Ministerstwo
Cyfryzacji

Sekretarz Stanu
Paweł Olszewski

BM.WP.057.42.2024
Warszawa, 15 lipca 2024 r.

Szanowny Pan
Szymon Hołownia
Marszałek Sejmu RP

Dot. pisma z 10 czerwca br. Posła na Sejm RP Pana Daniela Milewskiego w sprawie wprowadzenia ogólnokrajowej tarczy cyberprzestrzennej (interpelacja nr 3226)

Szanowny Panie Marszałku,

poniżej przedstawiam odpowiedzi na zadane przez Posła pytania.

Ad 1) Jakie konkretne kroki planuje rząd, aby wprowadzić ogólnokrajową ochronę programów komputerowych i baz danych w kontekście systemu ochrony własności przemysłowej?

Ad 2) W jaki sposób rząd zamierza zapewnić spójność tych rozwiązań na poziomie krajowym i UE?

Ad 4) Jakie przepisy prawne i regulacje są planowane, aby skutecznie chronić własność przemysłową w kontekście dynamicznego postępu technologicznego?

Ad 5) Jakie są plany rządu dotyczące współpracy z innymi krajami UE w zakresie ochrony programów komputerowych i baz danych?

Ad 7) Jakie mechanizmy zostaną wprowadzone, aby zapewnić skuteczność i efektywność nowego systemu ochrony własności przemysłowej?

Uprzejmie informuje, że ww. pytania są poza właściwością Ministra Cyfryzacji, właściwym do udzielenia odpowiedzi jest Minister Rozwoju i Technologii.

Ad 3) Jakie działania są podejmowane, aby monitorować i przeciwdziałać zagrożeniom cybernetycznym, które mogą wpływać na bezpieczeństwo programów komputerowych i baz danych?

W zakresie monitorowania i przeciwdziałania zagrożeniom w cyberprzestrzeni Minister Cyfryzacji wspiera rozwój systemu S46, który odpowiada za zgłaszanie i obsługę incydentów, wymianę informacji i współpracę pomiędzy podmiotami KSC, a także szacowanie ryzyka, czyli całościowego procesu identyfikacji, analizy i oceny ryzka na poziomie krajowym. Dane z CSIRT-ów 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.

Ministerstwo Cyfryzacji utrzymuje stałe kanały łączności między podmiotami KSC w zakresie wymiany informacji o zagrożeniach w cyberprzestrzeni RP, np. w ramach Projektu Połączonego Centrum Operacyjnego Cyberbezpieczeństwa (PCOC), współpracy między CSIRT-ami i komórkami bezpieczeństwa instytucji biorących udział w cyklicznych spotkaniach.

W zakresie utrzymania dostępności usług Ministerstwo Cyfryzacji zleciło NASK PIB realizację projektu AntyDDoS, zapewniającego ochronę przed tego typu atakom klilkudziesięciu podmiotom, które zawnioskowały o przyłączenie do systemu.

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

ul. Królewska 27
00-060 Warszawa

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 podejrzanej aktywności, wrogich działaniach wymierzonych w infrastrukturę krytyczną państwa, incydentach związanych z wyciekami danych.

Ad 6) Czy istnieją konkretne terminy i etapy realizacji planu wprowadzenia ogólnokrajowej ochrony cyberprzestrzennej i jakie są oczekiwane rezultaty tych działań?

W aspekcie ogólnokrajowej ochrony cyberprzestrzeni odwołać się należy do elementów kluczowych wskazanych w Strategii Bezpieczeństwa Narodowego RP z 2020 r. tj.:

- podniesienia poziomu odporności na cyberzagrożenia oraz zwiększenie poziomu ochrony informacji w sektorze publicznym, militarnym, prywatnym oraz promowanie wiedzy i dobrych praktyk umożliwiających obywatelom lepszą ochronę ich informacji;
- zwiększenia poziomu odporności systemów informacyjnych wykorzystywanych w sferze publicznej i prywatnej oraz militarnej i cywilnej oraz osiągnąć zdolność do skutecznego zapobiegania, zwalczania oraz reagowania na cyberzagrożenia.
- wzmacniania defensywny potencjał państwa poprzez zapewnienie ciągłego rozwoju krajowego systemu cyberbezpieczeństwa;
- uzyskania zdolności do prowadzenia pełnego spektrum działań militarnych w cyberprzestrzeni;
- rozwijania krajowych zdolności w obszarze testowania, badania, oceny i certyfikacji rozwiązań i usług z obszaru cyberbezpieczeństwa, a także rozwijania kompetencje, wiedzę oraz świadomość zagrożeń i wyzwań wśród kadr administracji publicznej oraz w społeczeństwie w obszarze cyberbezpieczeństwa.
- wzmacniania i rozbudowywania potencjału państwa m.in. poprzez rozwój rodzimych rozwiązań w zakresie cyberbezpieczeństwa oraz prowadzenie finansowanych przez państwo prac badawczo-rozwojowych w obszarze nowoczesnych technologii, m.in. uczenia maszynowego, Internetu Rzeczy, szerokopasmowych sieci łączności stacjonarnej i mobilnej (5G i kolejnych generacji), w tym także współpracę z uczelniami i instytucjami naukowymi oraz przedsiębiorstwami – zarówno z sektora publicznego, jak i prywatnego.

Aktualnie w przygotowaniu jest nowa „Strategia Cyberbezpieczeństwa RP na lata 2025-2029”. Przyjęcie Strategii wynika z ram czasowych określonych w ustawie o krajowym systemie cyberbezpieczeństwa. Musi być ona spójna z innymi dokumentami np. Strategią Bezpieczeństwa Narodowego RP oraz polityką wewnętrzną i zagraniczną państwa.

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