



Ministerstwo Cyfryzacji

Sekretarz Stanu
Paweł Olszewski

BM.WP.057.8.2025
Warszawa, 11 lutego 2025 r.

**Szanowny Pan
Szymon Hołownia
Marszałek Sejmu RP**

Dot. pisma z 15 stycznia br. Pośła na Sejm RP Pani Bożeny Lisowskiej w sprawie ataków
hakerskich w cyberprzestrzeni (zapytanie nr 2110)

Szanowny Panie Marszałku,

poniżej przedstawiam odpowiedź na zadane przez Panią Poseł pytanie będące we właściwości
Ministra Cyfryzacji.

**Ad 1) Jakie środki zastosuje Ministerstwo Cyfryzacji w celu zabezpieczenia infrastruktury
sieciowej instytucji publicznych?**

Ministerstwo Cyfryzacji (MC) prowadzi szereg czynności wpływających na wzrost poziomu
bezpieczeństwa infrastruktury sieciowej zarówno instytucji publicznych, jak i podmiotów
prywatnych, w zakresie monitorowania i przeciwdziałania zagrożeniom w cyberprzestrzeni. Do
kluczowy działań zaliczyć można:

- Rozwój krajowego systemu cyberbezpieczeństwa (KSC), poprzez aktualizację przepisów prawa, w tym ustawy o krajowym systemie cyberbezpieczeństwa¹. Zwiększy to efektywność systemu ochrony przed cyberzagrożeniami i dostosuje prawo krajowe do dyrektywy europejskiej NIS2. Omawiana ustawa zapewni szereg narzędzi wpływających na wzrost cyberbezpieczeństwa Polski. Do ww. rozwiązań zaliczyć można np. instytucje dostawcy wysokiego ryzyka (HRV), utworzenie CSIRTów (zespoły reagowania na incydenty komputerowe) sektorowych wspierających przeciwdziałanie i niwelowanie skutków cyberataków, jak i wprowadzenie nowych zasad nadzoru i kontroli stanu cyberbezpieczeństwa podmiotów kluczowych oraz ważnych dla bezpieczeństwa i stabilności RP do których zaliczyć można firmy z sektorów m.in. telekomunikacyjnego, energetycznego, bankowego;
- System AntyDDoS – MC (za pośrednictwem Naukowej i Akademickiej Sieci Komputerowej) zapewnia centralnie ochronę przed atakami DDoS dla 76 instytucji, w tym dla Sił Zbrojnych RP i służb specjalnych;
- Zakup Platformy Cyber Threat Intelligence (CTI) – MC zapewnia centralnie system rozpoznawania zagrożeń w cyberprzestrzeni na potrzeby własne i 8 innych instytucji odpowiedzialnych za bezpieczeństwo teleinformatyczne na poziomie krajowym, w tym dla wojska i służb specjalnych. Dane z CSIRTów poziomu krajowego są analizowane zarówno pod kątem ilościowym, jak również sektora którego incydent dotyczył i na tej podstawie sporządzane są analizy i zestawienia kierowane m.in. do Pełnomocnika Rządu ds. Cyberbezpieczeństwa;
- System S46 – MC zapewnia i rozwija system IT, który odpowiada i wspiera zgłaszanie i obsługę incydentów bezpieczeństwa, wymianę informacji oraz wpływa na współpracę pomiędzy podmiotami KSC, a także umożliwia szacowanie ryzyka na poziomie krajowym (system w stałym rozwoju, następuje podłączanie nowych użytkowników);
- Bezpieczna łączność – MC zapewnia bezpieczny komunikator na urządzenia służbowe dla administracji publicznej i podmiotów KSC, jak również mobilny system łączności niejawnego SKR-Z ;

¹ Ustawa z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz.U. z 2024 r. poz. 1077 z późn. zm)

- Fundusz Cyberbezpieczeństwa – MC zarządza Funduszem Cyberbezpieczeństwa, który umożliwia zapewnienie Świadczenia Teleinformatycznego wpływającego na zachowanie rynkowych płac dla specjalistów ds. cyberbezpieczeństwa w sektorze publicznym. Powyższe bezpośrednio wpływa na jakość zasobów ludzkich (w tym posiadaną specjalistyczną i unikalną wiedzę) w zakresie bezpieczeństwa teleinformatycznego podmiotów publicznych;
- Centrum Cyberbezpieczeństwa NASK – MC wspiera jego budowę i organizację. Podmiot będzie kluczową instytucją wpływającą na poziom bezpieczeństwa cyfrowego RP;
- Program Cyberbezpieczny Samorząd – projekt wspierający podnoszenie cyberbezpieczeństwa w jednostek samorządu terytorialnego (JST) poprzez dotowanie zakupu elementów zaawansowanej infrastruktury bezpieczeństwa;
- Program Cyberbezpieczny Rząd – wsparcie cyberbezpieczeństwa naczelnych i centralnych organów administracji rządowej oraz wojewodów w obszarach kompetencji, technologii i organizacji;
- Projekt Sektorowych zespołów CSIRT – wsparcie organów właściwych w poszczególnych sektorach w tworzeniu i rozbudowie sektorowych zespołów CSIRT;
- 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;
- Utworzenie Lokalnych Centrów Cyberbezpieczeństwa – wsparcie cyberbezpieczeństwa JST;
- Szkolenia online dla podmiotów krajowego systemu cyberbezpieczeństwa, w tym projekt SecureV – szkolenia z cyberbezpieczeństwa dla najważniejszych osób w państwie;
- Organizacja i funkcjonowanie Połączonego Centrum Operacyjnego Cyberbezpieczeństwa (PCOC) – MC utrzymuje stałe kanały łączności między podmiotami KSC w zakresie wymiany informacji o zagrożeniach w cyberprzestrzeni RP. W ramach PCOC odbywa się współpraca między CSIRTami i komórkami bezpieczeństwa instytucji biorących udział w cyklicznych spotkaniach. Jest to miejsce koordynacji i wymiany informacji między podmiotami tworzącymi KSC, w szczególności na poziomie operacyjno-technicznym;
- Wzmacnianie współpracy między sektorem prywatnym i publicznym w zakresie ochrony systemów teleinformatycznych oraz danych obywateli RP. Należy wskazać współpracę pomiędzy krajowymi organami KSC odpowiedzialnymi za cyberbezpieczeństwo kraju w poszczególnych sektorach z podmiotami sektora prywatnego w zakresie przyjmowania zgłoszeń o podejrzanym aktywności, wrogich działaniach wymierzonych w infrastrukturę krytyczną państwa, incydentach związanych z wyciekami danych.

Z wyrazami szacunku

Paweł Olszewski

Sekretarz Stanu

/dokument podpisany elektronicznie/

Do wiadomości:

Kancelaria Prezesa Rady Ministrów - Departament Spraw Parlamentarnych