

Skarga na Kierownika Jednostki JST w przedmiocie braku należytego nadzoru nad obszarem cyberbezpieczeństwa i obiegiem dokumentów

Skarga na Kierownika Jednostki JST w przedmiocie braku należytego nadzoru nad obszarem cyberbezpieczeństwa i obiegiem dokumentów

Od:

Wysłano:

Do:

DW:

Temat:

Załączniki:



poniedziałek, 23 lutego 2026 09:43

adresat.urzad@samorzad.pl

dwnik@nik.gov.pl; kancelaria@mc.gov

Skarga3 do Rady Gminy - w trybie art. 229 Ustawy Kodeks postępowania administracyjnego (t.j. Dz. U. z 2023 r.) w związku z art. 241 KPA +tel + cyber Sygnowno - sygnowane - kwalifikowanym podpisem elektronicznym

2020.docx.xades; Załącznik bez tytułu 00003.htm; sygnowno24.pdf; Załącznik bez tytułu 00006.htm; 3. KSWP_st_nr2_wniosek kompostowniki.pdf; Załącznik bez tytułu 00009.htm; Chlewiska Wojewoda Rozstrzygnięcie nadzorcze do Uchwały 39.pdf; Załącznik bez tytułu 00012.htm

Rada Gminy

KSİW*

Przewodniczący Rady Gminy

ex officio - wnosimy o przekazanie - za pośrednictwem - Kierownika Jednostki Samorządu Terytorialnego (dalej JST) - w rozumieniu art. 33 ust. 3 Ustawy o samorządzie gminnym (t.j. Dz. U. z 2024 r. poz. 1465, 1572.)

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).

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

Adresatem Pisma/Skargi* - jest Organ ujawniony w komparycji - jednoznacznie identyfikowalny za pośrednictwem adresu e-mail pod którym odebrano niniejszą skargę/wniosek/petycję/ *. **Rzeczony adres e-mail uzyskano z Biuletynu Informacji Publicznej Urzędu.**

W celu zapewnienia jak największej jawności i transparentności* naszych działań - wnosimy o publikację pełnego niniejszego dossier formalnego dot. rzeczony skargi w BIP adresata.

Skargodawca jest świadomy, że przepisy prawa nakazują publikację - jedynie petycji (w przypadku skargi taka możliwość jest fakultatywna). Jednakże wnosimy o publikację - publikację wszystkiego czego nie zabraniają przepisy prawa w BIP aby upowszechniać i promować zasady związane z zastosowaniem art. 241 Ustawy Kodeks Postępowania Administracyjnego (t.j. Dz. U. z 2024 r. poz. 572, z 2025 r. poz. 769.), upowszechniać dobre praktyki dot. cyberbezpieczeństwa i zasady uczciwej konkurencji przy wydatkowaniu środków podatników.

W razie wątpliwości co do trybu jaki należy zastosować do naszego pisma - wnosimy o bezwzględne zastosowanie dyspozycji art. 222 Ustawy z dnia 14 czerwca 1960 r. Kodeks postępowania administracyjnego (t.j. Dz. U. z 2020 r. poz. 256, 695)

Preambuła Skargi:

Głośne medialnie incydenty naruszenia zasad cyberbezpieczeństwa, które opisujemy naszych wnioskach/petycjach/skargach* (pismach) - stanowią niezwykle ważny przyczynek do zaznajamiania się z najczęściej popełnianymi przez Decydentów błędami w tym obszarze, które - jak opisujemy naszych pismach - skutkują stratami olbrzymich kwot i kompromitacją wielu urzędów - vide opis in fine.

Co więcej - jak sygnalizuje strona rządowa, media i specjaliści - ilość skutecznych cyberincydentów z tygodnia na tydzień wzrasta i oczywiście - częściowo spowodowane jest to wojną hybrydową i obecną sytuacją geopolityczną, ale również błędami strukturalnymi błędami w JST.

Dodatkowo rzeczoną problematykę i patologie w tym obszarze - dokładnie przeanalizowała Najwyższa Izba Kontroli - i wyciąg z przerażających wniosków NIK z protokołów pokontrolnych - publikujemy poniżej - szeroko cytujemy również in fine skargi. Sygnaturę akt rzeczonych protokołów pokontrolnych NIK podajemy w kontencie skargi - a w całości z tymi zarzutami NIK w stosunku do większości kontrolowanych JST - można zapoznać się w ramach podanych przez nas sygnatur - na stronach www.nik.gov.pl

Ad exemplum: Konstancin J. - kazus ówczesnego Burmistrza Konstancina J. , któremu odnośna miejscowo Prokuratura zajęła mieszkanie - omawiany jest na konferencjach również w krajach UE, w piśmiennictwie, a nawet na Wyższych Uczelniach i w szkołach na zajęciach dot. cyberhygieny.

vide <https://warszawa.wyborcza.pl/warszawa/7,54420,27390892,gminie-konstancin-jeziorna-skradziono-5-milionow-zlotych-jak.html>

Utrata 5 milionów pieniędzy podatników i próby mataczenia oraz ukrywania tego faktu przez ówczesnego Burmistrza - sprawiły, że - szczególnie młodzież uważa często - choć w naszym mniemaniu niesłusznie - wszystkich Urzędników za nieudaczników - marnotrawiących pieniądze Podatników.

Chcemy - naszymi wnioskami, skargami i petycjami - choćby nawet w minimalnym (mikroskopijnym) stopniu przyczynić się do sanacji tego obszaru.

Z drugiej strony nikt tak naprawdę (poza naszym podmiotem) - pomimo - wielu szkoleń zamawianych przez Gminy - nie wie jak rzeczywiście - w empirii doszło do deliktu w Konstancinie, czy w Gminie Rzęśnia (kilkukrotne włamanie, Piekary Śląskie, etc - jak skomplikowane zaistniały mechanizmy związane z inżynierią społeczną, socjotechniką, behawioryzmem jak koronkową długotrwałą i nieuczciwą pracę wykonali cyberprzestępcy lub cyberterroryści aby doprowadzić to takich zdarzeń.

Jak wynika z odpowiedzi na nasze skargi i wnioski z ogólnego obrazu jaki się wylania - być może nawet inicjatorem niektórych z tych włamań i prób włamań (które miały miejsce już w niemalże wszystkich JST) **są cyberprzestępcy powiązani z obcymi służbami - działającymi w ramach wojny hybrydowej. Ten fakt powinien szczególnie niepokoić.**

Na szkoleniach poruszane są zazwyczaj - wszystkim ogólnie znane (książkowe) modelowe (często abstrakcyjne - te same) przypadki, z drugiej strony - skąd ma być czerpana szczegółowa wiedza o zaistniałych kazusach - skoro - jak donoszą media nawet w prokuraturze np. rzeczony Burmistrz Konstancina J. - (jako podejrzewamy) może odmawiać zeznań i nie chce szczegółowo informować o swoich błędach - bazując na art 175 KPK.

Być może zajęcie mieszkania Burmistrza - miło również jakiś związek z brakiem należytej współpracy z Organami.

Z kolei Kazus Piekar Śląskich jest modelowy w ramach naszych analiz - mianowicie na oficjalnej stronie Gminy Piekary Śląskie funkcjonował film pornograficzny, a Urzędnicy w tym samym czasie nie byli w stanie skontaktować się z podmiotem odpowiedzialnym za utrzymanie na serwerach - rzeczonyj oficjalnej strony/profilu. W efekcie tego Urzędnicy - zmuszeni byli - gorączkowo - kontaktować się jedynie „z botami” dostawcy usług - co jest dobitnym przykładem tego że warto zaznajamiać się ze szczegółami takich deliktów gdyż w dosyć łatwy sposób można im

prewencyjnie przeciwdziałać i nie trzeba do tego sprzętu, skomplikowanych procedur czy „książkowych” szkoleń za dziesiątki tysięcy złotych. Notabene opisując rzeczoną sytuację Dziennikarze - niesłusznie i w sposób krzywdzący - pisali w tym czasie w mediach, że „Pani Prezydent Miasta udostępnia pornografię ...” .

Wszystkie tego typu przypadki - opisały nam szczegółowo (nieraz minuta po minucie) - skompromitowane - gminy w trybie ustawy o dostępie do informacji publicznej i taką wiedzę empiryczną chcemy się w ramach naszego zawodowego charakteru - pracy - ex porfesso - dzielić się z innymi gminami - ta aby ułatwiać wyciąganie wniosków i działania prewencyjne. Już sama wiedza o szczegółach tych włamań powoduje, że ich powtórzenie - w podobnym modelu - staje się trudniejsze dla cyberprzestępców.

W obecnej trudnej sytuacji geopolitycznej (wojna hybrydowa) -warto szczegółowo omawiać takie kazusy tym bardziej - że incydenty tego typu mają miejsce nagminnie, ich ilość (jak wynika z udzielanych nam odpowiedzi) wzrasta się z każdym miesiącem, a gros gmin nie wyciąga konstruktywnych wniosków - czego najlepszym dowodem, jest to, że w gminie Rzęśnia przypadek per analogiam wystąpił - **nawet dwukrotnie** - sic! vide: <https://tvn24.pl/lodz/rzasnia-gmina-stracila-5-mln-zlotych-jest-prokuratorskie-sledzwo-st5091169>

Tymczasem szczegółowe informacje o tym jak doszło do deliktów i jakie popełniono błędy - pozwalają na wyciąganie wniosków i przynajmniej - próbę korygowania najczęściej popełnianych błędów ludzkich.

Co więcej z ostatniej - z naszej korespondencji i dyskursu prowadzonego z Urzędami - w trybie ustawy o dostępie do informacji publicznej (t.j. Dz. U. z 2022 r. poz. 902, etc, etc), i w trybie ustawy o petycjach (Dz.U.2018.870 t.j. z dnia 2018.05.10) oraz w trybie art. 253 i art. 241 KPA - wynika, że - Paradoksalnie w Urzędach - gdzie nieraz sprzęt związany z cyberbezpieczeństwem został zakupiony za miliony złotych i wdrożono skomplikowane mechanizmy proceduralne (polityki normy PN 27001, etc) - a contrario - nie działają z kolei najprostsze mechanizmy kontrolne. Mechanizmy związane **stricte z socjotechniką i behawioryzmem urzędniczym czy najprostszymi błędami ludzkimi** jakie występują najczęściej (jak wynika z odpowiedzi nam udzielonych) i jakich nawet nie omawia się na szkoleniach gdyż wydają się zbyt trywialne.

Może pomijanie analizy najprostszych i najczęstszych zaistniałych przypadków jest powodem, że **z miesiąca na miesiąc w tym obszarze jest coraz to gorzej - pomimo wydatkowania takich olbrzymich środków Podatników na sprzęt, złożone procedury, polityki czy szkolenie prowadzone przez najbardziej renomowane firmy. Nawet tak skompromitowane i „renomowane” firmy jak Ernst & Young - vide <https://www.rp.pl/biznes/art38265271-ey-ma-problemy-w-niemczech-ma-zaplacic-kare-i-zakaz-prowadzenia-waznych-audytow>** - nastawiają się teraz na świadczenie usług dla naszego JST.

Tymczasem nikt nie szkoli w oparciu o zaistniałe kazusy - i to stało się naszą idee fixe - w tym obszarze podejmujemy sanację w trybie art. 241 KPA.

Inne przypadki opisujemy in fine skargi.

Specjalizujemy się w obszarze wniosków o udostępnienie informacji publicznej od 25 lat - vide www.szulc-euphenics.com - aby wyjaśnić naszą idee fixe posłużę się przykładem wnioskowania do upadłej gminy Ostrowice o udostępnienie informacji publicznej.

Część z uzyskanych informacji publicznych publikujemy - zatem - mam wrażenie że przyczyniliśmy się do tego, iż wiele cennych informacji o nieprawidłowościach - z punktu widzenia uzasadnionego interesu społecznego pro publico bono - w wielu gminach - ujrzało światło dzienne.

Być może informacje o zadłużeniu Gminy Ostrowice w parabankach na kwotę ponad 50 mln pln - również w jakim stopniu wypłynęły dzięki nam - wypłynęły szybciej (skoro RIO oraz Radni Opozycyjni nie podnosili tych spraw na odpowiednio wcześniejszych etapach)

Zatem w ramach mojej idee fixe staramy się łączyć ex professo - uzasadniony interes społeczny pro publico bono z naszymi interesami partykularnymi - jakie powinien posiadać posiada de facto każdy interesant przychodzący do Urzędu w ramach przepisów prawa, równości wobec prawa i zasad uczciwej konkurencji oraz racjonalnego wydatkowania przez Decydentów środków Podatników. Specjalizujemy się inter alia w dostępie do informacji publicznej i optymalizacji urzędów w trybie art 241 KPA.

Osnowa Skargi:

W związku z tym w trybie art 229 pkt. 3 Ustawy z dnia 14 czerwca 1960 r. Kodeks postępowania administracyjnego (t.j. Dz. U. z 2020 r. poz. 256, 695 - dalej KPA) składam niniejszym skargę na Kierownika Jednostki JST w przedmiocie braku należytego nadzoru nad obszarem cyberbezpieczeństwa i obiegiem dokumentów - formułując następujące zarzuty/zarzuty*:

Zarzut 1) Naruszenie obowiązku nałożonego na Kierownika Jednostki w zakresie - art. 8 Ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (t.j. Dz. U. z 2024 r. poz. 1077, 1222).(dalej KSC)

Zarzut 2)* W mniemaniu Skargodawcy - Organ podlegający niniejszej skardze - per analogiam jak wiele innych Urzędów - przywiązuje zbyt małą wagę do analizy zaistniałych incydentów związanych z cyberbezpieczeństwem jakie miały miejsce w innych gminach .

Zaistniałe w innych gminach błędy związane z cyberbezpieczeństwem w obszarze Decydentów: Wójt/Burmistrz-Sekretarz-Skarbnik

W naszym mniemaniu taka analiza jest równie ważna jak zakup sprzętu, szkolenia, etc i warto mały ułamek percepcji w obszarze cyberbezpieczeństwa - poświęcić również na analizę tego obszaru.

Zarzut3)* w mniemaniu Skargodawcy - taki stan faktyczny - biorąc pod uwagę trudną sytuację geopolityczną - narusza zasady uczciwej konkurencji - poprzez inter alia - narażenie danych osób fizycznych oraz przedsiębiorców na kradzież danych.

Notabene kiedy próbujemy w JST w formie naszych petycji, wniosków i skarg - optymalizować stan faktyczny w tym obszarze i prowadzić dyskurs w trybie art 241 KPA i w trybie ustawy o dostępie do informacji publicznej (t.j. Dz. U. z 2022 r. poz. 902, etc, etc) - odnosimy wrażenie eliminowania części firm spoza terenów Województwa - oraz całkową akceptację zmów cenowych jakie pojawiły się -w ciągu ostatnich dwóch lat ze względu na duży popyt na usługi informatyczne w skali Kraju - w obszarze informatyzacji działalności Jednostek Administracji Publicznej

Zdaniem skarżącego - taki stan faktyczny - również narusza zasady uczciwej konkurencji w związku z wydatkowaniem środków publicznych (środków podatników)

O naszej działalności pro publico bono - można czytać na naszym portalu www.szulc-euphenics.com - z deliktami (we wszystkich gminach - poza kilkunastoma gminami na terenie Kraju sytuacja jest per analogiam i ustawa o KSC - nie jest de facto respektowana nawet w 50% - co w rozmowie telefonicznej możemy wyjaśnić w empirii - powołując się na konkretne zapisy ustawowe) jakie popełniają Gminy w zakresie cyberbezpieczeństwa można - zapoznać się w kontencie przedmiotowej skargi i. w załącznikach do niniejszej.

Uzasadnienie Skargi:

W mniemaniu Skargodawcy - w ostatnim czasie dzięki staraniom i ciężkiej pracy wykonanej przez Ministerstwo Cyfryzacji - Gminy w skali makro mają/miały możliwość wydatkowania w ramach programów „Cyfrowa Gmina” i „Cyberbezpieczny Samorząd” w skali Kraju prawie 4 miliardy złotych.

To wielki przywilej, że JST mogą - dzięki Min. Cyfr. wydatkować środki Podatników - w obszarach wskazanych przez Grantodawcę.

Ze środków Podatników w tym obszarze korzysta/Korzysta również - jak wynika z naszej analizy - skrażony Organ.

Przed złożeniem niniejszej skargi dokonaliśmy analizy BIP Organu a także innych dostępnych informacji publicznych w tym wcześniejsze Odpowiedzi Organu(ów) na nasze wnioski/petycje/skargi oraz zamówień planowanych i realizowanych przez Organ(*y) w interwale okresu przyjętego do analizy.

Jesteśmy pełni uznania, że Urzędy (w tym skarżony Organ) wydatkują duże środki Podatników na cele związane z cyberbezpieczeństwem - nakłady te - w obliczu - trwającej wojny hybrydowej - i skomplikowanej sytuacji geopolitycznej - **należy nawet wykładniczo zwiększać.**

Jednakże - w mniemaniu Skargodawcy - jak zasygnalizowano w osnowie skargi - Urzędy przykładają zbyt małą wagę do analizy już zaistniałych w JST cyberincydentów.

Firmy szkoleniowe, którym urzędy płacą - w ostatnim czasie setki milionów złotych z pieniędzy Podatników - dzięki programom takim jak „Cyberb. Samorząd.” i wcześniej „Cyf. Gm.” - przekazują jedynie wiedzę modelową, modelowe abstrakcyjne przykłady - niemalże książkowe przykłady cyberincydentów, etc

Reasumując - w opinii - Skargodawcy - niemal we wszystkich Urzędach w tym - u Adresata niniejszej skargi - zbyt małą wagę przywiązuje się do poznania empirycznych aspektów i uwarunkowań związanych z już potwierdzoną praktyką i rzeczywistymi przyczynami skutecznych włamań do Urzędów.

Zły stan przygotowania naszych JST w obszarze cyberzagrożeń - par excellence- potwierdza w swoich protokołach NIK (poniżej opisujemy szerzej rzeczoną tezę)

Paradoksalnie więc - ad absurdum - nawet sami samorządowcy nie wiedzą tak naprawdę co było powodem głośnych cyberoszustw - ad exemplum: w Konstancinie, Rzęśni, Otwocku, dlaczego opublikowano film pornograficzny na oficjalnej stronie Piekarskich, dlaczego tytuł skarbników zostało dyscyplinarnie zwolnionych (inter alia Skarbnik Konst. Jez.), jak doszło - de facto - zaszyfrowania systemu Elektronicznego Zarządzania Dokumentami (EZD) w Urzędzie Marszałkowskim Woj. Mazowieckiego, dlaczego tytuł informatyków zostało dyscyplinarnie zwolnionych przez Wójtów/Burmistrzów/Prezydentów w tym informatyk jednej z najbogatszych Gmin - Gminy Nowiny. Dlaczego Wójtowie/Burmistrzowie - nieświadomie płacą quasi okupy - firmom, które rzekomo odszyfrowują dokumenty- po uprzednim zaszyfrowaniu dokumentów w urzędach, etc etc - sic - kilku Wójtów odpisało nam nawet że rzeczona firma wystawiła FV za odszyfrowanie dokumentów - sic ! Niemal wszyscy Samorządowcy - na forach - plotkują o tym, że Burmistrzowi Konstancina Jez. prokurator w związku z cyberoszustwem - zajął mieszkanie - ale prawie nikt nie wie tak naprawdę - co było tego powodem - sic ! i jakie błędy popełniono.

Taki patologiczny obraz niefrasobliwego wydatkowania pieniędzy podatników wyłania się w ramach uzyskiwanych przez nas informacji publicznych w ramach ustawy z dnia 6 września o dostępie do informacji publicznej (t.j. Dz. U. z 2022 r. poz. 902.), ustawy o petycjach (t.j. Dz.U. 2018 poz. 870) i skarg składanych w trybie art. 229 ustawy z dnia 14 czerwca 1960 r. Kodeks postępowania

administracyjnego (t.j. Dz. U. z 2024 r. poz. 572). W uzasadnionym interesie społecznym pro publico bono - w tych trybach pytamy już o wydatkowane pieniądze podatników od prawie 25 lat i większość doświadczonych samorządowców doskonale kojarzy nasze wnioski/petycje i skargi. W najbliższym czasie jeszcze zintensyfikujemy nasze działania - do końca roku zamierzamy - jeśli czas nam pozwoli - złożyć ponad 800 skarg do JST. Przy okazji żądamy aby wszystkie nasze skargi były publikowane do wiadomości publicznej w BIP JST oraz apelujemy o walkę ze zmonopolizowanymi cenami - jakie w tym obszarze w obliczu intensywnych i lawinowych wydatków permanentnie mają miejsce po gwałtownym (olbrzymim) popycie na usługi tego typu na rynku) uruchomieniu środków w ramach programu „Cyb. Sam” i „zmów cenowych” jakich samym UZP i „kryterium najniższej ceny „ nie da się ex officio wyeliminować - ad exemplum - wg. uzyskiwanych przez nas informacji publicznych z JST - koszt niektórych usług - w tym obszarze - za jakie Urzędy płacą z publicznych środków - wzrósł nawet o 400 % - sic !

Efektom tych patologii w Gminach jest to, że pomimo wydatkowania olbrzymich środków podatników i olbrzymiej pracy „u podstaw” wykonanej przez Ministerstwo Cyfryzacji - wg. wszelkich statystyk ilość skutecznych cyberwłamania rośnie lawinowo z tygodnia na tydzień - vide: <https://www.prawo.pl/samorzad/lokalne-centra-cyberbezpieczenstwa-cybercuw,533362.html> (...” Średnia dzienna liczba incydentów obsługiwanych przez NASK wzrosła z 220 do 283. Odnotowano również o 57 proc. więcej tzw. incydentów poważnych – czyli takich, które mogą wpływać na ciągłość działania instytucji. W sektorze publicznym odnotowano aż 58 proc. więcej incydentów, w samorządzie – o 53 proc. więcej. To pokazuje skalę wyzwania dla JST. ...”) całość materiału i statystyk w artykule jw.

Takie nieudacznictwo w Gminach - cieszy z pewnością obce służby związane z cyberterroryzmem - i problem nie leży w zbyt małych nakładach środków Podatników w ramach tego obszaru wypełniania zadań publicznych - lecz w naszym mniemaniu - jak opisywaliśmy powyżej - w zbyt małej wadze przykładowej - do analizy już zaistniałych w JST incydentów oraz w zbyt małej uwadze przykładowej do analizy najczęściej popełnianych przez Decydentów błędów (vide przykłady powyższej)

Ponadto zauważamy, że w Urzędach nie ma wiedzy co do Intencji Ustawodawcy w zakresie dobroczynności działania art. 241 KPA, na który często powołujemy się w naszych wnioskach/petycjach/skargach.

W związku z powyższym wnosimy jak określono w zarzucie i podstawie skargi.

Dodatkowo w ramach dekretacji w trybie KPA

§2) Wnosimy o ustalenie przez skarżony Organ - dogodnego dla obu stron terminu na podstawie art. 241 KPA (usprawnienia pracy i zapobiegania nadużyciom, ochrony własności, lepszego zaspokajania potrzeb ludności) w trybie art 253 KPA (Dzień przyjęć Interesantów w sprawach skarg i wniosków.) - ustalenie tego terminu może odbyć się w ramach konsultacji pod numerem 608-318-418

Prosimy aby RG tym razem podjęła próbę nadzoru nad Ogranem w ramach złożonych pism i odnośnych przepisów prawa

Uzasadnienie skargi:

Przed złożeniem niniejszego pisma Wnioskodawca dokonał analizy protokołów NIK, obowiązujących przepisów i trendów w UE oraz dyspozycji Ustawy z dnia 5 lipca 2018 r. o

krajowym systemie cyberbezpieczeństwa (t.j. Dz. U. z 2024 r. poz. 1077, 1222) , Rozporządzenia Rady Ministrów z dnia 21 maja 2024 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (Dz. U. z 22 maja 2024 r.) oraz prawa UE, a także odnośnych Polskich Norm.

Notabene poniżej - korzystając z okazji podzielimy się kilkoma uwagami dot. informatyzacji JST*

W ostatnim czasie w Gminach - z pieniędzy podatników zostały wydatkowane olbrzymie kwoty związane z obszarem cyberbezpieczeństwa.

Planowane jest wydatkowanie w najbliższych 2 latach - w gminach (JST) - kolejnych ok. 2 mld złotych - z pieniędzy Podatników - w ramach tzw. programu „Cyberbezpieczny Samorząd”

W mniemaniu skargodawcy - wzmiankowane - wydatkowane środki Podatników w obszarze cyberbezpieczeństwa - nie zostały właściwie, racjonalnie i oszczędnie zakumulowane w Gminach.

Jeszcze gorzej Gminy oceniane są przez Kontrolerów NIK - vide nik.gov.pl

W protokołach pokontrolnych NIK o wspólnym numerze ewidencyjnym - I/23/001/LSZ i częściowych protokołach dotyczących każdej z kontrolowanych gmin inter alia wystąpienie pokontrolne: LSZ.411.3.4.2023, etc - kontrolerzy NIK opisali wnioski pokontrolne, w których czytać można m.in.:

„ (...) W każdej ze skontrolowanych jednostek negatywnie oceniono zapewnienie bezpieczeństwa teleinformatycznego. Kontrola wykazała wieloletnie zaniedbania dotyczące cyberbezpieczeństwa, infrastruktury informatycznej, wiedzy i szkoleń pracowników, jak i wykorzystywanie nieaktualnego lub nieprawidłowo skonfigurowanego oprogramowania. W konsekwencji urzędy gmin nie były przygotowane na ataki cybernetyczne.

(...)

Ponadto ustalono, że w żadnym ze skontrolowanych urzędów pracownicy nie przeszli odpowiednich szkoleń w zakresie cyberbezpieczeństwa

(...)

„(...) Wieloletnie zaniedbania dotyczące cyberbezpieczeństwa, nieświadomość i brak skutecznych procedur reagowania na zagrożenia, a także wykorzystywanie oprogramowania, które miało krytyczne luki – to główne nieprawidłowości wykryte w urzędach gmin w województwie (...) . W konsekwencji samorządy te nie były w stanie zapewnić skutecznej ochrony przed potencjalnymi atakami cyberprzestępców. (...)”

W ostatnich latach liczba incydentów teleinformatycznych systematycznie rośnie. W raporcie za 2021 r. CSIRT GOV (Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego prowadzony przez Szefa ABW) wskazał na ponad 762 tys. zgłoszeń o potencjalnym wystąpieniu incydentu teleinformatycznego. Dla porównania w 2020 r. było to nieco ponad 246 tys. zgłoszeń i niecałe 227 tys. zgłoszeń w 2019 r.

W samych tylko urzędach miast i gmin zarejestrowano ponad 5,5 tys. incydentów. Jak wynika z danych uzyskanych przez NIK od CSIRT NASK (Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego działający na poziomie krajowym prowadzony przez NASK – PIB), (...) - liczba incydentów zgłaszanych (...) wzrosła aż o ponad 1000%. (...) „

Skargodawca pracuje z gminami już ponad 25 lat i uważa, że w niektórych gminach, które wykonały organiczną pracę związaną z Cyberbezpieczeństwem sytuacja nie jest aż tak tragiczna jak obrazuje to NIK.

W mniemaniu Skargodawcy - Jeśli Gmina współpracuje z doświadczonymi podmiotami, z którymi koncentruje się w pierwszym rzędzie na właściwym określeniu stanu początkowego dostosowanego do specyfiki gminy, wtedy na zasadzie zarządzania realnym ryzykiem - wszystkie kolejne działania wykonywane są w sposób racjonalny, a pieniądze podatników są wydatkowane oszczędnie i powyżej zawarte tezy i zarzuty formułowane przez NIK - są mało prawdopodobne.

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, że wg. szacunków łączne środki przekazane JST w ostatnim czasie przewyższają kwotę 2 mld pln.

Z kolei jak wynika z udzielanych nam odpowiedzi środki te są często 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 - si

Z kolei, jeśli Gmina - wykonuje działania - tylko po to aby utartymi ścieżkami - wydtkować środki Podatników - ponieważ otrzymała je z programu wsparcia - ad exemplum: „Cyfrowa Gmina” lub innego etc - wtedy jak obserwujemy - dochodzi to tego - co obserwujemy, że Gmina wiejska wykonuje działania na podobną skalę jak np. miasto Warszawa - sic !

Skutkiem tego zupełnie niezgodnie z zasadami zarządzania ryzykiem - środki Podatników - są w niektórych gminach marnotrawione - czy wręcz defraudowane., a kontrole NIK kończą się tak rążąc negatywnymi ocenami jak powyżej cytowane.

- Wnosimy o zwrotne potwierdzenie otrzymania niniejszego wniosku w trybie §7 Rozporządzenia Prezesa Rady Ministrów z dnia 8 stycznia 2002 r. w sprawie organizacji przyjmowania i rozpatrywania s. i wniosków. (Dz. U. z dnia 22 stycznia 2002 r. Nr 5, poz. 46) - na adres poczty elektronicznej: jawnosc-transparentnosc@szulc-euphenics.com

- Wnosimy o to, aby odpowiedź w przedmiocie powyższych pytań i petycji złożonych na mocy art. 63 Konstytucji RP - w związku z art. 241 KPA, została udzielona - zwrotnie na adres poczty elektronicznej jawnosc-transparentnosc@szulc-euphenics.com

- Wniosek został sygnowany bezpiecznym, kwalifikowanym podpisem elektronicznym - stosownie do wytycznych Ustawy z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej (Dz.U.2016.1579 dnia 2016.09.29)

PS: Oczywiście żądamy - aby przy jakichkolwiek procesach optymalizacyjnych zachować zasady uczciwej konkurencji przy racjonalnym wydatkowaniu środków podatników, i nawet przy niewielkich kwotach rzędu kilku tysięcy pln dodatkowo - **nadmiarowo** stosować dodatkowo art. 275 ust. 2 Ustawy z dnia 29 stycznia 2004 r. Prawo zamówień publicznych (t.j. Dz. U. z 2024 r.)



Zwyczajowy Komentarz do Pisma.

W naszym na każdym ciężcy obywatelski obowiązek uczestnictwa w usprawnianiu Administracji Publicznej - tak aby w ramach posiadanej wiedzy - kontrolować - w jaki sposób Urzędnicy wydają nasze podatki.

Zgodnie z intencją Ustawodawcy do osiągnięcia tego celu np. art 241 KPA: "Przedmiotem wniosku mogą być w szczególności sprawy ulepszenia organizacji, wzmocnienia praworządności, usprawnienia pracy i **zapobiegania nadużyciom**, ochrony własności, **lepszego zaspokajania potrzeb ludności**."

Pamiętajmy o przepisach zawartych inter alia: w art. 225 KPA: "**§ 1. Nikt nie może być narażony na jakiegokolwiek uszczerbek lub zarzut z powodu złożenia skargi lub wniosku albo z powodu dostarczenia materiału do publikacji o znamionach skargi lub wniosku**, jeżeli działał w granicach prawem dozwolonych. § 2. Organy państwowe, organy jednostek samorządu terytorialnego i inne organy samorządowe oraz organy organizacji społecznych są obowiązane przeciwdziałać hamowaniu krytyki i innym działaniom ograniczającym prawo do składania skarg i wniosków lub dostarczania informacji - do publikacji - o znamionach skargi lub wniosku."

Pomimo, że zgodnie z judykaturą: I OSK 1277/08 i jednostronnym piśmiennictwem - w mniemaniu wnioskodawcy - nie ma konieczności opatrywania pisma kwalifikowanym podpisem elektronicznym - w ramach wniosku o takiej formie - autor pisma - z ostrożności i chcąc działać bona fides - sygnował jednostronny załącznik zgodnie z przepisami Ustawy z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej (t.j. Dz. U. z 2019 r. poz. 162, 1590) oraz art. 4 ust. 5 Ustawy o petycjach (t.j. Dz.U. 2018 poz. 870)