Cyberdefence 24

23.01.2019

NOWA STRATEGIA CYBERBEZPIECZEŃSTWA POLSKI W III KWARTALE 2019

Rząd przyjmie nową uchwałę ws. Strategii Cyberbezpieczeństwa w III kwartale 2019 roku wynika z informacji podanych w wykazie prac legislacyjnych i programowych Rady Ministrów.

Opracowanie i przyjęcie Strategii Cyberbezpieczeństwa Rzeczypospolitej Polskiej jest wymogiem realizacji przepisu art. 68 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz.U. poz. 1560). Przepis ustawowy (art. 90) określa także datę graniczną, do której ww. Strategia ma zostać przyjęta tj.: do 31 października 2019 r. Strategia określa cele strategiczne oraz odpowiednie środki polityczne, które mają na celu osiągniecie i utrzymanie wysokiego poziomu cyberbezpieczeństwa RP. Pojawiła się również konieczność dokonania oceny i przeglądu w 2019 r. dotychczasowego dokumentu o charakterze strategicznym, czyli przyjętych uchwałą Nr 52/2017 Rady Ministrów z dnia 27 kwietnia 2017 r. Krajowych Ram Polityki Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017 – 2022 oraz wynikającego z tego Planu działań na rzecz wdrożenia Krajowych Ram Polityki Cyberbezpieczeństwa Rzeczypospolitej Polskiej na lata 2017 – 2022.

Stale zmieniające się uwarunkowania związane z bezpieczeństwem w cyberprzestrzeni wymagają szybkiej i zdecydowanej reakcji organów państwa. Również przeprowadzone kontrole Najwyższej Izby Kontroli wskazują na potrzebę aktualizacji oraz zapewnienia spójnej strategii działania RP w dziedzinie cyberbezpieczeństwa. W kontekście spójności, ważne jest przede wszystkim zapewnienie jak najszerszej współpracy przy wdrażaniu i rozwijaniu Krajowego Systemu Cyberbezpieczeństwa ze strony ministerstw i innych organów władzy państwowej.

Projektowana uchwała ma na celu ustanowienie Strategii Cyberbezpieczeństwa. Strategia ma charakter polityczno-strategiczny, natomiast na poziomie operacyjnym realizację jego zapisów zapewni szczegółowy plan działań. Plan działań opisze podmioty zaangażowane w realizację strategii oraz środki pozwalające na jej wdrożenie. Przy opracowywaniu strategii korzystano z dobrych praktyk i rozwiązań proponowanych przez Międzynarodowy Związek Telekomunikacyjny oraz doświadczeń innych państw. Strategia uwzględni następujące kwestie:

- cele i priorytety w zakresie cyberbezpieczeństwa, czyli opisane zostaną wizja, cel główny oraz cele szczegółowe strategii;
- podmioty zaangażowane we wdrażanie i realizację Strategii;
- środki służące realizacji celów Strategii;
- określenie środków w zakresie gotowości, reagowania i przywracania stanu normalnego, w tym zasady współpracy między sektorem publicznym i prywatnym;
- podejście do oceny ryzyka, czyli m.in. stworzenie systemu zarządzania ryzykiem na poziomie krajowym;
- działania odnoszące się do programów edukacyjnych, informacyjnych i szkoleniowych dotyczących cyberbezpieczeństwa, czyli m.in. zwiększenie kompetencji kadr (w sektorze publicznym i prywatnym), cyberbezpieczeństwo obywateli (edukacja i budowanie świadomości);

- działania odnoszące się do planów badawczo-rozwojowych w zakresie cyberbezpieczeństwa, czyli m.in. rozbudowa zasobów przemysłowych i technologicznych na potrzeby cyberbezpieczeństwa, stymulowanie badań i rozwoju

AK/Kprm.gov