W związku z kontynuacją praktyk organów adniministracji niezespolonej - organy PINB - przykład

https://powiatostrolecki.pl/2091/powiatowy-inspektorat-nadzoru-budowlanego-w-ostrolece.html

adres - pinb-oz@wp.pl

Ponawiam apel o uregulowanie stanu prawnego i zobowiązanie ich do "dostosowania adresu do wzorca"

Przykład dostosowania.

https://winb-lubuskie.bip.gov.pl/powiatowe-inspektoraty-nadzoru-budowlanego/powiatowe-inspektoraty-nadzoru-budowlanego.html

Poniżej liczba wystąpień. To tylko znikoma część sygnałów ale opisuje kilka problemów prawnych. Naruszenie zasad komunikacji, niedostosowanie do poziomu zagrożenia cybernetycznego, liczne praktyki które znam z autopsji.

Dnia 25 sierpnia 2023 12:56):

Poniżej propozycje. Proszę rozważyć z resztą czy posłuchać obywatela. Moze warto.

Po pierwsze

ROZPORZĄDZENIE RADY MINISTRÓW z dnia 8 stycznia 2002 r. w sprawie organizacji przyjmowania i rozpatrywania skarg i wniosków.

Które powinno być zaktualizowane po bez mała 20 latach. Takie proste a akt aktualny i nie zabrania stosowania gmail, wp.pl itd w korespondencji.

https://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20020050046

Nie zawiera nowelizacji związanej z cyfryzacją i zakazu stosowania skrzynek zewnętrznych przez administracje niezespoloną czy zespoloną.

Dnia 03 lipca 2023 10:07 napisał(a):

Powiem tak - po co Pinokio ogłasza stopnie zagrożenia?

- Drugi stopień alarmowy (BRAVO)
- Trzeci stopień alarmowy CRP (CHARLIE-CRP)

Obowiązki
https://www.gov.pl/web/mswia/stopien-alarmowy-bravo-crp

- monitorować i weryfikować, czy nie doszło do naruszenia bezpieczeństwa komunikacji elektronicznej;

I tu audyt haseł i maili.

- sprawdzić aktualny stan bezpieczeństwa systemów i ocenić wpływ zagrożenia na bezpieczeństwo teleinformatyczne na podstawie bieżących informacji i prognoz wydarzeń;

Nie wydano nakazu audytu ani nakazu rotacji haseł. Nie wydano nakazu badania prób naruszenia danych poprzez info nieudanych próbach logowania

Dnia 14 czerwca 2023 12:06 napisał(a):

Szanowny Panie Pośle. Poniżej ukazuje materiał przesłany do Poseł Małgorzaty Pępek która interpelowała w sprawie problemu stosowania przez organy administracji niezespolonej adresów które naruszaja zasady komunikacji cyfrowej w administracji.

Prośba dotyczy wprowadzenia usystematyzowania nazw pocztowych organów państwowych, administracji zespolonej i niezespolonej w sposób w który korespondencja nie przez epuap będzie znajdować się na serwerach pocztowych krajowych chronionych szybko przez CERT.
Jedynymi obszarami są serwery dla domen gov.pl/

Jak udowodniłem problem jest w rozporządzeniach i ustawach które nie przewiduje obowiązku ani konsekwencji.
Dlatego wystąpiłem do Pani poseł do audyt organów na portalu
https://haveibeenpwned.com/
I prewencje tam gdzie organy zostały zaatakowane informatycznie (wykazano utratę danych).
I regulaminy - bo cyfryzacja
To jest to akt do którego musi dojść na podstawie regulaminów PINB lub aktu ogólnego.
A to co macie zrobić to poprosić Premiera o zmianę w bardzo starym rozporządzeniu.
Patrz- https://pinb.bip.powiat.turek.pl/10020/Przyjmowanie_spraw/
Zacytowano tam ROZPORZĄDZENIE RADY MINISTRÓW z dnia 8 stycznia 2002 r. w sprawie organizacji przyjmowania i rozpatrywania skarg i wniosków.
Które powinno być zaktualizowane po bez mała 20 latach. Takie proste a akt aktualny i nie zabrania stosowania gmail, wp.pl itd w korespondencji.
https://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20020050046
Nie zawiera nowelizacji związanej z cyfryzacją i zakazu stosowania skrzynek zewnętrznych przez administracje niezespoloną czy zespoloną.
Dlatego proszę Pana posła o interwencje w zakresie "bezpieczeństwa" IT z prośba o wskazanie kto wykona pełen audyt adresów email urzędów pod kątem wycieku danych.
Tylko nie przez stronę rządową a "odpowiednie narzedzia lub" opisaną stronę https://haveibeenpwned.com/
Materiał dowodowy w sprawie.

Dnia 08 czerwca 2023 10:06 [redacted] napisał(a):

Czy potrzebuje Pani więcej dowodów?

Prosze o szybką intewencję w sprawie bezpieczeństwa.
Każdy organ weryfikacja 100 @ adresów mail i przejście na adresy z domeny gov.pl
Kary za utratę bezpieczeństwa dla tych kierowników którzy w okresie "wycieku danych" pełnili funkcję.
O skali infiltracji kont nie wspomnę.
Dnia 18 czerwca 2021 12:06 [redacted] napisał(a):

> Dnia 18 czerwca 2021 12:06 [redacted] napisał(a):
>
> Szanowni Państwo
> (No właśnie - adresat jeden - ilu ukrytych adresatów - nie wiadomo nie zdradzę).
> Zacznijmy od podstaw - piszę z prywatnego - darmowa skrzynka pocztowa, portal Wirtualna Polska - słabe hasło.
> Aspekt drugi - wyłączone uwierzytelnienie choć działało to trochę czasu.
> Aspekt trzeci - podany adres do odzyskania konta, telefon też. Jak ktoś mi hasło zmieni będę wiedział.
> Co istotne - na moim epuap [redacted] - numeru konta nie podam - adres wskazany jako korespondencyjny. Taki niuans.
> A teraz do rzeczy.
> 1. Administracja Państwowa a może tylko samorządowa stosuje nadal darmowe skrzynki poczatowe. Robią tak organy nad którymi nie ma systemowego nadzoru i ktore jako biedne nie mają środków na serwer pocztowy czy to zewnętrzny czy też własny.
> Tu jest opisany temat
> https://www.sejm.gov.pl/sejm9.nsf/interpelacja.xsp?typ=INT&nr=21702
> w sprawie korzystania przez inspektoraty nadzoru budowlanego z darmowych skrzynek pocztowych ulokowanych na publicznych serwerach
> Nie pokaże wam kto i co pisałem do INFOR o sprawie, jaki zareagował GUNB w sprawie ale trwa to długo i nadal trwa.
> https://serwisy.gazetaprawna.pl/samorzad/artykuly/945837,urzednicy-inspektoraty-nadzoru-budowlanego-darmowe-skrzynki-mailowe.html

Przeglądając biuletyny informacji publicznej powiatowych inspektoratów nadzoru budowlanego, nietrudno zauważyć, że część z nich dysponuje kontami e-mailowymi na zewnętrznych serwerach pocztowych. I tak pocztę na Google'u posiada m.in. urząd w Świeciu (pinb.swiecie@gmail.com), Wałbrzychu (pinb.walbrzych.miasto@gmail.com) czy Chrzanowie (pinb.chrzanow@gmail.com). Skrzynkę na Onecie wybrał nadzór w Żninie (pinbznin@onet.pl), a na Wirtualnej Polsce inspektorat w Kołobrzegu (pinb.pinb@wp.pl) oraz w Jaśle (jaslopinb@wp.pl). Z e-maila na Interii korzysta natomiast PINB powiatu grodzkiego w Toruniu (pinbpgtorun@interia.pl). I może nie byłoby w tym nic niestosownego, gdyby nie fakt, że na te skrzynki trafiają pisma zawierające dane wrażliwe Polaków.

2. Poprzez konfigurację serwera pocztowego organy te używają darmowych skrzynek pocztowych jako pośredników w zakresie świadczenia usługi.
W chwili obecnej zdiagnozowałem do w organach nadzoru budowlanego w skali "zatrważajacej". Sygnał wysłany do GUNB nie zadziałał. Wdrodzono co prawda serwer w skali GUNB i WINB ale już obraz stron WINB stanowią strony własne a nie "systemowe". Jedyna sytemowa jest na poziomie GUNB.
Wniosek - adresy administracji państwowej nie są znane, stabilne i nie podalegają "wzmocnionej ochronie" oprogramowaniem.
3. Pierwsza linia obrony i ataku. Pierwszą linią jest sekretariat który za pomocą człowieka filtruje dane i określa czy jest to informacja do organu czy "spam".
Wzmocnieniem tego punktu jest ... program antywirusowy (co kraj to obyczaj nie mamy jednej licencji każdy montuje sobie sam dla siebie).
Serwery pocztowe - zazwyczaj są na .... platformie "LINUX"? Efektywniejsze i ławiejsze w zabezpieczeniu.
Programy obsługi poczty są na systemie WINDOWs - pytanie ile ... czyli kto jeszcze ma oprogramowanie z dziurami.
Wniosek - jak powinno wyglądać stanowisko sekretariatu, jakie programy powinny tam działać, jakie ustawienia powinny być włączone aby większość ataków nie dotarła do "człowieka".
4. SPAM - muliti spam i rejestr spamerów.
Istotą korespondencji jest jej wysłanie lub rozesłanie. Powtórzenie czynności nie idzie w grę gdy treść jest ta sama i tak do podmiotu docierać może "multispam" czyli info wysłane do kilku np. od obywatela który nie wie do kogo.
wnioski - spam powstaje gdy serwisy pocztowe pozwalają na dowolną liczbę adresatów a nie ograniczoną liczbę komórek. I tak dzieki takiej praktyce mogę mieć prywatne adresy do dziennikarzy, ministrów, urzędników bo ktoś wrzuci w jednym mailu kilkanaście adresów.
Zbiory mam bogate od "listy wszystkich posłów" według adresów (posiadałem takie zestawienia) pozyskane z sieci.
Widząc mulitispam należy wdrożyć procedurę bezpieczeństwa "oceny nadawcy" wraz z nie przekierowaniem elektronicznym dokumentu dalej lecz "wydrukiem" tylko i wyłącznie.
5. Kontakt - nie sekretariat.
W wielu korespondencjach udało mi się skontaktować do urzędnika i tak mam na podstawie danych do poszczególnych urzędników możliwość ataku "ad personam". Znając adres wrażliwy lub podatność osoby na korespodencję każdy kto zna adres do urzędnika ma tylko taką linię obrony jaką taki urzędnik posiada.
Pytania - czy korespondencja urzędnika zawsze jest chroniona tak jak reszta poprzez antywirusa (przypadki gdy serwery pocztowe nie widzą ryzyka) a urzędnik klinkie na ZiP, LINK, czy DOC czy PDF tak przygotowany że będzie tego taki skutek jak w incydencie w KPRP. Wiadomo o jaki ZIP chodzi (działo się to trochę po tym jak w CO KPRP pracowałem).
6. Korespodencja zwrotna urzędnika - wydziały merytoryczne.
Prowadzenie przez urzędnika szybkiej korespodencji zwrotnej z swojego adresu który nie jest jawny w żadnym systemie (zasady nie publikowania np w KPRP czy KPRM adresów wewnętrznych) pozwala na targetowanie tego adresu. Podatność zależna jest od "ryzyka" uprzedniego przejęcia konta podmiotu z którym się prowadzi korespodnencję.
a) kancelarie adwokackie i inne biura prawne

b) osoby zaufania publicznego - inżynierowie, geodeci, lekarze itd.
c) osoby z którymi organ zawiera umowy zlecenie lub o dzieło
Zasady korespodencji z takimi nie są znane i nie ma "pośrednika" rejestrującego wystąpienie. Nie wysyła się treści na sekretariat bo by się "sekretariat" zarżnęło tymi mailami.
7. Wysyłanie danych lub korespondencji nie związanej z praca do domu czyli na adres priva.
I tu się kłania ostatni incydent. Zbiór adresów "biała księga" powinien być zamknięty. Urzędnik powinien móc wysłać tylko tam gdzie jest wpis w książce adresów że to "bezpieczne". Reszta powinna być niedopuszczalna.
Redukcja ryzyka wysłania pracy do domu i utraty tych danych po incydencie.
Wiadomo o co chodzi - ministrowie BRAWO WY.
8. Reguły i zasady zabezpieczenia książki adresowej lub "białej książki adresowej" lub pojawienie się mechanizmu 'książka" i "zabezpieczona przed dostępem książka adresowa"
Odpowiedzialność indywidulana dysponenta książką adresową została dawno opisana i podlega nadal tym samym restrukcjom.
W załączeniu podane w stanowisku opinia dotycząca "książki adresowej".
Korespondencja która poprzedzała odpowiedz dotyczyła braku ochrony zbioru adresów przed "automatycznym" pozyskaniem na zewnątrz - znasz hasło do konta - ściągasz książkę adresową.
Czy Premier czy minister przed usunięciem konta na społecznościowym zbiór "potencjalnych ofiar" przejęcia hasła określił czy wymazał - ciekawe czy na urządzeniu które mu służyło do tego ten zbiór "adresów" nadal posiada.
Utrata zbioru jest kwestią prywatnej odpowiedzialości z tytuły RODO.
Zalecenie - wprowadzenie zasady białej książki, czarnej książki i możliwość utrwalenia "koresponduję tylko z osobami z "białej książki".
Tego portale nie gwarantują nawet płatnie.
9. Adres email - mój jak widać z wp.pl ale nie widzicie tego czasami bo jest za nazwą użytkownika.
Tu podatność jest duża bo pomyłka polegająca na otworzeniu adresu łudząco przypominającego adres prawdziwy jest zależna od ... od uwidocznienia adresu i rozmiaru czcionki.
Portal nie ma obowiązku
1. Pokazywać jawnie w dużej czcionkce każdego adresu nadawcy jako "podstawowej" informacji o wiadomości.
Skąd to jest - zkątowni.gov.pl czy skontowni.gof.pl - czasami robi różnice. I tak można ataku uniknąć lub dostrzec spam po adresie.
Niestety ukrycie, mała czcionka, brak wymogów prawnych dla portali działających w Polsce.
10. Kontakt bezpieczny.
Żaden portal nie daje możliwości przesyłu kodu QR służącego do dobioru wiadomości szyfrowanej.
TOKENA też nie podają do odpalenia treści maila którego nie zobaczysz jak nie podasz kodu z twojego telefonu po rejestracji bio metrycznej że to ty.
Nie ma tego w żadnej specyfikacji usług płatnych a już nie w darmowych.
Jest jeszcze sporo do opowiedzenia od
11. Metoda tworzenia adresów
Prosze nie podawać adresu imię nazwisko do organu. Szybciej jest mieć po departamentach, numerach, alfa numerach z przypisaniem "w białej książce" kto to.
Piszesz że Ania K., kadry i wchodzi D12C2@mf.gov.pl
Departament D. pracownik 12, okres pracy C2. Setki rzeczy można tak zrobić jeśli chcemy "szyfrować na max".
Znacznie lepiej ustalić kanał komunikacji port X z którego i tylko z którego (port wewnętrzny) przejdzie info do osoby. A to już informatycy którzy zrobią tak że wszystko co z zewnątrz nie trafi.
Moim zwycięstwem w metodyce szukania adresów to.
Ustalenie adresu do Ministra na biurkowy.
Ustalenie adresu do sędziów TK - budowa cepa jak się wie jak został zastosowany mechanizm tworzenia adresów dla wszystkich.
12. Oprogramowanie rządowe do potwierdzenia korespodencji. Jest dwuskładnikowe logowanie się ale nikt nie ma potwiedzenia że "ja to ja".

I tak znając hasło może zrobić to każdy a dlaczego "logowanie się" lub uruchomienie programu nie może być uzależnione od rządowej apki połączonej z "danymi o numerze telefonu" wgrywanej "tylko z określonego źródła" nie Sklep play.
13. Praca zdalna - czyli rządowi informatycy już o ciebie na dysku tu byli.
Wiem coś o tym - szczegółów nie podaje bo był taki incydent który pokazał że pracując zdalnie można utracić kontakt z "dyskiem' bo osoba która ci to zapewnia może "otworzyć dostęp" do twojego komputera i oglądać na nim twoje dane.
Morał - pracując zdalnie należy zapewnić "ustawienia" priva oraz jeśli to ważna praca pracować na dysku podlegającym szyfrowaniu.
A teraz zapomnij hasła, zgub do tego klucz. Bitcoinów nie będzie - to żart z gubienia kluczy.
Zaczynamy od eDo App - wystarczy. Wystarczy za bio podpis. Tylko potrzebne "wygodniejsze" w stosowaniu lub rządowa wersja czyli zakładka - administracja.
Po cholerę klucz jak mam go w formie podpisu w eDO App.
https://www.edoapp.pl/
Polecam tą drogą kroczyć. Tylko to rozbudować.

14. Adresy sejmowe.
Do jasnej cholery dlaczego można zamieścić w Sejmie adresy prywatne na op.pl czy gmail a nie widnieje sejmowy.
Proponuje dwa adresy sejmowe. Jeden poselski czyli idzie korespondnecja rządowa - niejawny - tam idą projekty, pisma i reszta.
A drugi dla obywatela
Pierwszy - dysk szyfrowany, eDO App na wejście z wskazaniem max 3 osób które mogą operować skrzynką.
Drugi - publiczny jako adres dla obywateli.
15. Pojemność dysków dla posła, senatora.
wp.pl ma - 38 GB miejsca na skrzynce - skąd wiem ? To wersja bezpłatna.
Proszę o określenie granicznej wartości zawalania kont poselskich. Posłowie nie wierzą służbom, nie ufają nikomu i nie mając szyfrowanej skrzynki po prostu jej nie używają lub mając ją publicznie są skazani na "szukanie maila w stercie spamu".
16. Co by wam jeszcze napisać.
WP nie ma danych że podałem im ten adres w EPUAP. A powinno mi dać zakładkę rządową żebym nie szukał odpowiedzi. Jak coś wpłynie to ... można wymóc stworzenie takiego mechanizm.
17. Ostatnie. Nowy WHAT?
W ramach programy proszę o cyfryzację działów organ po organie, serwery pocztowe i jak trzeba dyski szyfrowane, mechanizmy dostępu celem redukcji emisji papieru, energii itd.
Plus - założenia bezpieczeństwa które same się będa stosować po odpowiedniej konfiguracji.
1) w miejscu pracy urząd
2) w miejscu pracy zdalnej.
3) wytyczne dla asystentów i posłów
4) serwery dla Sejm, Senat.
Pozdrowienia ze strony XR - oni mają swój mechanizm jak nie dać szansy wejść sobie na konto, nie stracić adresu, hasła nie dać się złamać cybernetycznie. Polecam ich opracowania - można się czegoś nauczyć.

Odpowiedz po identyfikacji epuap proszę przekazać na skrzynke obywatelską.
DW - dla kontroli systemowej - nie podaje ilu ale ... przeczytajcie, zastanówcie się nad słowami i tym co można poprawić.

A to drugi mail.
Dnia 8 lipca 2022 08:12 [redacted] napisał(a):
Szanowni Państwo - możemy sobie maglować temat.
"Ulubioną służbową skrzynką pocztową powiatowych inspektoratów nadzoru budowlanego wydaje się być ta należąca do Wirtualnej Polski. Ale nie tylko - instytucje mają swoje skrzynki email skonfigurowane

także na Neostradzie, Onecie, Gmail, o2, Gazecie, Interii czy poczciefm. Na takich służbowych skrzynkach pocztowych pracują m.in. powiatowe inspektoraty w Jaśle, Rykach, Stalowej Woli, Grodzisku Mazowieckim czy Skarżysku Kamiennej. Wymieniać można długo. Sporo urzędowych stron inspekcji budowlanej działania na otwartych oprogramowaniach, dedykowanych osobom prywatnym, a nie instytucjom publicznym.

- Sami czujemy, że coś jest nie tak. Niestety mam taki budżet jaki mam, który nie pozwala na zatrudnienie informatyka, który by profesjonalnie zajął się sprawami internetowymi. A takiego, który zechciałby nam pomóc na przykład na umowie zlecenia, nie mogę znaleźć – przyznaje Marek Bany, powiatowy inspektor budowlany w Rykach.

- O jakiej informatyzacji mówimy. Gdybym miał pieniądze, aby przenieść się na domenę gov.pl, to już dawno bym to zrobił. Nie mam w budżecie nawet tych 150 zł, aby opłacić rejestrację, a przecież co roku trzeba ją utrzymywać – mówi serwisowi Prawo.pl jeden z szefów PINB na Podkarpaciu.

Inspektorzy przyznają, że problem urzędowych skrzynek pocztowych w ich instytucjach wraca jak bumerang. Żalą się, że trudno mówić o standaryzacji poczty elektronicznej, skoro wciąż problemem jest przepustowość łącz internetowych i kłopoty z działaniem platformy ePUAP. A wiadomo, że w pandemii wszystko odbywa się zdalnie, przez internet.

Problem, gdy dochodzi do incydentów

Łukasz Jachowicz, specjalista ds. bezpieczeństwa IT w Mediarecovery - firmie zajmują się wdrażaniem rozwiązań z zakresu bezpieczeństwa IT i informatyką śledczą uważa, że stosowanie przez instytucje publiczne skrzynek darmowej poczty elektronicznej może mieć negatywne konsekwencje dla świadomości internautów, którzy przyzwyczajają się do powszechności tego zjawiska. Trudno im później odróżnić, czy wiadomość przychodząca z darmowego adresu poczty jest przygotowana przez przestępców, czy rzeczywiście pochodzi z danej instytucji. W efekcie mogą stać się łatwym celem dla włamywaczy, którzy infekują ich komputery i kradną dane kont bankowych i pocztowych.

- Z drugiej strony, skrzynki na popularnych portalach są, pod kątem technicznym, bezpieczniejsze niż źle zarządzane własne serwery e-mail. Jeżeli lokalny informatyk nie potrafi skonfigurować poczty we własnej domenie, to lepiej by skorzystał z dostępnych darmowych rozwiązań i nie zajmował się bezpieczeństwem poczty. Jednak dla bezpieczeństwa nas wszystkich, instytucje publiczne powinny mieć pewien budżet przeznaczony na wykup komercyjnych kont mailowych we własnych domenach – mówi Łuksza Jachowicz.

- Adres powinien wskazywać instytucję – mówi stanowczo Przemysław Krejza prezes Stowarzyszenia Instytut Informatyki Śledczej. Jego zdaniem to nie tylko kwestia bezpieczeństwo danych, ale także standardów publicznych i przetwarzania danych osobowych.

- Takie skrzynki można traktować jako skrzynki prywatne. Problemy pojawia się, kiedy dochodzi na przykład do incydentu naruszenia bezpieczeństwa. Chcemy zabezpieczyć dane, pracownik odmawia, uzasadniając, że to prywatna skrzynka i powołuje się na tajemnicę korespondencji. W świetle prawa ma rację, bo nie można sięgać do danych prywatnych, są one chronionych przez konstytucję. Trzeba angażować wtedy prokuraturę, sąd, a to wydłuża procedurę. Kiedy skrzynka pocztowa jest pracodawcy lub urzędu, ma on możliwość zablokowania pracownikowi dostępu do niej i zabezpieczenia danych, które się tam znajdują - mówi Przemysław Krejza.

Czytaj więcej na Prawo.pl:
https://www.prawo.pl/biznes/elektroniczne-skrzynki-pocztowe-urzedow-a-bezpieczenstwo-danych,507870.html

Niezależnie od mechanizmów potwierdzających tożsamość nadawcy, podmioty publiczne, realizując zadania publiczne (czyli np. organy administracji), powinny wykazywać się profesjonalizmem oraz rzetelnością zarówno w korespondencji wewnętrznej, jak i w kontakcie z obywatelem - zaznacza GIODO. Za złą praktykę uznaje np. wykorzystywanie przez podmioty publiczne adresów o nazwach domeny odmiennych niż wskazywana na oficjalnych stronach internetowych lub w BIP, bądź jednoznacznie wskazujących na komercyjny podmiot udostępniający bezpłatnie usługę poczty elektronicznej. Przykład? W maju 2016 roku „Dziennik Gazeta Prawna" donosił o inspektoratach nadzoru budowlanego korzystających z

darmowych skrzynek e-mailowych w domenie gmail.com, onet.pl, wp.pl czy interia.pl.
https://www.rp.pl/dane-osobowe/art10611841-bezpieczenstwo-poczty-elektronicznej-wskazowki-giodo
Ale jeśli kierownik może wprowadzić zarządzenie sposobu kontaktu.
https://pinb_pultusk.bip.gov.pl/zadania/379866_zarzadzenia.html
To jest to akt do którego musi dojść na podstawie regulaminów PINB lub aktu ogólnego.
A to co macie zrobić to poprosić Premiera o zmianę w bardzo starym rozporządzeniu.

Patrz- https://pinb.bip.powiat.turek.pl/10020/Przyjmowanie_spraw/

Zacytowano tam ROZPORZĄDZENIE RADY MINISTRÓW z dnia 8 stycznia 2002 r. w sprawie organizacji przyjmowania i rozpatrywania skarg i wniosków.

Które powinno być zaktualizowane po bez mała 20 latach. Takie proste a akt aktualny i nie zabrania stosowania gmail, wp.pl itd w korespondencji.

https://isap.sejm.gov.pl/isap.nsf/DocDetails.xsp?id=WDU20020050046

Nie zawiera nowelizacji związanej z cyfryzacją i zakazu stosowania skrzynek zewnętrznych przez administracje niezespoloną czy zespoloną.
Pana Ministra proszę o przekazanie wniosku o poprawki regulujące tzw. "cyfryzację" administracji niezespolonej której nikt nie nadzoruje pod kątem tworzenia regulaminów i wydawania zarządzeń - wprost do Rady Ministrów.
Może Minister też jedną poprawką uczynić PINBy elementem administracji zespolonej. Wystarczy tylko wskazać kto mianuje kierownika PINB w ustawie Prawo budowlane.
Rozumiem że to koszt i może spowodować masową ucieczkę inspektorów ale ... może tak należy... jak jest w innych krajach ? Czy nadzór budowlany to prywatne podwórka czy cały zespół organów Państwowych podległych pionowo w ramach "zespolenia".
Do Jana Nowaka - Prezesa UODO - proszę o rozważenie zasygnalizowania Radzie Ministrów potrzeby aktualizacji rozporządzenia które nie trzyma się KPA ani innych aktów z uwagi na trawnie procederu stosowania adresów nie wskazujących na "organy rządowe lub samorządowe" czyli administrację.