Ministerstwo
Cyfryzacji

Sekretarz Stanu
Paweł Olszewski

BM.WP.057.83.2025
Warszawa, 09 czerwca 2025 r.

Szanowny Pan
Szymon Hołownia
Marszałek Sejmu RP

Dot. pisma z 6 maja br. Posła na Sejm RP Pana Janusza Cieszyńskiego w sprawie realizacji programu "Cyberbezpieczny Rząd" oraz przygotowania administracji publicznej do zagrożeń cybernetycznych (interpelacja nr 9577)

Szanowny Panie Marszałku,

poniżej przedstawiam odpowiedzi na zadane przez Posła pytania.

Ad 1) Czy Ministerstwo dysponuje analizą największych luk i deficytów w zakresie cyberbezpieczeństwa w administracji publicznej, a jeśli tak, jakie są jej główne wnioski?

Ministerstwo Cyfryzacji (MC) we współpracy z Pełnomocnikiem Rządu ds. Cyberbezpieczeństwa (Pełnomocnik) oraz zespołami CSIRT poziomu krajowego (CSIRT NASK, CSIRT GOV, CSIRT MON), opracowują bieżące analizy dotyczące cyberbezpieczeństwa administracji publicznej, w ramach których m.in. określane są luki bezpieczeństwa lub deficyty organizacyjnie i infrastrukturalne, w celu ich niwelowania.

Praca kluczowych instytucji publicznych w zakresie zapewniania i wzrostu poziomu cyberbezpieczeństwa RP jest koordynowana m.in. na poziomie strategiczno-politycznym w ramach prac Kolegium ds. Cyberbezpieczeństwa oraz operacyjno-technicznym w ramach Połączonego Centrum Operacyjnego Cyberbezpieczeństwa (PCOC). Współpraca i koordynacja mają charakter cykliczny co umożliwia bieżące reagowanie na identyfikowane luki i deficyty.

Ponadto wyniki analiz są regularnie aktualizowane i publikowane w formie corocznego Sprawozdania Pełnomocnika Rządu ds. Cyberbezpieczeństwa[1], raportów rocznych poszczególnych CSIRT-ów lub w formie np. Rekomendacji Pełnomocnika w sprawach wymagających szczególnej interwencji. Wnioski z realizowanych analiz stanowią podstawę do planowania i podejmowania działań na poziomach strategicznym oraz operacyjnym.

W 2024 r. w samym CSIRT NASK zgłoszono 609 900 potencjalnych naruszeń bezpieczeństwa, co oznacza wzrost o 64% względem 2023 r. W trzech CSIRT-ach poziomu krajowego potwierdzono 111 660 incydentów, w tym 57% więcej incydentów poważnych oraz 58% więcej incydentów w sektorze publicznym. Dane te potwierdzają alarmujący wzrost skali zagrożeń oraz konieczność intensyfikacji działań w zakresie prewencji, reagowania i budowy odporności cyfrowej.

Ad 2) Czy środki przewidziane w konkursie (350 mln zł) są wystarczające w stosunku do zidentyfikowanych potrzeb, czy też planowane są kolejne nabory lub inne formy wsparcia?

Po dokonaniu oceny wszystkich złożonych wniosków o objęcie projektów wsparciem grantowym, suma planowanych wydatków będzie niższa od całkowitej alokacji środków przewidzianej na niniejszy konkurs, wynoszącej 350 mln zł. Tym samym należy uznać, że poziom środków zaplanowanych w ramach wskazanego naboru okazał się być wystarczający w stosunku do zidentyfikowanych i zweryfikowanych potrzeb zgłoszonych

[1] Portal Gov.pl

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

ul. Królewska 27
00-060 Warszawa

przez uprawnione do tych środków podmioty. Aktualnie nie przewiduje się ogłaszania kolejnych naborów w ramach tej edycji programu, jak również nie planuje się uruchamiania dodatkowych form wsparcia dla naczelnych i centralnych organów administracji rządowej oraz wojewodów.

Ad 3) W jaki sposób Ministerstwo zamierza monitorować efektywność wykorzystania przyznanych grantów i realny wzrost poziomu cyberbezpieczeństwa w instytucjach objętych wsparciem?

Pomiar prowadzony będzie poprzez porównanie stanu początkowego oraz wzrostu poziomu cyberbezpieczeństwa wykazany w jednostce objętej wsparciem na zakończenie realizacji wsparcia. Ocena skuteczności zwiększenia odporności dokonywana będzie na podstawie danych przekazanych przez podmiot który otrzymał wsparcie. Przekazanie danych jest warunkiem niezbędnym do rozliczenia końcowego grantu.

Ad 4) Czy program obejmuje również mechanizmy dzielenia się wiedzą i dobrymi praktykami między beneficjentami, tak aby zapewnić synergię działań i optymalne wykorzystanie zasobów?

Działania w obszarze cyberbezpieczeństwa dotyczące kluczowych instytucji publicznych są koordynowane w ramach działań, o których mowa w odpowiedzi na pyt. 1.

Na potrzeby realizacji projektu „Cyberbezpieczny Rząd", w ramach dzielenia się wiedzą i dobrymi praktykami, organizowane są dla wnioskodawców m.in. cykliczne webinary, z których nagrania dostępne są na stronie naboru gov.pl. Na tej samej stronie publikowane są również odpowiedzi na najczęściej zadawane pytania przez wnioskodawców za pośrednictwem dedykowanego adresu mailowego (HelpDesk projektu) oraz infolinii telefonicznej, obsługiwanych przez specjalistów NASK-PIB. Ponadto w ramach powyższych działań promowane jest również wykorzystanie przez Grantobiorców wcześniejszych publikacji opracowanych na potrzeby realizowanego równolegle projektu pn. „Cyberbezpieczny Samorząd", w tym m.in. opracowania dotyczącego bezpiecznych zamówień publicznych w obszarze IT i cyberbezpieczeństwa, tj. vademecum bezpiecznych zakupów oprogramowania i rozwiązań IT[2]. Działania te służą ujednoliceniu standardów oraz promowaniu skutecznych rozwiązań wśród jednostek objętych wsparciem.

Ad 5) Jakie konkretne działania Ministerstwo podejmuje lub planuje podjąć w zakresie podnoszenia kompetencji kadr administracji publicznej w obszarze cyberbezpieczeństwa, poza wsparciem infrastrukturalnym?

W obliczu dynamicznie rozwijających się zagrożeń w cyberprzestrzeni oraz rosnącego znaczenia technologii informacyjnych, inwestycja w rozwijanie kompetencji pracowników instytucji publicznych oraz całego krajowego systemu cyberbezpieczeństwa, jest jednym z priorytetów Ministerstwa Cyfryzacji. Dlatego, Ministerstwo Cyfryzacji prowadzi kompleksowe działania szkoleniowe w dziedzinie cyberbezpieczeństwa, które stanowią niezwykle istotny element budowania świadomości i kompetencji w obszarze bezpieczeństwa online.

Szkolenia online dla podmiotów krajowego systemu cyberbezpieczeństwa

Prowadzone są bezpłatne szkolenia online adresowane kadrom krajowego systemu cyberbezpieczeństwa, których celem jest zwiększenie świadomości o cyberzagrożeniach oraz podnoszenie praktycznych umiejętności radzenia sobie w sytuacjach kryzysowych. Szkolenia realizowane są we współpracy z ekspertami z dziedziny cyberbezpieczeństwa z Państwowego Instytutu Badawczego NASK oraz partnerów technologicznych Programu Współpracy w Cyberbezpieczeństwie – PWCyber.

[2] https://www.gov.pl/web/cppc/Otwarty-webinar-cyberbezpieczny-samorzad---vademecum

Dotychczas, przeprowadzono 135 szkoleń, w których uczestniczyło prawie 88 tys. osób. Szkolenia cieszą się coraz większym zainteresowaniem – tylko w 2025 r. (na dzień 15.05) odbyło się już 14 szkoleń, w których uczestniczyło ponad 20 tys. osób. Informacje o szkoleniach, w tym harmonogram są dostępne w bazie wiedzy o cyberbezpieczeństwie na portalu gov.pl.

Specjalistyczne warsztaty

W ramach Programu PWCyber oprócz szkoleń online opisanych powyżej, organizowane są także specjalistyczne warsztaty oraz konferencje branżowe, w których udział biorą przedstawiciele podmiotów krajowego systemu cyberbezpieczeństwa, w tym pracownicy: administracji rządowej, krajowych Zespołów Reagowania na Incydenty Bezpieczeństwa Komputerowego (CSIRT) oraz Centrów Operacyjnych Bezpieczeństwa (Security Operation Center - SOC). Dotychczas odbyło się kilkanaście warsztatów, ćwiczeń i wizyt studyjnych zorganizowanych we współpracy z partnerami PWCyber, tj.: Amazon Web Services, IBM Polska, Sevenet, Elproma, Yubico, Omnilogy, Google Cloud Poland.

Szkolenia z cyberbezpieczeństwa dla najważniejszych osób w państwie – projekty SecureV

W ramach projektów prewencyjno-edukacyjnych (SecureV) realizowane są stacjonarne szkolenia adresowane do najważniejszych osób w państwie. Są to szkolenia realizowane indywidualnie (lub w małych grupach), a terminy i zakres merytoryczny szkoleń dostosowywane są do konkretnych potrzeb szkolonej osoby. Każda indywidualnie przeszkolona osoba zostaje wyposażona w uniwersalne narzędzia służące do silnego uwierzytelnienia.

Szkolenia w ramach projektu SecureV są również kontynuowane w 2025 r., a szkoleniami tymi objęci są: przedstawiciele władzy ustawodawczej i wykonawczej, w tym kadra zarządzająca i pracownicy organów administracji rządowej, przedstawiciele jednostek samorządu terytorialnego, pracownicy sądów i prokuratury, przedstawiciele i członkowie Krajowego Biura Wyborczego oraz organów wyborczych.

Rozwijanie inicjatyw szkoleniowych

Działania szkoleniowe będą rozwijane we współpracy z innymi resortami – będą to specjalistyczne szkolenia adresowane w szczególności dla personelu odpowiedzialnego za bezpieczeństwo sieci i systemów informatycznych. Celem MC jest zbudowanie zasobów kadrowych wyposażonych w specjalistyczną wiedzę z zakresu cyberbezpieczeństwa.

Ad 6) Czy Ministerstwo prowadzi systematyczne analizy zagrożeń cybernetycznych dla administracji publicznej, a jeśli tak, jakie są trendy w tym zakresie na przestrzeni ostatnich 2 - 3 lat?

MC prowadzi systematyczne, coroczne analizy cyberzagrożeń oraz wykorzystuje analizy realizowane m.in. przez zespoły CSIRT poziomu krajowego, jak również w ramach funkcjonowania KSC (opisane powyżej – ad 1).

Trendy obserwowane w latach 2022–2024:

- Wzrost liczby incydentów:
    - W 2023 r. odnotowano ponad 90 784 tys. incydentów – wzrost o ponad 100% rok do roku;
    - W 2024 r. liczba zgłoszeń wzrosła o 60%, osiągając 627 339 przypadków (CSIRT NASK i GOV), z czego 111 660 zostało potwierdzonych jako incydenty (wzrost o 23%).
- Wzrost liczby incydentów poważnych i w sektorze publicznym:

    - Liczba incydentów poważnych, które mogą zakłócić ciągłość działania instytucji, wzrosła o 57%;
    - Liczba incydentów dotyczących sektora publicznego wzrosła o 58%, co wskazuje na rosnącą presję na instytucje administracji państwowej i samorządowej.
- Dominacja ataków socjotechnicznych:
    - Najczęściej występujące zagrożenia to phishing, ataki socjotechniczne oraz próby włamań do systemów administracji publicznej;
    - Celem ataków są systemy poczty elektronicznej, VPN oraz serwisy przetwarzające dane obywateli.
- Zmiana charakteru zagrożeń:
    - Odnotowano spadek liczby incydentów związanych z wirusami i dezinformacją, przy jednoczesnym wzroście aktywności grup APT (Advanced Persistent Threats) oraz cyberprzestępców o charakterze zarobkowym;
    - Wzrosła liczba ataków ukierunkowanych na infrastrukturę krytyczną, w tym sektor energetyczny i transportowy.

Ad 7) Jak program „Cyberbezpieczny Rząd" wpisuje się w szerszą strategię cyberbezpieczeństwa państwa i współpracę międzynarodową w tym zakresie, szczególnie na forum Unii Europejskiej i NATO?

Konkurs grantowy, pn. „Cyberbezpieczny Rząd" jest projektem o charakterze ogólnokrajowym i jednym z kluczowych przedsięwzięć państwa w obszarze cyberbezpieczeństwa, służącym wzmocnieniu odporności na cyberzagrożenia w urzędach obsługujących naczelne i centralne organy administracji rządowej oraz wojewodów, jak również w urzędach podległych tym organom, obejmującą modernizację systemów zarządzania bezpieczeństwem informacji oraz rozbudowę infrastruktury cyberbezpieczeństwa. Projekt ten istotnie przyczyni się do podniesienia cyberbezpieczeństwa państwa, a tym samym wniesie wkład we wzmacnianie cyberbezpieczeństwa UE i NATO na gruncie krajowym. Jest to przykład efektywnego i prorozwojowego wykorzystania funduszy europejskich do skokowego wzrostu potencjału w danym obszarze funkcjonowania państwa, przyczyniając się zarazem do podniesienia poziomu bezpieczeństwa obywateli.

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