Ministerstwo
Cyfryzacji

Sekretarz Stanu
Paweł Olszewski

BM.WP.057.50.2025
Warszawa, 31 marca 2025 r.

Szanowny Pan
Szymon Hołownia
Marszałek Sejmu RP

Dot. pisma z 11 marca br. Posła na Sejm RP Pana Filipa Kaczyńskiego w sprawie ataku hakerskiego na Polską Agencję Kosmiczną (interpelacja nr 8511)

Szanowny Panie Marszałku,

poniżej przedstawiam odpowiedzi na zadane przez Posła pytania.

Ad 1) Kiedy zakończą się prace nad obiecywaną od czerwca 2024 roku "Cybertarczą"?

Zgodnie z komunikatem opublikowanym na stronie Ministerstwa Cyfryzacji w dniu 21.06.2024 r. „Cybertarcza Rzeczypospolitej Polskiej – założenia realizacyjne programu" (dostępnym pod linkiem https://www.gov.pl/web/cyfryzacja/cybertarcza-rzeczypospolitej-polskiej--zalozenia-realizacyjne-programu), Cybertarcza RP to pakiet działań realizowanych lub koordynowanych przez Ministra Cyfryzacji oraz przyszłe zadania do realizacji w najbliższych latach, aby zwiększać odporność cyberbezpieczeństwa Polski. Działania te odpowiadają na bieżące potrzeby adresowane m.in. w nowelizowanej ustawie o krajowym systemie cyberbezpieczeństwa, która implementuje do polskiego porządku prawnego dyrektywę NIS 2. Mowa tutaj m.in. o już uruchomionych jak i planowanych do uruchomienia projektach współfinansowanych z programu Fundusze Europejskie na Rozwój Cyfrowy 2021-2027 (FERC) oraz w ramach Krajowego Planu Odbudowy i Zwiększania Odporności (KPO), wymienionych w ww. komunikacie. Zauważyć jednak należy, że lista tych inicjatyw nie jest listą zamkniętą i będzie sukcesywnie poszerzana o nowe przedsięwzięcia.

Ad 2) Czy Ministerstwo Cyfryzacji posiada fundusze na utworzenie skutecznego programu ochrony instytucji państwowych przed atakami hakerskimi?

Jednym z projektów współfinansowanych ze środków KPO (Inwestycja C3.1.1), o których mowa w odpowiedzi na pytanie nr 1, dotyczące „Cybertarczy RP", jest konkurs grantowy pn. „Cyberbezpieczny Rząd". Jest to przedsięwzięcie, którego celem jest wsparcie administracji rządowej w modernizacji i rozbudowie infrastruktury cyberbezpieczeństwa w sieciach IT. Wsparcie skierowane jest do podmiotów krajowego systemu cyberbezpieczeństwa, o których mowa w art. 4 pkt 7 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa, 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

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

ul. Królewska 27
00-060 Warszawa

„Cyberbezpieczny Rząd" został uruchomiony w dniu 28 lutego 2025 r., zgodnie z komunikatem dostępnym na stronie https://www.gov.pl/web/cyfryzacja/350-mln-zl-na-wzmocnienie-cyberbezpieczenstwa-administracji-rzadowej. Wnioski te mogą być składane do dnia 31 marca 2025 r. do godz. 16:00. Warunki naboru, w tym regulamin konkursu zostały opublikowane na stronie naboru https://www.gov.pl/web/cppc/inwestycja-c-311-konkurs-grantowy-cyberbezpieczny-rzad.

Ad 3) Czy w Ministerstwie Cyfryzacji prowadzone są analizy dot. problemów wynikających z wprowadzenia systemów opartych na AI dla cyberbezpieczeństwa?

Ministerstwo Cyfryzacji (MC) prowadzi analizy dotyczące problemów wynikających z wprowadzania rozwiązań opartych na sztucznej inteligencji (AI) dla cyberbezpieczeństwa. Wnioski z nich płynące będą zaimplementowane i upublicznione w tworzonej Strategii Cyberbezpieczeństwa Rzeczypospolitej Polski na lata 2025-2029 oraz zostały zamieszczone w szeregu publikacji na stronie www.gov.pl, do których zaliczyć należy m.in.:

- „*Generatywna sztuczna inteligencja w służbie pracowników administracji publicznej - pierwsze kroki*" (więcej informacji pod adresem: https://www.gov.pl/web/ai/generatywna-sztuczna-inteligencja-w-sluzbie-pracownikow-administracji-publicznej---pierwsze-kroki2);
- „*Pułapki związane z wykorzystywaniem sztucznej inteligencji – jak unikać zagrożeń*?" (więcej informacji pod adresem: https://www.gov.pl/web/baza-wiedzy/pulapki-zwiazane-z-wykorzystywaniem-sztucznej-inteligencji--jak-unikac-zagrozen);
- „*Sztuczna Inteligencja i cyberbezpieczeństwo*" (więcej informacji pod adresem: https://www.gov.pl/web/baza-wiedzy/sztuczna-inteligencja-i-cyberbezpieczenstwo).

Dodatkowo Ministerstwo wspiera, tworzy i promuje własne suwerenne, bezpieczne rozwiązania wykorzystujące modele AI. Przykładem takiego narzędzia jest „PLLuM". Został on opracowany ze środków publicznych przez krajowych specjalistów, a następnie bezpłatnie upubliczniony użytkownikom celem umożliwienia przetwarzanie danych zgodnie z obowiązującymi przepisami (model jest dostępny pod adresem: https://huggingface.co/CYFRAGOVPL).

Należy również zauważyć, że w ramach polskiego prawa kwestie związane z oceną bezpieczeństwa systemów informatycznych, w tym opartych na AI, reguluje ustawa o krajowym systemie cyberbezpieczeństwa (KSC) – mechanizm rekomendacji Pełnomocnika Rządu do Spraw Cyberbezpieczeństwa (art. 33 ustawy o KSC) pozwala na ocenę wpływu oprogramowania na bezpieczeństwo publiczne lub interes państwa. Dotychczas mechanizm ten, nie był wykorzystywany w zakresie rekomendacji dot. konkretnych rozwiązań opartych o AI ze względu na brak obiektywnych przesłanek.

Ponadto należy pamiętać, iż bieżąca koordynacja działań w zakresie cyberbezpieczeństwa, w tym analiza ryzyka i wymiana informacji o incydentach bezpieczeństwa teleinformatycznego, realizowana jest przez Połączone Centrum Operacyjne Cyberbezpieczeństwa (PCOC) oraz zespoły CSIRT NASK, CSIRT GOV i CSIRT MON, zgodnie z art. 26 ust. 3 pkt 1-2 ustawy o KSC.

Z wyrazami szacunku

Paweł Olszewski
Sekretarz Stanu
/dokument podpisany elektronicznie/

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

ul. Królewska 27
00-060 Warszawa

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