



Ministerstwo Cyfryzacji

Sekretarz Stanu
Paweł Olszewski

BM.WP.057.169.2026
Warszawa, 04 października 2026 r.

**Szanowny Pan
Włodzimierz Czarzasty
Marszałek Sejmu RP**

Dot. pisma z 25 sierpnia br. Pośła na Sejm RP Pana Dariusza Piontkowskiego w sprawie cyberbezpieczeństwa infrastruktury krytycznej jednostek samorządu terytorialnego oraz placówek oświatowych (interpelacja nr 19231)

Szanowny Panie Marszałku,

poniżej przedstawiam odpowiedzi na zadane przez Pośła pytania.

Ad 1) Ile incydentów cyberbezpieczeństwa odnotowano w latach 2024–2026 w jednostkach samorządu terytorialnego oraz placówkach oświatowych?

Właściwym zespołem reagowania na incydenty bezpieczeństwa komputerowego (CSIRT) dla jednostek samorządu terytorialnego (JST) oraz większości jednostek systemu oświaty, w tym szkół i placówek oświatowych, jest CSIRT NASK. Zespół ten realizuje zadania określone w ustawie o krajowym systemie cyberbezpieczeństwa¹, w szczególności w zakresie przyjmowania zgłoszeń, obsługi oraz koordynacji reagowania na incydenty cyberbezpieczeństwa.

Liczba incydentów cyberbezpieczeństwa odnotowanych przez CSIRT NASK przedstawiała się następująco:

Sektor oświaty i wychowania:

- 2024 r. – 579;
- 2025 r. – 1263;
- 2026 r. – 355 incydentów w okresie od stycznia do marca 2026 r.

Jednostki samorządu terytorialnego:

- 2024 r. – 2027;
- 2025 r. – 3249;
- 2026 r. – 607 incydentów w okresie od stycznia do marca 2026 r.

Należy przy tym wskazać, że od kwietnia 2026 r., w związku z wejściem w życie zmiany UKSC oraz metodologii raportowania stosowanej przez CSIRT NASK, dane nie są publikowane w podziale umożliwiającym jednoznaczne określenie liczby incydentów dotyczących poszczególnych kategorii jednostek systemu oświaty lub jednostek samorządu terytorialnego.

Ad 2) Ile spośród tych incydentów dotyczyło szkół podstawowych, ponadpodstawowych oraz innych jednostek systemu oświaty?

CSIRT NASK nie agreguje szczegółowych dane osobno dla szkół podstawowych, ponadpodstawowych czy innych konkretnych poziomów edukacji. Wszystkie te podmioty są agregowane do jednej, szerszej kategorii branżowej: „Oświata i wychowanie”, dla których dane w latach 2024–2026 przedstawiają się w sposób opisany w punkcie 1.

¹ Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz.U. z 2026 r. poz. 20 z późn. zm.) (dalej: ustawa UKSC)

Ad 3) Jakie były najczęstsze rodzaje zagrożeń?

Najczęściej odnotowywanym rodzajem zagrożeń zarówno w administracji publicznej, jak i w sektorze oświaty były oszustwa komputerowe, głównie phishing. Kolejne pod względem liczby incydentów były obraźliwe i nielegalne treści oraz szkodliwe oprogramowanie. W sektorze oświaty istotnym zagrożeniem pozostawały także włamania, których liczba wzrosła z 51 przypadków w 2024 r. do 123 przypadków w 2025 r. Trend ten utrzymał się również w I kwartale 2026 r., kiedy oszustwa komputerowe odpowiadały za ponad 60% wszystkich incydentów odnotowanych w oświacie.

Ad 4) Ile środków finansowych przeznaczono w latach 2024–2026 na poprawę cyberbezpieczeństwa jednostek samorządu terytorialnego oraz szkół?

Wsparcie finansowe z udziałem Ministerstwa Cyfryzacji dla samorządów w zakresie cyberbezpieczeństwa realizowane jest przede wszystkim ze środków programu Fundusze Europejskie na Rozwój Cyfrowy (FERC) oraz Krajowego Planu Odbudowy (KPO):

1. **„Cyberbezpieczny Samorząd”** – projekt grantowy finansowany ze środków programu FERC. Jego celem jest wzmacnianie cyberodporności JST w trzech obszarach: organizacyjnym, technologicznym i kompetencyjnym. Udzielone dofinansowanie w formie grantu jest przedziałem od 200 000 zł do 850 000 zł dla gmin oraz, do 850 000 zł dla powiatów oraz samorządów województw. Do JST przekazano łącznie 1 468 824 754,50 zł.
2. **„Cyberbezpieczne Wodociągi”** – konkurs grantowy współfinansowany ze środków Krajowego Planu Odbudowy i Zwiększania Odporności (KPO), skierowany m.in. do gmin i ich jednostek organizacyjnych oraz spółek samorządowych. Minimalna wartość grantu wynosi 130 000 PLN, a maksymalna zależna jest od limitu pomocy de minimis, który nie może przekroczyć 300 000 EUR w okresie trzech lat (ok. 1 270 000 zł). W ramach tego projektu zrealizowano przelewy do grantobiorców na kwotę 595 214 465,56 zł.

Niezależnie od powyższego należy również wskazać, że JST korzystają nieodpłatnie z narzędzi finansowanych z budżetu państwa i środków europejskich oraz utrzymywanych przez NASK-PIB na zlecenie Ministra Cyfryzacji, m.in.

- systemu S46, za pośrednictwem którego podmiot KSC zgłasza incydent w jednym miejscu, bez konieczności odrębnego kontaktowania się z wieloma instytucjami, a jednocześnie otrzymuje ostrzeżenia i rekomendacje kierowane do podmiotów krajowego systemu cyberbezpieczeństwa);
- usługi ochrony przed atakami DDoS,
- systemu SKR-Z do niejawnej łączności mobilnej, umożliwiający przetwarzanie informacji niejawnych o klauzuli ZASTRZEŻONE/NATO RESTRICTED/EU RESTRICTED;
- serwisu cyber.gov.pl, czyli centralnego portalu krajowego systemu cyberbezpieczeństwa, integrujący kluczowe narzędzia i usługi wspierające administrację publiczną, w tym jednostki samorządu terytorialnego. Portal zapewnia dostęp do informacji o zagrożeniach oraz do systemów służących zgłaszaniu i analizie incydentów.

Ad 5) Ile samorządów i placówek oświatowych skorzystało z programów wsparcia finansowego lub doradczego w zakresie cyberbezpieczeństwa?

1. **„Cyberbezpieczny Samorząd”** - umowy o powierzenie grantu podpisano z 2 490 JST, tj. blisko 90% wszystkich JST w Polsce. Do JST przekazano 1 468 824 754,50 zł.

2. „Cyberbezpieczne Wodociągi” - podpisano 732 umowy o powierzenie grantu z 732 podmiotami takimi jak samorządy gmin ich jednostki organizacyjne czy spółki samorządowe. Alokacja projektu pozwoliła objąć wsparciem wszystkie podmioty, których wnioski uzyskały pozytywną ocenę w naborze.

Ad 6) Czy Ministerstwo prowadzi ocenę poziomu zabezpieczeń informatycznych jednostek samorządu terytorialnego oraz szkół? Jeżeli tak, jakie są najczęściej wskazywane nieprawidłowości?

Ocena stanu bezpieczeństwa jednostek samorządu terytorialnego prowadzona jest m.in. w ramach programu „Cyberbezpieczny Samorząd”, gdzie warunkiem rozliczenia otrzymanego wsparcia jest przeprowadzenie audytu bezpieczeństwa oraz wdrożenie Systemu Zarządzania Bezpieczeństwem Informacji (SZBI).

Dodatkowo jednostki samorządu terytorialnego mogą korzystać z systemu Artemis, który umożliwia wykrywanie podatności oraz błędów konfiguracyjnych w publicznie dostępnej infrastrukturze teleinformatycznej. Mogą one również korzystać z innych bezpłatnych usług z zakresu cyberbezpieczeństwa udostępnianych przez administrację publiczną za pośrednictwem portalu cyber.gov.pl.

Do najczęściej identyfikowanych słabości w JST należą: niedobór wykwalifikowanej kadry i kompetencji w obszarze cyberbezpieczeństwa, niepełne wdrożenie systemów zarządzania bezpieczeństwem informacji oraz procedur ciągłości działania, braki w zakresie polityk tworzenia kopii zapasowych i aktualizacji oprogramowania, a także niewystarczająca kontrola uprawnień dostępu oraz bezpieczeństwa poczty elektronicznej. Wyzwania te znajdują odzwierciedlenie w założeniach projektu Budowa Lokalnych Centrów Cyberbezpieczeństwa (LCC), opisanego szerzej w odpowiedzi na pytanie nr 10.

Ad 7) Jakie działania podejmowane są w celu podnoszenia kompetencji pracowników administracji samorządowej oraz nauczycieli w zakresie cyberbezpieczeństwa?

W celu podnoszenia kompetencji pracowników administracji samorządowej oraz nauczycieli w zakresie cyberbezpieczeństwa realizowane są działania edukacyjne i szkoleniowe skierowane zarówno do sektora oświaty, jak i podmiotów krajowego systemu cyberbezpieczeństwa.

W odniesieniu do nauczycieli i kadry kierowniczej placówek oświatowych realizowany jest projekt Cyberlekcje 3.0, prowadzony przez Ministerstwo Cyfryzacji we współpracy z NASK-PIB. W jego ramach organizowane są szkolenia stacjonarne i webinaria, udostępniane są gotowe scenariusze lekcji, prezentacje, infografiki i materiały multimedialne, a uczestnicy zdobywają wiedzę i praktyczne umiejętności z zakresu cyberhigieny, przeciwdziałania cyberprzemocy, rozpoznawania dezinformacji, ochrony prywatności oraz bezpiecznego korzystania z technologii cyfrowych. Projekt wspiera również rozwój kompetencji niezbędnych do prowadzenia edukacji cyberbezpieczeństwa w szkołach.

Równolegle, w ramach Programu Współpracy w Cyberbezpieczeństwie (PWCyber), realizowane są specjalistyczne szkolenia oraz warsztaty skierowane do podmiotów krajowego systemu cyberbezpieczeństwa, w tym jednostek samorządu terytorialnego. Szkolenia te służą podnoszeniu kompetencji pracowników odpowiedzialnych za cyberbezpieczeństwo, zarządzanie bezpieczeństwem informacji oraz ciągłość działania. Obejmują m.in. zagadnienia związane z identyfikacją i analizą zagrożeń, obsługą incydentów, zarządzaniem ryzykiem, wdrażaniem środków organizacyjnych i technicznych, realizacją obowiązków wynikających z przepisów prawa oraz budowaniem odporności organizacji na cyberzagrożenia.

Dodatkowo, rozwój kompetencji pracowników stanowi jeden z filarów projektów grantowych „Cyberbezpieczny Samorząd” oraz „Cyberbezpieczne Wodociągi”. Środki przyznawane w ramach grantów mogą być przeznaczane m.in. na szkolenia z zakresu cyberhigieny, bezpiecznej obsługi systemów teleinformatycznych oraz działania podnoszące świadomość zagrożeń, w tym ataków socjotechnicznych, takich jak phishing. Uzupełnieniem tych działań są inicjatywy informacyjne i edukacyjne, w szczególności webinaria poświęcone systemowi S46 oraz serwisowi moje.cert.pl.

Podejmowane działania przyczyniają się do:

- zwiększania świadomości i wiedzy z zakresu cyberbezpieczeństwa;
- rozwoju praktycznych umiejętności rozpoznawania i reagowania na incydenty;
- upowszechniania zasad cyberhigieny i dobrych praktyk bezpieczeństwa;
- wzmacniania kompetencji osób odpowiedzialnych za bezpieczeństwo teleinformatyczne w administracji samorządowej i jednostkach oświatowych;
- budowy kultury cyberbezpieczeństwa oraz zwiększania odporności podmiotów publicznych na zagrożenia w cyberprzestrzeni.

Ad 8) Czy Ministerstwo planuje opracowanie jednolitych standardów bezpieczeństwa teleinformatycznego dla szkół oraz jednostek samorządu terytorialnego?

Kwestie dotyczące zapewnienia odpowiedniego poziomu bezpieczeństwa teleinformatycznego JST zostały uregulowane UKSC. Zgodnie z art. 8 ust. 3 podmiot ważny będący podmiotem publicznym opracowuje, wdraża, realizuje, monitoruje i utrzymuje w kontrolowanych przez siebie systemach informacyjnych system zarządzania bezpieczeństwem informacji (SZBI), spełniający wymagania określone w załączniku nr 4 do ustawy.

Rozwiązanie to ustanawia jednolite ramy w zakresie SZBI dla podmiotów publicznych objętych przepisami ustawy, obejmujące wymagania organizacyjne i techniczne służące zapewnieniu odpowiedniego poziomu cyberbezpieczeństwa. Wymagania te dotyczą m.in.: zarządzania ryzykiem, zarządzania incydentami, ciągłości działania, bezpieczeństwa zasobów ludzkich, kontroli dostępu, inwentaryzację zasobów ICT oraz stosowania odpowiednich środków technicznych i organizacyjnych.

Tym samym obowiązujące przepisy UKSC przewidują mechanizmy służące ujednoliceniu wymagań w zakresie cyberbezpieczeństwa podmiotów publicznych objętych jej zakresem.

Ad 9) Czy prowadzone są ćwiczenia lub audyty sprawdzające gotowość samorządów i placówek oświatowych do reagowania na incydenty cyberbezpieczeństwa?

UKSC przewiduje mechanizmy służące weryfikacji poziomu cyberbezpieczeństwa podmiotów objętych jej przepisami. Zgodnie z art. 15 ust. 1 ustawy podmiot kluczowy przeprowadza, na własny koszt, co najmniej raz na 3 lata audyt bezpieczeństwa systemu informacyjnego wykorzystywanego w procesie świadczenia usługi. Jednocześnie organ właściwy do spraw cyberbezpieczeństwa może nakazać audyt zewnętrzny w każdym czasie.

W przypadku podmiotu ważnego, audyt cykliczny nie jest wymagany. Jednakże organ właściwy może nakazać podmiotowi ważnemu przeprowadzenie zewnętrznego audytu tylko w przypadku wystąpienia poważnego incydentu lub innego naruszenia przepisów ustawy.

Powyższe rozwiązania umożliwiają okresową, jak i doraźną weryfikację sposobu realizacji obowiązków wynikających z UKSC przez podmioty objęte regulacją.

Ad 10) Jakie działania planowane są w latach 2027–2028 w celu zwiększenia odporności administracji samorządowej oraz placówek oświatowych na zagrożenia w cyberprzestrzeni?

Działania Ministerstwa Cyfryzacji w latach 2027–2028 skoncentrowane będą na poniższych kierunkach.

- 1. Wsparcie samorządów we wdrożeniu Lokalnych Centrów Cyberbezpieczeństwa.** To konkurs realizowany na podstawie znowelizowanego art. 16e UKSC, który umożliwia JST zawarcie porozumienia w sprawie powierzenia jednej z nich realizacji ustawowych obowiązków cyberbezpieczeństwa na rzecz pozostałych. Głównym celem konkursu jest zapewnienie wsparcia JST w zakresie skutecznej ochrony przed cyberzagrożeniami oraz upowszechnienie rozwiązań organizacyjnych umożliwiających współpracę JST w obszarze cyberbezpieczeństwa. Wnioski o dofinansowanie ze środków UE (program FERC) można składać do 30 października 2026 r. do Centrum Projektów Polska Cyfrowa. Po zakończeniu naboru konkurencyjnego i ocenie wniosków (IV kwartał 2026 r.) planowane jest zawieranie umów o dofinansowanie w I kwartale 2027 r. oraz start pierwszych projektów w II kwartale 2027 r. Docelowo alokacja pozwoli na powstanie co najmniej 30 centrów obejmujących swoim zasięgiem całą lokalną administrację - urzędy, szkoły, ośrodki pomocy społecznej, instytucje kultury. Dzięki współpracy wielu samorządów wspólnie tworzących Lokalne Centrum Cyberbezpieczeństwa możliwe będzie obniżenie kosztów, pozyskanie specjalistycznej wiedzy oraz spełnienie obowiązków wynikających z przepisów UKSC. Każde LCC obowiązkowo obsłuży siedem obszarów zadaniowych analogicznych do wskazanych w odpowiedzi na pytanie 6.
- 2. Budowa Centrum Cyberbezpieczeństwa NASK (CCN)** – projekt o wartości 362 mln zł (FERC), w ramach którego powstaje m.in. Krajowe Centrum Wsparcia Security dla JST, zapewniające wsparcie zaatakowanym jednostkom samorządu terytorialnego oraz identyfikację zagrożeń w ich infrastrukturze (więcej na stronie. [Naukowej i Akademickiej Sieci Komputerowej.](#))
- 3. Nowe, zwrotne instrumenty finansowe.** Uruchomiony 6 lipca 2026 r. Fundusz Bezpieczeństwa i Obronności (ponad 23 mld zł z KPO, blisko 2,5 mld zł na cyberbezpieczeństwo) będzie w latach 2027–2028 uzupełniającą ścieżką finansowania inwestycji JST w cyberbezpieczeństwo, w formule preferencyjnych pożyczek udzielanych przez Bank Gospodarstwa Krajowego (od 0% oprocentowania, do 500 mln zł, na okres do 20 lat, z możliwością częściowego umorzenia dla ponad 1800 gmin i powiatów).

Z wyrazami szacunku

Paweł Olszewski

Sekretarz Stanu

/dokument podpisany elektronicznie/

Do wiadomości:

Kancelaria Prezesa Rady Ministrów - Departament Spraw Parlamentarnych