

Do zaopiniowania przez Zespół ds. Społeczeństwa Informacyjnego Komisji Wspólnej Rządu i Samorządu Terytorialnego wpłynął projekt ustawy zmieniającej ustawę o krajowym systemie cyberbezpieczeństwa oraz ustawy – Prawo zamówień publicznych.

Jak wskazują projektodawcy, wprawdzie ustawa o krajowym systemie cyberbezpieczeństwa umożliwiła podjęcie prac nad budową systemu, jednak doświadczenia zebrane przez dwa lata jej obowiązywania wskazały potrzebę wprowadzenia zmian.

Cyberbezpieczeństwo w JST

Z informacji NIK z 2019 r. wynika, że negatywnie oceniono aż 70% kontrolowanych jednostek samorządu terytorialnego w zakresie wykonywania zadań związanych z zapewnieniem bezpieczeństwa przetwarzania informacji. NIK zalecił Ministrowi Cyfryzacji szeroką promocję wśród organów administracji wiedzy o wymogach w zakresie bezpieczeństwa informacji. Z analiz przeprowadzonych na zlecenie Ministra Cyfryzacji duże zastrzeżenia budzi poziom zabezpieczeń e-usług oferowanych przez samorządy.

Jak wskazano w uzasadnieniu projektu, jednostki samorządu terytorialnego są coraz częściej narażone na cyberataki, jednocześnie mają ograniczone zasoby w zakresie reagowania na incydenty. W celu skuteczniejszej koordynacji reagowania na incydenty na poziomie wojewódzkim, samorządy będą wspierane przez struktury podległe wojewodzie, w szczególności w wymianie informacji pomiędzy zespołami CSIRT poziomu krajowego i Pełnomocnikiem a podmiotami publicznymi w województwie. Ułatwi to wymianę informacji o zagrożeniach cyberbezpieczeństwa incydentach. Dzięki temu zwiększone zostaną możliwości przeciwdziałania incydentom w jednostkach samorządu terytorialnego oraz w innych podmiotach publicznych w województwie takich jak terenowa administracja rządowa czy też sądy.