Ministerstwo
Cyfryzacji

Sekretarz Stanu
Michał Gramatyka

BM.WP.057.7.2025
Warszawa, 15 kwietnia 2025 r.

Szanowny Pan
Szymon Hołownia
Marszałek Sejmu RP

Dot. pisma z 15 stycznia br. Posła na Sejm RP Pana Pawła Jabłońskiego w sprawie cyberataku w czasie wyborów parlamentarnych (interpelacja nr 7330)

Szanowny Panie Marszałku,

poniżej przedstawiam odpowiedzi na zadane przez Posła pytania.

Ad 1) Które ugrupowanie polityczne zostało, zgodnie ze słowami Pana Ministra, zaatakowane w trakcie ostatnich wyborów parlamentarnych w ramach opisanej „gigantycznej akcji pochodzącej ze wschodu"?

Przed wyborami parlamentarnymi 15 października 2023 r. doszło do zakrojonej na szeroką skalę akcji dezinformacyjnej, w ramach której rozesłano ok. 187 tys. SMS-ów zawierających agitację wyborczą o treści: "GlosujNaPiS! Przywrocilismy seniorom prawo do godnej starosci i zrobimy tez pogrzeby emerytow za darmo". Doszło, również do przejęcia ekranów w 20 centrach handlowych na terenie kraju. Wyświetlane na nich były treści z wizerunkiem polityków Prawa i Sprawiedliwości.

Ad 2) Z jakiego wschodniego kraju pochodził atak?

Organem właściwym do odpowiedzi to pytanie jest Prokuratura prowadzącą śledztwo bądź Agencja Bezpieczeństwa Wewnętrznego.

Ad 3) Jakie działania podjął rząd w tej sprawie?

Zarządzeniem nr 55 Prezesa Rady Ministrów została powołana komisja ds. wpływów rosyjskich i białoruskich na bezpieczeństwo wewnętrzne i interesy Rzeczypospolitej Polskiej w latach 2004–2024.

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

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

ul. Królewska 27
00-060 Warszawa

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 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 i Rządowe Centrum Cyberbezpieczeństwa (RCB) organizują 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. W procedowanej nowelizacji ustawy o KSC planowane jest sformalizowanie działania PCOC (faktycznie funkcjonującego od 2022 r.).

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.

Z wyrazami szacunku
Michał Gramatyka
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