Ministerstwo
Cyfryzacji

Sekretarz Stanu
Paweł Olszewski

BM.WP.057.59.2025
Warszawa, 25 kwietnia 2025 r.

Szanowny Pan
Szymon Hołownia
Marszałek Sejmu RP

Dot. pisma z 2 kwietnia br. Posła na Sejm RP Pani Moniki Pawłowskiej w sprawie cyberataku na Szpital MSWiA w Krakowie (interpelacja nr 8831)

Szanowny Panie Marszałku,

poniżej przedstawiam odpowiedzi na zadane przez Posła pytania.

Ad 1) Jakie kroki zostały podjęte przez rząd, aby wzmocnić systemy ochrony przed cyberzagrożeniami w Polsce?

Ministerstwo Cyfryzacji (MC) oraz Pełnomocnik Rządu do Spraw Cyberbezpieczeństwa działający w ramach resortu cyfryzacji realizują szereg działań pozwalających podnieść poziom bezpieczeństwa systemów państwowych. Najważniejsze przedsięwzięcie realizowane przez Ministerstwo to:

- Projekt AntyDDoS: MC zapewnia centralnie osłonę przed atakami DDoS dla 76 instytucji, w tym dla Sił Zbrojnych RP i służb specjalnych;
- Bezpieczna łączność dla administracji publicznej: MC zapewnia bezpieczny komunikator na urządzenia służbowe dla administracji publicznej i podmiotów KSC, jak również mobilny system łączności niejawnej SKR-Z.
- System CTI: MC zapewnia centralnie system rozpoznawania zagrożeń w cyberprzestrzeni (CTI) na potrzeby własne i 8 innych instytucji odpowiedzialnych za bezpieczeństwo teleinformatyczne na poziomie krajowym.
- System S46 – MC zapewnia system IT do wymiany informacji i zgłaszania incydentów w ramach KSC (rozwój systemu i podłączanie nowych użytkowników – 39,7 mln zł z KPO).
- Fundusz Cyberbezpieczeństwa – MC zarządza Funduszem Cyberbezpieczeństwa, który pozwala zapewnić specjalistom ds. cyberbezpieczeństwa w sektorze publicznym wynagrodzenie konkurencyjne z sektorem prywatnym (w 2025 r. 355 mln zł).
- Projekt „Cyberbezpieczny Samorząd": celem projektu jest zwiększenie poziomu bezpieczeństwa informacji jednostek samorządu terytorialnego poprzez wzmacnianie odporności oraz zdolności do skutecznego zapobiegania i reagowania na incydenty w systemach informacyjnych. Umowy o wsparcie grantowe w ramach projektu, na łączną kwotę blisko 1,5 mld zł zostały podpisane z 2495 jednostkami samorządu terytorialnego (środki FERC - Fundusze Europejskie na Rozwój Cyfrowy). Oznacza to że wsparcie finansowe na wzmocnienie cyberbezpieczeństwa faktycznie otrzyma prawie 90 % wszystkich samorządów w kraju.
- Cyberbezpieczny Rząd: wsparcie cyberbezpieczeństwa naczelnych i centralnych organów administracji rządowej oraz wojewodów w obszarach kompetencji, technologii i organizacji (350 mln zł z KPO – Krajowy Plan Odbudowy).
- Utworzenie wojewódzkich zespołów specjalistów cyberbezpieczeństwa – wsparcie na modernizację i profesjonalizację zespołów policji, które będą wspierać

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

ul. Królewska 27
00-060 Warszawa

zaatakowane podmioty krajowego systemu cyberbezpieczeństwa w obsłudze incydentów i odzyskiwaniu danych (37,5 mln zł z KPO).

- Utworzenie Lokalnych Centrów Cyberbezpieczeństwa – wsparcie cyberbezpieczeństwa JST (270 mln zł z FERC).
- Szkolenia online dla podmiotów krajowego systemu cyberbezpieczeństwa, a także stacjonarne szkolenia z cyberbezpieczeństwa dla najważniejszych osób w państwie w ramach projektu SecureV.

Poza tym, w celu należytej koordynacji bieżącego zarządzania cyberbezpieczeństwem Ministerstwo Cyfryzacji organizuje spotkania w formacie Połączonego Centrum Operacyjnego Cyberbezpieczeństwa (PCOC). Funkcjonowanie PCOC umożliwia szybką wymianę informacji oraz reagowania na pojawiające się incydenty. W spotkaniach PCOC uczestniczą CSIRT-y poziomu krajowego oraz inne podmioty kluczowe dla bezpieczeństwa państwa.

Ponadto Pełnomocnik Rządu ds. Cyberbezpieczeństwa wydaje rekomendacje i komunikaty, których wdrożeniem przez podmioty KSC (w tym instytucje publiczne) pozwala minimalizować ryzyka związane z identyfikowanymi podatnościami oraz kampaniami w cyberprzestrzeni.

Ad 2) Czy rząd posiada opracowany kompleksowy plan ochrony przed cyberatakami, obejmujący wszystkie wrażliwe sektory, w tym służbę zdrowia, administrację publiczną oraz instytucje odpowiedzialne za bezpieczeństwo narodowe?

Robocza koordynacja angażująca wszystkie sektory jest realizowana przez PCOC.

Trwają prace nad nowelizacją ustawy o krajowym systemie cyberbezpieczeństwa mające na celu m.in. wdrożenie dyrektywy NIS2. Ustawa ma wprowadzić wiele mechanizmów umożliwiających znaczne zwiększenie cyberodporności Rzeczpospolitej Polskiej.

Ponadto, Ministerstwo Cyfryzacji opracowało projekt Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2025-2029. Obecnie jesteśmy po konsultacjach merytorycznych z właściwymi ministerstwami i innymi instytucjami poziomu krajowego. W następnym etapie planowane jest przekazanie projektu wraz z wnioskiem o wprowadzenie projektu dokumentu rządowego do wykazu prac legislacyjnych Rady Ministrów. Dokument został opracowany z przyjęciem podejścia ewolucyjnego w stosunku do obecnie obowiązującej Strategii, odpowiednio ją adaptując w szczególności:

- do zmian technologicznych (proliferacja technologii zarówno stanowiących zagrożenie, jaki dających możliwość podnoszenia poziomu bezpieczeństwa),
- prawnych (m.in. wdrożenie dyrektywy NIS 2),
- zmian w środowisku bezpieczeństwa międzynarodowego,
- zmian jakie zaszły w funkcjonowaniu krajowego systemu cyberbezpieczeństwa (KSC) i wniosków, jakie wyciągnęliśmy z funkcjonowania KSC.

Ad 3) Jakie działania są podejmowane w celu koordynacji współpracy pomiędzy służbami specjalnymi, agencjami rządowymi oraz sektorem prywatnym w zakresie ochrony przed cyberatakami?

W celu koordynacji bieżącego zarządzania cyberbezpieczeństwem MC organizuje spotkania w formacie Połączonego Centrum Operacyjnego Cyberbezpieczeństwa (PCOC). Jest to nieformalna platforma koordynacyjna Ministra Cyfryzacji. Wykorzystywana jest do szybkiej wymiany danych i informacji w zakresie zdarzeń w cyberprzestrzeni na poziomie krajowym. Pozwala na znaczące skrócenie czasu reakcji na zdarzenia i podniesienie poziomu cyberbezpieczeństwa RP, w szczególności w zakresie reagowania na pojawiające

się incydenty cyberbezpieczeństwa. PCOC jest cyklicznym, zwykle cotygodniowym gremium zrzeszającym przedstawicieli CSIRTów poziomu krajowego oraz innych instytucji o kluczowym znaczeniu dla prawidłowego funkcjonowania KSC, oraz innych sfer bezpieczeństwa państwa. Spotkania mają charakter niejawny. Tematyka poruszana w trakcie posiedzeń oscyluje wokół technicznych aspektów omawianych zdarzeń w cyberprzestrzeni.

Z kolei współpraca na poziomie strategiczno-politycznym realizowana jest w ramach Kolegium do Spraw Cyberbezpieczeństwa. Z upoważnienia Prezesa Rady Ministrów Kolegium przewodniczy Wicepremier i Minister Cyfryzacji, Pełnomocnik Rządu do Spraw Cyberbezpieczeństwa. Obsługę Kolegium zapewnia Ministerstwo Cyfryzacji.

Ad 4) Jakie środki prewencyjne są wdrażane w celu minimalizowania ryzyka przyszłych ataków na kluczowe instytucje publiczne i prywatne?

Działania Ministerstwa Cyfryzacji opisane w odpowiedzi na pyt nr 1 mają na celu zapobieganie i reagowanie, a więc są działaniami prewencyjnymi w zakresie odporności na cyberagrożenia.

Warto również wspomnieć o kampaniach edukacyjnych realizowanych przez Ministerstwo Cyfryzacji, a w szczególności:

- Szkolenia online dla podmiotów krajowego systemu cyberbezpieczeństwa: od 2020 r. prowadzone są bezpłatne szkolenia online dla podmiotów krajowego systemu cyberbezpieczeństwa. Dotychczas przeprowadzono 123 szkolenia, w których uczestniczyło ponad 66 tys. osób, a w tym:
    - szkolenia dla kadr podmiotów publicznych;
    - szkolenia dla operatorów usług kluczowych;
    - szkolenia dla użytkowników Systemów Rejestrów Państwowych;
    - szkolenia dla podmiotów publicznych wykonujących działalność leczniczą.
- Szkolenie e-learningowe: w 2023 r. uruchomione zostało szkolenie e-learningowe pn. „Podstawowe zasady cyberbezpieczeństwa oraz zasady bezpieczeństwa stacji roboczych SRP", które jest dostępne na platformie https://szkolenia.obywatel.gov.pl/ . Od 2023 r. szkolenie odbyło ponad 1700 pracowników administracji publicznej.
- Projekty SecureV: Początkowo projekt SecureV obejmował wyłącznie parlamentarzystów i kadrę kierowniczą administracji centralnej. Jednak z uwagi na dynamiczną sytuację w cyberprzestrzeni oraz duże zainteresowanie szkoleniami, kolejne edycje projektu uwzględniają coraz większą grupę odbiorców. W 2023 r. szkoleniami objęci byli: parlamentarzyści, kadra kierownicza administracji rządowej (centralnej i terenowej) i samorządowej, przedstawiciele Krajowego Biura Wyborczego oraz pracownicy Podstawowej Opieki Zdrowotnej. Tylko w 2024 r. przeszkolono blisko 5 tys. osób.
- Projekt Cyberlekcje - Ministerstwo Cyfryzacji wspólnie z NASK-PIB realizuje projekt adresowany do nauczycieli i pedagogów, chcących podczas swoich zajęć przekazywać dzieciom i młodzieży zasady i wskazówki dotyczące bezpiecznego poruszania się w Internecie. W ramach projektu Cyber lekcje powstało 18 gotowych scenariuszy zajęć lekcyjnych o cyberbezpieczeństwie skierowanych do różnych grup wiekowych uczniów w szkołach podstawowych i ponadpodstawowych. W ramach projektu powstały również dodatkowe materiały, jak: infografiki, prezentacje, animacje oraz filmy z ekspertami, które wraz z scenariuszami są udostępnione dla wszystkich zainteresowanych w powszechnie dostępnej bazie wiedzy cyberbezpieczeństwa na portalu gov.pl w zakładce CyberEdukacja, a także na Zintegrowanej Platformie

Edukacyjnej, narzędziu rekomendowanym przez Ministerstwo Edukacji Narodowej. W 2024 r. zrealizowany został pilotaż w ramach którego przeprowadzono m.in. stacjonarne szkolenia dla kadry pedagogicznej.

- Konkurs CyberWizards 2024 – International Cyber Camp: Ministerstwo Cyfryzacji we współpracy z Ministerstwem Edukacji Narodowej zorganizował nabór do CyberWizards International Camp. Nagrodą był wyjazd na International Cyber Camp w Estonii dla zwycięskiej drużyny. Wysłanie do Estonii polskiej drużyny dziewcząt stanowi jeden z wielu elementów promujących od najmłodszych lat karierę kobiet w branży cyberbezpieczeństwa.

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