

Stanowisko
XXXII Zgromadzenia Ogólnego Związku Powiatów Polskich
w sprawie cyberbezpieczeństwa w samorządach

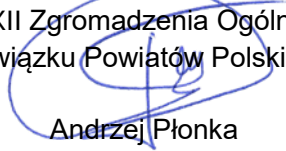
Karpacz, 12 czerwca 2025 roku

Jednostki samorządu terytorialnego stają obecnie wobec drastycznie rosnącej liczby ataków na szeroko rozumianą infrastrukturę teleinformatyczną. Wobec coraz bardziej wyrafinowanych metod wykorzystywanych przez cyberprzestępców, jednostkom samorządu terytorialnego, dysponującym ograniczonymi zasobami finansowymi i kadrowymi, jest coraz trudniej skutecznie chronić posiadane dane i wykorzystywane systemy.

Jednostki samorządu terytorialnego muszą równocześnie mierzyć się z dynamicznie zmieniającym się otoczeniem prawnym; zarówno na poziomie krajowym, jak i unijnym. Szczególnie istotne są w tym kontekście nowe regulacje, takie jak projektowana zmiana ustawy o krajowym systemie cyberbezpieczeństwa czy wdrożenie Dyrektywy NIS2. Nie jest to koniec niezbędnych regulacji – tempo rozwoju poszczególnych technologii, w szczególności sztucznej inteligencji, wymusi szybką nową legislację. Przyjmowane przepisy wprowadzają dodatkowe wymogi, z którymi samorządy będą musiały się zmierzyć, aby sprostać rosnącym oczekiwaniom w zakresie ochrony danych i zapewnienia bezpieczeństwa teleinformatycznego.

W interesie państwa jest zapewnienie narzędzi umożliwiających jednostkom samorządu terytorialnego sprostanie tym oczekiwaniom. Kluczowym elementem przeciwdziałania zagrożeniom cyberbezpieczeństwa w samorządach powinno być połączenie działań edukacyjnych, wsparcia finansowego oraz stworzenia nowych rozwiązań prawnych umożliwiających wspólną realizację zadań. Niezbędne jest zwiększenie liczby szkoleń dla urzędników i pracowników samorządowych, w tym szkoleń specjalistycznych, które pozwolą im zrozumieć złożoność zagrożeń cybernetycznych oraz skutecznie stosować przepisy prawa. Zapewnienie zewnętrznego źródła finansowania przedsięwzięć w zakresie cyberbezpieczeństwa jest dobrą inwestycją w bezpieczeństwo państwa jako całości. Stworzenie warunków do powstawania profesjonalnych Powiatowych Centrów Cyberbezpieczeństwa – obsługujących nie tylko powiat i jego jednostki organizacyjne, ale również zainteresowane gminy wchodzące w skład powiatu – przeloży się na budowanie odporności państwa.

Zgromadzenie Ogólne Związku Powiatów Polskich apeluje zatem o podjęcie skoordynowanych działań, które umożliwią powiatom i miastom na prawach powiatu efektywne wdrażanie wymogów w zakresie cyberbezpieczeństwa, a tym samym przyczynią się do zapewnienia bezpieczeństwa danych oraz ciągłości świadczenia usług publicznych na rzecz obywateli.

Przewodniczący
XXXII Zgromadzenia Ogólnego
Związku Powiatów Polskich

Andrzej Płonka