciem nr KPOD.05.10-IW.06-0001/24-00 w ramach krajowego planu odbudowy i zwiększenia odporności, z dnia 30 sierpnia 2025 r.

Zadanie koncentrowało się na dalszym rozwoju i upowszechnieniu systemu S46 w ramach krajowego systemu cyberbezpieczeństwa. Jego głównymi celami było: zwiększenie liczby podmiotów podłączonych do Systemu, podniesienie kompetencji personelu w zakresie obsługi S46 poprzez szkolenia i praktyczne wykorzystanie narzędzi, a także zapewnienie wyższej wydajności i zdolności do obsługi rosnącej liczby podłączeń. Istotnym elementem jest również udostępnienie usług umożliwiających samorejestrację podmiotów kluczowych i ważnych oraz dostosowanie mechanizmów komunikacji do nowych wymagań.

Planowany koszt zadania to 41 741 692,14 zł (w tym odpowiednio 39 711 482,14 zł z funduszy UE oraz 2 030 210,00 zł z budżetu państwa).

(akta kontroli str. 75-78, 109, 117-195)

Jak wspomniano wyżej projekt S46 był realizowany głównie przez NASK-PIB, przy kierunkowym udziale Ministerstwa, które określało potrzeby i zatwierdzało zakres działań. Współpraca obu instytucji miała charakter ścisły i powtarzalny. Podmiotom/osobom zewnętrznym zlecono realizację czynności uzupełniających związanych m.in. ze świadczeniem usług L3VPN[17]; instalacją urządzeń końcowych; audytem Systemu Zarządzania Bezpieczeństwem Informacji na potrzeby certyfikacji ISO 27001; przygotowaniem ekspertyz z zakresu bezpieczeństwa; serwisem pogwarancyjnym urządzeń i oprogramowania.

(akta kontroli str. 75-78, 117-195)

[17] L3VPN (wirtualne sieci prywatne warstwy 3.) – rozwiązanie, które służy do tworzenia prywatnych sieci w ramach współdzielonej infrastruktury dostawcy usług internetowych, umożliwiając firmom i instytucjom bezpieczne i wydajne połączenie oddziałów, tak jakby istniała dedykowana, prywatna sieć.

Realizacja każdego z ww. zadań przebiegała zgodnie z przyjętą metodyką zarządzania projektami IT, co zapewniło spójność działań oraz zgodność z ustalonymi standardami. Dla każdego zadania ustalono strukturę organizacyjną projektu, a dla poszczególnych zespołów projektu określono role wytwórcze oraz zakresy odpowiedzialności. Ustalono plan komunikacji, plany spotkań wraz z ich celami, zakresami oraz częstotliwością, ustalono terminy, autorów i odbiorców raportów okresowych. Ustalono metodykę zarzadzania projektem oraz wskazano narzędzia organizacyjne dla prowadzenia i raportowania projektu, realizacji zadań wytwórczych oraz zarzadzania i gromadzenia kolejnych wersji kodu. Dzięki stosowaniu dobrych praktyk struktura i organizacja we wszystkich zadaniach objętych kontrolą były zbliżone, co ułatwiało ich weryfikację.

(akta kontroli str. 117-195)

W ramach kontroli dokonano przeglądu gromadzonych w narzędziu JIRA zbiorów dokumentów projektowych dotyczących realizacji zakończonych zadań związanych z rozwojem lub utrzymaniem S46. We wszystkich przeglądanych zbiorach dokumentów znajdowały się założone zgodnie z przyjętą metodyką dokumenty rejestru doświadczeń, jednak nie były one wypełniane. Kierownik projektu wyjaśnił: ”Rejestr doświadczeń nie był wypełniany, ze względu na to, że transfer wiedzy dotyczącej realizacji projektu zachodził podczas ścisłej współpracy z zespołem po stronie NASK i MC (transfer doświadczeń specyficznych dla projektu) i ścisłej współpracy operacyjnej z innymi kierownikami projektów (transfer wiedzy ogólnej dotyczącej prowadzenia projektów dofinansowanych)”.

NIK zwraca jednak uwagę, że w przyjętej przez NASK metodyce opartej o PRINCE2 rejestr doświadczeń był jednym z dokumentów wspierających ciągłe doskonalenie. Jego celem było: dokumentowanie wniosków i doświadczeń z bieżącego projektu, umożliwienie ich wykorzystania w przyszłych projektach, wspieranie procesu uczenia się organizacji. Brak treści w takim rejestrze może wskazywać na: niedostateczne formalizowanie procesu uczenia się, ryzyko utraty wiedzy po zakończeniu projektu, trudności w przekazywaniu doświadczeń między zespołami. Wyjaśnienia kierownika wskazują na proces nieformalnego transferu wiedzy wynikającej z prowadzonych projektów. Izba uznaje to za wartościową praktykę, która nie może jednak zastąpić formalnego rejestru doświadczeń. Rejestr taki zapewnia trwały zasób wiedzy dla organizacji i daje pewność, że wiedza przekazana została w pełni i że została właściwie zrozumiana.

(akta kontroli str. 68, 89, 117-195)

S46 był realizowany głównie własnymi siłami NASK z niewielkimi wyjątkami. Podmiotom osobom/zewnętrznym zlecono mi. in.: realizację zadań związanych ze świadczeniem usług L3VPN; instalację urządzeń końcowych (NASK SA); rozwój systemu S46 w etapie przejściowym, po przekazaniu na polecenie Ministra Cyfryzacji zespołu rozwojowego do Centralnego Ośrodka Informatyki; audyt SZBI na potrzeby certyfikacji ISO 27001; przygotowywanie ekspertyz z zakresu bezpieczeństwa ekspertom z CSIRT GOV; serwis pogwarancyjny urządzeń i oprogramowania. W ramach kontroli dokonano przeglądu rejestru 127 umów dotyczących dostaw sprzętu lub usług, zawartych w ramach realizacji

S46. Zweryfikowano siedem dobranych celowo w oparciu o analizę ryzyka. We wszystkich sprawdzanych umowach ich przedmiot został prawidłowo dostarczony i protokólarnie odebrany.

(akta kontroli str. 117-195)

W umowach dotacyjnych związanych z rozwojem i utrzymaniem S46 Minister wymagał od NASK uzyskiwania wyrażonej na piśmie lub za pomocą środków komunikacji elektronicznej zgody na ujawnienie osobom trzecim dokumentów lub informacji dostarczonych przez Ministra w związku z realizacją umowy, jak również dokumentów przygotowanych przez NASK w ramach jej realizacji. W toku kontroli ustalono, że NASK nie uzyskiwał takich zgód dla podwykonawców lub kontraktorów zewnętrznych biorących udział w realizacji umów dotacyjnych. Dyrektor NASK wyjaśnił: „W przypadku tych umów z wykonawcami założono, że zlecenie wykonania zadania wyrażone podczas spotkania roboczego Komitetu Sterującego, we wniosku lub umowie dotacyjnej jest równoznaczne ze zgodą na publikacje informacji niezbędnych do realizacji postępowania zakupowego i wykonaniu zamówienia". Zastępca dyrektora NASK ds. Projektów Infrastrukturalnych i Edukacyjnych wyjaśnił również „W związku z przekazanymi wątpliwościami planujemy zwrócić się do Ministra Cyfryzacji z prośbą o potwierdzenie możliwości stosowania domniemania udzielenia zgody na udostępnienie danych w umowach/zamówieniach podpisywanych na potrzeby realizacji umów dofinansowanych dotyczących systemu S46. Aktualnie konsultujemy treść stosownego pisma mającego na celu uzyskanie wyżej wymienionego potwierdzenia."

(akta kontroli str. 117-195)

Dla uczestników S46 został wdrożony system szkoleń. Na dzień 1 lipca 2025 r. przeszkolono 606 uczestników Systemu. Otrzymywali oni certyfikat ukończenia szkolenia. System szkoleń został uzupełniony o aplikację typu Wikipedia zawierającą praktyczne informacje niezbędne dla użytkowników S46. Aplikacja ta była dostępna bezpośrednio w interfejsie Systemu. Przygotowano również filmy i prezentacje szkoleniowe wyjaśniające role zdefiniowane w systemie oraz sposób korzystania z poszczególnych jego funkcjonalności. Dodatkowo dla operatorów usług kluczowych oraz operatorów będących podmiotami leczniczymi opracowano instrukcje wspomagające początkowe wprowadzanie za pomocą ankiet informacji charakteryzujących ich działalność. Materiały szkoleniowe podlegały przeglądom i aktualizacjom wraz z kolejnymi modyfikacjami Systemu.

(akta kontroli str. 91, 117-196)

Po nowelizacji ustawy o KSC system S46 ma zostać ustanowiony jako centralne narzędzie komunikacji i przetwarzania informacji w ramach krajowego systemu cyberbezpieczeństwa. Projektowane zmiany przewidują m.in. obowiązek korzystania z systemu przez CSIRT krajowe i sektorowe, organy właściwe do spraw cyberbezpieczeństwa oraz Prezesa UODO, co zastąpi dotychczasowy fakultatywny model współpracy. System ma również służyć do prowadzenia wykazu podmiotów kluczowych i ważnych, obsługi zgłoszeń incydentów

poważnych, przekazywania informacji o cyberzagrożeniach, podatnościach i technikach ataków, a także do realizacji obowiązków wynikających z RODO[18].

(akta kontroli str. 19-21, 44-45, 117-196)

Stwierdzone nieprawidłowości

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

OCENA CZĄSTKOWA

Dyrektor NASK-PIB zapewnił skuteczną organizację realizacji projektu S46. Realizacja zadań przebiegała zgodnie z przyjętą przez NASK-PIB metodyką zarządzania projektami IT (z wyjątkiem zaniechania związanego z rejestrem doświadczeń), co przełożyło się na spójność działań, właściwy podział odpowiedzialności oraz efektywne planowanie komunikacji i raportowania. Umożliwiło to dotrzymanie ustawowych terminów oraz zapewniło ciągłość działań, jednak nie doprowadziło do realizacji głównego celu projektu, tj. realnego wsparcia uczestników KSC i podniesienia poziomu bezpieczeństwa cyberprzestrzeni.

Zdecydowana większość prac została wykonana przez NASK jako jednostkę podległą Ministrowi, przy wsparciu zewnętrznych wykonawców jedynie w zakresie wyspecjalizowanych usług, takich jak instalacja urządzeń, świadczenie usług sieciowych czy przygotowanie ekspertyz bezpieczeństwa. Jednocześnie stwierdzono uchybienie polegające na braku formalnego uzyskiwania przez NASK zgód Ministra na ujawnienie informacji podwykonawcom. Wymaga to doprecyzowania zasad współpracy między obiema instytucjami.

Pozytywnie należy ocenić zapewnienie szkoleń dla uczestników systemu, które objęły do 1 lipca 2025 r. 606 osób, a także rozwój materiałów dydaktycznych – od filmów i prezentacji po aplikację typu Wikipedia dostępną w interfejsie systemu. Dzięki temu zapewniono nie tylko dostęp do systemu, lecz również skuteczne wsparcie merytoryczne i praktyczne dla jego uczestników.

OBSZAR

3. Funkcjonalność i bezpieczeństwo systemu

Opis stanu faktycznego

Problematyka związana z bezpieczeństwem systemu została ujęta na etapie jego projektowania (tzw. podejście *security by design*[19]). Ze względów na ograniczenia w finansowaniu S46 dedykowany system backupu, system klasy SIEM[20] i system archiwizacji danych zostały wdrożone w ramach realizacji kolejnych zadań dotyczących rozwoju. Dla bezpieczeństwa System S46 został zlokalizowany

[18] Dokumentacja z tego etapu jest dostępna na stronie https://legislacja.rcl.gov.pl/projekt/12384504

[19] *Security by design* to podejście do tworzenia systemów, w którym bezpieczeństwo uwzględnia się już od etapu projektowania, a nie dopiero po wdrożeniu. Oznacza to, że mechanizmy ochrony (np. szyfrowanie, kontrola dostępu, odporność na awarie) są wbudowane w system od początku, a nie dodawane dopiero na późniejszych etapach jego rozwoju.

[20] SIEM to system, który w jednym miejscu zbiera informacje o zdarzeniach z różnych urządzeń IT (np. serwerów, routerów, programów). Analizuje je i alarmuje, gdy wykryje coś podejrzanego, np. próbę włamania.

w odrębnych geograficznie ośrodkach przetwarzania danych DC (Data Center). Skalowalność Systemu została zapewniona poprzez funkcjonalności uruchamiania dodatkowych serwerów sprzętowych i oprogramowania usługowego oraz rozkładania obciążenia przez mechanizm równoważenia obciążenia.

Jako bazę do wytwarzania produktów Projektu S46 służyły rezultaty zadań projektu badawczo rozwojowego Narodowego Centrum Badań i Rozwoju pt.: Narodowa Platforma Cyberbezpieczeństwa objętego umową nr CYBERSECIDENT/369195/I/NCBR/2017. W stopniu maksymalnie możliwym wykorzystano rozwiązania otrzymane w wyniku realizacji projektów NPC i NPCnet. Uprawnienie do wykorzystania oprogramowania wytworzonego w projekcie NPC, finansowanego przez NCBiR, zostało przekazane do Ministerstwa Cyfryzacji, co umożliwiło realizację prac nad oprogramowaniem i zbudowanie Systemu S46. Utworzona została sieć łącząca uczestników oraz ośrodki przetwarzania danych S46 (podstawowe i zapasowe), zbudowana z wykorzystaniem istniejących sieci telekomunikacyjnych, umożliwiająca w modelu docelowym obsłużenie do tysiąca podmiotów.

(akta kontroli str. 42-43, 117-195)

System S46 podlegał wewnętrznej polityce bezpieczeństwa NASK. W ramach przydzielonych odpowiedzialności kierownik projektu S46 wprowadził do niej dodatkowe dokumenty wykonawcze dotyczące procedur specyficznych dla tego systemu. Polityka ta została wprowadzona zarządzeniem Dyrektora NASK. Wraz z załączonymi dokumentami podlegała cyklicznym przeglądom oraz odpowiednim aktualizacjom.

(akta kontroli str. 15, 19, 117-195)

W wyniku działań kontrolnych ustalono, że Polityka bezpieczeństwa dla systemu S46 nie była zakomunikowana podwykonawcom/kontraktorom zewnętrznym. Zapoznanie podwykonawców z taką polityką oraz potwierdzenie przez nich tego faktu jest – zgodnie z uznanymi standardami – istotnym działaniem w zarządzaniu ryzykiem i utrzymaniu wysokiego poziomu bezpieczeństwa.

Dyrektor NASK wyjaśnił, że Norma ISO 27001 pozostawia dowolność w wyborze stron, którym jest udostępniana polityka bezpieczeństwa informacji. Umowy z zewnętrznymi wykonawcami zawierają niezbędne klauzule o poufności. W umowach wskazywane są osoby kontaktowe, które mogą również powiadamiać Zamawiającego o wystąpieniu incydentu bezpieczeństwa. Ze względu na zawarcie w umowach wymienionych wcześniej zapisów nie zidentyfikowano potrzeby udostępnienia polityki bezpieczeństwa informacji wykonawcom.

Zdaniem NIK umieszczanie zapisów dotyczących bezpieczeństwa informacji odrębnie w każdej umowie stanowi jednak ryzyko braku jednolitości i spójności

standardów. Zgodnie z ISO 27001:2022 (Annex A, A.5.1), „polityka

bezpieczeństwa informacji musi być zdefiniowana, zatwierdzona przez kierownictwo, opublikowana i zakomunikowana pracownikom oraz

odpowiednim stronom zewnętrznym”[21] (np. dostawcom i partnerom biznesowym).

(akta kontroli str. 68, 97, 117-195)

W ramach systemu S46 wdrożono szereg rozwiązań mających na celu zapewnienie ciągłości działania oraz minimalizację ryzyka przerw w świadczeniu usług. Do kluczowych mechanizmów należały:

- Rozproszenie geograficzne – usługi aplikacyjne były świadczone z kilku ośrodków przetwarzania danych, objętych ochroną fizyczną, zasilanych niezależnie i posiadających odrębne podłączenia do sieci transmisji danych.
- Redundancja zasilania – krytyczne elementy systemu oraz infrastruktury sieciowej chroniono poprzez zastosowanie zdublowanych źródeł zasilania.
- Tryb aktywno-pasywny ośrodków – dane były równolegle przesyłane do ośrodków pracujących w trybie pasywnym, co umożliwiało nieprzerwane świadczenie usług w przypadku przełączenia ośrodka w tryb aktywny. Przełączenie następowało w sposób półzautomatyzowany, z udziałem obsługi.
- Bezpieczna transmisja danych – komunikacja odbywała się poprzez wydzielone sieci, odseparowane od publicznego Internetu.
- Dwutorowa transmisja – wykorzystano dwóch niezależnych dostawców usług transmisji danych, z mechanizmem automatycznego przełączania ruchu w razie awarii jednego z nich.
- Redundancja systemowa – zastosowano zwielokrotnione maszyny wirtualne obsługujące usługi oraz replikację baz danych.
- Kopie zapasowe – dane były regularnie archiwizowane na odrębnych nośnikach i zabezpieczone przy użyciu dedykowanego oprogramowania do zarządzania kopiami.

(akta kontroli str. 79-85, 117-195)

Stwierdzone nieprawidłowości

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

W trakcie kontroli ustalono, że mechanizmy utrzymania ciągłości działania S46 nie podlegały cyklicznym dedykowanym testom, co mogło skutkować zwiększonym ryzykiem niezdolności do utrzymania ciągłości działania w sytuacjach awaryjnych, a w konsekwencji przerwami w świadczeniu usług systemu.

Zastępca Dyrektora NASK ds. Projektów Infrastrukturalnych i Edukacyjnych wskazał, że nie realizowano dedykowanych testów wymienionych wyżej mechanizmów, ale są one wykorzystywane w trakcie prac rozwojowych oraz

[21] Tekst oryginalny z Normy: „A security policy must be defined, approved by management, published and communicated to employees and relevant external parties”. (ISO 27001:2022 Annex A Control 5.1).

że rozwiązania te były testowane przed i po wdrażaniu ich na środowisko produkcyjne w celu weryfikacji poprawności wdrożenia. Wyjaśnił także, co następuje: „Przyjmuje się, że warto testować mechanizmy zapewnienia ciągłości działania przynajmniej raz do roku. W trakcie prac rozwojowych wydania systemu są wdrażane przynajmniej raz, a często kilka razy do roku. W trakcie wdrożenia wykorzystywane są mechanizmy zachowania ciągłości działania, więc można przyjąć, że mechanizmy były testowane raz do roku. W przypadku mechanizmów wykonywania kopii zapasowych polegano na informacjach o poprawności wykonania kopii zapasowej przekazywanej przez oprogramowanie zarządzające kopiami zapasowymi".

Izba podkreśla, że przeprowadzane testy akceptacyjne, związane z wdrożeniem mechanizmów utrzymania ciągłości działania oraz ich wykorzystywaniem w trakcie prac rozwojowych – zapewniają jedynie częściową możliwość weryfikacji sprawności tych rozwiązań. Stwierdzony stan wskazuje na istnienie szeregu ryzyk: braku dokumentowanych scenariuszy testowych opartych o realne sytuacje, braku mierzalnych celów procesu utrzymania ciągłości działania, braku dowodów, że cały system potrafi w warunkach kryzysu odzyskać niezbędną funkcjonalność w wyznaczonym czasie. Testy okazjonalne i niepełne mogą nie obejmować ekstremalnych scenariuszy (np. niespodziewana nagła utrata całego centrum przetwarzania danych, awaria wielu usług naraz) oraz opierać się na wiedzy konkretnego zespołu np. deweloperskiego, co osłabia odporność organizacyjną.

Backup, który nigdy nie został przetestowany metodą rzeczywistego odtworzenia, nie może być uznany za wiarygodny. Weryfikacja za pomocą specjalistycznych aplikacji pozwala co prawda ocenić integralność danych, jednak nie zabezpiecza przed szeregiem ryzyk: błędami logicznymi w danych (np. błędną konfiguracją backupu, brakującymi plikami, brakami w danych, zależnościami systemowymi, które mogą nie zostać prawidłowo odtworzone) oraz błędami związanymi ze zmiennością środowiska (backup wykonany w starszym środowisku może być nieprzywracalny w nowym, zaktualizowanym środowisku). Weryfikacja integralności nie równa się testowi przywracalności funkcjonalnej. Jeśli nie przeprowadzono pełnego testu odtworzenia (np. przywrócenie systemu, bazy, aplikacji do stanu używalnego), to funkcjonalność backupu należy ocenić jako ograniczoną.

Zastępca Dyrektora NASK ds. Projektów Infrastrukturalnych i Edukacyjnych oświadczył, że planowane jest uzupełnienie procedur, które obejmą regularne testy ww. mechanizmów.

(akta kontroli str. 83, 97, 117-195)

OCENA CZĄSTKOWA

System S46 został zaprojektowany zgodnie z zasadą *security by design* i wyposażony w mechanizmy umożliwiające skalowalność oraz utrzymanie ciągłości działania, m.in. poprzez rozproszenie geograficzne ośrodków przetwarzania danych, redundancję kluczowych elementów infrastruktury, mechanizmy równoważenia obciążenia oraz replikację danych. Wdrożone rozwiązania odpowiadały założeniom bezpieczeństwa i zapewniały możliwość dalszego rozwoju systemu. Ponadto system podlegał wewnętrznej polityce bezpieczeństwa NASK, uzupełnionej o procedury specyficzne dla tego rozwiązania, która była poddawana cyklicznym przeglądom i aktualizacjom.

Skuteczność przyjętych rozwiązań obniżał fakt, że mechanizmy utrzymania ciągłości działania nie były poddawane cyklicznym, dedykowanym testom, co zmniejszało pewność co do ich sprawności i gotowości do użycia w sytuacjach awaryjnych.

OBSZAR

4. Efekty realizacji projektu

Opis stanu faktycznego

W projekcie S46 osiągnięto cele i mierniki określone w dokumentacji planistycznej. Jak opisano jednak powyżej, były to cele i mierniki techniczne, takie jak listy produktów, indeksy liczby podłączeń czy dostępności systemu (tj. odporności na awarie). Odnosząc się natomiast do celów postawionych systemowi w ustawie o KSC, należy stwierdzić, że nie zostały one dotychczas w praktyce zrealizowane (więcej w sekcji *Stwierdzone nieprawidłowości*).

Na dzień 22 maja 2025 r. na 637 podmiotów KSC do systemu S46 podłączonych było 284 (a do końca czerwca 286), w tym 8 CSIRT i OW (organy właściwe). Kolejnych 10 podmiotów było na etapie podłączania; 5 podmiotów na etapie podpisywania umowy z NASK; 36 podmiotów - na etapie podpisywania porozumienia z Ministrem Cyfryzacji. Zdecydowana większość podłączonych uczestników to instytucje z sektora ochrony zdrowia i jednostki samorządu terytorialnego (łącznie 201 podmiotów).

(akta kontroli str. 15, 117-195)

Głównym problemem dotyczącym wykorzystania i efektywności S46 było niskie zainteresowanie systemem u podłączonych uczestników. Przykładowo w II kwartale 2025 r. na 296 podmiotów nie zalogowało się do niego ani razu 100 (34%). W I kwartale 2025 r. na 278 podmiotów nie zalogowało się ani razu 105 (38%). W ujęciu miesięcznym dane te wyglądają znacznie gorzej. Przykładowo, w grudniu 2024 r. na 252 użytkowników systemu 136 nie zalogowało się ani razu (54%). 116 zalogowało się przynajmniej raz, ale tylko 75 zalogowało się przynajmniej trzy razy (29%). W lutym 2025 r. system miał podłączonych 272 podmioty. Spośród nich 157 nie zalogowało się do systemu ani razu (58%). 115 zalogowało się przynamniej raz. Jedynie 62 (23%) zalogowało się do sytemu przynajmniej trzy razy. W ujęciu miesięcznym jedynie około jednej trzeciej podmiotów wykazywało minimalną, regularną aktywność (tj. przynajmniej trzy logowania w ciągu miesiąca).

(akta kontroli str. 117-195)

Przyczyną takiego stanu rzeczy była zdaniem NIK m.in. niewielka praktyczna wartość systemu dla uczestników. System nie zawierał żadnych unikalnych lub trudno dostępnych w innych miejscach informacji. Dane o podatnościach i ostrzeżeniach – w takiej formie, w jakiej były przekazywane w S46 – można było stosunkowo łatwo znaleźć poza systemem. Natomiast unikatowe dla S46 funkcje, takie jak analiza ryzyka oparta na sieci powiązań, nie działały zgodnie z założeniami.

(akta kontroli str. 64, 117-195)

S46 wyróżniał się natomiast wysoką niezawodnością działania dzięki wykorzystywaniu dodatkowych, specjalnych urządzeń brzegowych, do których

podłączany był każdy uczestnik systemu. Aby działanie Systemu S46 było maksymalnie niezawodne, podłączający się podmiot miał za zadanie zapewnić dwa niezależne łącza dostępowe do zakończenia sieci wirtualnych w sieciach telekomunikacyjnych NASK SA i EXATEL SA. Dzięki temu niezawodność systemu przewyższała inne rozwiązania funkcjonujące wyłącznie w oparciu o Internet, bowiem opierała się na sieci odseparowanej od publicznego Internetu. To gwarantowało usługę S46 bez względu na możliwe ataki na ogólnodostępną sieć internetową. Powstała w ten sposób sieć była w okresie kontrolowanym wykorzystywana wyłącznie dla systemu S46.

Jednocześnie to, w jaki sposób System funkcjonował, nie uzasadniało tak wysokiego poziomu izolacji i kosztów infrastrukturalnych. System S46, mimo zaawansowanej architektury sieciowej i zastosowania dedykowanych urządzeń brzegowych, w praktyce nie przewidywał intensywnej komunikacji pomiędzy uczestnikami. Wyjątki stanowiły przypadki przesyłania ankiet oraz zgłoszeń incydentów, a więc zarezerwowane dla ściśle zdefiniowanych sytuacji.

Zasadnicza funkcjonalność systemu sprowadzała się do jednostronnego przekazywania informacji. Dodatkowo większość uczestników korzystała z powiadomień za pośrednictwem poczty elektronicznej, a więc w oparciu o publiczną sieć Internet (na 305 uczestników S46 303 miało włączone powiadamianie e-mail). Tym samym, mimo deklarowanej niezależności od Internetu, kluczowy kanał komunikacji pozostawał podatny na typowe zagrożenia związane z jego wykorzystaniem.

Dodatkowo konieczność zapewnienia dwóch niezależnych łączy dostępowych oraz zakupu specjalistycznych urządzeń brzegowych generowała istotne koszty po stronie podmiotów przyłączających się do systemu. Wysoki próg wejścia skutecznie ograniczał skalowalność rozwiązania i hamował jego szersze wdrożenie, co w konsekwencji podważało zasadność utrzymywania tak rozbudowanej i kosztownej infrastruktury dla realizacji funkcji, które mogłyby być obsłużone w sposób prostszy i bardziej ekonomiczny.

Należy raz jeszcze zaznaczyć, że S46 został uruchomiony na bazie dorobku projektu NPC i w ramach sieci szkieletowej systemu Narodowej Platformy Cyberbezpieczeństwa (NPCnet). NPC miało być jednak przeznaczone dla kilkunastu lub kilkudziesięciu kluczowych podmiotów KSC. W tym kontekście architektura sieci NPCnet była racjonalna – zapewniała wysoki poziom ochrony przy akceptowalnych kosztach i ograniczeniach operacyjnych. Wraz z rozbudową Systemu S46 do kilkuset uczestników, a obecnie – w związku z nowelizacją ustawy o KSC – planowanym przyłączeniem kilkudziesięciu tysięcy nowych podmiotów, pierwotna koncepcja zarówno architektury NPC, jak i sieci NPCnet stała się dla systemu S46 problematyczna. Sieć NPCnet/S46net ma

ograniczenie maksymalnej liczby podmiotów sięgającej dwóch tysięcy, co nie odpowiada obecnym wymaganiom skalowalności.

(akta kontroli str. 46-69, 117-195)

Dotychczasowe rozwiązania przyjęte w Systemie S46 nie zapewniały wystarczającej efektywności operacyjnej, w szczególności w obszarach kluczowych dla realizacji celów określonych w art. 46 ust. 1 ustawy o KSC[22].

1. Generowanie i przekazywanie rekomendacji dotyczących działań podnoszących poziom cyberbezpieczeństwa;

Stwierdzono, że zakładka „Rekomendacje" w systemie S46 nie zawierała żadnych pozycji. Funkcjonalność ta miała służyć podnoszeniu dojrzałości i poziomu bezpieczeństwa uczestników systemu. Na podstawie zebranych w ankiecie informacji o uczestniku oraz zaimplementowanej metodyki system miał automatycznie generować dla niego zestaw wskazówek, które służyłyby podniesieniu jego poziomu bezpieczeństwa. W systemie przygotowano co prawda profile oraz wymagania dotyczące bezpieczeństwa, jednak funkcjonalność ta nigdy nie została ostatecznie użyta, tj. nie wydano żadnej rekomendacji. Z uzyskanych w NASK-PIB wyjaśnień wynika, że przyczyną był zbyt skomplikowany mechanizm ich generowania (skomplikowanie samej funkcji). Właściwą przyczyną mógł być jednak brak zainteresowania tą funkcją ze strony CSIRT. Zdaniem kierownika Zespołu Analiz i Wsparcia Cyberbezpieczeństwa w NASK-PIB funkcja rekomendacji została źle umiejscowiona w systemie, ponieważ CSIRT brakuje ludzi, by zajmować się systemową poprawą dojrzałości uczestników S46, a wykorzystaniem takiej funkcji powinien zająć się organ właściwy w ramach danego sektora (co zapewniłoby porównywalność danych o podmiotach, na podstawie których rekomendacje są generowane).

(akta kontroli str. 46-69, 88-89, 93-94, 117-195)

2. Ostrzeganie o zagrożeniach

W systemie S46 wydano 2948 ostrzeżeń o zagrożeniach i podatnościach (2632 o statusie wysoki, 234 średni, 60 niski i 22 krytyczny). Przy publikacji 2398 ostrzeżeń zaangażowany był CSIRT GOV, 206 - NASK, 147 - MON. Za resztę ostrzeżeń odpowiadali inni uczestnicy systemu, w tym organy właściwe oraz CSIRT-y sektorowe. Ponad połowę ostrzeżeń stanowiły raporty dotyczące złośliwego ruchu sieciowego wydawane przez CSIRT GOV w związku ze stopniem alarmowym BRAVO-CRP, przy czym miały one bardziej charakter informacyjny niż ostrzegawczy, ponieważ były publikowane z jednodniowym opóźnieniem (nie odnosiły się do aktualnej sytuacji).

Ostrzeżenia mogły być przekazywane w ramach *constituency*[23] poszczególnych podmiotów odpowiedzialnych za cyberbezpieczeństwo, a także powielane i przekazywane dalej do innych *constituency*. Poza tym nie były jednak w żaden sposób kierowane czy profilowane. Informacja o podatności dotyczącej

[22] Ponieważ odpowiedzialność za powyższą nieprawidłowość ponosi Minister Cyfryzacji jako właściciel Systemu S46, została ona sformułowana w sekcji „Stwierdzone nieprawidłowości" w wystąpieniu pokontrolnym skierowanym do Ministra.

[23] To powszechnie używany przez zespoły CSIRT termin, pod którym należy rozumieć zbiór podmiotów, które zobowiązane są raportować danemu CSIRT i którym świadczy on wsparcie.

określonego rodzaju sprzętu czy oprogramowania nie była kierowana do jego uczestników w szczególny sposób, ponieważ w systemie nie zbierano informacji o infrastrukturze uczestników. System nie udostępniał na poziomie interfejsu informacji, kto zapoznał się z danym ostrzeżeniem, nie rejestrował również, kto podjął w związku z nimi określone działania. Informacja o nowym ostrzeżeniu nie była też w ocenie NIK wystarczająco zaznaczona w interfejsie systemu. Nawet ostrzeżenie o krytycznej podatności pojawiało się w S46 w formie małej cyferki w prawym górnym rogu, oznaczającej nową aktywność w systemie. Z uzyskanych w NASK-PIB wyjaśnień wynika, że nie przeprowadzano testów użyteczności (UX) pod kątem przekazywania ostrzeżeń, ich widoczności i powiadomień. Powiadomienia o ostrzeżeniach mogły być natomiast przekazywane za pośrednictwem e-mail, jeśli uczestnik zdecydował się na skonfigurowanie takiej usługi.

Taki sposób funkcjonowania ostrzeżeń budzi jednak zasadnicze zastrzeżenia pod kątem jego skuteczności. Brak kierowania ich na podstawie danych o infrastrukturze, charakterystyce lub zagrożeniach danego podmiotu oznacza, że system nie wspierał realnie podejmowania działań adekwatnych do odkrytych podatności. Wysyłanie powiadomień do wszystkich uczestników w ramach danej *constituency* lub grupy *constituency,* niosło ze sobą ryzyko zjawiska *alert fatigue* (zmęczenie nadmiarem komunikatów o zagrożeniach). Brak monitorowania, kto otrzymał ostrzeżenie, kto zareagował, kto nadal pozostaje w stanie zagrożenia – prowadził do braku możliwości oceny skuteczności podjętych działań, doskonalenia KSC, analizy luk i zaplanowania działań naprawczych. Ponieważ system działał w trybie masowym, a nie celowanym, nie dostarczał realnej wartości użytkownikom końcowym. Nie różnił się bowiem od takich rozwiązań jak lista mailingowa, czy dedykowana strona WWW.

W toku kontroli zbadano, jak S46 zareagował w przypadku pojawienia się dwóch grup krytycznych podatności, które mogły stwarzać realne zagrożenie dla uczestników sytemu. Pierwszą z nich były podatności CVE-2025-49704/49706 oraz CVE-2025-53770/53771 dotyczące lokalnej wersji Microsoft SharePoint. Drugą grupą – podatności CVE-2024-42009 oraz CVE2025-49113 dotyczące popularnego przeglądarkowego klienta poczty elektronicznej Roundcube. Zagrożenia stwarzane przez te podatności ocenione zostały w skali CVSS (Common Vulnerability Scoring System) odpowiednio jako wysokie i krytyczne. Działania podjęte w S46 sprowadziły się do przepisania z dostępnego publicznie źródła w jęz. angielskim informacji o ww. podatnościach do zakładki w Systemie pn. "Podatności Publiczne". Choć zagrożenie oceniono jako wysokie lub nawet krytyczne, do uczestników Systemu nie zostało wysłane ostrzeżenie o ich wykryciu (a tak np. w przypadku podatności dotyczących Microsoft SharePoint postąpiła CISA[24], informując potem na bieżąco o wszelkich postępach w tej sprawie).

Ostrzeżenie zostało natomiast wysłane w związku z wykryciem wykorzystania podatności CVE-2024-42009 w kampanii mailowej grupy UNC1151. CSIRT NASK

[24] Cybersecurity and Infrastructure Security Agency - federalna agencja Stanów Zjednoczonych, której głównym zadaniem jest ochrona krytycznej infrastruktury kraju przed zagrożeniami cybernetycznymi i fizycznymi.

opisał ją w Raporcie Tygodniowym 30 maja - 5 czerwca 2025 r. Raport został opublikowany w S46 9 czerwca 2025 r. w zakładce Analizy Techniczne. Natomiast dla porównania zespół CSIRT GOV stosowne ostrzeżenie[25] do podległych podmiotów wysłał już 4 czerwca 2025 .

Na podstawie opisanej wyżej reakcji systemu S46 należy ocenić, że system w obecnej postaci nie realizuje skutecznie funkcji wczesnego ostrzegania o podatnościach i incydentach. Brak mechanizmów targetowania komunikatów, monitorowania reakcji oraz mierzenia skuteczności powoduje, że system pełni jedynie rolę pasywnego źródła informacji. Niespójność działań CSIRT-ów w przypadku wykrycia działań grupy UNC115 (ostrzeżenie wydane tylko przez jeden z trzech zespołów) dodatkowo obniża wiarygodność i spójność całego ekosystemu. W konsekwencji uczestnicy nie otrzymywali adekwatnego wsparcia w reagowaniu na krytyczne zagrożenia, co mogło zmniejszać efektywność KSC.

(akta kontroli str. 101-106, 117-195, 196-199)

3. Zgłaszanie i obsługa incydentów

W systemie S46 zarejestrowanych zostało 740 incydentów, w tym 25 ważnych i 37 istotnych. Zgłoszenie incydentu było wspierane przez dyżurnych CSIRT. System mógł realizować także obserwację postępów wsparcia w obsłudze incydentu oraz wymianę informacji służb CSIRT i administratorem uczestnika w trakcie obsługi incydentu oraz po jej zamknięciu. Jednak podczas szkoleń użytkownicy byli instruowani, że pomocy dyżurnych CSIRT w zgłoszeniu incydentu nie należy mylić z pomocą przy jego obsłudze, która powinna być realizowana samodzielnie przez zgłaszającego. Badanie obsługi pięciu incydentów o wysokim priorytecie wykazało, że w zależności od charakteru incydentu oraz możliwości CSIRT, działania obsługujących zgłoszenie po stronie S46 te nie ograniczały się wyłącznie do rejestracji zgłoszeń, lecz obejmowały również podejmowanie inicjatywy w zakresie pozyskiwania dodatkowych informacji, weryfikacji okoliczności zdarzenia oraz oceny adekwatności zastosowanych środków zaradczych.

Wątpliwości kontrolerów wzbudziła struktura danych o incydentach i ich jakość. Za 80 proc. zgłoszonych incydentów odpowiadały cztery podmioty: NASK-PIB (272), PERN (205), PGE SA (95) oraz ENEA Operator (21). 24 uczestników zgłosiło tylko jeden incydent. Te różnice w liczbie zgłoszonych incydentów wynikały z różnego podejścia uczestników do ich zgłaszania[26]. Ponadto część zgłoszonych incydentów miała wartość *null* w polu „data zgłoszenia" (15 przypadków) oraz „data zakończenia" (210 przypadków), co oznacza kolejno, że część incydentów została utworzona i zapisana, ale nie została wysłana, a w przypadku części użytkownicy nie uzupełnili w formularzu pola z datą zakończenia incydentu, co według wyjaśnień NASK nie było wymagane.

System S46 nie był w kontrolowanym okresie zasadniczym systemem do zgłaszania i rejestracji incydentów. Minister Cyfryzacji przy ocenie terminowości zgłoszeń bazował na danych spoza S46 (tj. na raportach z CSIRT), które zawierały

[25] Aktywnie wykorzystywana podatność „CVE-2024- 42009" w oprogramowaniu Roundcube.

[26] Zgodnie z uzyskanymi wyjaśnieniami NASK-PIB jest jednym z pierwszych przyłączonych podmiotów i aktywnie zgłasza incydenty oraz zagrożenia (które mogą doprowadzić do incydentu).

wszystkie zgłoszone incydenty istotne i poważne. Raport CSIRT NASK także nie opierał się wyłącznie na danych o incydentach zebranych za pośrednictwem S46. Dane pochodziły z systemu S46 oraz formularza CSIRT.

Proporcje przesłanych zgłoszeń, spełniających progi tzw. incydentu poważnego, przedstawiały się następująco: w 2023 r. zgłoszono co CSIRT NASK łącznie 40 takich incydentów – jeden za pomocą S46 i 39 za pomocą formularza CSIRT NASK; w 2024 r. przesłano 57 incydentów poważnych – dwa za pomocą S46 i 55 za pomocą formularza; w 2025 r. (I półrocze) 22 incydenty – dwa za pomocą S46 i 20 za pomocą formularza.

S46 został zintegrowany z RTIR (tj. narzędziem do zarządzania zgłoszeniami incydentów bezpieczeństwa, pozwalającymi je rejestrować, przypisywać do odpowiednich osób, śledzić postęp prac i dokumentować działania) wykorzystywanym przez CSIRT NASK oraz CSIRT GOV. Dzięki temu możliwe było przekazywanie zgłoszeń incydentów bezpośrednio do właściwych zespołów reagowania.

Zgłoszone w systemie S46 incydenty stanowiły dynamiczny element wpływający na poziom ryzyka przypisanego poszczególnym uczestnikom systemu. Oznacza to, że każde zgłoszenie incydentu mogło prowadzić do zmiany oceny ryzyka – zarówno dla podmiotu, którego incydent dotyczył bezpośrednio, jak i dla innych powiązanych uczestników. W zamierzeniu incydenty te powinny być uwzględniane w bieżącej analizie ryzyka, co miało pozwolić na szybsze reagowanie na zmieniające się zagrożenia. Jednak zaimplementowana w S46 metodyka szacowania takiego szybkozmiennego ryzyka okazała się trudna do wdrożenia i nie dała oczekiwanych rezultatów, a rola funkcji zgłaszania incydentów w Systemie pozostała ograniczona. Choć odnotowano przypadki, w których osoby przyjmujące zgłoszenia wykazywały aktywne podejście, angażując się w proces obsługi incydentu – co wskazuje na potencjał systemu do pełnienia bardziej operacyjnej roli – to ograniczona jakość danych, dysproporcje w zgłoszeniach między podmiotami, niski poziom wykorzystania systemu przez większość uczestników oraz niedziałający model szacowania ryzyka szybkozmiennego stanowiły istotne bariery dla efektywnego wykorzystania systemu S46 jako narzędzia wspierającego zarządzanie incydentami w sposób systemowy i operacyjnie użyteczny.

(akta kontroli str. 16, 34-35, 72-74, 99-101, 110, 117-195)

4. <u>Współpraca podmiotów wchodzących w skład krajowego systemu cyberbezpieczeństwa;</u>

System, który powinien wspierać współpracę pomiotów KSC, nie miał jasno określonych procedur i instrukcji dotyczących komunikacji między uczestnikami. W systemie były techniczne możliwości uruchomienia, a nawet wykorzystania takiej komunikacji, jednak nie były one intuicyjne. Komunikacja zarezerwowana była dla określonych czynności (np. uzgodnienia ankiety czy obsługi zgłoszenia incydentu), natomiast poza takimi zdefiniowanymi sytuacjami użytkownicy sytemu nie mieli do dyspozycji odpowiedniej procedury porozumiewania się. Zdarzało się, że wykorzystywali w tym celu funkcje do tego nieprzeznaczone – jeden z podmiotów służby zdrowia próbował np. zwrócić uwagę na nieprawidłowe jego zdaniem działanie Systemu poprzez zgłoszenie ryzyka

dynamicznego o następującej treści: „nie działa system P1 od CeZ. Brak jakichkolwiek informacji na ten temat w systemie S46?? Dlaczego systemy Cez świecą na zielono w S46 mimo, że nie działają ? Czy system S46 jest martwy?" (pisownia oryginalna).

W praktyce komunikacja pomiędzy uczestnikami systemu odbywała się jednak za pomocą zewnętrznych komunikatorów. W 2025 r. rozpoczęto zbieranie wymagań dotyczących wykorzystania komunikatora w S46. 73 proc. uczestników systemu opowiedziało się za ustanowieniem bezpośredniej, bieżącej komunikacji między podmiotami Krajowego Systemu Cyberbezpieczeństwa w ramach systemu S46 – np. poprzez chat, komunikator szyfrowany, kanał dyskusyjny lub forum.

Problem ze współpracą i komunikacją w S46 wykazany został podczas przeprowadzonego przez kontrolerów eksperymentu. Polegał on na próbie przesłania do wszystkich podmiotów systemu komunikatu zawierającego dwa polecenia. Pierwsze polecenie dotyczyło niezwłocznego potwierdzenia za pomocą mechanizmów łączności wbudowanych w S46 otrzymania powyższego komunikatu; drugie - wymagało udzielenia tą samą drogą odpowiedzi na pytanie z zakresu praktycznej wiedzy o aktualnych zagrożeniach bezpieczeństwa dotyczących powszechnie stosowanych systemów operacyjnych. Wynikiem eksperymentu miał być stosunek liczb udzielonych odpowiedzi do wysłanych komunikatów. Operator S46 w CSIRT NASK zdecydował o wysłaniu komunikatu w formie ostrzeżenia o średnim priorytecie. Wynik eksperymentu był następujący: pojawiły się trzy odpowiedzi na wysłane ostrzeżenie. Dwa z nich zostały przesłane poprzez e-mail na adres cert@cert.pl., a jeden poprzez zgłoszenie incydentu. Za pomocą analizy logów, przeprowadzonej miesiąc po eksperymencie, wykazano, że ostrzeżenie w samym systemie odczytało tylko 14 jego uczestników (na blisko 300 zarejestrowanych)[27]. CSIRT GOV i MON nie przekazały dalej otrzymanego ostrzeżenia (ostrzeżenie zostało wysłane przez operatora z CSIRT NASK w trybie tylko do odczytu, więc nie mogło być przekazane dalej, jednak gdyby CSIRT MON lub GOV uznały, że mimo wszystko chcą przekazać ostrzeżenie do swojego *constituency*, mogły utworzyć nowy obiekt ostrzeżenia, albo poprosić innym kanałem o nadanie uprawnień edytora).

(akta kontroli str. 28, 46-69, 110-111, 117-195)

5. Szacowanie ryzyka na poziomie krajowym

Na potrzeby wsparcia zarządzania cyberbezpieczeństwem na poziomie krajowym w systemie S46 zaimplementowano metodykę szacowania ryzyka wolno- i szybkozmiennego[28]. Jednak w ocenie NIK wdrożenie tej metodyki

[27] Możliwe, że część uczestników otrzymała powiadomienie o ostrzeżeniu za pomocą e-mail.

[28] Szacowanie ryzyka wolnozmiennego oparte było na informacjach wolnozmiennych, tj. takich, które charakteryzują się niską częstotliwością zmian w czasie i mają względnie stabilny charakter. Do tej grupy zalicza się m.in. poziom krytyczności danej usługi, statyczne ryzyko własne przypisane do usługi czy zbiorcze statystyki podatności. Informacje te stanowiły podstawę do oceny ryzyka w perspektywie długoterminowej, niezależnie od bieżących incydentów czy zmian operacyjnych.
Szacowanie ryzyka szybkozmiennego opierało się na informacjach dynamicznych, tj. takich, które zmieniają się często i odzwierciedlają bieżącą sytuację operacyjną. W szczególności uwzględniono dane o incydentach bezpieczeństwa przesyłane przez uczestników procesu oraz dynamiczne ryzyko własne przypisane do zgłoszonej usługi. Informacje te miały pozwolić na bieżące

okazało się nieefektywne – jej złożoność i brak dostosowania do realiów operacyjnych podmiotów KSC sprawiły, że była trudna do praktycznego zastosowania i nie przyniosła oczekiwanych rezultatów w zakresie oceny i zarządzania ryzykiem. Diagnozę tę potwierdziło Ministerstwo Cyfryzacji w projekcie Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2025–2029.

Dane do ryzyka wolnozmiennego pochodziły przede wszystkim z ankiet wypełnianych przez uczestników systemu. Weryfikacja tych danych w Systemie nie obejmowała stanu faktycznego – przyjmowano, że uczestnik podaje prawidłowe, prawdziwe i aktualne informacje. Jak wspomniano wyżej, w ramach ankiet nie zbierano informacji o systemach uczestników, co uniemożliwiało praktyczne wykorzystanie S46 do ich ochrony czy zwiększenia poziomu bezpieczeństwa. Podstawowym mankamentem ankietowania był jednak fakt, że ankiety te nie były w praktyce aktualizowane. W systemie pozostawały więc często dane już historyczne, na podstawie których wykonywano kolejne szacowania ryzyka. W projekcie NPC, z którego przejęto ten mechanizm, zakładano cykliczną aktualizację ankiet w określonych odstępach czasu, co stanowiło warunek konieczny dla uzyskania wiarygodnych i użytecznych wyników szacowania ryzyka. W systemie S46 odstąpiono w praktyce od tego założenia, co podważyło zasadność wykorzystania pozyskanych danych do oceny ryzyka i ograniczyło użyteczność całego mechanizmu. Podejmowano co prawda działania mające ułatwić proces ankietowania (takie jak przygotowanie standardu, opracowanie FAQ czy szkolenia uczestników systemu) – jednak służyły one przede wszystkim usprawnieniu wypełnienia pierwszej ankiety oraz zredukowaniu liczby ankiet niewypełnionych.

Z kolei szacowanie ryzyka szybkozmiennego oparte było w założeniach m.in. na zgłaszanych przez uczestników ryzykach dynamicznych[29]. Do dnia 13 czerwca 2025 r. w systemie nie zgłoszono ani jednego takiego ryzyka. W trakcie trwania kontroli zgłoszono jedno ryzyko dynamiczne, które – jak wspomniano wyżej – można potraktować jako próbę komunikacji uczestnika z administratorami systemu. Według wyjaśnień kierownika Zespołu Analiz i Wsparcia Cyberbezpieczeństwa w NASK-PIB uczestnicy systemu S46 niechętnie dzielili się informacjami o swoich podatnościach i słabościach, ograniczając zgłoszenia głównie do incydentów wymaganych przepisami prawa. Powodem mogła być obawa przed ujawnieniem podwyższonego poziomu ryzyka klientom (system jest tak skonstruowany, że powiązane usługi są dla siebie nawzajem widoczne) jak i wysoka złożoność metodyki analizy ryzyka, która mogła być niezrozumiała dla podmiotów dysponujących ograniczonymi zasobami z zakresu cyberbezpieczeństwa.

System S46 pełnił istotną funkcję w zakresie szacowania ryzyka na poziomie krajowym, jednak opierał się na danych o uczestnikach, które nie były aktualizowane, weryfikowane merytorycznie ani potwierdzone audytem.

---

identyfikowanie obszarów podwyższonego ryzyka i podejmowanie działań adekwatnych do aktualnego poziomu zagrożeń.

[29] Element ryzyka szybkozmiennego, który odnosi się do informacji operacyjnych uczestnika Systemu, np. zgłoszenia incydentów, zmiany konfiguracji, aktualizacji systemów, nowych podatności.

W konsekwencji przez kilka lat takie analizy ryzyka były prowadzone na podstawie informacji o nieznanej jakości i wiarygodności, co wpływało na rzetelność i użyteczność wniosków wyciąganych na poziomie krajowym.

(akta kontroli str. 28-30, 46-59, 62-65, 96, 117-195, 197)

Ustalenia NIK znajdują potwierdzenie w wynikach analiz przeprowadzonych przez Ministerstwo Cyfryzacji oraz NASK, a także w podjętych działaniach, w zakresie wdrożonych zmian, a przede wszystkim w planach jego dalszej modyfikacji. I tak w opracowanej w 2023 r. przez NASK *Analizie metod podłączania użytkowników systemu S46* jako podstawowy i powszechny model dostępu zarekomendowany został model SaaS (System as a Service) z WK (Węzłem Krajowym), tj. udostępnienie usług systemu S46 bezpośrednio w sieci Internet z uwierzytelnieniem poprzez Węzeł Krajowy. Model taki został opracowany i zgodnie z rekomendacją ma być podstawowym modelem przyłączania uczestników do S46 (przy czym kluczowi użytkownicy – np. zespoły CSIRT - mają w dalszym ciągu korzystać z dedykowanej odizolowanej sieci stworzonej na potrzeby tego Systemu). Zastosowanie modelu SaaS z WK jest odpowiedzią na dotychczasowe istotne ograniczenia związane z pracochłonnością połączeń za pomocą izolowanej sieci i ich wysokimi kosztami. Wyeliminuje także ograniczenia w zakresie liczby użytkowników możliwych do podłączenia, co jest szczególnie istotne wobec przewidywanego znacznego zwiększenia ich liczby.

(akta kontroli str. 42-45, 117-195)

Po dokonaniu przez kontrolerów NIK oględzin w systemie S46 wyłączone zostały zakładki lub podzakładki, które nie spełniały swojej funkcji lub po prostu nie były używane. Dotyczyło to zakładek: „Rekomendacje", „Zdarzenia", „Biuletyny" i „Wyszukiwanie".

(akta kontroli str. 111-113)

W trakcie kontroli, tj. 7 lipca 2025 r. Pełnomocnik ds. Cyberbezpieczeństwa skorzystał po raz pierwszy z możliwości wysłania ostrzeżenia zawierającego rekomendację podjęcia działań zabezpieczających do wszystkich uczestników systemu. 21 lipca wprowadzona została do Systemu poprawka umożliwiająca mu załączenie pliku w przesyłanym ostrzeżeniu. Tym samym w systemie wykorzystano mechanizm jednoczesnego powiadamiania wszystkich uczestników, niezależnie od ich przynależności do poszczególnych CSIRT-ów. Jest to istotne z punktu widzenia efektywności reagowania – niektóre ostrzeżenia, ze względu na swój charakter, powinny być dystrybuowane natychmiastowo i globalnie, z pominięciem modelu *constituency*. Obserwowane wdrożenie w powiązaniu ze zmianą dotychczasowej praktyki potwierdza zasadność takiego mechanizmu w kontekście podniesienia poziomu bezpieczeństwa operacyjnego systemu.

(akta kontroli str. 34, 111-113)

S46 ma w zamierzeniu Ministerstwa Cyfryzacji pełnić funkcję rejestru ważnych i istotnych incydentów. Głównym warunkiem jest wprowadzenie ustawowego obowiązku dołączenia do systemu S46 podmiotów KSC oraz operacyjne korzystanie przez nich z systemu S46, w szczególności do zgłaszania incydentów.

Stosowne zmiany nakładające ww. obowiązek zostały zaplanowane w projekcie nowelizacji ustawy o KSC.

(akta kontroli str. 32-35)

W trakcie kontroli trwały prace nad opracowaniem i zaimplementowaniem w systemie S46 innego podejścia dotyczącego szacowania ryzyka, w powiązaniu z osiąganiem oczekiwanego poziomu cyberbezpieczeństwa, zarówno na poziomie podmiotów KSC, jak i ryzyka uogólnionego na poziomie krajowym. Wykorzystywane będą w tym celu informacje przekazywane przez podmioty kluczowe i podmioty ważne, oraz informacje o zagrożeniach, podatnościach i incydentach pozyskiwane z innych źródeł, w szczególności z CSIRT. Nowe rozwiązanie w zakresie szacowania ryzyka będzie mogło być efektywniej wykorzystane, jak również będzie łatwiejsze w implementacji w podmiotach o różnej wielkości.

(akta kontroli str. 32-35)

W przypadku S46 planowane jest także tworzenie spersonalizowanych raportów, zgłoszeń i ostrzeżeń, w tym o podatnościach dotyczących konkretnych uczestników. Po nowelizacji ustawny o KSC zmienić ma się również model rejestracji uczestników. System ma wykorzystywać rejestr podmiotów kluczowych i ważnych (tzw. rejestr KSC). Trwają prace nad testami FUT (Friendly User Test). Umożliwiają one wykrycie błędów, przy jednoczesnym zaangażowaniu uczestników. Takie podejście zwiększa szanse na dopracowanie rozwiązania przed jego pełnym udostępnieniem.

W trakcie kontroli trwały również działania mające na celu zwiększenie wartości operacyjnej danych dostępnych w S46 poprzez ich uzupełnienie o informacje ekskluzywne, niedostępne poza Systemem, co ma podnieść jego użyteczność dla uczestników. Równolegle prowadzone były prace nad integracją z projektami zewnętrznymi, w tym z systemem Artemis, służącym do automatycznego skanowania stron internetowych w celu wykrywania podatności i błędnych konfiguracji. W ramach tej integracji planowane jest umożliwienie podmiotom zgłaszania adresów IP i domen do systemu S46, które będą automatycznie weryfikowane. Wyniki skanowania będą udostępniane zarówno w przestrzeni danego podmiotu w systemie S46, jak i przesyłane na wskazany adres e-mail. Działania te mają na celu zwiększenie funkcjonalności systemu oraz jego interoperacyjności z innymi rozwiązaniami.

MC zleciło również NASK zaplanowanie zmian w funkcjach komunikacyjnych systemu S46 w celu zwiększenia jego użyteczności i elastyczności.

Zakres zmian zaplanowanych w S46, obejmujących m.in. usprawnienia w obszarze komunikacji, ostrzeżeń, rekomendacji oraz szacowania ryzyka, potwierdza zasadność ustaleń kontroli wskazujących na istotne braki funkcjonalne w tych obszarach.

(akta kontroli str. 30, 40-44, 60-69, 73-74)

Stwierdzone nieprawidłowości

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

OCENA CZĄSTKOWA

W projekcie S46 realizowanym przez NASK-PIB osiągnięto cele i mierniki określone w dokumentacji planistycznej. Zapewniono wysoką niezawodność działania Systemu poprzez wykorzystanie dedykowanej infrastruktury sieciowej oraz wdrożenie mechanizmów, które pozwoliły utrzymać ciągłość usług nawet w przypadku zagrożeń dla publicznego Internetu. Do 2025 r. (I półrocze) przyłączono do S46 zamierzoną liczbę uczestników, tj. blisko połowę docelowych uczestników KSC[30].

Stwierdzono jednak, że wskutek błędów popełnionych na etapie przygotowania i inicjowania projektu system S46, mimo znacznych nakładów, charakteryzował się bardzo niską użytecznością i wręcz incydentalnym poziomem wykorzystania przez uczestników. Mechanizmy generowania rekomendacji, ostrzegania o zagrożeniach i szacowania ryzyka nie działały zgodnie z oczekiwaniami, przez co system pełnił w praktyce rolę pasywnego źródła informacji, niewnoszącego realnej wartości dla jego uczestników. Niska liczba logowań potwierdza, że S46 nie spełniał funkcji narzędzia wspierającego bezpieczeństwo, a jego rola w praktyce była formalna (literalne wypełnienie wymagań ustawowych) i nieistotna (brak wpływu na podniesie poziomu cyberbezpieczeństwa).

Pozytywnie należy ocenić fakt, że NASK-PIB i Minister Cyfryzacji dostrzegli niedoskonałości systemu i podejmowali działania naprawcze w kierunku zwiększenia jego użyteczności. W ocenie NIK instytucje te będą jednak musiały zmierzyć się z kryzysem zaufania ze strony dotychczasowych uczestników, wynikającym z wcześniejszych niedoskonałości systemu w obszarach komunikacji, ostrzeżeń, rekomendacji oraz szacowania ryzyka. Szybkie i skuteczne wdrożenie zapowiadanych zmian będzie kluczowe dla odbudowy wiarygodności systemu.

OBSZAR

5. Nadzór nad realizacją projektu

Opis stanu faktycznego

W ramach dokumentów inicjujących projekty w poszczególnych zadaniach zarządzano głównymi ryzykami projektowymi identyfikując je, szacując ich poziom oraz określano sposoby ich mitygacji. Zgodnie ze stosowaną metodyką prowadzenia projektów dla każdego z nich zainicjowano i aktualizowano rejestr ryzyk w którym dokumentowano proces zarzadzania nimi.

Powołano Komitet Sterujący, w ramach którego podejmowano kluczowe decyzje dotyczące finansowania, akceptacji produktów czy otwierania i zamykania etapów projektu. W pracach komitetu brali udział reprezentanci głównego użytkownika (MC lub KPRM) i głównego wykonawcy (NASK). W przypadku potrzeby omówienia zagadnień szczegółowych uzupełniano skład komitetu o wybranych specjalistów. Z cyklicznych spotkań Komitetu Sterującego sporządzane były notatki dokumentujące omawiane zagadnienia oraz podejmowane decyzje. W notatkach tych oraz rejestrach ryzyk oceniano między innymi adekwatność zasobów wymaganych i przypisanych do realizacji

[30] Na dzień 22 maja 2025 r. do S46 przyłączono 284, a do końca czerwca 286 spośród 637 podmiotów wchodzących w skład KSC. W związku z przygotowywaną nowelizacją ustawy o KSC liczba przeznaczonych do przyłączenia do S46 podmiotów może znacząco wzrosnąć (szacuje się, że nawet do ponad 60 tys. podmiotów).

poszczególnych produktów, realizacje harmonogramów ich wytwarzania oraz wskazywano niezbędne działania korygujące.

(akta kontroli str. 117-195)

W wyniku ustaleń kontroli nr P/21/042 „Działania państwa w zakresie zapobiegania i zwalczania skutków wybranych przestępstw internetowych, w tym kradzieży tożsamości”[31] Minister Cyfryzacji wraz nadzorowanym NASK-PIB podjęli z własnej inicjatywy szereg działań naprawczych. Przeprowadzono działania informacyjne, które wraz z pozyskiwaniem dodatkowych źródeł finansowania podłączeń, także spoza części 27 budżetu państwa, znacząco przyczyniły się do zwiększenia liczby uczestników Systemu.

(akta kontroli str. 7-9)

Opracowano i wdrożono narzędzia raportowania o usterkach i propozycjach zmian. Na potrzeby obsługi zgłoszeń podmiotów S46 skonfigurowano dwa specjalne portale. W styczniu 2022 roku została udostępniona użytkownikom S46 dedykowana dla helpdesk skrzynka poczty elektronicznej. Uruchomiono również System Genesis, który rejestrował informacje o kontaktach komórki wsparcia z użytkownikami. W roku 2023 uruchomiono system JiraSD obsługujący zgłoszenia uczestników S46. W roku 2021 Operator Systemu S46 obsłużył 74 zgłoszenia. W roku 2022 nie sporządzano raportu dotyczącego zgłoszeń. W roku 2023 zarejestrowano 232 zgłoszenia w tym najczęstsze: *niedostępny host* 62, *brak dostępu* 25, *hasło* 25. W roku 2024 zarejestrowano 820 zgłoszeń w tym najczęstsze: *informacja* 224, *awaria* > *sieć* 219, *wsparcie* > *odblokowanie dostępu* 87. W roku 2025, ze względu na planowany wzrost liczby podłączeń spodziewany jest dalszy wzrost liczby zgłoszeń związanych z obsługą.

Zespół realizacyjny działał zgodnie z harmonogramem, reagował na bieżące problemy oraz utrzymywał efektywną współpracę. Transfer wiedzy odbywał się w sposób ciągły, a działania operacyjne były zgodne z przyjętym planem. Pomimo tych pozytywnych aspektów, opisane we wcześniejszych punktach wystąpienia pokontrolnego ograniczenia, wynikające z błędnych założeń przyjętych w fazie inicjacji projektu, uniemożliwiły pełne osiągnięcie zakładanych celów.

(akta kontroli str. 76-77, 117-195)

Stwierdzone nieprawidłowości

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

OCENA CZĄSTKOWA

Nadzór operacyjny nad projektem S46 działał prawidłowo. NASK wraz z Ministerstwem Cyfryzacji realizowały zadania zgodnie z harmonogramem, skutecznie reagowały na pojawiające się problemy oraz utrzymywały efektywną współpracę. Proces transferu wiedzy przebiegał w sposób ciągły (pomimo że brak wypełnionego rejestru doświadczeń groził utratą zdobytej wiedzy

[31] Wyniki kontroli dostępne na stronie NIK: https://www.nik.gov.pl/kontrole/P/21/042/KPB/

w przyszłych projektach), a działania operacyjne były prowadzone zgodnie z zatwierdzonym planem.

Na etapie inicjacji projektu sformułowano jednak błędne założenia, które – pomimo właściwej realizacji operacyjnej – istotnie ograniczyły możliwość osiągnięcia zakładanych celów całego przedsięwzięcia. Brak odpowiedniego dostosowania rozwiązań o charakterze badawczo-naukowym do warunków i potrzeb biznesowych spowodował, że dotychczasowe działania nadzorcze nie mogły zapewnić skutecznego wykorzystywania S46, a System ten nie przyczynił się do poprawy poziomu cyberbezpieczeństwa w ramach KSC.

Na ocenę działań nadzorczych NASK wpływa jednak fakt, że w ramach kierownictwa projektu prawidłowo zdefiniowano potrzebne działania naprawcze, które wraz z MC częściowo podjęto jeszcze przed zakończeniem kontroli.

IV. 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. Zapewnienia konsekwentnego stosowania przez NASK-PIB mechanizmów identyfikacji i uwzględniania wymagań użytkowników końcowych na etapie projektowania i realizacji systemów teleinformatycznych – również w warunkach silnej presji czasowej – w celu zagwarantowania pełnej funkcjonalności oraz efektywnego wykorzystania wdrażanych rozwiązań.
2. Spowodowanie wdrożenia w NASK-PIB cyklicznych, udokumentowanych testów mechanizmów utrzymania ciągłości działania systemu S46 – w tym pełnych testów odtworzeniowych kopii zapasowych – z wykorzystaniem scenariuszy obejmujących różne warianty sytuacji awaryjnych, w celu zapewnienia wiarygodnej weryfikacji zdolności systemu do odzyskania funkcjonalności w wymaganym czasie.

V. Pozostałe informacje i pouczenia

Wystąpienie pokontrolne sporządzono w postaci elektronicznej z użyciem kwalifikowanych podpisów elektronicznych.

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 dyrektora jednostki organizacyjnej 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, 18 września 2025 r.

Kontroler

Daniel Michalecki

główny specjalista kontroli państwowej

/podpisano elektronicznie/

Najwyższa Izba Kontroli

Departament Porządku i Bezpieczeństwa Wewnętrznego

Dyrektor

Tomasz Sordyl

/podpisano elektronicznie/