Ministerstwo
Cyfryzacji

Sekretarz Stanu
Paweł Olszewski

BM.WP.057.194.2025
Warszawa, 11 stycznia 2026 r.

Szanowny Pan
Włodzimierz Czarzasty
Marszałek Sejmu RP

Dot. pisma z 23 października br. Posła na Sejm RP Pana Krzysztofa Piątkowskiego w sprawie cyberbezpieczeństwa Polski (interpelacja nr 12933)

Szanowny Panie Marszałku,

poniżej przedstawiam odpowiedzi na zadane przez Posła pytania.

Ad 1) Jakie konkretne działania zostały dotychczas podjęte przez Ministerstwo Cyfryzacji w celu poprawy cyberbezpieczeństwa obywateli oraz infrastruktury krytycznej?

Działania Ministerstwa Cyfryzacji i innych instytucji Krajowego Systemu Cyberbezpieczeństwa (KSC) zapewniających cyberbezpieczeństwo Polski przedstawione są Sprawozdanie Pełnomocnika Rządu do Spraw Cyberbezpieczeństwa za 2024 rok[1]. W 2025 r. większość tych działań jest kontynuowana. W szczególności należy zwrócić uwagę na działania związane z cyberbezpieczeństwem tegorocznych wyborów prezydenckich[2] oraz następujące inicjatywy:

- regulacyjno-systemowe:
  - np. procedowany projekt nowelizacji ustawy o krajowym systemie cyberbezpieczeństwa, który wdroży w Polsce dyrektywę NIS 2;
  - przygotowywana nowa Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2025-2029;
- szkoleniowo-kompetencyjne i kadrowe, np.:
  - liczne inicjatywy szkoleniowe, dla ogółu społeczeństwa, dla różnych grup społecznych, dla specjalistów;
  - Fundusz Cyberbezpieczeństwa zapewniający w sektorze publicznym konkurencyjne wynagrodzenia dla specjalistów ds. cyberbezpieczeństwa w stosunku do sektora prywatnego;
- programy wsparcia dla poszczególnych sektorów, np.:
  - Cyberbezpieczny Samorząd, Cyberbezpieczny Rząd, Cyberbezpieczne Wodociągi;
- organizacyjno-koordynacyjne, np.:
  - działania Kolegium do Spraw Cyberbezpieczeństwa na poziomie strategicznym oraz
  - Połączonego Centrum Operacyjnego Cyberbezpieczeństwa (PCOC) na poziomie operacyjnym;
  - rekomendacje i komunikaty dla podmiotów KSC wydawane przez Pełnomocnika Rządu do Spraw Cyberbezpieczeństwa;

[1] https://www.gov.pl/web/cyfryzacja/krajobraz-cyberprzestrzeni-roczne-sprawozdanie-o-cyberbezpieczenstwie
[2] https://www.gov.pl/web/cyfryzacja/raport-z-programu-parasol-wyborczy---kompleksowa-ochrona-wyborow-prezydenckich-2025

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

ul. Królewska 27
00-060 Warszawa

- techniczne, np.:
    - system rozpoznawania zagrożeń w cyberprzestrzeni (CTI) zapewniany przez Ministerstwo Cyfryzacji na potrzeby własne i 9 innych instytucji zapewniających cyberbezpieczeństwo na poziomie krajowym;
    - środki bezpiecznej łączności Komunikator i SKR-Z zapewniane przez MC;
    - system AntyDDoS, którym MC zapewnia osłonę przed atakami DDoS dla kilkudziesięciu instytucji, w tym dla Sił Zbrojnych RP;
    - system zarządzania cyberbezpieczeństwem S46 zapewniany przez MC.

Ad 2) Jakie działania legislacyjne planuje podjąć Ministerstwo oraz Rada Ministrów w celu wzmocnienia szeroko rozumianego cyberbezpieczeństwa w Polsce?

W Sejmie obecnie procedowany jest projekt ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa oraz niektórych innych ustaw. Celem projektowanej ustawy jest wdrożenie dyrektywy Parlamentu Europejskiego i Rady (UE) 2022/2555 z dnia 14 grudnia 2022 r. w sprawie środków na rzecz wysokiego wspólnego poziomu cyberbezpieczeństwa na terytorium Unii, zmieniająca rozporządzenie (UE) nr 910/2014 i dyrektywę (UE) 2018/1972 oraz uchylająca dyrektywę (UE) 2016/1148 (dyrektywa NIS 2) (Dz. Urz. UE L 333 z 27.12.2022 str. 80), zwanej dalej „dyrektywą NIS2". Projektowane przepisy będą miały istotny wpływ na zwiększenie cyberbezpieczeństwa. Jednym z takich rozwiązań jest nałożenie obowiązków z zakresu środków zarządzania ryzykiem na podmioty kluczowe i podmioty ważne w cyberbezpieczeństwie, dotyczące w szczególności stosowania odpowiednich i proporcjonalnych środków technicznych, operacyjnych i organizacyjnych w celu zarządzania ryzykiem dla bezpieczeństwa sieci i systemów informatycznych. Ponadto podmioty te będą musiały dokonywać analizy łańcucha dostaw, co pozytywnie wpłynie na świadczone przez nie usługi. Projekt ustawy wprowadza również możliwości zgłaszania incydentów przez podmioty kluczowe i podmioty ważne, za pomocą systemu teleinformatycznego (system S46), do właściwych zespołów CSIRT sektorowych i CSIRT poziomu krajowego. Zapewni to sprawną i szybką obsługę incydentów, a uzyskane w ten sposób informacje pomogą w zwiększeniu cyberbezpieczeństwa.

Ministerstwo Cyfryzacji planuje podjąć działania legislacyjne związane z dopuszczalnością bezpiecznego przetwarzania danych administracji w chmurze obliczeniowej. Ta materia obecnie regulowana jest jedynie przez uchwałę Rady Ministrów, co jest niewystarczające z punktu widzenia cyberbezpieczeństwa. Trwają prace nad projektem ustawy o chmurze obliczeniowej w administracji, który kompleksowo będzie regulował możliwość przetwarzania danych podmiotów administracji w chmurze obliczeniowej - zarówno tej, którą dostarczają podmioty komercyjne, jak i rządowej chmurze obliczeniowej. Dzięki tej regulacji ustalimy jednolity standard cyberbezpieczeństwa, jednolite wymagania dla dostawców i zmniejszymy obciążenie podmiotów administracji, na których obecnie spoczywa obowiązek weryfikacji, czy dostawcy spełniają wymagania określone w standardach cyberbezpieczeństwa chmur obliczeniowych.

Planowane działania Ministerstwa Cyfryzacji w zakresie wzmocnienia cyberbezpieczeństwa Polski – nie tylko legislacyjne - ujęte są również w procedowanym obecnie projekcie Strategii Cyberbezpieczeństwa Rzeczypospolitej na lata 2025-2029. Dokument dostępny jest w Biuletynie Informacji Publicznej Ministerstwa Cyfryzacji[3].

Ad 3) Jakie środki finansowe zostały dotychczas przeznaczone przez obecny Rząd oraz Ministerstwo na poprawę poziomu cyberbezpieczeństwa w naszym kraju?

[3] https://mc.bip.gov.pl/projekty-aktow-prawnych-mc/projekt-uchwaly-rady-ministrow-w-sprawie-strategii-cyberbezpieczenstwa-rzeczypospolitej-polskiej-na-lata-2025-2029-id131.html

Poniżej informacja nt. wydatków na cyberbezpieczeństwo, które zostały poniesione w 2024 r. lub są planowane do poniesienia w 2025 roku przez Ministerstwo Cyfryzacji.

Rok 2024:

- 63 mln zł w dotacjach celowych,
- 34 mln zł na bieżącą działalność Zespołu Reagowania na Incydenty Bezpieczeństwa Komputerowego poziomu krajowego, prowadzonego przez NASK-PIB,
- 317 mln zł – wydatki poniesione z Funduszu Cyberbezpieczeństwa dla podmiotów kluczowych.

Rok 2025:

- blisko 89,5 mln zł w dotacjach celowych,
- blisko 40 mln zł na bieżącą działalność Zespołu Reagowania na Incydenty Bezpieczeństwa Komputerowego poziomu krajowego, prowadzonego przez NASK-PIB,
- 387,5 mln zł z Funduszu Cyberbezpieczeństwa.

Ponadto w latach 2024-2025 na wsparcie cyberbezpieczeństwa przeznaczone zostały również środki pochodzące z następujących programów:

- KPO (Krajowy Plan Odbudowy i Zwiększania Odporności) – łącznie ok. 860 mln zł, na realizację nw. przedsięwzięć:
    - Utworzenie lub rozwój przynajmniej 5 sektorowych Zespołów Reagowania na Incydenty Bezpieczeństwa Komputerowego (CSIRT sektorowych) – więcej informacji pod linkiem https://www.gov.pl/web/cyfryzacja/prawie-66-mln-zl-na-rozwoj-csirt-ow-sektorowych;
    - Podłączenie 385 nowych podmiotów krajowego systemu cyberbezpieczeństwa do zintegrowanego systemu zarządzania cyberbezpieczeństwem (system S46) – więcej informacji pod linkiem https://www.gov.pl/web/cppc/c311-cyberbezpieczenstwo--cyberpl;
    - Utworzenie wojewódzkich zespołów specjalistów cyberbezpieczeństwa (CROPT) – więcej informacji pod linkiem https://www.gov.pl/web/cyfryzacja/375-mln-zl-na-wsparcie-polskiej-policji-w-zakresie-cyberbezpieczenstwa;
    - Konkurs grantowy „Cyberbezpieczny Rząd” – więcej informacji pod linkiem https://www.gov.pl/web/cyfryzacja/cyberbezpieczny-rzad--wszystkie-umowy-juz-podpisane oraz https://www.gov.pl/web/cyfryzacja/350-mln-zl-na-wzmocnienie-cyberbezpieczenstwa-administracji-rzadowej;
    - Konkurs grantowy „Cyberbezpieczne Wodociągi” – więcej informacji pod linkiem https://www.gov.pl/web/cyfryzacja/cyberbezpieczne-wodociagi--rusza-nabor-wnioskow-o-wsparcie-na-ochrone-przed-cyberatakami;
- FERC (Fundusze Europejskie na Rozwój Cyfrowy) – łącznie ok. 1,8 mld zł, na realizację nw. projektów:
    - „Cyberbezpieczny Samorząd” (1 474 mln zł) – więcej informacji pod linkiem https://www.gov.pl/web/cppc/cyberbezpieczny-samorzad;
    - „Centrum Cyberbezpieczeństwa NASK” (310 mln zł) – więcej informacji pod linkiem https://www.gov.pl/web/cppc/centrum-

cyberbezpieczenstwa-nask-akronim-ccn oraz
https://www.nask.pl/projekty/centrum-cyberbezpieczenstwa-nask.

Ministerstwo Cyfryzacji nie dysponuje danymi nt. wydatków poniesionych na cyberbezpieczeństwo przez inne resorty, w ramach odrębnych części budżetowych. Pełną sprawozdawczością dot. wydatków wszystkich Ministerstw może dysponować Ministerstwo Finansów.

Ad 4) Jakie środki planuje przeznaczyć Ministerstwo oraz Rada Ministrów w najbliższych latach na dalsze wzmacnianie cyberbezpieczeństwa w Polsce?

W planie budżetu na 2026 r. Ministra Cyfryzacji jako dysponenta części 27 – Informatyzacja, znalazły się nw. wydatki:

Rok 2026:

Poniżej szczegółowe dane dotyczące projektu planu wydatków na 2026 r.:

- blisko 195,6 mln zł w dotacjach celowych,
- blisko 45,5 mln zł na bieżącą działalność Zespołu Reagowania na Incydenty Bezpieczeństwa Komputerowego poziomu krajowego, prowadzonego przez NASK-PIB,
- 364,6 mln zł z Funduszu Cyberbezpieczeństwa.

Na etapie prac rządowych nad ustawą budżetową na rok 2026 zakłada się wzrost środków na cyberbezpieczeństwo, jednakże z uwagi na otrzymane z Ministerstwa Finansów limity środków oraz trwający proces legislacyjny nie wyklucza się zmian w tym zakresie.

Ponadto należy wyjaśnić, że Minister Cyfryzacji wchodzi w skład Rady Ministrów i dysponuje budżetem części 27 - Informatyzacja. Nie posiadamy informacji dotyczącej budżetu na zadania związane z cyberbezpieczeństwem pozostałych członków Rady Ministrów.

Z wyrazami szacunku
Paweł Olszewski
Sekretarz Stanu
/dokument podpisany elektronicznie/

Do wiadomości:
Kancelaria Prezesa Rady Ministrów - Departament Spraw Parlamentarnych

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

ul. Królewska 27
00-060 Warszawa