Ministerstwo Cyfryzacji

Sekretarz Stanu
Paweł Olszewski

BM.WP.057.69.2026
Warszawa, 04 maja 2026 r.

Szanowny Pan
Włodzimierz Czarzasty
Marszałek Sejmu RP

Dot. pisma z 8 kwietnia br. Posła na Sejm RP Pana Marka Matuszewskiego w sprawie bezpieczeństwa danych w administracji publicznej (interpelacja nr 16347)

Szanowny Panie Marszałku,

poniżej przedstawiam odpowiedzi na zadane przez Posła pytania.

Ad 1) Ile incydentów związanych z utratą lub nieuprawnionym ujawnieniem danych odnotowano w ostatnich 5 latach?

W poprzednich 5 latach, w ramach ówcześnie obowiązujących przepisów prawa, zgodnie z ustawą o krajowym systemie cyberbezpieczeństwa[1] podmioty Krajowego Systemu Cyberbezpieczeństwa (KSC), w tym podmioty publiczne, zobowiązane były zgłaszać incydenty cyberbezpieczeństwa do właściwego jednego z trzech zespołów reagowania na incydenty bezpieczeństwa komputerowego (CSIRT) poziomu krajowego, o których mowa w art. 2 pkt 1-3 ustawy o KSC:

a) CSIRT GOV - prowadzony przez Szefa Agencji Bezpieczeństwa Wewnętrznego;
b) CSIRT NASK - prowadzony przez Naukową i Akademicką Sieć Komputerową – Państwowy Instytut Badawczy;
c) CSIRT MON - prowadzony przez Ministra Obrony Narodowej;

- zgodnie z zakresem odpowiedzialności poszczególnych CSIRT określonym w art. 26 ustawy o KSC.

Statystki zespołów CSIRT poziomu krajowego nie wyszczególniają utraty lub nieuprawnionego ujawnienia danych jako rodzaju incydentu. Raporty roczne wraz z statystykami incydentów publikowane są przez zespół CSIRT GOV[2] oraz CERT Polska[3] (wchodzącego w skład CSIRT NASK).

Ad 2) Jakie były główne przyczyny tych incydentów?

Jak wskazano w odpowiedzi na pytanie nr 1, statystki zespołów CSIRT poziomu krajowego nie wyszczególniają utraty lub nieuprawnionego ujawnienia danych jako rodzaju incydentu. Jednocześnie warto wskazać, że raport roczny CERT Polska za 2025 r. do najczęstszego typu incydentów należą oszustwa komputerowe (97,1%), złośliwe oprogramowanie (1,3%), podatne usług (0,7%). W związku z tym najczęstszym powodem wystąpienia incydentu jest socjotechnika stosowana przez cyberprzestępców. Dlatego też Ministerstwo Cyfryzacji realizuje liczne działania w zakresie podnoszenia kompetencji i świadomości w obszarze cyberbezpieczeństwa i higieny cyfrowej.

Ad 3) Jakie standardy bezpieczeństwa danych obowiązują obecnie w administracji publicznej?

[1] Art. 22 ust. 1 pkt 2 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz.U. z 2024 r. poz. 1077 z późn. zm.) (ustawa o KSC)
[2] https://csirt.gov.pl/cer/publikacje/raporty-o-stanie-bezpi
[3] https://cert.pl/publikacje/#raport

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

ul. Królewska 27
00-060 Warszawa

W dniu 3 kwietnia 2026 r. weszła w życie nowelizacja ustawy o KSC[4], która m.in. wdrożyła w Polsce dyrektywę NIS 2. Zgodnie z nowymi przepisami podmioty publiczne zaliczają się obecnie do podmiotów kluczowych lub podmiotów ważnych w rozumieniu tejże ustawy. W związku z tym podmioty publiczne zobowiązane są wdrożyć system zarządzania bezpieczeństwem informacji w systemie informacyjnym wykorzystywanym w procesach wpływających na świadczenie usługi przez ten podmiot, zapewniający:

1) prowadzenie systematycznego szacowania ryzyka wystąpienia incydentu oraz zarządzanie tym ryzykiem;
2) wdrożenie odpowiednich i proporcjonalnych do oszacowanego ryzyka środków technicznych i organizacyjnych, uwzględniających najnowszy stan wiedzy, koszty wdrożenia, wielkość podmiotu, prawdopodobieństwo wystąpienia incydentów, narażenie podmiotu na ryzyka, skutki społeczne i gospodarcze, w szczególności:
   a) polityki szacowania ryzyka oraz bezpieczeństwa systemu informacyjnego, w tym polityki tematyczne,
   b) bezpieczeństwo w procesie nabywania, rozwoju, utrzymania i eksploatacji systemu informacyjnego, w tym testowanie systemu informacyjnego,
   c) bezpieczeństwo fizyczne i środowiskowe uwzględniające kontrole dostępu,
   d) bezpieczeństwo zasobów ludzkich,
   e) bezpieczeństwo i ciągłość łańcucha dostaw produktów ICT, usług ICT i procesów ICT, od których zależy świadczenie usługi, z uwzględnieniem związków pomiędzy bezpośrednim dostawcą sprzętu lub oprogramowania a podmiotem kluczowym lub podmiotem ważnym,
   f) wdrażanie, dokumentowanie, testowanie i utrzymywanie planów ciągłości działania umożliwiających ciągłe i niezakłócone świadczenie usługi oraz zapewniających poufność, integralność, dostępność i autentyczność informacji, planów awaryjnych oraz planów odtworzenia działalności umożliwiających odtworzenie systemu informacyjnego po zdarzeniu, które spowodowało straty przekraczające zdolności podmiotu do odbudowy za pomocą własnych środków,
   g) objęcie systemu informacyjnego wykorzystywanego do świadczenia usługi systemem monitorowania w trybie ciągłym,
   h) polityki i procedury oceny skuteczności środków technicznych i organizacyjnych,
   i) edukację z zakresu cyberbezpieczeństwa dla personelu podmiotu,
   j) podstawowe zasady cyberhigieny,
   k) polityki i procedury stosowania kryptografii, w tym w stosownych przypadkach szyfrowania,
   l) stosowanie bezpiecznych środków komunikacji elektronicznej w ramach krajowego systemu cyberbezpieczeństwa oraz wewnątrz podmiotu, uwzględniających uwierzytelnianie wieloskładnikowe w stosownych przypadkach,
   m) zarządzanie aktywami,
   n) polityki kontroli dostępu;
3) zbieranie informacji o cyberzagrożeniach i podatnościach na incydenty systemu informacyjnego wykorzystywanego do świadczenia usługi;

[4] Dz.U. z 2026 r. poz. 20 późn. zm.

4) zarządzanie incydentami;
5) stosowanie środków zapobiegających i ograniczających wpływ incydentów na bezpieczeństwo systemu informacyjnego wykorzystywanego do świadczenia usługi, w tym:
   a) stosowanie mechanizmów zapewniających poufność, integralność, dostępność i autentyczność danych przetwarzanych w systemie informacyjnym,
   b) regularne przeprowadzanie aktualizacji oprogramowania, stosownie do zaleceń producenta, z uwzględnieniem analizy wpływu aktualizacji na bezpieczeństwo świadczonej usługi oraz poziomu krytyczności poszczególnych aktualizacji,
   c) ochronę przed nieuprawnioną modyfikacją w systemie informacyjnym,
   d) niezwłoczne podejmowanie działań po dostrzeżeniu podatności lub cyberzagrożeń, w tym również czasowe ograniczenie ruchu sieciowego przychodzącego do infrastruktury podmiotu kluczowego lub podmiotu ważnego, które może skutkować zakłóceniem usług świadczonych przez ten podmiot, z uwzględnieniem konieczność minimalizacji skutków ograniczenia dostępności tych usług, z uwagi na podjęte działania.

Ad 4) Jak często przeprowadzane są audyty bezpieczeństwa w jednostkach administracyjnych?

Zgodnie z udzieloną odpowiedzą na pytanie nr 3 podmioty publiczne, w zależności od ich rodzaju, zaliczają się do podmiotów kluczowych lub podmiotów ważnych w rozumieniu ustawy o KSC. Zgodnie z art. 15 ust. 1 ustawy o KSC podmiot kluczowy przeprowadza, na własny koszt, co najmniej raz na 3 lata, audyt bezpieczeństwa systemu informacyjnego wykorzystywanego w procesie świadczenia usługi, zwany dalej „audytem", licząc od dnia sporządzenia i podpisania przez audytorów przeprowadzających audyt raportu z ostatniego audytu. Jednocześnie zgodnie z art. 15 ust. 1b. organ właściwy do spraw cyberbezpieczeństwa w dany sektorze (określony w art. 41) może nakazać podmiotowi kluczowemu w każdym czasie lub podmiotowi ważnemu w przypadku wystąpienia incydentu poważnego lub innego naruszenia przepisów ustawy przez ten podmiot, w drodze decyzji, przeprowadzenie zewnętrznego audytu bezpieczeństwa systemu informacyjnego wykorzystywanego w procesie świadczenia usługi.

Ad 5) Jakie procedury obowiązują w przypadku wykrycia naruszenia bezpieczeństwa danych?

Zgodnie z przywołanymi powyżej przepisami, w przypadku incydentu cyberbezpieczeństwa podmiot publiczny zobowiązany jest zarządzić tym incydentem, stosować środki zapobiegające i ograniczające wpływ incydentu na bezpieczeństwo systemu informacyjnego wykorzystywanego do świadczenia usługi oraz zgłosić incydent do właściwego zespołu CSIRT, który udzieli wsparcia podmiotowi dotkniętemu incydentem.

Ad 6) Jakie są plany zwiększenia nakładów na cyberbezpieczeństwo i szkolenia pracowników?

Ministerstwo Cyfryzacji przykłada dużą wagę do należytego finansowania cyberbezpieczeństwa oraz prowadzenia działalności szkoleniowej w zakresie cyberbezpieczeństwa.

Odnosząc się do kwestii finansowania, plany zwiększenia nakładów na cyberbezpieczeństwo przedstawiają się następująco.

Ministerstwo Cyfryzacji zapewnia wsparcie finansowe, w tym w obszarze podnoszenia kompetencji cyberbezpieczeństwa, w ramach programów krajowych i europejskich, w szczególności poprzez program Fundusze Europejskie na Rozwój Cyfrowy 2021–2027 (FERC). Wartość projektów dofinansowanych ze środków UE (FERC) oraz budżetu państwa na projekty wynosi ponad 1,8 mld zł.

- Kluczowym instrumentem wsparcia dla jednostek samorządu terytorialnego jest projekt „Cyberbezpieczny Samorząd" (1,5 mld zł, lata 2023–2027), umożliwiający finansowanie inwestycji w infrastrukturę, systemy bezpieczeństwa oraz podnoszenie kompetencji kadr. Wdrażanie projektów przez JST zakończy się 30.09.2026 r.
- Wsparcie systemowe zapewnia również projekt „Centrum Cyberbezpieczeństwa NASK" (310 mln zł, lata 2023–2029), którego celem jest budowa zaplecza eksperckiego, budynku biurowego w Warszawie oraz rozwój usług wspierających administrację publiczną.

W ramach Krajowego Planu Odbudowy (inwestycja C3.1.1 „Cyberbezpieczeństwo – CyberPL") realizowane są projekty o łącznej wartości ponad 1 mld zł, obejmujące m.in.:

- 886,5 mln na wsparcie administracji rządowej i sektora zaopatrzenia w wodę pitną poprzez konkursy grantowe „Cyberbezpieczny Rząd" – 273,1 mln zł oraz „Cyberbezpieczne Wodociągi" – 613,4 mln zł.
- rozwój i budowę CSIRT sektorowych (46,6 mln zł) – zespoły reagowania na incydenty bezpieczeństwa komputerowego (CSIRT) na poziomie krajowym i sektorowym, które zapewniają bezpośrednie wsparcie w obsłudze incydentów, analizie zagrożeń oraz rekomendacjach działań naprawczych są podstawowym mechanizmem wsparcia operacyjnego podmiotów krajowego systemu cyberbezpieczeństwa,
- integrację podmiotów krajowego systemu cyberbezpieczeństwa poprzez system S46 (39,7 mln zł) – zintegrowany system zarządzania cyberbezpieczeństwem (S46), umożliwia monitorowanie, raportowanie i koordynację reakcji na incydenty w skali krajowej,
- tworzenie wojewódzkich zespołów specjalistów cyberbezpieczeństwa w strukturach Policji (CROPT) (37,5 mln zł);

W 2026 r. planowane jest uruchomienie kolejnych instrumentów wsparcia w ramach programu FERC, o łącznej alokacji ok. 770 mln zł, w tym:

- konkurs dla samorządów na utworzenie Lokalnych Centrów Cyberbezpieczeństwa (270 mln zł), umożliwiający współpracę JST w obszarze cyberbezpieczeństwa, optymalizację kosztów oraz zasobów;
- wsparcie dla CSIRT sektorowych i Organów Właściwych ds. cyberbezpieczeństwa (150 mln zł);
- rozwój Bezpiecznej Komunikacji Mobilnej w tym m.in. aplikacji mSzyfr dla podmiotów krajowego systemu cyberbezpieczeństwa (120 mln zł),
- wsparcie Połączonego Centrum Operacyjnego Cyberbezpieczeństwa (230 mln zł), zapewniającego koordynację działań z obszaru cyberbezpieczeństwa na poziomie krajowym, co umożliwia szybką i skoordynowaną reakcję na zagrożenia.

Dodatkowo wydatki Ministerstwa Cyfryzacji na cyberbezpieczeństwo w 2026 r. z budżetu państwa wyniosą łącznie 450 mln zł, z czego znaczna część tej kwoty zostanie przeznaczona na dotacje dla NASK-PIB, który m.in. realizuje zadanie CSIRT poziomu krajowego. Zadania CSIRT NASK wiążą się z zapewnieniem bezpieczeństwa obywateli i

ochroną podstawowych interesów państwa poprzez zwiększenie odporności na cyberzagrożenia. Działalność Zespołu CSIRT NASK przyczynia się do wzmacniania cyberbezpieczeństwa państwa m.in. poprzez monitorowanie i wykrywanie zagrożeń i incydentów oraz wsparcie podmiotów kluczowych i ważnych, w tym poprzez edukację i podnoszenie świadomości cyberzagrożeń.

Ponadto, Ministerstwo Cyfryzacji w ramach nowelizacji ustawy o KSC, zadbało żeby znalazły się w niej zapisy znacznie zwiększające dotychczasowe limity wydatków z budżetu państwa, w wyniku wejścia w życie tej ustawy, dla części budżetowych znajdujących się w dyspozycji ministrów pełniących rolę Organów Właściwych do spraw cyberbezpieczeństwa dla podmiotów z kluczowych i ważnych sektorów gospodarki.

W ramach Funduszu Cyberbezpieczeństwa, jako państwowego funduszu celowego, kontynuowane jest również wsparcie działań zmierzających do zapewnienia bezpieczeństwa systemów teleinformatycznych przed cyberzagrożeniami poprzez finansowanie świadczenia teleinformatycznego, tj. dodatku do wynagrodzenia za pracę, a w przypadku funkcjonariuszy i żołnierzy zawodowych świadczenia pieniężnego. Minister Cyfryzacji realizuje ww. zadanie przy pomocy kierowników jednostek objętych wsparciem, którzy zgodnie z *ustawą o szczególnych zasadach wynagradzania osób realizujących zadania z zakresu cyberbezpieczeństwa* przyznają świadczenia teleinformatyczne w kierowanych przez siebie instytucjach.

Budżet Funduszu Cyberbezpieczeństwa w 2026 r. wynosi 364,65 mln zł.

Świadczenie teleinformatyczne może zostać przyznane osobom realizującym zadania z zakresu cyberbezpieczeństwa na rzecz podmiotów wymienionych w niniejszej ustawie, m.in. w CSIRT poziomu krajowego, służbach odpowiedzialnych za bezpieczeństwo państwa oraz bezpieczeństwo powszechne, a także niektórych urzędach administracji publicznej. W katalogu podmiotów uprawnionych do utrzymania wsparcia jest około 4 tys. instytucji publicznych.

Odnosząc się do kwestii szkoleń, należy wskazać, że Ministerstwo Cyfryzacji prowadzi i nadzoruje liczne programy prewencyjno-edukacyjne oraz szkolenia dla pracowników różnych organizacji i urzędów.

Szkolenia online dla podmiotów krajowego systemu cyberbezpieczeństwa

Nieprzerwanie od 2020 r. realizowane są w bezpłatne szkolenia online prowadzone przez ekspertów oraz praktyków na co dzień zajmujących się kwestiami cyberbezpieczeństwa - ekspertów NASK-PIB oraz partnerów technologicznych Programu Współpracy w Cyberbezpieczeństwie (PWCyber). Celem szkoleń jest nie tylko zwiększenie świadomości kadr KSC na temat cyberzagrożeń, ale również podniesienie umiejętności praktycznych związanych z wykorzystywaniem narzędzi informatycznych oraz radzenia sobie w sytuacjach kryzysowych. Realizowane są na różnym poziomie zaawansowania wiedzy z zakresu cyberbezpieczeństwa, dostosowane do bieżącej sytuacji i zgłaszanych potrzeb. Część szkoleń realizowana jest z udziałem tłumaczy na Polski Język Migowy (PJM). Wyszczególniono trzy kategorie w ramach kwalifikacji użytkowników:

a) Szkolenia 100 - cyberhigiena dla każdego – podstawowe porady i najlepsze praktyki z zakresu cyberbezpieczeństwa dla wszystkich pracowników.
b) Szkolenia 200 - dla kadry zarządzającej, pracowników działów IT – podstawy prawne krajowego systemu cyberbezpieczeństwa, obowiązki podmiotów wynikające z ustawy, procedury zgłaszania incydentów, najczęstsze cyberzagrożenia i sposoby ochrony.
c) Szkolenia 300 - warsztaty dla specjalistów IT, programistów, osób zarządzających cyberbezpieczeństwem w podmiotach krajowego systemu

cyberbezpieczeństwa - prezentacje projektów wspierających cyberbezpieczeństwo w organizacji, analizy rodzajów cyberataków, reagowanie na incydenty, zgłaszanie incydentów, profilaktyka cyberbezpieczeństwa
w organizacji, szkolenia specjalistyczne dotyczące zastosowania konkretnych rozwiązań prowadzone przez partnerów technologicznych.

Oficjalny harmonogram jest zamieszczony na stronie gov.pl.

Od 2020 r. przeprowadzono 168 szkoleń, w których udział wzięło przeszło 130 tys. uczestników. Od 2026 r. w szkoleniach udział biorą także przedstawiciele operatorów infrastruktury krytycznej.

Szkolenia będą kontynuowane w kolejnych latach.

Szkolenia adresowane do specjalistów sektorowych zespołów reagowania na incydenty bezpieczeństwa komputerowego (CSIRT sektorowe)

Ministerstwo Cyfryzacji w ramach zawartego Porozumienia o współpracy z Ministerstwem Obrony Narodowej – Eksperckim Centrum Cyberbezpieczeństwa rozpoczęło w 2025 r. organizację szkoleń dla pracowników administracji odpowiedzialnych za IT oraz bezpieczeństwo informacji. Program obejmuje praktyczne warsztaty, ćwiczenia z reagowania na incydenty oraz zajęcia z najnowszych technologii ochrony danych.

Od września 2026 r. planowany jest kolejny blok szkoleń z obszaru cyberbezpieczeństwa przeprowadzany wspólnie przez MC oraz ECSC.

Prowadzone są strony internetowe, które mają na celu zapoznawać z najnowszymi informacjami związanymi z cyberbezpieczeństwem i cyberzagrożeniami oraz promować szkolenia i programy edukacyjne.

W Bazie Wiedzy o cyberbezpieczeństwie na portalu gov.pl (Rekomendacje cyberbezpieczeństwa - Baza wiedzy - Portal Gov.pl)[5] publikowane są rekomendacje dobrych praktyk i zalecenia konfiguracyjne podnoszące poziom cyberbezpieczeństwa w ramach skutecznego zarządzania ryzykiem, osiągania bezpieczeństwa w systemach informacyjnych oraz przetwarzania w chmurze.

Ponadto wspólnie z Partnerami Programu Współpracy w Cyberbezpieczeństwie (PWCyber) opracowywane i zamieszczane są Poradniki PWCyber.

Działania prewencyjno-edukacyjne z zakresu cyberbezpieczeństwa podnoszenie odporności Rzeczypospolitej Polskiej na zagrożenia w przestrzeni cyfrowej

Prowadzone są działania prewencyjno-edukacyjne z zakresu cyberbezpieczeństwa ukierunkowane na podnoszenie odporności Rzeczypospolitej Polskiej na zagrożenia w przestrzeni cyfrowej kierowane do najważniejszych osób w państwie:

a) przedstawicieli władzy ustawodawczej i wykonawczej,
b) przedstawicieli jednostek samorządu terytorialnego,
c) pracowników sądów i prokuratury,
d) przedstawicieli i członków Krajowego Biura Wyborczego oraz organów wyborczych.

[5] https://www.gov.pl/web/baza-wiedzy/aktualnosci

Działania będą kontynuowane w kolejnych latach, a formuła działań pozwala na rozszerzenie katalogu odbiorców w przypadku potrzeby wynikającej z bieżącej sytuacji w kraju.

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