

W naszym mniemaniu już samo informowanie o kazusach jakie miały miejsce w gminach oraz o incydentach opisywanych nam w trybie ustawy o dostępie do informacji publicznej - działa jak swoista szczepionka, która uodparnia poprzez budzenie niepokoju i szukanie środków zaradczych.

Osnowa Petycji:

02.152.6.2025

Sekcja I §1) Wnosimy rozważenie zainicjowania procedury sanacji przedmiotowego obszaru w Jednostce i 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.

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 okolicznościach ich zaistnienia w innych JST.

Aby zachować zasady uczciwej konkurencji oraz jawności i transparentności wnosimy o opublikowanie niniejszej petycji wraz z załącznikami w BIP.

Uzasadnienie petycji:

Ataki z 2025 r. - na Gminy i na system rejestrów państwowych (w tym system PIT) etc - świadczą o tym, że nawet najlepiej chronione systemy (zrealizowane w przetargach za miliony złotych) nie są bezpieczne i widać, że celem ataku hakerów jest utrudnianie życia obywatelom, ośmieszanie Decydentów w samorządach, i dezinformacja - jak miało to miejsce w przypadku ataku na PAP lub dezinformacji w Mieście Tychy

A ataki na takie Urzędy gmin jak Werbkowice, Tucznia czy Nowa Sarzyna - ze względu na złożone umiejętności atakujących - mnożna nazwać jedynie mianem cyberterroryzmu tylko przypadek sprawił, że dotyczyły akurat wzmiankowanych Urzędów - a nie innych.

Afery i cyberataki jakie miały miejsce na instytucje samorządowe w Estonii, na gminy w Finlandii czy w Norwegii są świadectwem, że nawet najlepsze zabezpieczenia serwerów nie wystarczą jeśli nie zadba się odpowiednio o dobre praktyki.

Notabene w Finlandii jeden z głośniejszych w i brzemiennych w skutkach cyberataków zaczął się od małej gminy Vellinge (gdzie popełniono szereg prostych błędów) a jego efektem końcowym - na zasadzie kolejnych kostek domina - było ujawnienie niezwykle wrażliwych danych olbrzymiej ilości osób.

Ilość ataków jest na tyle duża i nasila się w takim tempie, że ze strony Ministerstwa Cyfryzacji padają nawet stwierdzenia typu „Samorządy są miękkim podbrzuszem bezpieczeństwa cyfrowego” a celem ataków coraz to częściej może być nawet złośliwe ośmieszanie polskich urzędników wysokiego i niskiego szczebla.

Według danych Ministerstwa Cyfryzacji i w zeszłym roku mieliśmy ponad 111 tysięcy incydentów z tym związanych. Widać wyraźną falę wzrostową,

vide: <https://samorząd.pap.pl/kategoria/aktualnosci/samorzady-miekkim-podbrzuszem-bezpieczestwa-cyfrowego-mc-zapowiada-miliardowe>

<https://cyberdefence24.pl/cyberbezpieczenstwo/rosyjskie-sluzby-atakuja-polske-nie-tylko-wojna-jest-zagrozeniem>

Tymczasem jak wynika z udzielonych nam odpowiedzi w trybie ustawy o dostępie do informacji publicznej - w niektórych gminach problematyka jest prawie ignorowana, a Decydenci uważają, że środki otrzymane z Ministerstwa wyczerpują problematykę związaną z zarządzaniem ryzykiem w gminach - sic !

Szerokie, skuteczne i efektywne działania Ministerstwa kontrastują z niefrasobliwością jaką obserwujemy w Gminach i jaka wynika z udzielanych nam odpowiedzi.

Opisane powyżej przypadki są wierzchołkiem góry lodowej - a incydenty tego typu miały miejsce w setkach innych gmin i wynika to z udzielanych odpowiedzi na nasze wnioski w trybie ustawy o dostępie do informacji publicznej i nasze skargi złożone do Rad Gmin w trybie art 229 KPA

Pomimo zalewu informacji o nieprawidłowościach w JST o jakimi zasypują nas w ostatnim czasie media (patrz: linki - zamieszczone in fine niniejszego pisma) oraz częstych niejasności wynikających z udzielanych nam informacji publicznych (świadczących często o nieracjonalności w wydatkowaniu powierzonych Decydentom środków podatków) - mamy nadzieję, że ewentualne postępowanie zainicjowane niniejszą petycją będzie prowadzone nie tylko zgodnie z przepisami prawa ale również lege artis - czyli poza bezwzględnym stosowaniem przepisów prawa również zgodnie z zasadami etyki i uczciwej konkurencji.

Zawsze sugerujemy aby Decydenci - również w przypadku kwot stanowiących mały ułamek granicznej kwoty 130 tys. pln - (uwzględniając oczywiście zapisy wewnętrznych regulaminów) nawet nadmiarowo posiłkowali się dyspozycją art 275 pkt. 2 Ustawy z dnia 11 września 2019 r. Prawo zamówień publicznych (t.j. Dz. U. z 2022 r. poz. 1710, 1812, 1933, 2185, z 2023 r. poz. 412)

I.§2) Aby zachować pełną jawność i transparentność działań - wnosimy o opublikowanie treści petycji (Sekcja dot. petycji) na stronie internetowej podmiotu rozpatrującego petycję lub urzędu go obsługującego (Adresata) - na podstawie art. 8 ust. 1 ww. Ustawy o petycjach - co jest jednoznaczne z wyrażeniem zgody na publikację wszystkich danych naszej osoby prawnej. Chcemy działać w pełni jawnie i transparentnie.

Reasumując - biorąc pod uwagę powyższe wnosimy - jak w osnowie petycji.

Część formalna:

W niniejszym piśmie znajdują się trzy sekcje, które w mniemaniu autora podlegają różnym trybom ustawowym, a co za tym idzie powinny być dekretowane oddzielnie w zależności od aktu prawnego określającego charakter sekcji.

Powyższa część to petycja, natomiast poniżej znajduje się odrębna sekcja, która wg. autora powinna być dekretowana - trybem ustawy Kodeks Postępowania Administracyjnego (t.j. Dz. U. z 2020 r. poz. 256, 695)

Wg. piśmiennictwa i judykatury - taka forma jest jak najbardziej dopuszczalna przyczynia się do oszczędności papieru i pozwala traktować sprawy i pisma Interesantów w sposób kompleksowy. Oczywiście - na urzędnikach ciąży obowiązek dokonania odrębnych odpowiednich dekretacji w zależności od charakteru pisma - w tym przypadku najlepiej w postaci elektronicznej.

Interpretacja wg. piśmiennictwa - vide - J. Borkowski (w:) B. Adamiak, J. Borkowski, Kodeks postępowania..., s. 668; por. także art. 12 ust. 1 komentowanej ustawy - dostępne w sieci Internet.