Ministerstwo
Cyfryzacji

Sekretarz Stanu
Paweł Olszewski

BM.WP.057.57.2025
Warszawa, 15 kwietnia 2025 r.

Szanowny Pan
Szymon Hołownia
Marszałek Sejmu RP

Dot. pisma z 19 marca br. Posła na Sejm RP Pana Janusza Cieszyńskiego w sprawie cyberataku na Polską Agencję Kosmiczną oraz działań rządu w zakresie cyberbezpieczeństwa (interpelacja nr 8711)

Szanowny Panie Marszałku,

poniżej przedstawiam odpowiedzi na zadane przez Posła pytania będące we właściwości Ministra Cyfryzacji.

Ad 1) Jakie były przyczyny i potencjalne skutki cyberataku na Polską Agencję Kosmiczną? Czy znane są już szczegóły dotyczące sprawców tego incydentu?

Skutkiem cyberataku było uzyskanie dostępu przez atakującego do infrastruktury Polskiej Agencji Kosmicznej (dalej: POLSA). W kwestii przyczyn ataku na systemy POLSA, w chwili obecnej CSIRT NASK jest nadal w trakcie analizy. Tym samym, zespoły CSIRT poziomu krajowego nie są aktualnie w posiadaniu oficjalnych danych pozwalających na ostateczną atrybucję ataku.

Ad 2) Jakie dane lub systemy mogły zostać naruszone w wyniku ataku na POLSA, a tym samym jakie mogą być konsekwencje dla polskiego przemysłu kosmicznego i bezpieczeństwa narodowego?

Ministerstwo Cyfryzacji nie jest właściwe do formułowania oceny w zakresie konsekwencji zdarzenia dla polskiego przemysłu kosmicznego czy bezpieczeństwa narodowego.

Ad 3) Jakie konkretne środki zostały podjęte w celu zabezpieczenia infrastruktury teleinformatycznej POLSA po wykryciu ataku oraz jak długo potrwa przywrócenie pełnej operacyjności Agencji?

CSIRT NASK w ramach swojej aktywności podjął standardowe działania wchodzące w zakres wsparcia POLSA w obsłudze incydentu, w szczególności, wraz z CSIRT MON przystąpił do analizy okoliczności incydentu. POLSA otrzymała dalsze rekomendacje właśnie ze strony CSIRT MON w kwestii zabezpieczenia środowiska teleinformatycznego. Przywrócenie pełnej operacyjności systemów jest w zakresie właściwości POLSA.

Ad 4) W jaki sposób rząd planuje wzmocnić ochronę kluczowych instytucji państwowych, takich jak POLSA, w obliczu rosnącej liczby cyberataków, zwłaszcza w kontekście napiętej sytuacji geopolitycznej?

Rząd prowadzi intensywne działania w zakresie zapewnienia cyberbezpieczeństwa podmiotom odpowiedzialnym za funkcjonowanie państwa, w szczególności administracji publicznej, zarówno rządowej jak i samorządowej. Jednym z przedsięwzięć za pomocą których realizowane jest wzmacnianie ochrony kluczowych instytucji państwowych w obliczu rosnącej liczby cyberataków jest współfinansowany ze środków KPO (Inwestycja C3.1.1), konkurs grantowy pn. „Cyberbezpieczny Rząd”. Jest to przedsięwzięcie, którego celem jest wsparcie administracji rządowej w modernizacji i rozbudowie infrastruktury

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

ul. Królewska 27
00-060 Warszawa

cyberbezpieczeństwa w sieciach IT. Wsparcie skierowane jest do podmiotów krajowego systemu cyberbezpieczeństwa, o których mowa w ustawie o krajowym systemie cyberbezpieczeństwa[1], takich jak naczelne lub centralne organy administracji rządowej oraz wojewodowie. Urzędy obsługujące te organy, wraz z jednostkami im podległymi, są uprawnione do otrzymania grantów na poprawę odporności na cyberzagrożenia, w tym sfinansowanie modernizacji systemu zarządzania bezpieczeństwem informacji oraz rozbudowy infrastruktury cyberbezpieczeństwa. Celem projektu „Cyberbezpieczny Rząd" jest zwiększenie poziomu bezpieczeństwa informacji poprzez wzmacnianie odporności na incydenty w naczelnych i centralnych instytucjach państwowych. Wsparcie to obejmuje trzy kluczowe obszary cyberbezpieczeństwa, tj.: obszar organizacji, technologii i kompetencji. Stopień intensywności wsparcia w każdym z tych obszarów jest zależny od konkretnych potrzeb każdej organizacji. Budżet całego konkursu wynosi 350 mln zł, a wysokość grantu dla jednego wnioskodawcy może wynosić maksymalnie 10 mln zł netto. Nabór wniosków o granty w ramach projektu „Cyberbezpieczny Rząd" został uruchomiony w dniu 28 lutego 2025 r., zgodnie z komunikatem dostępnym na stronie gov.pl. Wnioski te mogły być składane do dnia 31 marca 2025 r. do godz. 16:00. Warunki naboru, w tym regulamin konkursu zostały opublikowane na stronie Centrum Projektów Polska Cyfrowa.

Ad 5) Czy incydent z niewłaściwą komunikacją w sprawie szczątków rakiety Falcon 9 oraz obecny cyberatak wskazują na szersze problemy systemowe w zarządzaniu cyberbezpieczeństwem i koordynacją między instytucjami rządowymi? Jeśli tak, jakie kroki zostaną podjęte, aby je rozwiązać?

Komunikacja dot. szczątków rakiety Falcon 9 nie jest związana z cyberbezpieczeństwem. 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;
- 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.

[1] Art. 4 pkt 7 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz.U. 2024 poz. 1077)

- 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 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. 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 wdrożenie przez podmioty KSC (w tym instytucje publiczne) pozwala minimalizować ryzyka związane z identyfikowanymi podatnościami oraz kampaniami w cyberprzestrzeni.

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