Ministerstwo
Cyfryzacji

Sekretarz Stanu
Paweł Olszewski

BM.WP.057.208.2026
Warszawa, 27 października 2026 r.

Szanowny Pan
Włodzimierz Czarzasty
Marszałek Sejmu RP

Dot. pisma z 14 października br. Posłanki na Sejm RP Pani Olgi Ewy Semeniuk-Patkowskiej w sprawie skuteczności przeciwdziałania cyberatakom i wyciekom danych osobowych oraz ochrony obywateli przed ich następstwami (interpelacja nr 20302)

Szanowny Panie Marszałku,

poniżej przedstawiam odpowiedzi na zadane przez Posłanki pytania.

Ad 1) Jak resort ocenia skalę cyberataków prowadzących do kradzieży lub ujawnienia danych osobowych? Jakie tendencje i najważniejsze słabości systemu ochrony zidentyfikowano?

Zagrożenia w cyberprzestrzeni mają charakter dynamiczny i stale rosnący, dlatego w celu kompleksowej rozbudowy i wzmocnienia Krajowego Systemu Cyberbezpieczeństwa (KSC) w 2026 roku uchwalono nowelizację ustawy o krajowym systemie cyberbezpieczeństwa[1]. Przepisy te wprowadzają nowe mechanizmy zwiększające bezpieczeństwo usług i systemów, z których codziennie korzystają obywatele, przedsiębiorcy oraz instytucje publiczne, w tym w zakresie nadzoru. Przy czym obecnie obowiązują przewidziane prawem okresy dostosowawcze – wprowadzone m.in. w wyniku poprawek w Sejmie – co oznacza, że pełną skuteczność oraz kompletność narzędzi zarządczych i kontrolnych rząd uzyska po ich zakończeniu.

Równolegle przyjęto nową Strategię Cyberbezpieczeństwa RP[2], stanowiącą kluczowy dokument kierunkowy dla dalszego rozwoju KSC oraz wyznaczającą długofalowe cele w zakresie budowania odporności cyfrowej państwa.

Analiza ostatnich incydentów wykazała, że będące ich skutkiem wycieki danych w dużej mierze wynikają z niewystarczających zabezpieczeń i luk w procedurach po stronie prywatnych firm (np. zewnętrznych dostawców oprogramowania)

W trakcie wystąpienia incydentów cyberbezpieczeństwa państwo podjęło natychmiastowe i skoordynowane działania: zespół CSIRT NASK nawiązywał kontakt z podmiotem dotkniętym incydentem i podjął koordynację obsługi incydentu, prowadząc jednocześnie ciągły monitoring sieci oraz darknetu pod kątem potencjalnego upublicznienia danych.

W zależności od sektora, którego dotyczy incydenty, działania podejmują też inne CSIRT-y poziomu krajowego lub sektorowe, np. w przypadku incydentów dotyczących sektora ochrony zdrowia zespół CSIRT CeZ zrealizował prewencyjne i osłonowe działania w sektorze ochrony zdrowia obejmujące m.in. stopniową wymianę certyfikatów P1 w celu dodatkowego zabezpieczenia infrastruktury medycznej.

[1] Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz.U. z 2026 r. poz. 20 z późn. zm.) (ustawa o KSC)
[2] Uchwała nr 92 Rady Ministrów z dnia 10 marca 2026 r. w sprawie Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej (M.P. z 2026 r. poz. 309).

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 przypadku przestępstw związanych z incydentami cyberbezpieczeństwa Centralne Biuro Zwalczania Cyberprzestępczości (CBZC) prowadzi śledztwa w celu ustalenia przebiegu ataku, identyfikacji sprawców oraz zabezpieczenia materiału dowodowego, aby pociągnąć sprawców do odpowiedzialności.

Z kolei Połączone Centrum Operacyjne Cyberbezpieczeństwa (PCOC) zapewniło koordynację działań oraz stały kanał komunikacji w celu bieżącej wymiany informacji operacyjnych pomiędzy kluczowymi organami, służbami i ministerstwami.

Ad 2) Ile takich incydentów zgłoszono właściwym zespołom CSIRT w ostatnich trzech latach? Proszę o dane według lat i sektorów, z odrębnym wskazaniem administracji publicznej oraz przedsiębiorstw.

Liczba incydentów zgłaszanych i obsługiwanych przez zespoły reagowania na incydenty bezpieczeństwa komputerowego (CSIRT) poziomu krajowego[3] w latach 2023–2025 przedstawia się następująco:

- 2023 rok: 90 784 incydenty;
- 2024 rok: 111 660 incydentów (+23% r/r);
- 2025 rok: 272 941 incydentów (+144,4% r/r).

Szczegółowe dane znajdują się w Sprawozdaniach Pełnomocnika Rządu do Spraw Cyberbezpieczeństwa za 2023[4], 2024[5] oraz 2025[6] rok.

Ad 3) Jakie były największe potwierdzone wycieki według dostępnych jawnych danych? Ilu rekordów i — odrębnie — ilu unikalnych osób dotyczyły oraz jakie kategorie informacji ujawniono?

Ad 4) Czy istnieje sposób oceny liczby osób poszkodowanych, który ogranicza wielokrotne liczenie tych samych osób w różnych bazach i incydentach? Jeżeli nie, jak państwo ustala rzeczywistą skalę zagrożenia?

Ministerstwo Cyfryzacji nie prowadzi klasyfikacji incydentów według kryterium liczby osób, których dane dotyczą, nie są również klasyfikowane pod kątem kategorii przetwarzanych danych osobowych, w tym danych szczególnych kategorii, o których mowa w art. 9 RODO. Koordynacje obsługi incydentów prowadzą właściwe zespoły reagowania na incydenty bezpieczeństwa komputerowego (CSIRT).

Naruszenia dotyczące ochrony danych osobowych zgłaszane są zgodnie z unijnym rozporządzeniem 2016/679 (RODO) oraz ustawą o ochronie danych osobowych[7] - zgodnie z tą ustawą organem właściwym w sprawie ochrony danych osobowych jest Prezes Urzędu Ochrony Danych Osobowych (art. 34 ust. 1). Należy wyjaśnić, że Prezes UODO nie jest organem administracji rządowej podległym Radzie Ministrów, lecz niezależnym organem nadzorczym. Statystyki dotyczące naruszeń danych osobowych udostępnione są w sprawozdaniach z działalności Prezesa UODO[8]. W 2024 r. liczba zgłoszeń naruszeń to 14 842, a w 2025 r. to 22 435. Dane z 2026 r. nie są jeszcze dostępne.

Ponadto należy podkreślić, że w zakresie informowania o wyciekach danych, które stanowią naruszenie ochrony danych osobowych (w myśl RODO) i/lub incydent

[3] CSIRT NASK, CSIRT GOV, CSIRT MON.
[4] https://www.gov.pl/web/cyfryzacja/krajobraz-cyberprzestrzeni
[5] https://www.gov.pl/web/cyfryzacja/krajobraz-cyberprzestrzeni-roczne-sprawozdanie-o-cyberbezpieczenstwie
[6] https://www.gov.pl/web/baza-wiedzy/krajobraz-cyberprzestrzeni-sprawozdanie-o-stanie-cyberbezpieczenstwa-polski-za-rok-2025
[7] Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (Dz.U. z 2019 r. poz. 1781 z późn. zm.)
[8] https://uodo.gov.pl/pl/487/2279

cyberbezpieczeństwa (w myśl ustawy o KSC), bezpośrednio właściwe i odpowiedzialne są podmioty, których te zdarzenia dotyczą (tj. poszczególni administratorzy danych oraz podmioty przetwarzające dane).

Ministerstwo Cyfryzacji pozyskiwało informacje o skali wycieków na bazie informacji od zespołów CSIRT i służb w ramach PCOC. Ponadto niektóre z firm dotknięte incydentami przekazywały te informacje w swoich publicznych komunikatach.

Ad 5) W ilu przypadkach stwierdzono wykorzystanie wcześniej znanych podatności, niewykonanie zaleceń lub brak podstawowych zabezpieczeń? Jakie działania naprawcze podjęto w zakresie właściwości resortu?

Ministerstwo Cyfryzacji nie prowadzi ewidencji ani klasyfikacji incydentów wedle kryterium wykorzystania wcześniej znanych podatności, niewykonania zaleceń czy braku podstawowych zabezpieczeń. Analiza szczegółowych przyczyn incydentu, zastosowanych technologii oraz wykorzystanych podatności w systemach prywatnego podmiotu należy do kompetencji CSIRT-ów koordynujących obsługę danego incydentu, zgodnie z ich zadaniami określonymi w art. 26 ustawy o KSC.

W zakresie właściwości resortu cyfryzacji podjęto oraz przygotowano wielopoziomowe działania naprawcze i prewencyjne:

- Nowelizacja ustawy o KSC: wdrożono nowelizację ustawy o KSC wprowadzającą podwyższone wymogi w zakresie zarządzania ryzykiem, kontroli dostępu oraz bezpieczeństwa łańcucha dostaw. Należy przy tym uwzględnić ustawowe okresy przejściowe (dostosowawcze), które dają podmiotom czas na pełne dostosowanie systemów i procedur przed uzyskaniem pełnej egzekwowalności i stosowaniem sankcji.
- Rekomendacje Pełnomocnika Rządu ds. Cyberbezpieczeństwa w trybie art. 33 ust. 4a UKSC (dotyczące podatnych rozwiązań, które mogą prowadzić do powstania incydentu krytycznego), jak również na podstawie art. 67a ustawy o KSC (obejmujące dobre praktyki i zalecenia pozwalające podnieść poziom cyberbezpieczeństwa przez podmioty, które je zastosują). Wszystkie rekomendacje są dostępne w Biuletynie Informacji Publicznej Ministra Cyfryzacji[9].
- Komunikaty Pełnomocnika Rządu ds. Cyberbezpieczeństwa, np. komunikat Pełnomocnika Rządu do Spraw Cyberbezpieczeństwa z zaleceniami dla sektora ochrony zdrowia i innych podmiotów KSC[10].
- Realizowana jest bieżąca dystrybucja ostrzeżeń – zarówno bezpośrednio kierowanych do podmiotów krajowego systemu cyberbezpieczeństwa przez właściwe CSIRT-y, jak i publikowanych w internecie (cyber.gov.pl, moje.cert.pl).

Ad 6) Jakie konkretne rozwiązania techniczne, organizacyjne i prawne wdrożono, aby ograniczyć ryzyko masowych wycieków? W jaki sposób sprawdzono ich skuteczność?

Incydenty w firmie MyDr i u innych dostawców oprogramowania dla sektora ochrony zdrowia były przedmiotem prac Połączonego Centrum Operacyjnego Cyberbezpieczeństwa (PCOC), w ramach którego koordynowana działania instytucji państwa. Ponadto, w ramach realizacji zadań Pełnomocnika Rządu ds. Cyberbezpieczeństwa Ministerstwo Cyfryzacji na bieżąco koordynowało działania w ramach kanału komunikacji PCOC oraz w innych roboczych dwu- lub wielostronnych kontaktach pomiędzy właściwymi instytucjami.

[9] https://www.gov.pl/web/cyfryzacja/rekomendacje-pelnomocnika-rzadu-ds-cyberbezpieczenstwa
[10] https://www.gov.pl/web/cyfryzacja/komunikat-pelnomocnika-rzadu-do-spraw-cyberbezpieczenstwa--zalecenia-dla-sektora-ochrony-zdrowia-i-innych-podmiotow-ksc

Zespół CSIRT NASK realizował zadania w zakresie koordynacji obsługi incydentu (zgodnie ze swoimi zadaniami określonymi w art. 26 ustawy o KSC) zarówno w przypadku incydentu w firmie MyDr jak i u innych dostawców oprogramowania medycznego, którzy zgłosili incydent.

Natomiast wsparcie sektorowe zapewniał CSIRT CeZ. Warto podkreślić znaczenie jednego z działań CSIRT CeZ, które pomaga podnieść poziom cyberbezpieczeństwa u innych dostawców oprogramowania dla sektora ochrony zdrowia, tj. opracowanie zaleceń bezpieczeństwa dla dostawców rozwiązań IT dla ochrony zdrowia. Zalecenia obejmują m.in. obszary zarządzania bezpieczeństwem, ochrony danych, architektury systemów, zarządzania dostępami oraz monitorowania i reagowania na incydenty. Materiał został rozpowszechniony za pośrednictwem organizacji zrzeszających dostawców i producentów oprogramowania[11].

Równolegle czynności dochodzeniowo-śledcze prowadzi Centralne Biuro Zwalczania Cyberprzestępczości (CBZC) pod nadzorem Prokuratury, a Urząd Ochrony Danych Osobowych (UODO) prowadzi działania kontrolne w zakresie ochrony danych.

W zakresie rozwiązań systemowych należy podkreślić, że wdrożono nowelizację ustawy o KSC wprowadzającą podwyższone wymogi w zakresie zarządzania ryzykiem, kontroli dostępu oraz bezpieczeństwa łańcucha dostaw. Należy przy tym uwzględnić ustawowe okresy przejściowe (dostosowawcze), które dają podmiotom czas na pełne dostosowanie systemów i procedur przed uzyskaniem pełnej egzekwowalności i stosowaniem sankcji.

Wydawane są także rekomendacje Pełnomocnika Rządu ds. Cyberbezpieczeństwa w trybie art. 33 ust 4a ustawy o KSC (dotyczące podatnych rozwiązań, które mogą prowadzić do powstania incydentu krytycznego), jak również na podstawie art. 67a UKSC (obejmujące dobre praktyki i zalecenia pozwalające podnieść poziom cyberbezpieczeństwa przez podmioty, które je zastosują).

Opracowano także rozwiązania uszczelniające system ochrony danych pod nazwą „Cyber Piątka", wprowadzające minimalne wymagania technologiczne, wymóg natychmiastowego przekazywania informacji o naruszeniach.

Ad 7) Jakie są czasy wykrywania incydentów i przekazywania informacji właściwym instytucjom? Czy określono mierniki pozwalające wykrywać oraz usuwać opóźnienia?

Podmioty wchodzące w skład KSC, tj. obecnie ponad 70 tys. podmiotów kluczowych i podmiotów ważnych w 18 sektorach mają obowiązek zgłaszać do właściwego CSIRT incydenty poważne niezwłocznie, nie później niż w ciągu 72 godzin od momentu jego wykrycia (art. 11 ust. 1 pkt 4a ustawy o KSC).

Ad 8) Jak skoordynowano współpracę zespołów CSIRT, organów ścigania i Prezesa UODO, z poszanowaniem kompetencji oraz niezależności poszczególnych organów? Kto odpowiada za eliminowanie luk w wymianie informacji?

Sprawny przepływ informacji oraz uzgadnianie działań operacyjnych realizowane są poprzez posiedzenia oraz stały kanał komunikacji w ramach Połączonego Centrum Operacyjnego Cyberbezpieczeństwa (PCOC), działającego przy Pełnomocniku Rządu ds. Cyberbezpieczeństwa, o którym mowa w art. 62 ustawy o KSC, w skład którego wchodzą m.in. Ministerstwo Cyfryzacji, CSIRT, służby oraz organy właściwe ds. cyberbezpieczeństwa w poszczególnych sektorach.

[11] https://www.cez.gov.pl/pl/page/o-nas/aktualnosci/tylko-do-wrzesnia-2026-roku-wykryto-blisko-1400-incydentow-rosnie

Natomiast Prezes Urzędu Ochrony Danych Osobowych działa jako niezależny organ nadzorczy w sprawach ochrony danych osobowych. Niemniej Ministerstwo Cyfryzacji współpracuje w tym zakresie także z UODO.

Ad 9) Jakie kontrole i audyty bezpieczeństwa przeprowadzono w podmiotach pozostających we właściwości Ministra? Jaki odsetek zaleceń wykonano w terminie i jak zweryfikowano ich realizację?

Kontrole w obszarze cyberbezpieczeństwa są jednym z instrumentów nadzoru nad realizacją obowiązków wynikających z ustawy o KSC.

Zgodnie z obowiązującymi przepisami ustawy o KSC Minister Cyfryzacji jako organ właściwy do spraw cyberbezpieczeństwa dla sektorów określonych w art. 41 ustawy o KSC sprawuje nadzór nad podmiotami kluczowymi i podmiotami ważnymi w zakresie wykonywania przez nie obowiązków ustawowych. W ramach posiadanych kompetencji może przeprowadzać kontrole (art. 42 ust. 1 pkt 8 oraz art. 53 ust. 2 pkt 1 ustawy o KSC), w tym kontrole doraźne, w siedzibie kontrolowanego podmiotu, w miejscu wykonywania przez niego działalności gospodarczej lub zdalnie. W przypadku podmiotów kluczowych i podmiotów ważnych przepisy przewidują również możliwość zobowiązania podmiotu, w drodze decyzji, do przeprowadzenia audytu bezpieczeństwa, a także zlecenia oceny bezpieczeństwa systemu informacyjnego właściwemu zespołowi CSIRT.

Audyty bezpieczeństwa systemów informacyjnych są realizowane przez podmioty objęte ustawą o KSC, zgodnie z ciążącymi na nich obowiązkami. Minister Cyfryzacji jako organ właściwy do spraw cyberbezpieczeństwa nie zastępuje podmiotu w realizacji tych obowiązków. Może natomiast korzystać z przewidzianych prawem instrumentów nadzorczych, w tym żądać informacji i dokumentów niezbędnych do oceny zgodności z wymaganiami ustawy o KSC.

W odniesieniu do kontroli przeprowadzonych na podstawie przepisów ustawy o KSC obowiązujących przed nowelizacją informuję, że latach 2021-2026 Minister Cyfryzacji jako organ właściwy do spraw cyberbezpieczeństwa przeprowadził kontrole wszystkich operatorów usług kluczowych pozostających w jego właściwości. Łącznie przeprowadzono 9 kontroli. Wszystkie dotychczas wydane zalecenia pokontrolne zostały zrealizowane w wyznaczonych terminach.

Realizacja zaleceń była weryfikowana w ramach czynności podejmowanych przez Ministra Cyfryzacji jako organ właściwy do spraw cyberbezpieczeństwa, zgodnie z obowiązującymi przepisami prawa. Weryfikacja obejmowała analizę informacji przekazanych przez kontrolowane podmioty o sposobie wykonania zaleceń oraz dokumentów potwierdzających usunięcie stwierdzonych nieprawidłowości. Czynności te były prowadzone z uwzględnieniem właściwych przepisów ustawy o KSC oraz — w zakresie mającym zastosowanie do danej kontroli — przepisów regulujących kontrolę w administracji rządowej i kontrolę działalności gospodarczej przedsiębiorców.

Ad 10) Jaką pomoc może uzyskać obywatel, którego dane zostały ujawnione? Czy istnieje jedno, łatwo dostępne miejsce zapewniające informację o incydencie, możliwych działaniach ochronnych i sposobie zgłoszenia oszustwa?

Głównym, oficjalnym i łatwo dostępnym miejscem zapewniającym wiedzę oraz informacje z zakresu cyberbezpieczeństwa, bieżących incydentów i działań ochronnych jest portal cyber.gov.pl. Za pośrednictwem tego portalu obywatel może bezpośrednio zgłosić incydent bezpieczeństwa (np. podejrzaną stronę internetową, wiadomość SMS czy próbę oszustwa)[12].

[12] https://cyber.gov.pl/zg%C5%82o%C5%9B-incydent

Z kolei w przypadku zaistnienia przestępstwa sprawę należy zgłosić organom ścigania – Policji lub Prokuraturze[13].

Obywatele mogą zastrzec PESEL w prosty sposób zarówno w aplikacji mObywatel, jak i na stronie internetowej w domenie gov.pl[14] oraz w urzędzie gminy. Możliwość zastrzeżenia numeru PESEL to bezpłatna usługa publiczna. Chroni przed skutkami kradzieży tożsamości[15].

Portal bezpiecznedane.gov.pl umożliwia weryfikację, czy dany numer PESEL znalazł się w potwierdzonym wycieku. Obywatele mogą ponadto na portalu skorzystać z powiadomień mailowych o wyciekach. Na portalu bezpiecznedane.gov.pl udostępniane są również konkretne zalecenia i wytyczne bezpieczeństwa

Służby oraz zespoły CSIRT prowadzą ciągły monitoring sieci, forów przestępczych oraz darknetu, analizując potencjalne upublicznienie skradzionych baz i wyszukując anomalie oraz wskaźniki zagrożeń wskazujące na próby ich wykorzystania.

Ad 11) Jak oceniono skuteczność zastrzegania numeru PESEL wobec zagrożeń powstających po wyciekach? Jakie rodzaje nadużyć pozostają poza ochroną tego mechanizmu i jakie dodatkowe rozwiązania są planowane?

Usługa zastrzeżenia numeru PESEL to skuteczne, podstawowe narzędzie chroniące obywateli przed kradzieżą tożsamości oraz zaciąganiem nieuprawnionych zobowiązań finansowych. Mechanizm ten nie zabezpiecza jednak przed innymi konsekwencjami wycieków, takimi jak ujawnienie wrażliwych informacji medycznych czy wykorzystanie danych osobowych poza sektorem bankowym. W związku z tym planowane są dodatkowe rozwiązania, obejmujące m.in. powiadomienia w aplikacji mObywatel o zdarzeniach medycznych, alerty SMS o wyciekach oraz wdrożenie regulacji w ramach pakietu „Cyber Piątka".

Ad 12) Jakie działania przewidziano w przypadkach ujawnienia danych medycznych, danych dzieci oraz kopii dokumentów tożsamości? Czy pomoc uwzględnia charakter i długotrwałość zagrożeń związanych z tymi informacjami?

W przypadku naruszenia poufności danych dotyczących zdrowia administrator ma obowiązek bez zbędnej zwłoki zawiadomić osoby, których dane dotyczą, zgodnie z art. 34 RODO, natomiast w ramach pakietu legislacyjnego „Cyber Piątka" przewidziano wprowadzenie powiadomień w aplikacjach mObywatel i mojeIKP o zdarzeniach medycznych (np. wystawieniu recepty lub wizycie), co pozwala szybko wykryć próby wyłudzenia świadczeń, a także minimalne wymagania technologiczne dla podmiotów przetwarzających dane medyczne

Ad 13) Czy analizuje się przestępstwa wykorzystujące dane pochodzące z wcześniejszych wycieków? Jakie wnioski z tych analiz wykorzystano do ostrzegania obywateli i zapobiegania kolejnym oszustwom?

Służby oraz zespoły CSIRT prowadzą ciągły monitoring sieci, forów przestępczych oraz darknetu, analizując potencjalne upublicznienie skradzionych baz i wyszukując anomalie oraz wskaźniki zagrożeń wskazujące na próby ich wykorzystania.

Ad 14) Jakie braki kadrowe, techniczne i finansowe ograniczają zdolność instytucji pozostających we właściwości resortu do zapobiegania wyciekom i reagowania na nie? Jakie środki przeznaczono na usunięcie tych braków i jakie efekty uzyskano?

[13] https://www.gov.pl/web/gov/zglos-przestepstwo
[14] https://www.gov.pl/web/gov/zastrzez-swoj-numer-pesel-lub-cofnij-zastrzezenie
[15] https://www.gov.pl/web/cyfryzacja/chron-swoje-dane-z-mobywatelem-zastrzez-numer-pesel-w-aplikacji

Ad 15) Jakie mierzalne cele ograniczenia liczby poważnych incydentów, skrócenia czasu reakcji i poprawy ochrony poszkodowanych przyjęto na najbliższe miesiące? Kto odpowiada za ich wykonanie i kiedy zostaną przedstawione rezultaty?

Ministerstwo Cyfryzacji oraz Pełnomocnik Rządu do spraw Cyberbezpieczeństwa konsekwentnie realizują zadania związane z zapewnieniem skutecznego systemu cyberbezpieczeństwa państwa w oparciu o obowiązujące ramy prawne. Odpowiedzią na rosnącą skalę oraz dynamikę zagrożeń w cyberprzestrzeni było uchwalenie nowelizacji ustawy o KSC, która wprowadziła kompleksowe rozwiązania i podwyższone standardy ochrony. Należy jednak zaznaczyć, że w toku prac parlamentarnych – m.in. w wyniku poprawek przyjętych w Sejmie – do ustawy wprowadzono okresy dostosowawcze dla podmiotów objętych nowymi obowiązkami. W konsekwencji pełny wachlarz instrumentów prawnych, zarządczych i kontrolnych przewidzianych w znowelizowanych przepisach da rządowi pełne narzędzia do skutecznego egzekwowania bezpieczeństwa cyfrowego po zakończeniu tych okresów przejściowych.

Warto dodać, że Ministerstwo Cyfryzacji przekazuje corocznie dotację podmiotową na zapewnienie funkcjonowania CSIRT NASK, która na 2026 r. wyniosła 51 879 000,00 zł. Ponadto Ministerstwo Cyfryzacji w br. wsparło CSIRT NASK dotacją w wysokości 5 mln zł przeznaczoną na modernizację i rozbudowę ich infrastruktury teleinformatycznej.

Za funkcjonowanie CSIRT GOV odpowiada Agencja Bezpieczeństwa Wewnętrznego, natomiast za CSIRT MON odpowiada Ministerstwo Obrony Narodowej.

Należy również podkreślić, że Ministerstwo Cyfryzacji realizuje strategiczne projekty cyberbezpieczeństwa, które realnie przyczyniają się do ograniczenia liczby poważnych incydentów, skrócenia czasu reakcji i poprawy ochrony poszkodowanych, w szczególności:

1) System S46 to kluczowa system zarządzania cyberbezpieczeństwem, który stanowi fundament KSC. Głównym zadaniem systemu jest pełnienie roli scentralizowanego hubu, który umożliwia podmiotom KSC zgłaszanie incydentów, wymianę informacji i ostrzeganie.
2) Cyber.gov.pl to ogólnodostępny rządowy portal – nie wymaga logowania do przeglądania treści. Pełni rolę „Twojego Centrum Cyberbezpieczeństwa": dostarcza ostrzeżenia, komunikaty, aktualności oraz praktyczne materiały o cyberhigienie i reagowaniu na zagrożenia.
3) Bezpieczne dane - Jest to rządowy serwis: bezpiecznedane.gov.pl, który powstał z inicjatywy Ministerstwa Cyfryzacji jako narzędzie dla obywateli do sprawdzania, czy ich dane wyciekły w cyberatakach. Aktualnie w bazie znajdują się 22 historyczne wycieki. Jego główną funkcjonalnością jest wyszukiwarka, która pozwala użytkownikom na szybką weryfikację, czy ich dane, przeznaczone do uwierzytelniania w innych serwisach internetowych, nie znalazły się w puli wycieków.
4) AntyDDoS - Projekt Ministerstwa Cyfryzacji to państwowa usługa ochrony przed atakami typu Distributed Denial of Service, realizowana przez NASK PIB na zlecenie MC. Jego celem jest zapewnienie dostępności kluczowych usług publicznych nawet przy dużych atakach na infrastrukturę IT. System chroni centralnie ok. 80 instytucji kluczowych dla bezpieczeństwa państwa, w tym m.in. Siły Zbrojne RP.
5) CTI - Platforma Cyber Threat Intelligence służąca do dostarczania i analizy w czasie rzeczywistym informacji o zagrożeniach w cyberprzestrzeni. Ministerstwo Cyfryzacji zapewnia centralnie system rozpoznawania zagrożeń w cyberprzestrzeni (CTI) na potrzeby własne i 10 innych instytucji zapewaniających cyberbezpieczeństwo na poziomie krajowym i sektorowym

6) mSzyfr - Ministerstwo Cyfryzacji wspólnie z NASK PIB wdrożyło w tym roku pierwszy polski, bezpłatny szyfrowany komunikator mSzyfr dla administracji publicznej i podmiotów KSC.
7) SKR-Z - system niejawnej łączności mobilnej dla administracji publicznej.

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