MINISTERSTWO CYFRYZACJI ORGANIZATOREM KRAJOWEGO SYSTEMU CYBERBEZPIECZEŃSTWA

Organizatorem krajowego systemu cyberbezpieczeństwa będzie resort cyfryzacji, którego kompetencje określi specjalna ustawa – przewidują ogłoszone wczoraj założenia strategii cyberbezpieczeństwa dla RP. Za przygotowanie ustawy o krajowym systemie cyberbezpieczeństwa odpowiada sekretarz stanu w Ministerstwie Cyfryzacji Witold Kołodziejski.

Do 8 marca Ministerstwo Cyfryzacji przyjmuje wnioski i uwagi do zamieszczonych na stronie resortu założeń „Strategii Cyberbezpieczeństwa dla RP". Opisują one strukturę i funkcjonowanie krajowego systemu cyberbezpieczeństwa. Organizatorem systemu ma być minister cyfryzacji, którego kompetencje i uprawnienia ministra określi ustawa o krajowym systemie cyberbezpieczeństwa.

Ustawa ta – jak czytamy w założeniach Strategii Cyberbezpieczeństwa dla RP – „usankcjonuje prawnie rolę ministra (cyfryzacji – przyp. red.) w zakresie:

a) opracowania krajowej strategii cyberbezpieczeństwa,

b) przygotowywania projektów aktów prawnych z zakresu cyberbezpieczeństwa, w tym:

- · ustalenia ustawowych wymagań i powinności z zakresu cyberbezpieczeństwa w obszarze organizacyjnym i technologicznym,
- · opracowania kryteriów kwalifikacji podmiotów gospodarki narodowej jako świadczących usługi kluczowe z punktu widzenia przepisów prawa dotyczących cyberbezpieczeństwa,
- · opracowania, prowadzenia i aktualizacji wykazu usług kluczowych i podmiotów świadczących takie usługi w rozumieniu przepisów prawa,
- · opracowania propozycji progów istotności incydentu bezpieczeństwa dla podmiotów z administracji publicznej i każdego z sektorów zobowiązanych do notyfikacji incydentów,
- · opracowania uregulowań i wytycznych dotyczących mechanizmów wymiany informacji z zakresu cyberbezpieczeństwa w administracji publicznej, sferze gospodarki narodowej, zarządzania kryzysowego a także w zakresie relacji z organami ścigania i organami odpowiedzialnymi za zapewnienie bezpieczeństwa narodowego,
- · przygotowania wytycznych w zakresie ustanowienia odpowiednich i proporcjonalnych środków ochrony systemów teleinformatycznych i informacji na podstawie procesu zarządzania ryzykiem,

c) prowadzenia kontroli przestrzegania przepisów z zakresu cyberbezpieczeństwa w administracji publicznej i podmiotach świadczących usługi kluczowe,

d) prowadzenia spraw związanych z uruchomieniem i sprawowaniem nadzoru nad krajową siecią CSIRT/CERT i CSIRT Narodowym, w tym zapewnieniem mu odpowiednich zasobów technicznych,

ludzkich i finansowych,

e) ustanowienia i zapewnienia funkcjonowania pojedynczego punktu kontaktowego, w tym zagwarantowania mu odpowiednich zasobów technicznych, ludzkich i finansowych,

f) zapewnienia funkcjonowania krajowego systemu reagowania na incydenty komputerowe w wymiarze operacyjnym, przy czym powyższa funkcjonalność będzie mogła być zbudowana na bazie pojedynczego punktu kontaktowego.

Z założeń strategii przygotowanej przez zespół zadaniowy resortu kierowanego przez Annę Streżyńską wynika, że zasadnicza część zmian organizacyjnych w krajowym systemie cyberbezpieczeństwa będzie związana z precyzyjnym zdefiniowaniem roli organizatora systemu, czyli Ministerstwa Cyfryzacji w ustawie o krajowym systemie cyberbezpieczeństwa. Częściowa centralizacja systemu, za którą – jak informują autorzy założeń strategii - opowiadają się kluczowi interesariusze, oznacza, że Ministerstwo Cyfryzacji jako koordynator strategiczno-polityczny będzie ustalać politykę i cele do realizacji, proponować i wdrażać rozwiązania legislacyjne, oddziaływać prawnie na inne instytucje, opracowywać wieloletnie programy działania (np. w zakresie działalności badawczo-rozwojowej) i koordynować współpracę międzynarodową.

Istotne jest, że przyjęta w założeniach do strategii koncepcja krajowego systemu cyberbezpieczeństwa oznacza przebudowanie definicji cyberprzestrzeni i jej rozciągnięcie na sferę kluczowych operatorów funkcjonujących w sferze gospodarczej . Dotychczasowa definicja była ograniczona do sektora publicznego (administracja państwowa, sądownictwo, administracja rządowa, część podmiotów z sektora finansów publicznych). Wprowadzenie szczególnych wymogów wobec elementów teleinformatycznych ochrony infrastruktury krytycznej może również oznaczać potrzebę uzupełnienia definicji infrastruktury krytycznej, tak aby nie pozostawiała wątpliwości, że obejmuje również infrastrukturę wirtualną (informacyjną). Autorzy założeń „Strategii Cyberbezpieczeństwa dla RP" przewidują możliwość wprowadzenia tej definicji do ustawy o krajowym systemie cyberbezpieczeństwa lub ustawy o świadczeniu usług drogą elektroniczną.

Brak jest szczegółowych informacji dotyczących poziomu zaawansowania prac nad przygotowaniem ustawy o krajowym systemie cyberbezpieczeństwa. Wiadomo jedynie, że od 5 lutego br. w Biuletynie Informacji Publicznej Kancelarii Prezesa Rady Ministrów znajduje się informacja o włączeniu projektu do wykazu prac legislacyjnych i programowych rządu. Obejmuje ona adnotację o tym, że projektowana ustawa wpisuje się w cel 5 Strategii Rozwoju Systemu Bezpieczeństwa Narodowego Rzeczypospolitej Polskiej 2022 – *Tworzenie warunków do rozwoju zintegrowanego systemu bezpieczeństwa narodowego*, priorytet 5.3 *Zapewnienie bezpieczeństwa informacyjnego i telekomunikacyjnego*, kierunek interwencji 5.3.2 – *Rozwijanie Systemu Reagowania na Incydenty Komputerowe* w kontekście zintegrowanego systemu bezpieczeństwa narodowego.

Osobą odpowiedzialną za przygotowanie projektu ustawy o krajowym systemie cyberbezpieczeństwa jest sekretarz stanu w Ministerstwie Cyfryzacji Witold Kołodziejski.

Do czasu przyjęcia ustawy o krajowym systemie cyberbezpieczeństwa, co będzie równoznaczne z wdrożeniem docelowego, kompleksowego systemu bezpieczeństwa teleinformatycznego, zadania realizowane przez Ministerstwo Cyfryzacji we współpracy z Urzędem Komunikacji Elektronicznej (UKE), NASK, CERT.GOV.PL (Rządowy Zespół Reagowania na Incydenty Komputerowe działający w strukturze Departamentu Bezpieczeństwa Teleinformatycznego ABW – przyp. red.) będą wykonywane w oparciu umowy, porozumienia wynikające z dotychczasowych przepisów (prawa administracyjnego, ustawy o finansach publicznych, ustawy o instytutach badawczych).