Ministerstwo
Cyfryzacji

Sekretarz Stanu
Paweł Olszewski

BM.WP.057.40.2024
Warszawa, 11 lipca 2024 r.

Szanowny Pan
Szymon Hołownia
Marszałek Sejmu RP

Dot. pisma z 10 czerwca br. Posła na Sejm RP Pana Janusza Cieszyńskiego w sprawie cybertarczy (interpelacja nr 3267)

Szanowny Panie Marszałku,

poniżej przedstawiam odpowiedzi na zadane przez Posła pytania.

Ad 1) Ile dokładnie środków zostanie przeznaczonych na budowę zapowiedzianej cybertarczy? Na co zostaną przeznaczone te środki? Proszę o odpowiedź wraz z rozbiciem na konkretne pozycje kosztowe.

Na realizację programu planowane są nakłady w wysokości co najmniej 3 mld zł w perspektywie 2 najbliższych lat. Środki zostaną przeznaczone m.in. na realizację następujących działań:

- Cyberbezpieczny Samorząd, w ramach którego zostanie wzmocnione cyberbezpieczeństwo jednostek samorządu terytorialnego;
- projekt wsparcia budowy i rozwijania Lokalnych Centrów Cyberbezpieczeństwa (LCC) działających jako Centra Usług Wspólnych w obszarze IT, które zapewnią wysoki poziom cyberbezpieczeństwa dla wielu instytucji działających na poziomie samorządu terytorialnego;
- budowa Centrum Cyberbezpieczeństwa NASK, którego celem jest zwiększenie potencjału NASK do wykrywania i zwalczania zagrożeń z cyberprzestrzeni;
- projekty realizowane w ramach KPO, tj.: rozwój Systemu S46, który będzie dostępny dla wszystkich podmiotów krajowego systemu cyberbezpieczeństwa do wymiany informacji o cyberzagrożeniach, działania mające na celu wsparcie zwalczania cyberprzestępczości, wsparcie budowy lub rozwój CSIRT sektorowych oraz wsparcie inwestycyjne podmiotów krajowego systemu cyberbezpieczeństwa w poprawę cyberbezpieczeństwa w organizacji;
- wspieranie bieżących działań w zakresie zapewniania bezpieczeństwa systemów teleinformatycznych przed cyberzagrożeniami wśród kluczowych podmiotów odpowiadających za bezpieczeństwo państwa poprzez finansowanie świadczenia teleinformatycznego, tj. dodatku do wynagrodzenia dla osób realizującym zadania z zakresu cyberbezpieczeństwa;
- toczące się prace nad kompleksową nowelizacją ustawy o krajowym systemie cyberbezpieczeństwa w celu poprawy jego funkcjonowania i wprowadzenia rozwiązań adekwatnych do pojawiających się zagrożeń, w tym mających na celu harmonizację przepisów z prawodawstwem unijnym, tj. wdrożenie dyrektywy NIS2, które również przewidują mechanizmy niezbędne do finansowania działań administracji;
- prace nad nową Strategią Cyberbezpieczeństwa RP, która nakreśli kierunki rozwoju cyberodporności Państwa na kolejne 5 lat i zainicjuje kolejne działania.

Kolejne środki i cele są obecnie w fazie szczegółowego planowania.

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

ul. Królewska 27
00-060 Warszawa

Ad 2) Jakie będzie źródło finansowania ww. przedsięwzięć? Na jaki okres zostanie przeznaczona ta kwota?

Działania realizowane w ramach programu zostaną sfinansowane ze środków UE (Fundusze Europejskie na Rozwój Cyfrowy 2021-2027 oraz Krajowego Planu Odbudowy i Zwiększania Odporności), Funduszu Cyberbezpieczeństwa oraz budżetu państwa.

Ad 3) W jaki sposób planowana Cybertarcza ma realizować przeglądy bezpieczeństwa?

Jednym z działań będących elementem programu jest nowelizacja ustawy o krajowym systemie cyberbezpieczeństwa. Zgodnie z projektem nowelizacji tego aktu prawnego zespoły CSIRT poziomu krajowego będą mogły przeprowadzać ocenę bezpieczeństwa systemów informacyjnych podmiotów krajowego systemu cyberbezpieczeństwa. Ocena ta będzie mogła być przeprowadzona w uzgodnieniu z podmiotem krajowego systemu cyberbezpieczeństwa albo na zlecenie organu właściwego do spraw cyberbezpieczeństwa. Celem oceny bezpieczeństwa będzie sprawdzenie zabezpieczeń systemu informacyjnego i ich odporności na cyberzagrożenia. Taka ocena jest przewidziana jako działanie nadzorcze także przez dyrektywę NIS2. Dodatkowo zespoły CSIRT poziomu krajowego otrzymają kompetencję do identyfikowania podatności systemów dostępnych w otwartych sieciach teleinformatycznych, a także powiadamiania właścicieli tych systemów o wykrytych podatnościach oraz cyberzagrożeniach. Przykładowo chodzi o możliwość identyfikacji podatności stron internetowych należących do podmiotów krajowego systemu cyberbezpieczeństwa.

Ad 4) Czy Cybertarcza obejmie wyłącznie podmioty zaliczające się do infrastruktury krytycznej?

Zgodnie z ww. listą działań, program obejmie m.in. instytucje i podmioty krajowego systemu cyberbezpieczeństwa, w tym w szczególności jednostki samorządu terytorialnego.

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