Stan cyberbezpieczeństwa wg sprawozdania KPRM

Kategoria: Sejm, Senat i Prezydent
Opublikowano: środa, 20, styczeń 2021 15:36
Monika Małowiecka
Odsłony: 1135

Sekretarz stanu w Kancelarii Prezesa Rady Ministrów i pełnomocnik rządu do spraw cyberbezpieczeństwa Marek Zagórski na ostatnim posiedzeniu sejmowej Komisji Cyfryzacji, Innowacyjności i Nowoczesnych Technologii przedstawili informację na temat realizacji założeń „Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019–2024" oraz informację na temat realizacji prac nad narodowymi standardami cyberbezpieczeństwa (NSC).

Przedstawiciel rządu poinformował, że „Strategia Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2019–2024" ma za zadanie realizację pięciu celów szczegółowych. Pierwszy z nich to rozwój krajowego systemu cyberbezpieczeństwa. Drugim jest podniesienie poziomu odporności systemów informacyjnych administracji publicznej i sektora prywatnego oraz osiągnięcie zdolności do skutecznego zapobiegania i reagowania na incydenty. Kolejnym celem jest zwiększenie potencjału narodowego w zakresie technologii cyberbezpieczeństwa. Cel szczegółowy czwarty to budowanie świadomości i kompetencji społecznych w zakresie cyberbezpieczeństwa. Celem piątym jest zbudowanie silnej pozycji międzynarodowej RP w obszarze cyberbezpieczeństwa. Wszystkie te cele są realizowane.

Najważniejsze zadania, które zostały zrealizowane w okresie od 31 października 2019 r. do 31 października br. to przede wszystkim opracowanie oraz skonsultowanie w ramach administracji rządowej planu działania na rzecz wdrożenia strategii cyberbezpieczeństwa. W planie wskazano konkretne działania, wiodące oraz współpracujące podmioty odpowiedzialne za realizację danego działania, źródła finansowania tych działań oraz mierniki pozwalające na ocenę postępów realizacji danego działania. Utworzony też został pierwszy w Polsce sektorowy zespół cyberbezpieczeństwa przy Komisji Nadzoru Finansowego, który rozpoczął funkcjonowanie dnia 1 lipca. Zapewnia on wsparcie w obsłudze incydentów dla podmiotów z całego sektora finansowego. Jest to bardzo ważny moment, dlatego że cały krajowy system cyberbezpieczeństwa opiera się na trzech podstawowych zespołach reagowania na incydenty komputerowe (CSIRT), ale jednym z jego głównych, podstawowych elementów jest utworzenie sieci sektorowych zespołów CSIRT.

Dnia 2 października 2020 r., rozpoczął funkcjonowanie pierwszy w Polsce zespół ISAC, czyli centrum wymiany i analizy informacji. To centrum powstało na kolei z oddolnej inicjatywy podmiotów podsektora kolei przy bardzo silnym wsparciu ze strony Ministerstwa Infrastruktury oraz eksperckiej pomocy ze strony Zespołu Reagowania na Incydenty Bezpieczeństwa Komputerowego Naukowej i Akademickiej Sieci Komputerowej (CSIRT NASK). Również w tym roku Instytut Łączności – Państwowy Instytut Badawczy uruchomił pierwsze w Polsce laboratorium oceny i certyfikacji bezpieczeństwa produktów i usług na zgodność z normą common criteria w ramach realizacji projektu „Krajowy schemat oceny i certyfikacji bezpieczeństwa oraz prywatności produktów i systemów IT zgodny z Common Criteria" (KSO3C). Ponadto opracowano standardy cyberbezpieczeństwa chmur obliczeniowych (SCCO) w ramach NSC, które zostały opublikowane w lutym 2020 przez Departament Cyberbezpieczeństwa dawnego Ministerstwa Cyfryzacji.

Przygotowane zostały założenia do realizacji przez KPRM kampanii #CyberbezpiecznySamorząd, która ma na celu wsparcie jednostek samorządu terytorialnego w obszarze podnoszenia wiedzy oraz kompetencji.

Ministerstwo Obrony Narodowej kontynuowało prace związane z rozwojem Wojsk Obrony Cyberprzestrzeni. Trwa także wdrażanie unijnego zestawu środków strategicznych, technicznych i wspierających, harmonizujących na poziomie Unii Europejskiej bezpieczeństwo technologii mobilnej piątej generacji (5G), czyli tzw. 5G Toolbox.

Ponadto, przygotowany został projekt ustawy o zmianie ustawy o krajowym systemie cyberbezpieczeństwa i ustawy – Prawo zamówień publicznych. Projekt zakłada w pierwszej kolejności rozbudowę krajowego systemu cyberbezpieczeństwa poprzez umożliwienie tworzenia centrów ISAC, takich jak ten kolejowy, instytucjonalizację operacyjnych centrów bezpieczeństwa, czyli SOC, jak również wsparcie jednostek samorządu terytorialnego. Do systemu dodani zostaną także przedsiębiorcy komunikacji elektronicznej w zakresie wymogów bezpieczeństwa sieci i usług oraz zgłaszania incydentów, co m.in. umożliwi wdrożenie dyrektywy ustanawiającej europejski kodeks łączności elektronicznej (EKŁE). Wprowadzona zostanie możliwość oceny ryzyka dostawców sprzętu lub oprogramowania dla podmiotów krajowego systemu cyberbezpieczeństwa. Sektorowe zespoły CSIRT staną się obowiązkowe. Dotychczas były tylko potencjalną możliwością organów właściwych. Będzie także możliwe wydawanie ostrzeżeń oraz poleceń zabezpieczających na czas reakcji na incydent krytyczny.

Jeśli chodzi o realizację prac nad NSC, to trzeba przypomnieć, że chodzi o standardy i tzw. dobre praktyki w dziedzinie cyberbezpieczeństwa. Standardy te będą miały charakter zbioru różnego rodzaju rekomendacji, które będą wdrażane w poszczególnych obszarach. Pierwszą rekomendacją, która została przyjęta, są standardy dotyczące cyberbezpieczeństwa chmury obliczeniowej, które stanowiły wkład do uchwały Rady Ministrów w sprawie inicjatywy „Wspólna Infrastruktura Informatyczna Państwa” (WIIP). W przygotowaniu jest kilkanaście podobnych dokumentów, które szczegółowo będą regulować poszczególne obszary.