

RZĄD ZREALIZUJE STRATEGIĘ CYBERBEZPIECZEŃSTWA

Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019-2024 jest już gotowa i oczekuje na podpis premiera Mateusza Morawieckiego - poinformował we wtorek minister cyfryzacji Marek Zagórski. Dokument zastępuje Krajowe Ramy Polityki Cyberbezpieczeństwa RP.

O zakończeniu prac nad Strategią i spodziewanym złożeniu podpisu pod nią przez premiera Mateusza Morawieckiego minister Zagórski poinformował na konferencji prasowej zorganizowanej we wtorek, pierwszego dnia 5. Europejskiego Forum Cyberbezpieczeństwa Cybersec w Katowicach.

„Strategia Cyberbezpieczeństwa jest kontynuacją dotychczasowych prac i działań. Co istotne, to dokument powstały po tym, jak weszła w życie ustawa o krajowym systemie cyberbezpieczeństwa, gdy ten system instytucjonalny został utworzony. W związku z tym jej głównym celem jest wzmocnienie tego systemu instytucjonalnego, także zwiększenie odporności systemu na zagrożenia cybernetyczne” - wyjaśniał minister Zagórski.

„Mamy w tym kilka celów szczegółowych, w tym m.in. podnoszenie świadomości, rozwijanie narzędzi, także wytwarzanych w Polsce. Ważnym elementem jest współpraca międzynarodowa, która powinna być kontynuowana i będzie dlatego, że jeśli chodzi o tego typu zagrożenia i ten komponent naszego bezpieczeństwa, żadne państwo nie jest go w stanie zrealizować w pełni samodzielnie” - mówił szef MC.

Pytany przez dziennikarzy, kto będzie wykonawcą Strategii, Zagórski wskazał na rząd. Koordynatorem ma być Pełnomocnik Rządu ds. Cyberbezpieczeństwa, a realizatorami: trzy podstawowe jednostki, tzw. zespoły CSIRT (Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego).

Odnosząc się do kwestii, czy dla realizacji Strategii potrzebne będą dodatkowe akty wykonawcze, szef MC odpowiedział, że resort przede wszystkim będzie reagował na pojawiające się w tym zakresie potrzeby.

„Tutaj rozwój sytuacji jest bardzo dynamiczny. Dzisiaj na pewno wiemy, że będziemy wdrażać przepisy w zakresie bezpieczeństwa sieci 5G. Zresztą mamy już przygotowany projekt rozporządzenia, które bazuje na obecnym prawie telekomunikacyjnym, a które będzie dotyczyło bezpieczeństwa sieci telekomunikacyjnych, ale prawdopodobnie będą potrzebne jeszcze dodatkowe korekty w prawie, abyśmy mogli zadbać o bezpieczeństwo tej sieci, ale nie tylko, bo tak naprawdę powinniśmy mówić o bezpieczeństwie całej infrastruktury wrażliwej” - zaznaczył Zagórski.

Nawiązał także do fragmentu odczytanego na wtorkowym Cybersec listu Prezydenta RP, w którym Andrzej Duda zwrócił uwagę na potrzebę skonsolidowania dwóch obszarów ustaw: o zarządzaniu kryzysowym oraz o bezpieczeństwie. „To na pewno przed nami” - ocenił Zagórski.

Jak wynika z informacji kierowanego przezeń resortu, Strategia Cyberbezpieczeństwa RP określa strategiczne cele oraz środki polityczne i regulacyjne, które trzeba zrealizować, aby systemy informacyjne, operatorzy usług kluczowych, operatorzy infrastruktury krytycznej, dostawcy usług cyfrowych oraz administracja publiczna były odporne na incydenty w cyberprzestrzeni.

Przyjęty w formie uchwały Rady Ministrów dokument zastępuje Krajowe Ramy Polityki Cyberbezpieczeństwa na lata 2017-2022. Główne zmiany w Strategii (wobec Ram) wynikają z: wejścia w życie ustawy o krajowym systemie cyberbezpieczeństwa oraz aktualnych wyzwań związanych z cyberbezpieczeństwem - jak zabezpieczenie rozwiązań w ramach technologii 5G, upowszechnienie przetwarzania w chmurze czy konieczność poszerzania świadomości w społeczeństwie.

MC wskazuje, że wdrożenie Strategii jest kolejnym etapem realizacji ustawy o krajowym systemie cyberbezpieczeństwa, będącej implementacją do polskiego porządku prawnego dyrektywy NIS (tj. dyrektywy Parlamentu Europejskiego i Rady ws. środków na rzecz wysokiego, wspólnego poziomu bezpieczeństwa sieci i systemów informatycznych na terytorium Unii Europejskiej).

Główny cel Strategii to podniesienie poziomu odporności na cyberzagrożenia oraz poziomu ochrony informacji w sektorach: publicznym, militarnym i prywatnym (przy czym zwiększeniu poziomu ochrony informacji ma sprzyjać promowanie wiedzy i dobrych praktyk wśród obywateli).

Szczegółowe cele Strategii to m.in. rozwój Krajowego Systemu Cyberbezpieczeństwa (KSC) oraz zwiększenie poziomu odporności sieci i systemów teleinformatycznych administracji publicznej oraz sektora prywatnego - wraz z osiągnięciem zdolności do skutecznego zwalczania skutków incydentów (poprzez opracowanie m.in. Narodowych Standardów Cyberbezpieczeństwa czy utworzenie krajowego systemu ds. certyfikacji cyberbezpieczeństwa).

Kolejnym celem szczegółowym jest zwiększenie potencjału Polski w zakresie technologii cyberbezpieczeństwa (poprzez rozbudowę zasobów przemysłowych i technologicznych czy współpracę międzynarodową). Strategia zakłada także rozwijanie świadomości społecznej w obszarze bezpiecznego korzystania z wirtualnej przestrzeni. Ostatnim celem szczegółowym jest zbudowanie silnej pozycji międzynarodowej Polski w obszarze cyberbezpieczeństwa.

Koordynatorem wdrożenia Strategii jest minister cyfryzacji, który jest zobowiązany do corocznego składania sprawozdania o postępkach jej wdrażania Strategii w formie raportu, przedkładanego Radzie Ministrów. W ciągu pół roku od przyjęcia dokumentu minister ma przedstawić plan działań na rzecz wdrożenia Strategii - z określeniem zadań, źródeł finansowania oraz mierników.

Czytaj też: ["Polska chce odgrywać rolę lidera w cyberbezpieczeństwie" - Premier o Strategii Cyberbezpieczeństwa RP](#)