Kleszczów, 07.08.2025 roku

SZULC-EUPHENICS.COM

PROSTA SPÓŁKA AKCYJNA

Prezes Zarządu

Adam Szulc

ul. Poligonowa 1

04-051 Warszawa

ORG.152.2.2025

Odpowiedź na petycję z dnia 13.05.2025 roku

Na podstawie art. 13 ust. 1 ustawy z dnia 11 lipca 2014 roku o petycjach zawiadamiam, że po dokonaniu analizy petycji wniesionej pismem z dnia 13.05.2025 roku w sprawie „rozważenia zainicjowania procedury sanacji przedmiotowego obszaru w jednostce i pozyskania z rynku „raportu dobrych praktyk" traktującego o zaistniałych kazusach (incydentach związanych z cyberbezpieczeństwem)", petycja została rozpatrzona negatywnie.

Ustalono, że wniesiona petycja spełnia wymagania formalne stawiane petycjom.

Petycja z dnia 13 maja 2025 r. zawiera w swej treści postulat sformułowany na dość wysokim poziomie ogólności, tj. swoistą propozycję sanacji (uzdrowienia, reformy, naprawy) przedmiotowego obszaru – przez który to obszar rozumieć należy cyberbezpieczeństwo jednostki oraz pozyskania z rynku „raportu dobrych praktyk" traktującego o zaistniałych kazusach (incydentach związanych z cyberbezpieczeństwem), które pozwolą na unikanie błędów, jakie występują notorycznie w większości JST. Zdaniem autora petycji materiał taki w założeniach miałby być przeznaczony dla Kierownictwa Jednostki, powinien służyć jako krótka informacja zwracająca percepcję – na najczęściej występujące i powtarzające się błędy w JST, jakich można łatwo uniknąć posiadając świadomość o ich metodologii i okolicznościach ich zaistnienia w innych JST.

Na tak zakreślonym poziomie ogólności nie sposób się nie zgodzić, że ciągły rozwój, inwestycje w infrastrukturę techniczną i w systemy cyberbezpieczeństwa, ulepszanie procedur, w szczególności w zakresie cyberbezpieczeństwa, jest ideą słuszną i potrzebną.

Cyberbezpieczeństwo, według definicji z ustawy o krajowym systemie cyberbezpieczeństwa, to odporność systemów informacyjnych na działania naruszające poufność, integralność, dostępność i autentyczność przetwarzanych danych lub związanych z nimi usług oferowanych przez te systemy. Odporność systemów informacyjnych buduje się wielopoziomowo: od zapewnienia bezpieczeństwa sieci teleinformatycznej, poprzez bezpieczeństwo komputerów i innych urządzeń oraz oprogramowania, aż po procedury i praktyki obowiązujące w danej organizacji.

Zbudowanie odpowiedniego poziomu odporności nie jest łatwe i wymaga odpowiedniego przygotowania organizacyjnego, właściwie dobranych narzędzi i systematycznie podnoszonych kompetencji, zarówno użytkowników, jak i specjalistów zajmujących się utrzymaniem IT i bezpieczeństwem podmiotu publicznego.

Mając na uwadze powyższe w Urzędzie Gminy w Kleszczowie podjęto czynności związane z realizacją projektu „Cyberbezpieczny Samorząd". Ponadto wdrożone zostały odpowiednie polityki bezpieczeństwa, prowadzone są audyty bezpieczeństwa, dokonywane są zakupy niezbędnego sprzętu IT, pracownicy biorą udział oraz zaplanowane są szkolenia podnoszące świadomość i kompetencje z zakresu cyberbezpieczeństwa.

W ocenie Wójta Gminy Kleszczów podejmowane na bieżąco działania w szeroko rozumianej dziedzinie cyberbezpieczeństwa jednostki ukierunkowane na zabezpieczenie potrzeb w tym zakresie, szkolenia pracowników, monitorowanie i eliminowanie ewentualnych zagrożeń są działaniami, które zabezpieczają zdolności jednostki do skutecznego zapobiegania incydentom bezpieczeństwa teleinformatycznego, wykrywania ich i reagowania na nie.

W związku z powyższym nie planujemy pozyskiwania dodatkowego „raportu dobrych praktyk".

Zgodnie z art. 13 ust. 2 ustawy o petycjach sposób załatwienia petycji nie może być przedmiotem skargi.

Wójt Gminy Kleszczów

/-/ Dariusz Michałek