URZĄD MIASTA CZELADŹ
ul. Katowicka 45
41-250 Czeladź

SE-OR.152.3.2026

Czeladź, dnia 2.07.2026 r.

Szanowny Pan
Adam Szulc
Prezes Zarządu
SZULC-EUPHENICS.COM PROSTA SPÓŁKA AKCYJNA
ul. Poligonowa 1
04-051 Warszawa
e-mail: jawnosc-transparentnosc@szulc-euphenics.com

Zawiadomienie o sposobie załatwienia petycji

Dotyczy: podjęcia próby zapoznania się z najczęściej występującymi przyczynami skutecznych cyberwłamań do innych JST.

W odpowiedzi na petycję wniesioną w sprawie podjęcia działań zmierzających do pogłębienia wiedzy o najczęściej występujących przyczynach skutecznych cyberwłamań oraz cyberincydentów w jednostkach samorządu terytorialnego, działając na podstawie art. 13 ust. 1 ustawy z dnia 11 lipca 2014 r. o petycjach, zawiadamia się o uznaniu petycji za zasadną w zakresie postulatu stałego analizowania zagrożeń i podnoszenia świadomości w obszarze cyberbezpieczeństwa.

Uzasadniając powyższe, wskazuje się, że problematyka cyberbezpieczeństwa pozostaje przedmiotem bieżącego zainteresowania Burmistrza oraz właściwych komórek organizacyjnych Urzędu. Burmistrz posiada świadomość, że do najczęstszych przyczyn skutecznych incydentów bezpieczeństwa należą m.in. błędy ludzkie, niewystarczająca ochrona kont i uprawnień, podatności wynikające z braku aktualizacji systemów, a także zagrożenia związane z phishingiem i innymi metodami socjotechnicznymi; z tego względu zagadnienia te są uwzględniane w działaniach organizacyjnych i nadzorczych podejmowanych w Urzędzie.

Jednocześnie wskazuje się, że analiza przypadków cyberincydentów występujących w innych jednostkach samorządu terytorialnego, wymiana doświadczeń oraz upowszechnianie wiedzy o przyczynach naruszeń bezpieczeństwa stanowią działania celowe i pozostające w zgodzie z interesem publicznym. Zgłoszony w petycji postulat wzmacniania wiedzy decydentów oraz kadry kierowniczej w tym obszarze zasługuje więc na aprobatę i wpisuje się w potrzebę stałego doskonalenia mechanizmów ochrony informacji oraz systemów teleinformatycznych.

Mając powyższe na uwadze, petycję rozpatrzono pozytywnie, przyjmując zawarte w niej stanowisko jako zasadne co do kierunku działań służących podnoszeniu poziomu bezpieczeństwa informacji i odporności organizacyjnej Urzędu na zagrożenia cybernetyczne.

Z wyrazami szacunku

Podpisano elektronicznie