Or. 152. 3. 2025

Temat: Oficjalny Wniosek/Petycja* w nawiązaniu do art 241 Ustawy Kodeks postępowania administracyjnego (t.j. Dz. U. z 2023 r. poz. 775) - v25064ofZnanyZmowy
Data: Sat, 12 Jul 2025 19:48:57 +0200
Nadawca: Inicjatywa- Cyberbezpieczna Gmina- Jawność i Transparentność- petycje wnioski i skargi pomocne w zmiejszaniu kosztów publicznych <jawnosc-transparentnosc@szulc-euphenics.com>
Adresat: gmina@rosciszewo.pl
Kopia: dwnik@nik.gov.pl

Komparycja Pisma:

Kierownik Jednostki Samorządu Terytorialnego - w rozumieniu art. 33 ust. 3 Ustawy o samorządzie gminnym (t.j. Dz. U. z 2024 r. poz. 1465, 1572, 1940)
Adresatem niniejszego pisma - jest Organ ujawniony w komparycji - jednoznacznie identyfikowalny za pośrednictwem adresu e-mail pozyskanego z Biuletynu Informacji Publicznej Urzędu/Adresata - pod którym odebrano niniejsze pismo.

Aby zachować pełną jawność i transparentność - wnosimy o opublikowanie - niniejszego pisma - w części dot. petycji w BIP Adresata, wyrażając jednocześnie zgodę na publikację wszystkich danych - poniżej podpisanej Osoby Prawnej. (Nadawcy niniejszego pisma) Podstawa prawna, na którą powołujemy się wnosząc o publikację - w Internecie w **BIP Urzędu** - kontentu dotyczącego niniejszej petycji - określona została w art. 8 ustawy z dnia z dnia 11 lipca 2014 r. o petycjach (tj. Dz.U. 2018 poz. 870)

Dane nadawcy (Osoba Prawna) - znajdują się poniżej w stopce oraz - w załączonym pliku sygnowanym podpisem elektronicznym, weryfikowanym kwalifikowanym certyfikatem - stosownie do dyspozycji Ustawy z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej (t.j. Dz. U. z 2024 r. poz. 1725). W miarę możliwości prosimy o niedrukowanie niniejszego pisma i dekretowanie i archiwizowanie go w postaci elektronicznej.

Data dostarczenia pisma do Urzędu - dla potrzeb ewentualnej procedury odwoławczej i sądowo-administracyjnej - rejestrowana jest po stronie nadawcy zgodnie z dyspozycją art. 61 pkt. 2 ustawy Kodeks Cywilny (t.j. Dz. U. z 2024 r. poz. 1061, 1237)

W niniejszym piśmie znajdują się 3 sekcje, które w naszym mniemaniu powinny być dekretowane - oddzielnie - w trzech różnych trybach ustawowych.
Zgodnie z art 222 KPA to na urzędnikach ciąży obowiązek podziału pisma na 3 sprawy, które w mniemaniu autora podlegają różnym trybom ustawowym, a co za tym idzie powinny być dekretowane - oddzielnie - w zależności od aktu prawnego na który powołuje się autor pisma w danej sekcji.
Prosimy o ile to możliwe aby nie drukować pisma ale procedować je w postaci elektronicznej - vide judykatura i piśmiennictwo: "J. Borkowski (w:) B. Adamiak, J. Borkowski, Kodeks postępowania..., s. 668; por. także art. 12 ust. 1 komentowanej ustawy (...) Dzielenie pisma na kilka spraw i dekretacja w różnych trybach - Postanowienia WSA i piśmiennictwo - dostępne w sieci Internet.

Preambuła pisma *(petycji/Wniosku*)*

Tematyką niniejszego pisma jest walka z incydentami naruszającymi cyberbezpieczeństwo danych powierzonych Urzędnikom przez Obywateli. Znany jestem z tego, że od 20 lat pytam w tym trybie wszystkie jednostki administracji publicznej w kraju w tym jednostki centralne, jednostki związane z edukacją, kulturą, uczenie wyższe, etc - vide www.szulc-euphenics.com

Duże uszczegółowienie niniejszego pisma, drobiazgowe powoływanie się na podstawy prawne oraz stosowana nomenklatura słowna wynikają ważkości tematyki, oraz z olbrzymiej skali zagrożeń jakie pojawiają się w związku z incydentami godzącymi w cyberbepieczeństwo danych powierzonych Urzędnikom oraz z katastrofalnych skutków - jakie niesie ze sobą nasilający się w ostatnim czasie - cyberterroryzm.

Każdy, kto analizuje doniesienia prasowe oraz ma dostęp do uzyskiwanych od 25 lat przez nasz podmiot informacji w trybie ustawy o dostępie do informacji publicznej - jest zaszokowany bezczynnością gmin i marnotrawstwem środków publicznych w tym obszarze.
Każdy kto analizuje te materiały - nabiera przekonania, że coraz liczniejsze skuteczne cyberwłamania i incydenty (vide: linki do doniesień prasowych zamieszczone na końcu pisma) - są oczywistym i naturalnym następstwem nieracjonalnego wydatkowania środków w tym obszarze kompetencji przez Urzędy oraz ignorowania rzeczonej problematyki przez Decydentów.
Problem staje się szczególnie istotny w obecnej - złożonej sytuacji geopolitycznej.

W mniemaniu wnioskodawcy - Ministerstwo Cyfryzacji skutecznie i efektywnie zabiega o dodatkowe środki w ramach kolejnych grantów przeznaczanych dla JST.
Miarą skuteczności i zaangażowania Ministerstwa Cyfryzacji jest to, ze wg. szacunków łączne środki przekazane JST w ostatnim czasie przewyższają kwotę 2 mld pln.

Z kolei w niektórych gminach - w naszym mniemaniu - nie przykłada się należytej wagi do praktycznej strony spożytkowania tych środków, a ciągle i wykładniczo zwiększająca się ilość skutecznych incydentów tego typu świadczy że być może oddolnie popełniany jakiś powtarzający się błąd - związany ad exemplum - z bagatelizowaniem pewnych wynikających z empirii - najczęściej powtarzających się zagrożeń.

Osnowa Petycji:
Sekcja I
§1) **Wnosimy rozważenie podjęcia działań związanych z sanacją obszaru cyberbezpieczeństwa - scilicet - aby - oprócz wydatkowania olbrzymich kwot na sprzęt,**

procedury i szkolenia (gminy zwykle w ramach programu Cyb. Sam. wydatkują w 2025 r. średnio pól miliona zł - dotychczas uzykałem z ok. 1000 gmin szczegółowe odpowiedzi dot. wydatkwan ia tych środków w ramach projektu) - mały promil tych kwot przeznaczyć (ze środków programu lub ze środków własnych) na dodatkowe położenie nacisku na analizę najczęściej dotychczas popełnianych przez Decydentów "błędów ludzkich" w tym obszarze.
Ze skarg jakie składamy do Rad Gmin (a kierownicy JST ad exemplum: vide: Konstancin Jeziorna często nie infomują Rady Gminy o incydentach https://www.facebook.com/GdzieJest5mln/ i unikają udzilania inofmacji publicznych - dopiero skarga do WSA lub Kom. SKarg i wnioskOw RG -powoduje opisaniue incydnetu **) wynika że to nie sprawy sprzętowe lub procedury są najczęściej powodem skutecznych cyberataków ale proste błędy ludzkie (behawioryzm, socjotechnika) . Zatem w minimalnym stopniu dbając również o ten aspekt - można skuteczniej walczyć ze zwiększającą się cały czas plagą incydentów i skutecznych aktów cyberterrozymu w JST.**
Oczywiście na sprzęt, szkolenia i procedury - należy wydatkować średnio pól miliona złotych - autor petycji prosi tylko o rozważenie zachowania status quo

Uzasadnienie Petycji:
Jak wynika z otrzymanych z JST odpowiedzi na nasze wnioski/petycje do Kierowników JST i skargi do RG - dotyczące obszaru cyberbezpieczeństwa - Urzędy w ostatnim czasie notabene - jedynie dzięki grantom z Ministerstwa Cyfryzacji - wydatkowały/będą wydatkować od 182 tys. pln do 1,6 mln zł. - środków pochodzących z pieniędzy Podatników.

Zakupywany jest sprzęt za setki tys. zł, szkolenia za dziesiątki tys. zł., tworzy się procedury, dokumentację i polityki bezpieczeństwa - i w mniemaniu autora pisma - bezwzględnie należy tak dalej czynić, a nawet więcej - zwiększając rzeczone nakłady o środki własne JST i preferując w jeszcze większym stopniu podejście holistyczne do tematyki cyberbezpieczeństwa i przeciwadzialania aktom cyberterryzmu.

Jednakże - jak wynika z publikowanych danych Ministerstwa Cyfryzacji i udzielanych nam przez Gminy odpowiedzi w trybie Ustawy z dnia 6 września o dostępie do informacji publicznej (t.j. Dz. U. z 2022 r. poz. 902) - z każdym tygodniem zwiększa ilość skutecznych cyberataków i aktów cyberterroryzmu - być może sterowanych przez zagraniczne służby w ramach wojny hybrydowej.

Co dziwne - jak wynika z udzielanych nam odpowiedzi - gros z tych incydentów i aktów cyberterroryzmu nie jest związanych ze złamaniem zabezpieczeń sprzętowych, skomplikowanych procedur czy błędami pracowników szeregowych lub średniego szczebla w JST. Błędy te to najczęściej błędy Decydentów zarządzających JST - na linii Skarbnik/Sekreatrz/Wójt/Burmistrz/Prezydent, a modus operandi i metodologia stosowana przez cyberprzestępców - dotyka socjotechniki, inżynierii społecznej i "behawioryzmu urzędniczego"

Tak było w przypadku głośnych medialnie incydentów (czy jak pisze prasa „kompromitacji") jakie miały miejsce w zasobnych i bogatych gminach - inter alia: Konstancin Jeziorna, Rząśnia, Piekary Śląskie i setki innych.

Do każdego z tych urządów, równolegle z postępowaniem prowadzonym przez odnośne miejscowo Prokuratury - staramy się - w miarę naszych możliwości czasowych złożyć szczegółowe zapytanie w trybie ustawy z dnia 6 września o dostępie do informacji publicznej (t.j. Dz. U. z 2022 r. poz. 902) w przedmiocie na czym de facto polegał ten błąd/kompromitacja Decydenta. Jeśli urząd odpowiada enigmatycznie składamy skargę na Kierownika JST w trybie art 229 KPA do Rady Gminy, aby Rada Gminy lub WSA nadzorowała dopilnowano udzielenia odpowiedzi zgodnej ze stanem faktycznym, intencjami Ustawodawcy i uzasadnionym interesem społecznym pro publico

bono - zastrzegając aby nie udzielano nam ewentualnych informacji określonych w przepisach o ochronie informacji niejawnych oraz o ochronie innych tajemnic ustawowo chronionych.

W przypadku Konstancina Jeziornej i głośnej kradzieży 5 mln zł. pieniędzy podatników, w ramach „dziecinnego" błędu popełnionego na linii Skarbnik - Burmistrz - Sekretarz - znaleźliśmy czas aby złożyć - zarówno skargę do Rady Gminy jak i Skargę do Wojewódzkiego Sądu Administracyjnego - vide: https://warszawa.wyborcza.pl/warszawa/7,54420,32051994,referendum-w-konstancinie-radni-na-wojnie-z-burmistrzem-odmowili.html

W miarę możliwości czasowych zamierzamy złożyć Petycję i Skargę do każdego Urzędu, w którym miał miejsce incydent per analogiam.

Łącząc uzasadniony interes pro publico bono ze statutowymi celami naszej osoby prawnej, zawodowym charakterem naszej działalności, celami merkantylnymi i podatkowymi - zamierzamy - działając lege artis i zgodnie z zasadami uczciwej konkurencji - uzyskiwane w ten sposób informacje udostępniać zwrotnie JST - tak aby w ten sposób podjąć próbę sanacji tego obszaru w trybie art. 241 KPA i próbę zatrzymania zwiększającej się fali incydentów tego typu.
Są to o tyle cenne informacje, gdyż mówią o idee fixe - jaka wyłania się z tej analizy - a clou tych ciągle powtarzających się błędów Decydentów - związana jest z prostymi - wręcz infantylnymi błędami na linii Wójt/Burmistrz/Skarbnik/Sekreatrz.

Naszą idee fixe jest to aby uzyskiwane w ten sposób informacje publiczne - działały jak quasi panaceum czy dobrze przetestowana szczepionka - przestrzegając zapoznających się z nimi Decydentów przez najczęściej popełnianymi błędami tego typu.
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 i wiedzy wynikającej z empirii dot.okoliczności i szczegółów ich wystąpienia w innych JST.

Są to o tyle unikalne i cenne informacje, że Decydenci, których Prokuratura pyta o szczegóły ich błędów i deliktów, często korzystają z możliwości "odmowy zaznań" przed Prokuratorem tak aby nie narazić się na dodatkową odpowiedzialność karną i cywilną. Kiedy z kolei nasz Podmiot pyta o ten sam incydent (cyberatak/akt cyberterroryzmu) w trybie ustawy o dostępie do informacji publicznej (t.j. Dz. U. z 2022 r. poz. 902) odpowiedź musi być zgodna ze stanem faktycznym pod groźbą sankcji karnej ipso iure art. 23 tejże ustawy - dlatego informacje zebrane w ten sposób są tak cenne, unikalne i tak skutecznie chronią przez ewentualnym popełnianiem błędów tego typu.

Notabene nie mogąc sobie poradzić ze zwiększającą się plagą tego typu praktyk, mataczeniem, etc - w końcu od 3 lat - prokuratury zaczęły zajmować majątek Decydentów
vide: https://warszawa.wyborcza.pl/warszawa/7,54420,29295633,prokuratura-zajela-mieszkanie-burmistrza-konstancina-jeziorny.html

De facto - jak wynika z analizy uzyskiwanych przez nas odpowiedzi - w skali makro - charakter tych cyberprzestępstw czy aktów cyberterroryzmu - choć każdy polega na innym pomyśle - to jednak charakteryzują się podobnymi mechanizmami. Nawet jeśli cyberprzestępca „pracuje" nad Decydentem w interwale roku czasu - tak było w przypadku głośnej kompromitacji Konstancina Jeziorna - to błąd Decydenta jest zawsze w naturze swojej „odruchowy, prosty wręcz prymitywny" i niweczy ciężką pracę związaną z uprzednio dokonanymi zakupami sprzętu, szkoleniami wykonanymi

za „grube pieniądze" na koszt podatników, czy opracowanymi skomplikowanymi politykami - zajmującymi w tych urzędach nieraz całą szafę i zgodnymi Rozporządzeniem KRI, Normą PN 2700, Ustawą o KSC , etc

Wspólnym mianownikiem jest to, że ofiarą skutecznych ataków tego typu padają Urzędy Gmin całkowicie niezależnie od zaawansowania we wdrażaniu procedur, zakupie specjalistycznego sprzętu czy ilości dobrze wyszkolonych pracowników działu IT. W urzędach takich jak Piekary Ślaskie - działy IT liczą kilku Informatyków zajmujących się stricte jedynie tym obszarem, a - a contrario - w Urzędach takich jak Werbkowice - Informatyk zmuszony jest wykonywać dziesiątki pochodnych i często niezwiązanych z informatyzacją czynności, w pierwszym z urzędów dochody budżetu sięgają prawie pół miliarda zł. rocznie * 500 000 000 w drugim grubo poniżej 50 000 000 pln (50 mln)

vide:
1) ad exemplum - kazus mała Gmina Wiejska -
Werbkowice: https://www.kronikatygodnia.pl/artykul/44281,werbkowice-kto-zaszyfrowal-serwery-w-gminie-czy-wyciekly-dane-osobowe-interesantow
2) ad exemplum: kazus - duże Miasto - Piekary Ślaskie - Materiał tygodnika
Wprost: https://www.wprost.pl/kraj/11626381/piekary-slaskie-porno-na-profilu-urzedu-miasta-na-facebooku-krzysztof-turzanski-zabral-glos.html

Biorąc pod uwagę powyższe wnosimy jak w osnowie petycji.
Może dzięki temu uda się przynajmniej zatrzymać ciągły wykładniczy wzrost incydentów tego typu i oszczędzić małą część z ciągle zwiększającej się kwoty marnowanych/kradzionych w ten sposób pieniędzy podatników. W najgorszym razie może uda się przynajmniej w minimalnym stopniu zmniejszyć ciągle rosnący wskaźnik incydentów tego typu - w zamyśle chcemy aby nasze działania byly przynajmniej czymś w rodzaju inhibitora na ten rosnący trend, nawet jeśli cześć z tych incydentów ma charakter cyberterrozymu sterowanego przez zagraniczne służy w ramach wojny hybrydowej - to demaskowanie prostoty tych mechanizmów - może być jednym z działań jakie przyczynią się do zahamowania ich ciągłego wzrostu.

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

Dodatkowe uzasadnienie/rozwinięcie petycji:
Jak wzmiankowano powyżej - pytamy gminy o przebieg i okoliczności skutecznych incydentów związanych z cyberatakami oraz o wcześniejsze środki Podatników wydatkowane i związane z obszarem cyberbezpieczeństwa.
Z kolei jak wynika z udzielanych nam odpowiedzi środki te są czesto nieracjonalnie wydatkowane w Gminach - i absorbowane inter alia przez Zmowy Cenowe.
Ad exemplum - w niektórych gminach dochodzi do zakupu corocznego audytu, o którym mowa w §19 pkt. 14 Rozporządzenia KRI za kwotę ponad 20 tys. pln.
Ten sam audyt kosztował 3 lata temu 5000 pln - i miało to miejsce do czasu uruchomienia miliardowych środków z Programu Cyberbezpieczny Samorząd - sic !

To tylko jeden z przykładów, a mamy doskonały tego obraz gdyż - jak wiadomo od 25 lat zadajemy szczegółowe pytania Gminom w trybie ustawy o dostępie do informacji publicznej i udzielając odpowiedzi pod takimi absurdalnymi zmowami cenowymi podpisują się Decydenci.
Takich patologii nie wyeliminuje samo stosowanie przepisów związanych z zamówieniami publicznymi - i wszędzie na Świecie wypracowano już skuteczne mechanizmy pozwalające

walczyć ze zmowami cenowymi - w przypadku dodatkowych środków finansowych zwiększających w krótkim okresie podaż w danym obszarze usług.
Jak wykazały udzielane nam odpowiedzi część Decydentów całkowicie ignoruje tematykę - niwecząc tym samym ciężką i efektywną Pracę Ministerstwa Cyfryzacji.

W innych obszarach (np.inwestycje drogowe) wypracowano już mechanizmy weryfikujące zmowy cenowe - o czym można czytać w linkach pond koniec pisma w artykule dot. Prezydenta Tarnowa.
Miejmy nadzieję, że w obszarze cyberbepieczeństwa już niedługo dojdzie do podobnych weryfikacji - chętnie udostępnimy wtedy uzyskane kwantyfikacje.

Wyjaśnienie przedmiotu naszej petycji:
Naszą idee fixe jest działanie łączące - uzasadniony interes pro publico bono - z partykularnymi zdrowo-pojętymi gospodarczymi interesami naszej osoby prawnej.

Większość podmiotów zwracających sie do Urzędów nastawiona jest aby uzyskiwać partykularnie - jakąś osobistą wartość dodaną (zezwolenia/zapomogi/zwolnienia/dokumenty, etc)
W naszym przypadku natomiast - zgodnie z definicją artykułów 28 i 241* Ustawy Kodeks Postępowania Administracyjnego (t.j. Dz. U. z 2020 r. poz. 256, 695) - pragniemy „nie tylko brać" - jak czyni to większość zwracających się do Urzędów Podmiotów - ale w ramach zawodowego charakteru działalności staramy się osiągać synergię z urzędami oraz wnosić wartość dodaną poprzez dzielenie się wiedzą, którą w trybie ustawy o dostępie do informacji publicznej uzyskiwaliśmy w ciągu ostatnich 25 lat i dzięki której poddajemy sanacji i usprawniamy funkcjonowanie administracji publicznej.
W ramach wzmiankowanego art . 241 KPA* namawia do tego Ustawodawca: "Przedmiotem wniosku mogą być w szczególności sprawy ulepszenia organizacji, wzmocnienia praworządności, usprawnienia pracy i zapobiegania nadużyciom, ochrony własności, lepszego zaspokajania potrzeb ludności."
Usprawnianie i zwracanie uwagi na obszary związane z cyberbezpieczeństwem wydaje się szczególnie istotne z punktu widzenia uzasadnionego interesu społecznego pro publico bono.
A jak wynika z udzielanych nam informacji publicznych - o czym pisaliśmy powyżej - stan faktyczny w gminach jest katastrofalny.

Biją na alarm również media (linki do niewielkiej części doniesień prasowych opisujących skuteczne cyberataki na Urzędy - zamieszczamy in fine niniejszego pisma.

Per analogiam - pomimo wydana olbrzymich pieniędzy podatników w ostanim czasie - Najwyższa Izba Kontroli opatruje wnioski pokontrolne z 2025 r. - znaczącym tytulem „Cyberbezpeiczeństwo w samorządach kuleje" dalej w protokołach pokontrolnych NIK zaznacza expressis verbis: „(...) Ponad 70 proc. skontrolowanych przez NIK urzędów samorządowych nie byłoby w stanie zapewnić ciągłości działania systemów informatycznych w przypadku wystąpienia sytuacji kryzysowej. Kontrolerzy Izby wykryli też wiele innych niedociągnięć dotyczących bezpieczeństwa cyfrowego JST. (...) „ od lat NIK zwraca uwagę Samorządowców inter alia również na ataki hybrydowe, etc.
O wszystkich tych negatywnych ocenach można czytać w protokole NIK z lutego 2025 r. - sygnatura akt: KAP.430.9.2024 Nr ewid. 123/2024/P/24/004/KAP - dostępny w pełnej postaci na stronach nik.gov.pl

Skutek wydatkowania olbrzymich środków podatników w tym obszarze jest taki, że o ile w 2019 r. NIK ocenił negatywnie 70% ze skontrolowanych JST w tym obszarze - to w kontroli per analogiam wzmiankowanej powyżej i wykonanej w 2025 r. negatywną oceną objął już nie 70% ze skontrolowanych Urzędów, ale 71% - sic !

Analizują odpowiedzi uzyskiwane z Gmin - nie dziwimy się wcale i uważamy że Minister Cyfryzacji - ma w 100% rację - kiedy powtarza podczas udzielanych wywiadów, że **"Polska jest na cyfrowej wojnie"**
Ministerstwo Cyfryzacji wykonuje tytaniczną pracę, uruchamiając kolejne programy pomocowe podczas kiedy w w gminach chętnie bezrefleksyjnie wydatkowane są środki publiczne na ten cel, beneficjentami są powtarzające się nazwy tych samych firm ... efektem tych wdrożeń mnożą się stosy kopiowanej dokumentacji - w której zmieniają się tylko nazwy gmin.
I wszystko jak mawiają Decydenci - w zgodzie z dokumentacją tylko nieliczne gminy starają się walczyć ze zmowami cenowymi i weryfikować setki stron uzyskiwanej dokumentacji - w której jak pokazują nasze analizy np. po złożeniu skargi do Rady Gminy (gdy rzeczona dokumentacja jest poddawana analizie przez Komisję Skarg i Wniosków) - nawet nazwy gmin są czesto mylone w ramach stosowanej przez Usługodawców techniki /kopiuj/wklej - sic !

Jednakże - jak pokazują uzyskiwane przez nas informacje w trybie ustawy o dostępie do informacji publicznej - skuteczne cyberataki zazwyczaj wiążą się z wyjątkowo prostymi błędami popełnianymi przez Urzędników. Co więcej gros skutecznych ataków wykorzystujących proste błędy Urzędników ma miejsce po wdrożeniu programu „Cyfrowa Gmina" i w trakcie wdrażania programu „Cyberbepieczny Samorząd" - tak jakby hakerzy chcieli udowodnić sobie lub Urzędnikom, że oprócz sprzętu i procedur - ważny jest również aspekt psychologiczny i praca przede wszystkim nad obszarem behawioralnym w Urzędach.
Jak wykazują odpowiedzi na nasze wnioski - w których Decydenci opisują genezę incydentów - pracy nad obszarem behawioralnym - nie zastąpi żaden żaden sprzęt zakupiony za pieniądze podatników i żadne procedury usprawniane i kopiowane w stosach dokumentów na papierze.

Wnioskodawca z premedytacją wydłużył niniejszy wstęp - tak aby w BIP gminy - opublikowana została powyższa analiza oparta na wnioskach instytucji kontrolnych analizujących stan faktyczny w skali makro oraz na uzyskiwanych przez nas informacjach publicznych.
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.

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, Tuczna czy Piekary Ślaskie - ze względu na złożone umiejętności atakujących skutkujące popełnieniem odruchowych i prostych błędów przez Decydentów - mnożna nazwać jedynie mianem cyberterroryzmu i tylko przypadek sprawił, że dotyczyły akurat wzmiankowanych Urzędów - a nie innych.

W krajach UE w większym stopniu działania sanacyjne skupiają się na analizie dobrych praktyk i zaistniałych kazusów. Ataki jakie miały miejsce na terenie Krajów UE i jakie miały miejsce na instytucje samorzadowe w Estonii, na gminy w Finlandii czy w Norwegii - są dokładnie poznane, omówione i przeanalizowane pod kątem każdego szczegółu. choć bazują już na bardziej skomplikowanych mechanizmach i są świadectwem, że nawet najlepsze zabezpieczenia serwerów nie wystarczą jeśli nie zadba sie 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.
W naszym kraju niewiele podmiotów (poz nami) posiada elementarną wiedzę o tym co tak naprawdę wydarzyło się w Konstancinie Jeziornej, Piekarach Śląskich czy w głośnych cyberatakach na Urzędy Marszałkowskie

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://samorzad.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 odwiedzi 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 podatników) - mamy nadzieję, że ewentualne postępowanie zainicjowane niniejszą petycją bedzie prowadzone nie tylko zgodnie z przepisami prawa ale rownież 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)

Ponadto:
W trybie Ustawy o petycjach (Dz.U.2018.870 tj. z dnia 2018.05.10) wnosimy o przeprowadzenie analizy art 275 pkt. 2 Ustawy Prawo zamówień Publicznych pod kątem zastosowania dyspozycji tego przepisu tak aby przeciwdziałać opisanym przez NIK i przez wnioskodawcę - występującym permanentnie ZMOWOM CENOWYM
Rzeczone ZMOWY CENOWE powodują defraudację i marnotrastwo środków publicznych. Petycjoidawca ma na myśli zastosowanie przedmiotowego przepisu również do zamówień - poniżej 130 tys. pln.

Uzasadninienie tej części petycji:

Wiadomym dla wszystkich jest, że - zawsze po wejściu w życie programów dofinansowania usług w Jednostkach Administracji Publicznej - ceny na rynku wzrastają i jest to oczywiste z punktu widzenia prawa popytu i podaży.

Natomiast w przypadku programu „Cyberb. Sam." wzrost kwantyfikacji cenowych określanych przez firmy biorące udział w postępowaniach jest na tyle drastyczny, że wzmiankowana zmowa cenowa - sięga czasami nawet 250% (w przeciągu 4 lat) - sic! - I wynika to nie z naszej oceny - lecz z uzyskiwanych przez nas z JST odpowiedzi.

Przypominamy, że w naszych wnioskach/petycjach i skargach podajemy konkretne przykłady w których - po uzyskaniu środków z Grantu - Decydenci w Gminach:

- wydatkują zawyżone środki w postępowaniach (zmowa cenowa)

- marnotrawią środki - gdyż poziom bezpieczeństwa nie wzrasta - o dziwo skuteczne włamania najczęściej mają miejsce - w końcowej fazie konsumpcji grantu tak jakby cyberprzestępcy w ten sposób dodatkowo chcieli ośmieszyć polskie gminy (lub udowodnić w swoim przestępczym kręgu - że pokonali wyższą poprzeczkę.

- zbyt mało percepcji poświęcają na analizę błędów ludzkich - wynikających w empirii i kazusów jakie już zaistniały

Wszystko to nie wynika z jakiegoś „badania naukowego oderwanego od rzeczywistości" - wynika to z udzielanych nam odpowiedzi w trybie ustawy o dostepie do informcji publicznej i tym chcemy się podzielić z Decydentami.

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 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 znajduje się kilka sekcji, 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.

Nadawca Pisma:
Osoba Prawna:
Szulc-Euphenics.com p. Spółka Akcyjna
Prezes Zarządu - A. Szulc
ul. Poligonowa 1
04-051 Warszawa
tel. 608-318-418
nr KRS: 0001 007 117
www.szulc-euphenics.com

Aby zobrazować jak - na wszelkich polach staramy się walczyć ze zmowami cenowymi i nieprawidłowościami - załączmy poniżej merytoryczną i konstruktywną analizę naszego wniosku przeprowadzoną przez Marszałka Woj. Małopolskiego (oczywiście w innym obszarze niż cyberbezpeiczenstwo) . Liczymy, że JST z taką samą atencją i wnikliwością potraktują kontent powyższego naszego pisma. Pełna treść dokumentacji w tej mierze i wnikliwej analizy jaką przeprowadził Marszałek wraz z podległymi służbami w tej mierze - znajduje się w BIP Urzędu Marszałkowskiego.
W naszym mniemaniu tematyka poruszana w niniejszym powyższym piśmie - jest par excellence - nawet - jeszcze bardziej istotna niż w przypadku tematyki analizowanej przez Marszałka - mamy nadzieję, że w przypadku powyższego wniosku zostanie dokonana równie wnikliwa analiza.
Prosimy aby adresat równie poważnie potraktował nasze powyższe pismo.