NOWELIZACJA USTAWY O KRAJOWYM SYSTEMIE CYBERBEZPIECZEŃSTWA

Sprawniejsze działanie najistotniejszych podmiotów w systemie cyberbezpieczeństwa Polski oraz wdrożenie zaleceń unijnych w obszarze bezpieczeństwa sieci telekomunikacyjnych stanowią podstawowe cele nowelizacji ustawy o krajowym systemie cyberbezpieczeństwa, której projekt został skierowany do konsultacji.

„Zebraliśmy dwa lata doświadczeń funkcjonowania ustawy o krajowym systemie cyberbezpieczeństwa (ksc)" - wskazuje Ministerstwo Cyfryzacji. - „W oparciu o własne analizy, jak i informacje otrzymywane od partnerów społecznych, dokonaliśmy przeglądu ustawy i zidentyfikowaliśmy obszary wymagające usprawnienia". Równocześnie doszło do istotnych dla cyberbezpieczeństwa zmian na poziomie europejskim. Efekty tych działań zostały przekazane do konsultacji w formie projektu nowelizacji ustawy o krajowym systemie cyberbezpieczeństwa.

Europejskie priorytety

Jak wskazuje Ministerstwo Cyfryzacji, jednym z priorytetów Komisji Europejskiej stało się cyberbezpieczeństwo sieci telekomunikacyjnych. Po pierwsze - pojawił się Europejski Kodeks Łączności Elektronicznej, który umożliwia m.in. ujednolicenie procedur zgłaszania incydentów bezpieczeństwa na poziomie krajowym. Po drugie - Komisja Europejska kładzie nacisk na zapewnienie bezpieczeństwa szerokopasmowej sieci łączności nowej generacji, czyli technologii 5G.

„Kwestię bezpieczeństwa sieci telekomunikacyjnych wielokrotnie podnosiliśmy na forum europejskim. Niezawodność i niezakłócone świadczenie usług telekomunikacyjnych ma i będzie miało coraz większe znaczenie dla cyberbezpieczeństwa usług kluczowych i cyfrowych" – mówi minister cyfryzacji Marek Zagórski, pełnomocnik rządu ds. cyberbezpieczeństwa. „Projekt zmian w ustawie o ksc jest naszą odpowiedzią na rosnące wyzwania cyberbezpieczeństwa" – dodaje szef MC.

Proponowane w ustawie zmiany są konieczne z powodu podjętych na poziomie europejskim zobowiązań - podkreśla resort.

„Chodzi tutaj o wdrożenie zaleceń i standardów opublikowanych w tak zwanym 5G Toolbox, czyli zestawie narzędzi przygotowanych przez Komisję Europejską, Agencję Unii Europejskiej ds. Cyberbezpieczeństwa (ENISA), przy aktywnym udziale państw członkowskich, w tym Polski" - czytamy w komunikacie Ministerstwa Cyfryzacji. Zawiera on minimalny poziom harmonizacji na poziomie UE rozwiązań cyberbezpieczeństwa sieci 5G. Są to zarówno narzędzia o charakterze strategicznym i technicznym oraz wspierającym.

Będzie sprawniej

Analizy Ministerstwa Cyfryzacji oraz zgłaszanie przez partnerów społecznych uwagi m.in. w trakcie

prac nad Strategią Cyberbezpieczeństwa RP na lata 2019-2024, wskazały na potrzebę usprawnienia krajowego systemu cyberbezpieczeństwa m.in. w takich obszarach jak:

- ujednolicenie na poziomie krajowym procedur zgłaszania incydentów, w tym także incydentów raportowanych przez przedsiębiorstwa telekomunikacyjne;
- zapewnienie warunków do utworzenia zespołów reagowania na incydenty komputerowe (CSIRT) w sektorach i podsektorach gospodarki o kluczowym znaczeniu dla społeczno-ekonomicznego bezpieczeństwa państwa (sektorowe CSIRT);
- wzmocnienie współpracy operatorów usług kluczowych z organami właściwymi oraz zespołami CSIRT poziomu krajowego w zakresie wymiany informacji o incydentach, podatnościach, zagrożeniach i dobrych praktykach;
- umożliwienie tworzenia centrów analizy i wymiany informacji (ISAC).

Co ulegnie zmianie?

Oto najważniejsze, proponowane w nowelizacji zmiany, jakie wyróżnia ministerstwo:

- Kolegium ds. Cyberbezpieczeństwa otrzyma kompetencje do oceny ryzyka dostawców sprzętu lub oprogramowania istotnego dla cyberbezpieczeństwa podmiotów krajowego systemu cyberbezpieczeństwa. Prowadzenie przez państwa członkowskie UE tego typu ocen ryzyka zostało uzgodnione z Komisją Europejską i ENISA, jako jeden ze środków strategicznych w dokumencie 5G Toolbox;
- Sektorowe CSIRT – mimo istnienia takiej możliwości, dotychczas powstał tylko jeden sektorowy zespół cyberbezpieczeństwa - Sektorowy Zespół Cyberbezpieczeństwa dla Sektora Bankowości i Infrastruktury Rynków Finansowych (CSIRT-KNF). Zmiany umożliwią powstanie sektorowych CSIRT we wszystkich kluczowych dla społeczno-ekonomicznego bezpieczeństwa państwa i obywateli sektorach gospodarki;
- Wprowadzenie do krajowego systemu cyberbezpieczeństwa operacyjnych centrów bezpieczeństwa, czyli SOC. Ponadto, doprecyzowane zostaną zadania i rola SOC w systemie cyberbezpieczeństwa RP;
- Tworzenie i funkcjonowanie ISAC - zmiany umożliwią tworzenie ISAC, czyli specjalistycznych organizacji, dzięki którym podmioty ksc będą miały możliwość bieżącej wymiany informacji o incydentach, zagrożeniach, podatnościach oraz dobrych praktykach. ISAC usprawnią także współpracę podmiotów z zespołami CSIRT poziomu krajowego.

Konsultacji otwarte dla wszystkich

„Czekamy na Państwa opinie, propozycje i uwagi do zaproponowanych przez nas zmian” - zachęca resort cyfryzacji. Ministerstwu zależy przede wszystkim na udziale w konsultacjach stowarzyszeń branżowych, fundacji, instytutów naukowych, środowisk akademickich, przedsiębiorstw świadczących usługi z zakresu cyberbezpieczeństwa oraz branżowych specjalistów.

„Liczymy na kontynuację dobrej współpracy z operatorami usług kluczowych, dostawcami usług cyfrowych, partnerami społecznymi, zapoczątkowanej przy uzgodnieniach projektu Strategii Cyberbezpieczeństwa. Zachęcamy Państwa do aktywnego udziału w konsultacjach. Powinno nam szczególnie zależeć na tym, aby planowana nowelizacja zwiększyła skuteczność krajowego systemu cyberbezpieczeństwa i pomogła wszystkim jego podmiotom w podniesieniu odporności na cyberzagrożenia” – mówi Robert Kośla, dyrektor Departamentu Cyberbezpieczeństwa Ministerstwa Cyfryzacji.

Uzgodnienia i konsultacje publiczne potrwają 14 dni.

Projekt nowelizowanej ustawy jest dostępny na stronie Rządowego Centrum Legislacji.

Informacja prasowa Ministerstwa Cyfryzacji

Czytaj też: Minister Cyfryzacji: Zarzuty wobec aplikacji ProteGo Safe są całkowicie nieuzasadnione [WYWIAD]