



Ministerstwo Cyfryzacji

Sekretarz Stanu
Paweł Olszewski

BM.WP.057.75.2026
Warszawa, 06 maja 2026 r.

**Szanowny Pan
Włodzimierz Czarzasty
Marszałek Sejmu RP**

Dot. pisma z 17 kwietnia br. Posłanki na Sejm RP Pani Urszuli Pastawskiej w sprawie ochrony baz danych urzędów gmin i miast przed cyberatakami typu ransomware oraz finansowania zabezpieczeń cyfrowych w samorządach (interpelacja nr 16581)

Szanowny Panie Marszałku,

poniżej przedstawiam odpowiedzi na zadane przez Posłanki pytania.

Ad 1) Jakiego rodzaju wsparcia udzielił resort samorządom Obrazowa i Myszkowa po cyberatakach? Czy była to pomoc finansowa, organizacyjna lub ekspercka, w tym np. wsparcie przy odzyskiwaniu danych i przywracaniu systemów?

Zespół reagowania na incydenty bezpieczeństwa komputerowego poziomu krajowego CSIRT NASK¹ otrzymał zgłoszenia dotyczące wystąpienia ataku ransomware bezpośrednio od przedstawicieli gminy Obrazów oraz Urzędu Miasta Myszków. Niezwłocznie zostały przeprowadzone telekonferencje z administratorami zaatakowanych zasobów, które pozwoliły analitykom na poznanie infrastruktury posiadanej przez podmioty oraz pozyskanie innych informacji potrzebnych do rozpoczęcia analizy. Po telekonferencjach zostały do podmiotów przesłane informacje dotyczące potrzebnych do przeprowadzenia analizy powłamaniowej zasobów (takich jak logi, pliki, czy obrazy maszyn wirtualnych).

Oba podmioty przekazały zespołowi CSIRT NASK oczekiwane dane, z wyłączeniem tych, do których dostęp został utracony, lub które zostały usunięte przez atakujących. Zespół Komunikacji Strategicznej Cyberbezpieczeństwa działający w strukturze CSIRT NASK udzielił podmiotom wsparcia w przygotowaniu komunikacji zewnętrznej dotyczącej incydentów. Każdy z podmiotów otrzymał wyniki przeprowadzonej przez CSIRT NASK analizy powłamaniowej niezwłocznie po jej zakończeniu, wraz ze wskazaniem potencjalnego wektora ataku oraz informacją o ograniczeniach wynikających z niedostępności pełnego zakresu logów z zaatakowanych zasobów. CSIRT NASK przez czas obsługi incydentów oferował podmiotom wsparcie merytoryczne dotyczące pozyskania potrzebnych logów oraz odtworzenia infrastruktury w sposób bezpieczny. W ataku na Urząd Miasta Myszków zostało wykorzystane oprogramowanie ransomware Gunra. CSIRT NASK wszedł w posiadanie dekryptora tego oprogramowania. Po weryfikacji poprawności jego działania, dekryptor został przekazany administratorom w celu odszyfrowania danych. Odszyfrowanie plików w infrastrukturze gminy Obrazów nie było możliwe.

Ad 2) Czy ministerstwo prowadzi obecnie ocenę poziomu przygotowania jednostek samorządu terytorialnego do przeciwdziałania atakom typu ransomware?

Poziom cyberbezpieczeństwa jednostek samorządu terytorialnego (JST), w tym w obszarach, które są kluczowe dla zapewnienia odporności na ataki typu ransomware, był przedmiotem badania realizowanego w ramach projektu pn. "Cyberbezpieczny Samorząd", na podstawie analizy złożonych wniosków o granty oraz dołączonych do nich ankiet dojrzałości cyberbezpieczeństwa w JST i jednostkach im podległych. Jednocześnie warto wskazać, że w ramach konkursu grantowego pn. "Cyberbezpieczne Wodociągi", którego

¹ CSIRT NASK funkcjonuje w strukturze Naukowej i Akademickiej Sieci Komputerowej - Państwowego Instytutu Badawczego (NASK-PIB), jednostki nadzorowanej przez Ministra Cyfryzacji.

głównymi beneficjentami są JST bądź spółki komunalne, podczas oceny wniosków o dofinansowanie, premiowane punktowo były działania deklarowane do zrealizowania w ramach projektów grantowych, których celem jest zwiększenie odporności na cyberzagrożenia, w tym ataki typu ransomware.

W celu podniesienia poziomu cyberbezpieczeństwa JST i jednostek podległych, co obejmuje także przeciwdziałanie atakom typu ransomware, Ministerstwo Cyfryzacji realizuje inicjatywy opisane w odpowiedzi na pytania nr 3 i 4.

Jednocześnie należy wskazać, że obecnie dla zwiększenia przygotowania JST do przeciwdziałania atakom typu ransomware (oraz innym cyberzagrożeniom) kluczowe znaczenie będzie mieć realizacja przez JST zadań wynikających z nowelizacji ustawy o krajowym systemie cyberbezpieczeństwa² (ustawa o KSC), która weszła w życie w dniu 3 kwietnia 2026 r. Zgodnie z nowymi przepisami podmioty publiczne zaliczają się obecnie do podmiotów kluczowych lub podmiotów ważnych (w tym JST) w rozumieniu tejże ustawy. W związku z tym podmioty publiczne zobowiązane są zapewnić spełnianie odpowiednich wymogów w zakresie cyberbezpieczeństwa, określone w art. 8-16a, w szczególności poprzez wdrożenie systemu zarządzania bezpieczeństwem informacji w systemie informacyjnym wykorzystywanym w procesach wpływających na świadczenie usługi przez ten podmiot, zapewniającym:

- 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;

² Dz.U. z 2026 r. poz. 20 późn. zm.

- 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) 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 konieczności minimalizacji skutków ograniczenia dostępności tych usług, z uwagi na podjęte działania.

Ad 3) Jakie środki finansowe zostały przekazane jednostkom samorządu terytorialnego w latach 2025–2026 na poprawę cyberbezpieczeństwa?

Ministerstwo Cyfryzacji w latach 2025-2026 wspierało jednostki samorządu terytorialnego środki w zakresie poprawy cyberbezpieczeństwa w ramach konkursów grantowych pn. „Cyberbezpieczny Samorząd” oraz „Cyberbezpieczne Wodociągi”.

W ramach konkursu grantowego pn. „Cyberbezpieczny Samorząd” jednostkom samorządu terytorialnego w roku 2025 r. zostało przekazane 592 187 634,36 zł, a w roku 2026, do dnia 24 kwietnia, przekazano 123 752 382,15 zł (środki wypłacone).

Konkurs grantowy pn. „Cyberbezpieczny Samorząd” to projekt współfinansowany ze środków UE oraz budżetu państwa, w ramach programu Fundusze Europejskie na Rozwój Cyfrowy 2021-2027 (FERC). Łączna kwota grantów w tym projekcie wynosi blisko 1,5 mld zł, z czego do dnia 24 kwietnia 2026 r., samorządom wypłacono łącznie już 1 410 354 719,36 zł. Środki te są wypłacane w transzach proporcjonalnie do postępu realizacji projektów grantowych. Operatorem projektu jest Centrum Projektów Polska Cyfrowa (CPPC) w partnerstwie z NASK PIB.

Ministerstwo Cyfryzacji uruchomiło projekt „Cyberbezpieczny Samorząd”, aby samorządy wzmocniły swoją odporność na cyberzagrożenia, tj. zdolność do skutecznego zapobiegania i reagowania na incydenty w systemach informacyjnych. Jednostki Samorządu Terytorialnego otrzymują dofinansowanie w formie grantu w przedziale od 200 000 zł do

850 000 zł dla gmin oraz, do 850 000 zł dla powiatów oraz samorządów województw. Środki te mogą przeznaczyć na wszystkie działania, które są związane z poprawą ich cyberbezpieczeństwa. Są to m.in.: audyty oraz wdrożenie lub aktualizacja polityki bezpieczeństwa informacji (SZBI), nowoczesne technologie które zwiększają odporność na ataki w cyberprzestrzeni oraz szkolenia personelu.

Jednostki samorządu terytorialnego mogły również pozyskać środki w ramach konkursu grantowego pn. „Cyberbezpieczne Wodociągi”. Konkurs ten jest współfinansowany ze środków Krajowego Planu Odbudowy i Zwiększania Odporności (KPO).

Celem tego przedsięwzięcia jest wzmocnienie cyberodporności przedsiębiorstw działających w sektorze zbiorowego zaopatrzenia w wodę, które są objęte Krajowym Systemem Cyberbezpieczeństwa, w szczególności poprzez: modernizację systemów IT/OT, audyty bezpieczeństwa oraz szkolenia pracowników. Przedsięwzięcie to pozwoli wzmocnić ochronę infrastruktury krytycznej przed cyberatakami, zapewniając ciągłość dostaw wody poprzez wsparcie we wdrażaniu środków organizacyjnych i technicznych oraz rozwój kompetencji personelu w zakresie cyberbezpieczeństwa.

Nabór wniosków o granty w ramach konkursu „Cyberbezpieczne Wodociągi”, został uruchomiony w dniu 1 września 2025 r. i zakończył się 2 października 2025 r. W jego wyniku zostało złożonych 896 wniosków o dofinansowanie, o łącznej wartości ponad 730 mln zł. Wnioski o granty składały zarówno gminy i ich jednostki organizacyjne jak i spółki samorządowe (sp. z o.o. lub S.A.). Wnioski o dofinansowanie w formie grantów wpłynęły od cztery grup podmiotów krajowego systemu cyberbezpieczeństwa, które reprezentują różne formy organizacyjne sektora wodno-kanalizacyjnego, tj.:

- spółki z ograniczoną odpowiedzialnością – 622 wnioski o łącznej wartości ok. 576 mln zł;
- gminy lub ich związki – 155 wniosków o wartości ponad 118 mln zł;
- gminne samorządowe jednostki organizacyjne – 105 wniosków o wartości ok. 83 mln zł;
- spółki akcyjne – 14 wniosków o wartości blisko 12 mln zł.

Największą grupę wnioskodawców stanowiły spółki z ograniczoną odpowiedzialnością – ponad 69% wszystkich złożonych wniosków. Wysoki udział gmin i ich jednostek organizacyjnych potwierdza, że przedsięwzięcie objęło szerokie i zróżnicowane grono podmiotów odpowiedzialnych za świadczenie usług wodno-kanalizacyjnych.

W lutym 2026 r. CPPC ogłosiło wyniki konkursu i opublikowało listę rankingową projektów wybranych do dofinansowania. W ramach konkursu pozytywnie oceniono 759 wniosków o łącznej wartości ponad 624 mln zł. Z podmiotami, których wnioski uzyskały pozytywną ocenę aktualnie podpisywane są umowy o powierzenie grantu oraz sukcesywnie przekazywane są środki na realizację projektów grantowych.

Na dzień 24 kwietnia 2026 r. podpisanych zostało już 578 umów o powierzenie grantu oraz przekazano już środki do grantobiorców o łącznej wysokości 260 688 371,44 zł.

Ad 4) Czy resort rozważa uruchomienie dedykowanego programu wsparcia dla małych i średnich samorządów na audyty bezpieczeństwa, testy penetracyjne, tworzenie bezpiecznych kopii zapasowych oraz szkolenia pracowników?

Ministerstwo Cyfryzacji, jeszcze w bieżącym roku planuje uruchomienie naboru wniosków o dofinansowanie dla jednostek samorządu terytorialnego (JST) w ramach projektu utworzenia lub rozwoju Lokalnych Centrów Cyberbezpieczeństwa (LCC), o łącznej wartości 270 mln zł. Projekt ten będzie współfinansowany ze środków UE w ramach programu Fundusze Europejskie na Rozwój Cyfrowy 2021-2027 (FERC), a jego

założeniem jest zainspirowanie samorządów do rozpoczęcia lub rozszerzenia współpracy w obszarze cyberbezpieczeństwa obejmującej swoim zasięgiem więcej niż jeden samorząd. Głównym celem projektu jest zapewnienie wsparcia JST w zakresie skutecznej ochrony przed cyberzagrożeniami oraz upowszechnienie rozwiązań organizacyjnych umożliwiających współpracę JST w obszarze cyberbezpieczeństwa.

Zakłada się ponadto, że w ramach realizacji projektu, Lokalne Centra Cyberbezpieczeństwa wypracują i utrzymają warunki stabilnego finansowania swojego funkcjonowania również po zakończeniu współfinansowania ze środków UE w ramach programu FERC.

Podstawę do uruchomienia tego projektu stanowią przepisy art. 16e znowelizowanej ustawy o KSC, które przewidują możliwość zawierania porozumień pomiędzy samorządami w celu realizacji zadań związanych z cyberbezpieczeństwem.

Zgodnie z aktualnymi założeniami programu FERC projekt utworzenia i rozwoju LCC będzie mógł być realizowany do końca 2030 r., więc do tego czasu centra które powstaną w wyniku jego realizacji powinny już osiągnąć zdolność operacyjną do skutecznej ochrony przed cyberatakami jednostek, które zostaną objęte ich obszarem funkcjonowania.

LCC będą realizować zadania z zakresu cyberbezpieczeństwa na rzecz obsługiwanych samorządów, w oparciu o porozumienia między JST. Dzięki takiej współpracy możliwe będzie podniesienie kompetencji kadr administracji samorządowej, wzmocnienie technologiczne oraz spełnianie obowiązków wynikających z ww. ustawy o krajowym systemie cyberbezpieczeństwa.

Zakres zadań realizowanych przez LCC może obejmować m.in.:

- opracowanie, wdrożenie i cykliczne przeglądy Systemu Zarządzania Bezpieczeństwem Informacji (SZBI);
- przeprowadzanie co najmniej raz na 3 lata audytów bezpieczeństwa systemów informacyjnych, wykorzystywanych w procesie świadczenia usług publicznych;
- objęcie systemu informacyjnego wykorzystywanego do świadczenia usługi publicznej systemem monitorowania w trybie ciągłym;
- reagowanie na incydenty (koordynowanie działań w przypadku incydentów cyberbezpieczeństwa);
- wsparcie techniczne (usługi doradcze i techniczne, obejmujące audyty bezpieczeństwa, wdrażanie środków ochrony, zarządzanie ryzykiem oraz tworzenie polityk bezpieczeństwa);
- wspólne zakupy sprzętu/usług/licencji IT;
- edukację i szkolenia (szkolenia i warsztaty dla lokalnych pracowników, specjalistów IT i przedstawicieli instytucji publicznych).

Z wyrazami szacunku

Paweł Olszewski

Sekretarz Stanu

/dokument podpisany elektronicznie/

Do wiadomości:

Kancelaria Prezesa Rady Ministrów - Departament Spraw Parlamentarnych