NASK

Ataki na JST, profilaktyka, budowanie świadomości cyberbezpieczeństwa

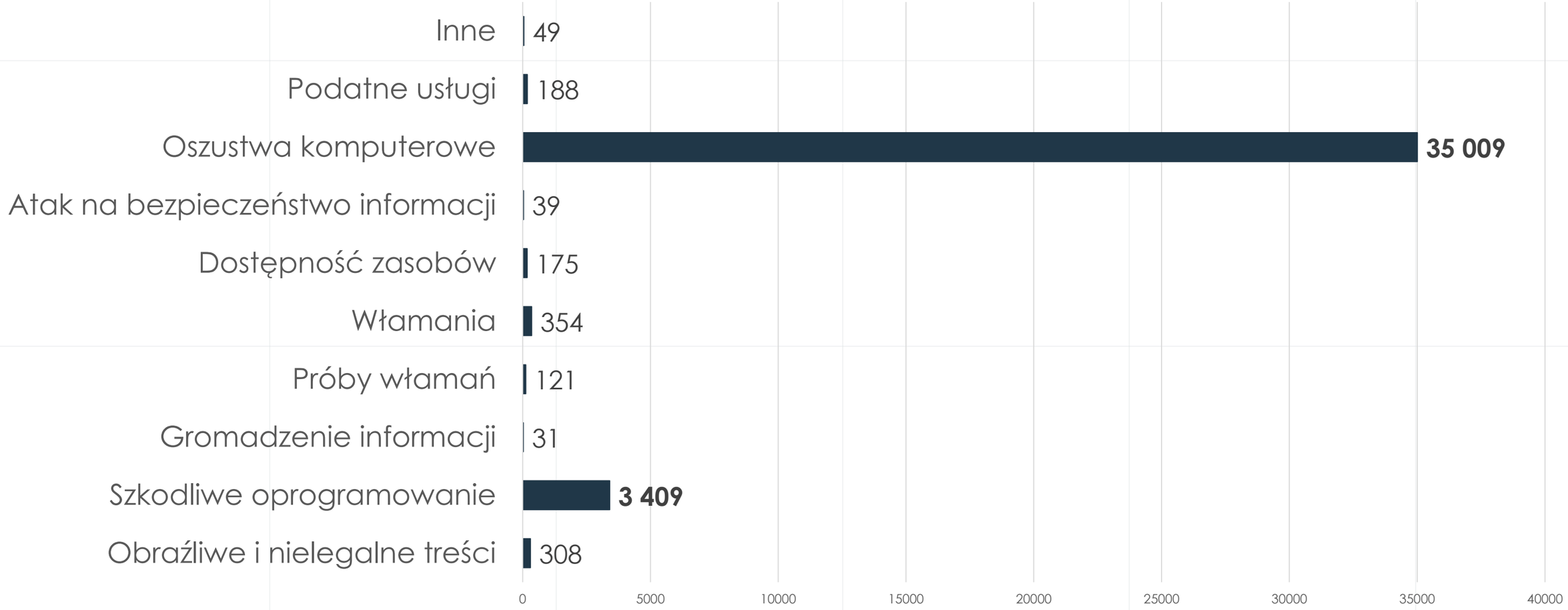
Łódź, 7 grudnia 2023 r.

nask.pl

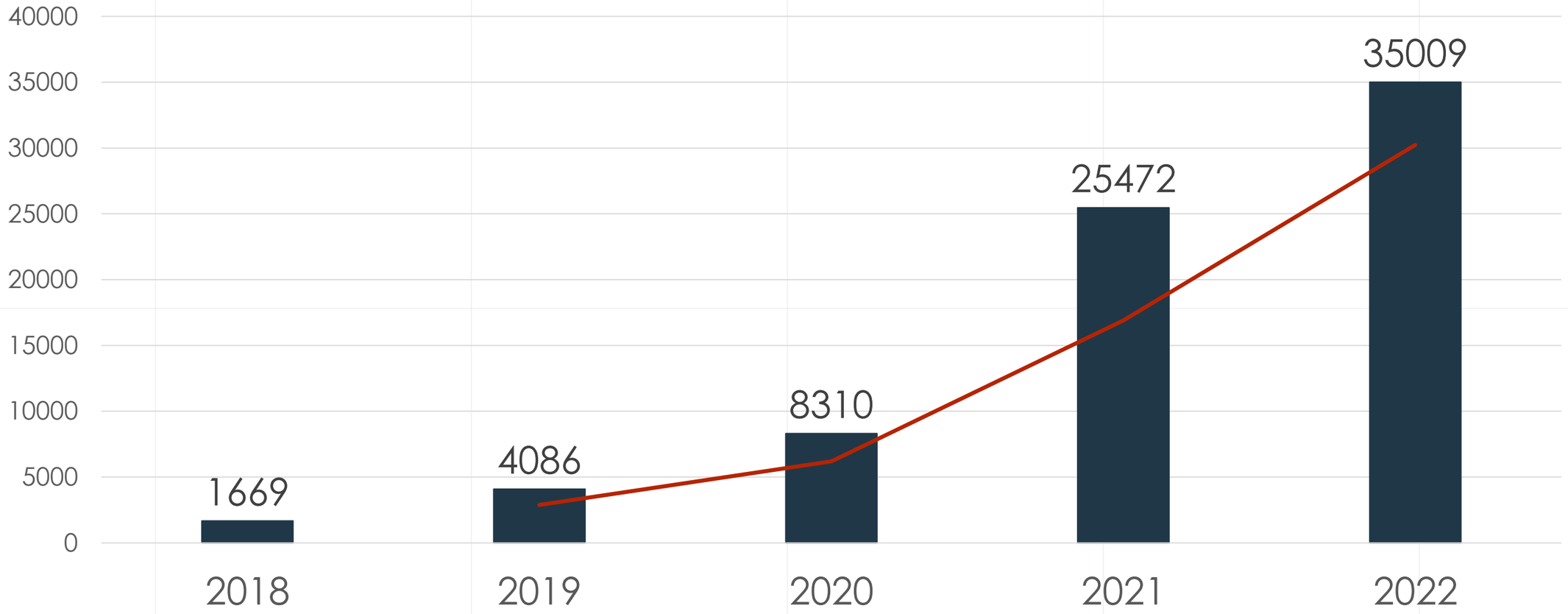
Trochę statystyk

Czyli co nam grozi

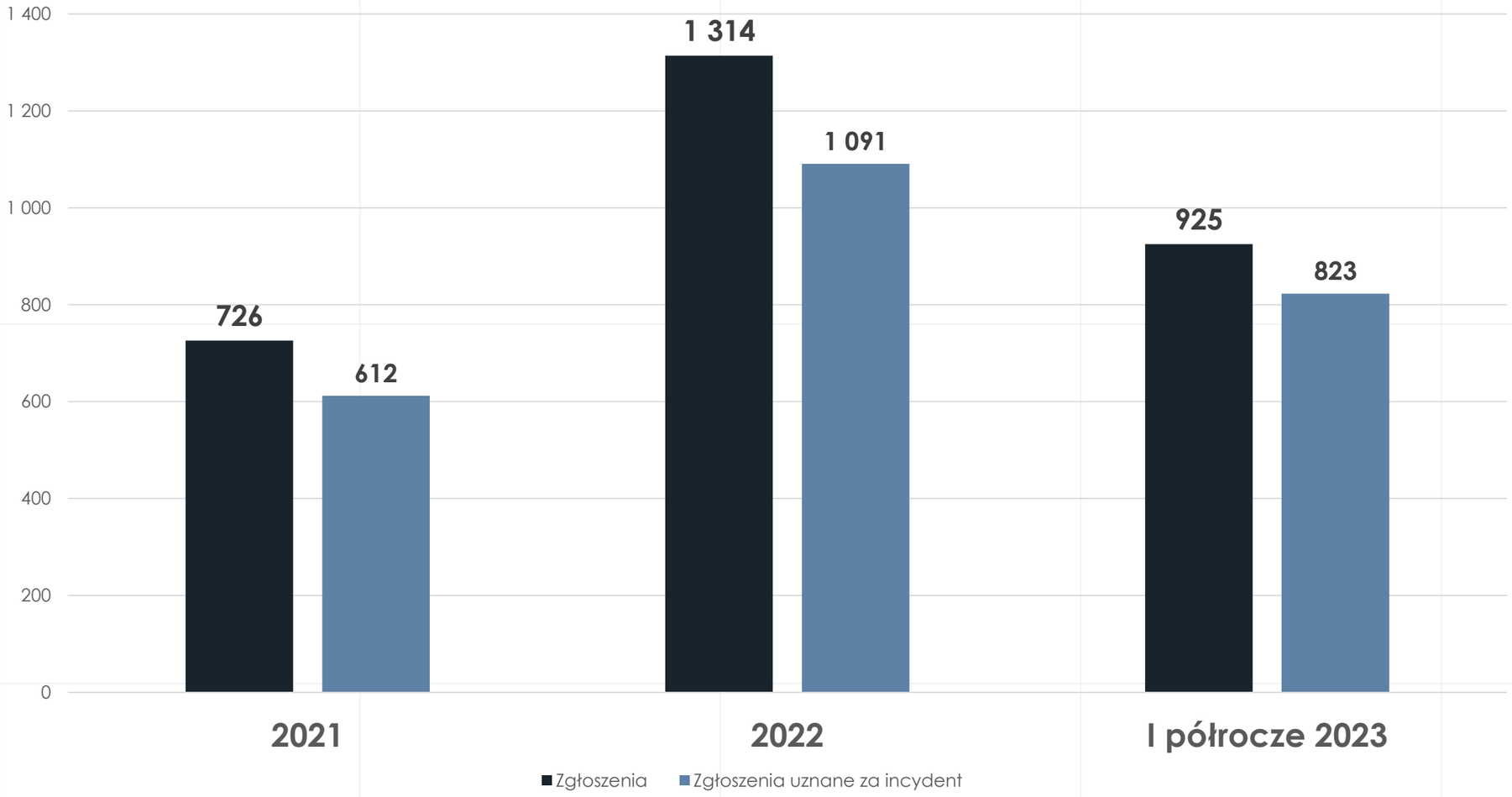
Incydenty zarejestrowane przez CERT Polska w 2022 roku



Oszustwa zarejestrowane przez CERT Polska w latach 2018-2022

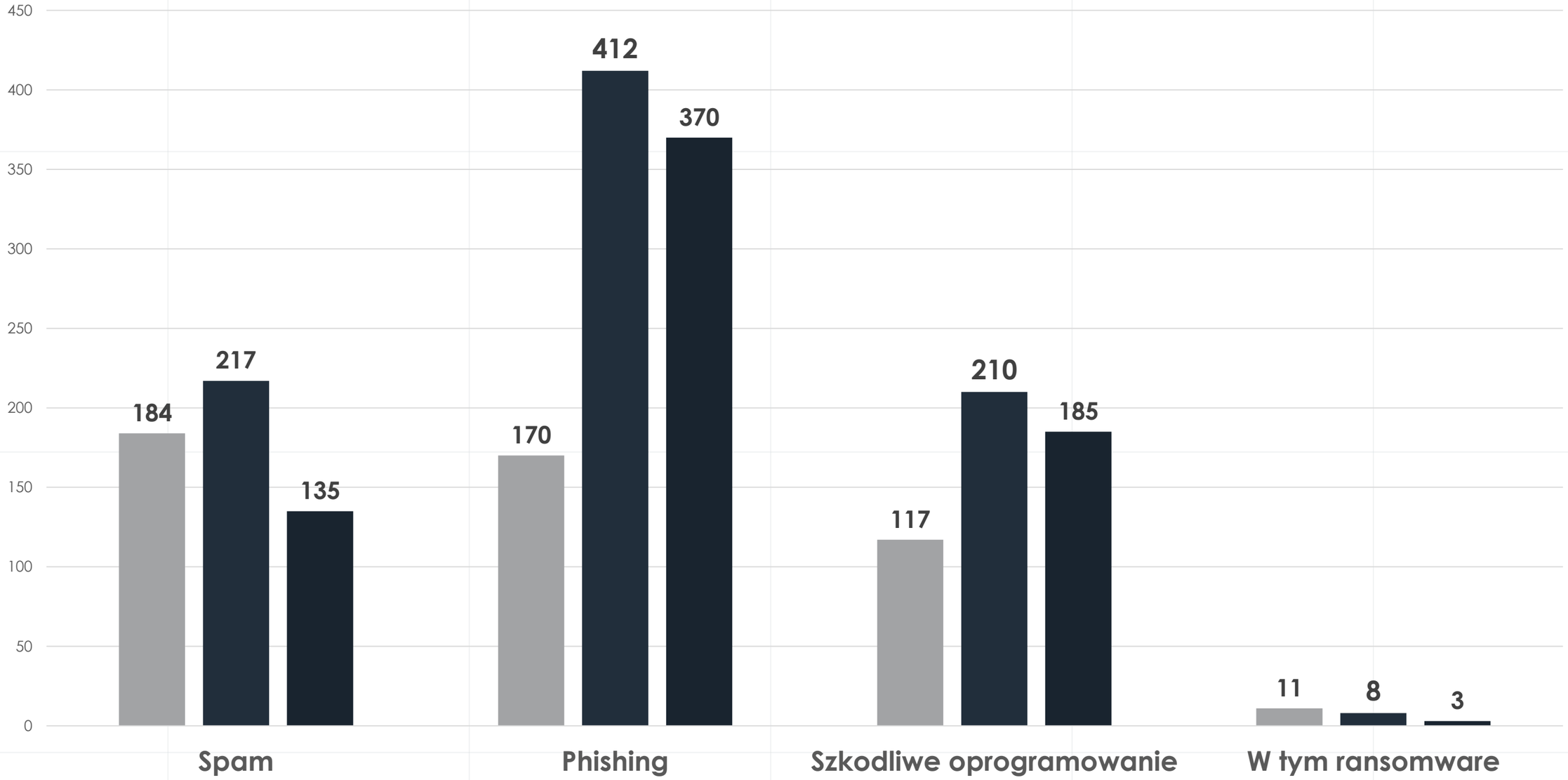


Skala zagrożeń w podmiotach publicznych wg danych CERT Polska



NASK

Rodzaje zagrożeń w podmiotach publicznych



NASK

Dane częściowe za 2023 (do listopada)

305507

zgłoszeń

72601

incydentów

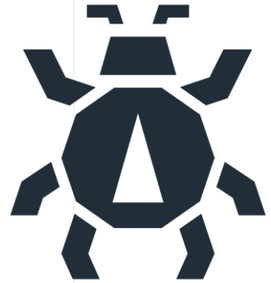
1959

incydentów

podmioty publiczne

36582

phishing



1416

szkodliwe/ złośliwe oprogra-mowanie

Najczęstsze/najgroźniejsze ataki

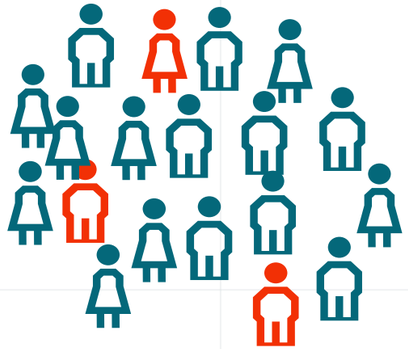
- Phishing masowy w celu ułatwienia dalszych ataków (spear phishing/whaling)
- Złośliwe oprogramowanie w plikach (obecnie najczęściej: .zip .rar .iso .img)

  w tym: Ransomware
- DDoS

Phishing

I inne techniki oszustw

Rodzaje phishingu,
podział ze względu na grupę docelową

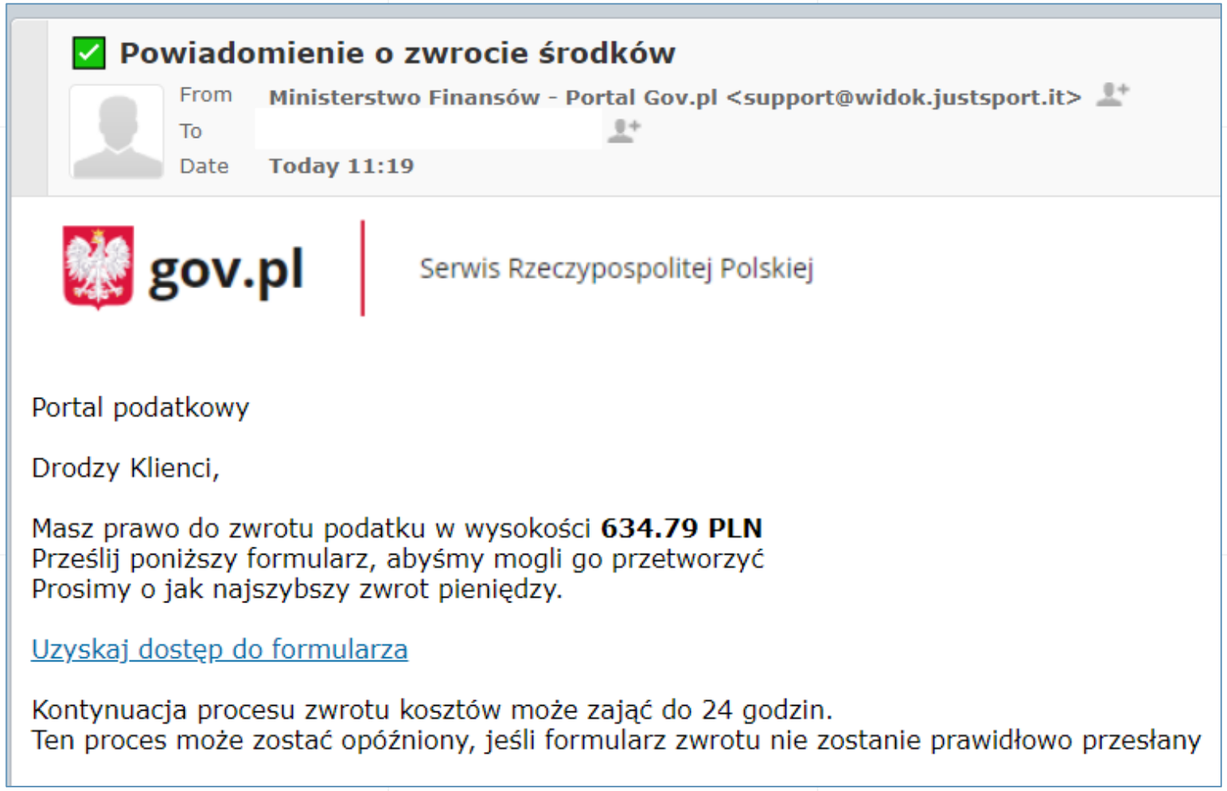


masowy

spersonalizowany

NASK

Podszywanie się pod instytucje publiczne



Powiadomienie o zwrocie środków

From **Ministerstwo Finansów - Portal Gov.pl <support@widok.justsport.it>**
To
Date **Today 11:19**

gov.pl | Serwis Rzeczypospolitej Polskiej

Portal podatkowy

Drodzy Klienci,

Masz prawo do zwrotu podatku w wysokości **634.79 PLN**
Prześlij poniższy formularz, abyśmy mogli go przetworzyć
Prosimy o jak najszybszy zwrot pieniędzy.

Uzyskaj dostęp do formularza

Kontynuacja procesu zwrotu kosztów może zająć do 24 godzin.
Ten proces może zostać opóźniony, jeśli formularz zwrotu nie zostanie prawidłowo przesłany

Nowe powiadomienie o paczce

From **No-Replay <support@vertexplus.net>**
To
Date **Thu 14:40**

Poczta Polska

Szanowny Kliencie

Dziękujemy za skorzystanie z Poczty Polskiej, Twoja przesyłka czeka na Ciebie.
Należy dokończyć wpłatę (9,06 zł).

co muszę zrobić ?

Kliknij poniższy bezpieczny link, aby dokończyć uiszczenie opłat za wysyłkę

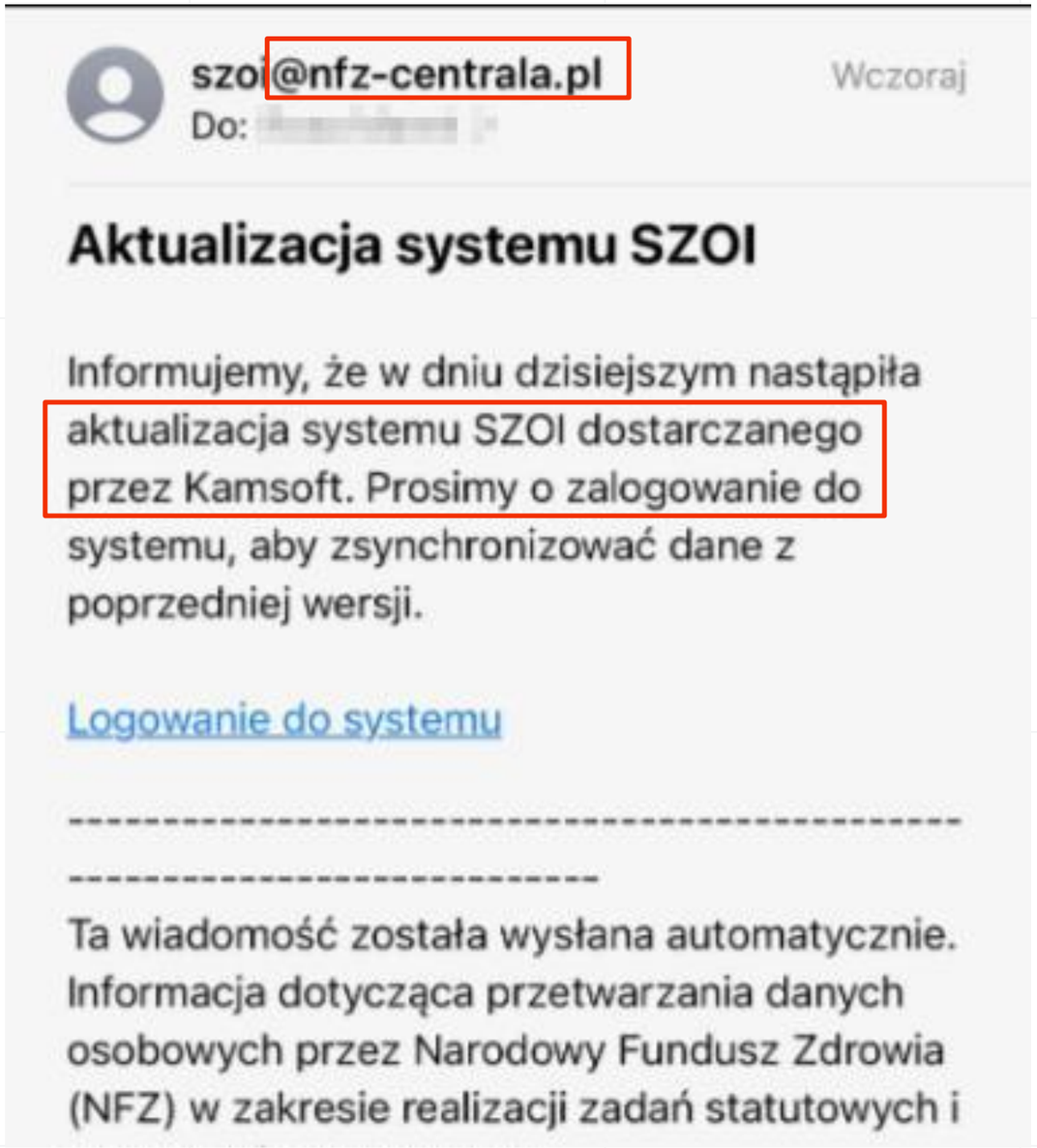
Przewidywany termin dostawy: 25 października przed końcem dnia roboczego.

Z poważaniem.
Obsługa klienta Poczty Polskiej.

Zapłać teraz

NASK

Ale też:
na instytucje publiczne



szoi@nfz-centrala.pl Wczoraj
Do:

Aktualizacja systemu SZOI

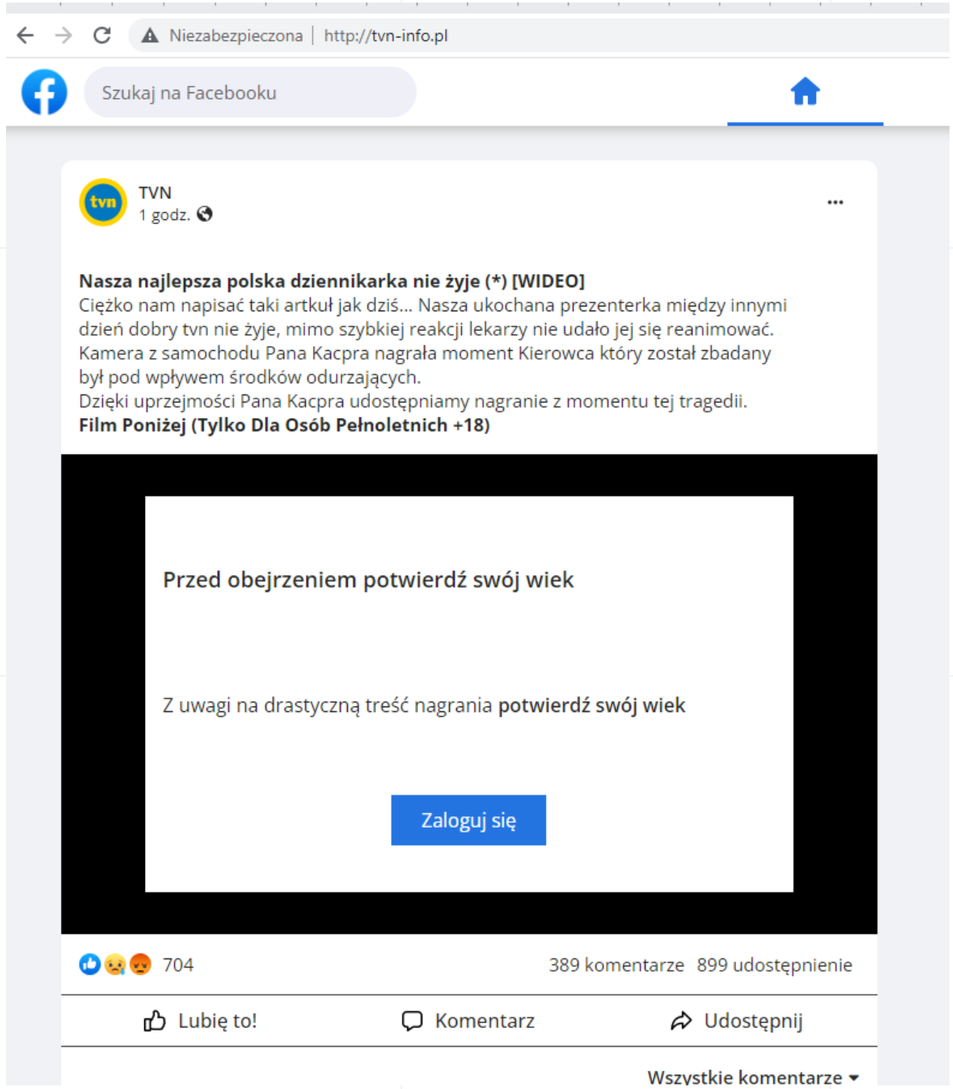
Informujemy, że w dniu dzisiejszym nastąpiła aktualizacja systemu SZOI dostarczanego przez Kamsoft. Prosimy o zalogowanie do systemu, aby zsynchronizować dane z poprzedniej wersji.

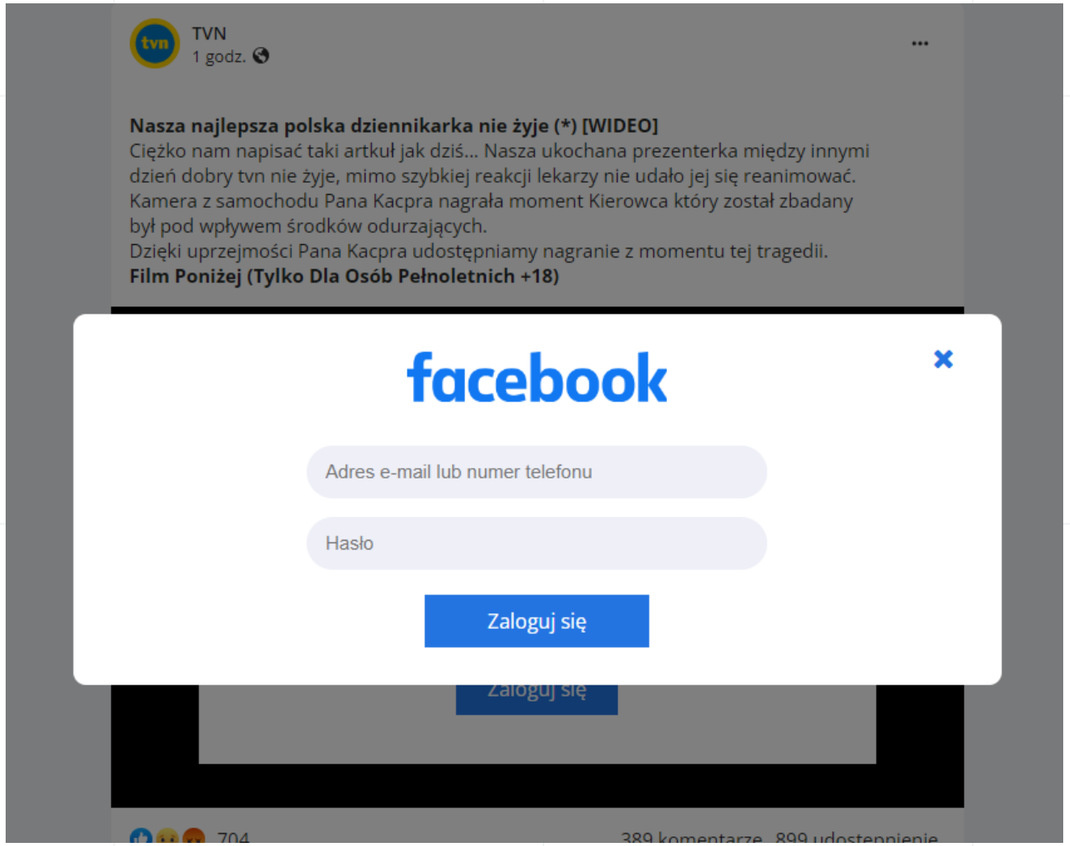
Logowanie do systemu

Ta wiadomość została wysłana automatycznie. Informacja dotycząca przetwarzania danych osobowych przez Narodowy Fundusz Zdrowia (NFZ) w zakresie realizacji zadań statutowych i

Źródło: www.nfz.gov.pl

Przejęcie mediów społecznościowych





NASK

Samorządów to też dotyczy:
straty wizerunkowe

Przykład – skutek wyłudzenia danych do logowania do Facebooka – przejęte konto

Przykład – skutek wyłudzenia danych do logowania do Facebooka – nowy fanpage gminy

Gmina Tarnów

SAMORZĄD GMINA BIP PUB

Oświadczenie – oficjalny profil Gminy Tarnów na facebooku skradziony

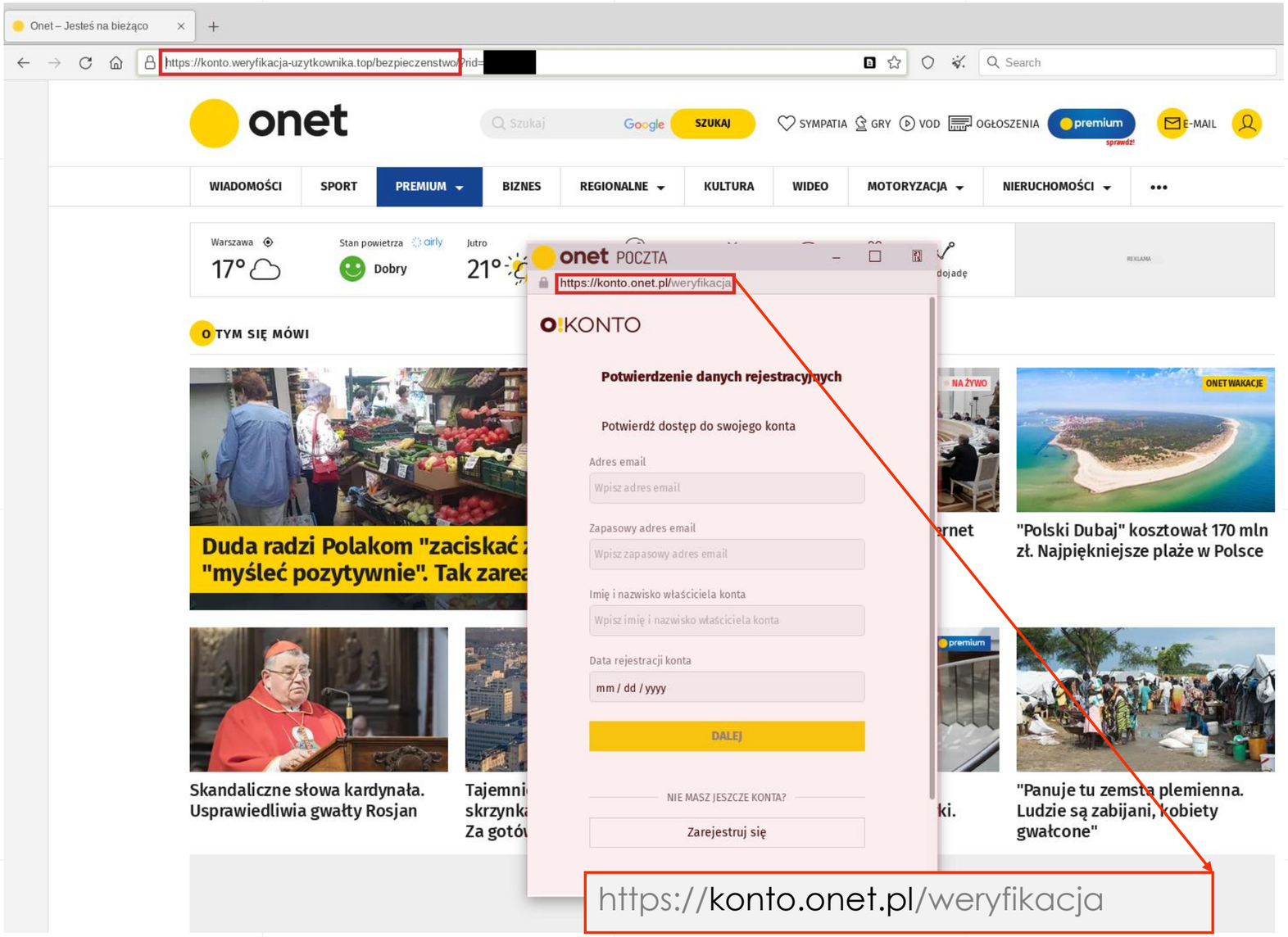
Gmina Tarnów padła ofiarą cyberataku. Oficjalny profil gminy Tarnów prowadzony na portalu społecznościowym FACEBOOK został skradziony – przejęty przez hakerów. Sprawa została zgłoszona na policję. Trwa również próba odzyskania konta.

Ostatnia informacja została zamieszczona przez administratora – Urząd Gminy Tarnów, w dniu 26 września 2023. Oświadczamy, że wszystkie treści i informacje zamieszczane od tej pory na dawnym profilu facebook Gminy Tarnów, jak również wysyłane poprzez facebook'a w imieniu gminy Tarnów wiadomości, nie pochodzą od Urzędu Gminy Tarnów.

Opublikowano: 30 październik 2023

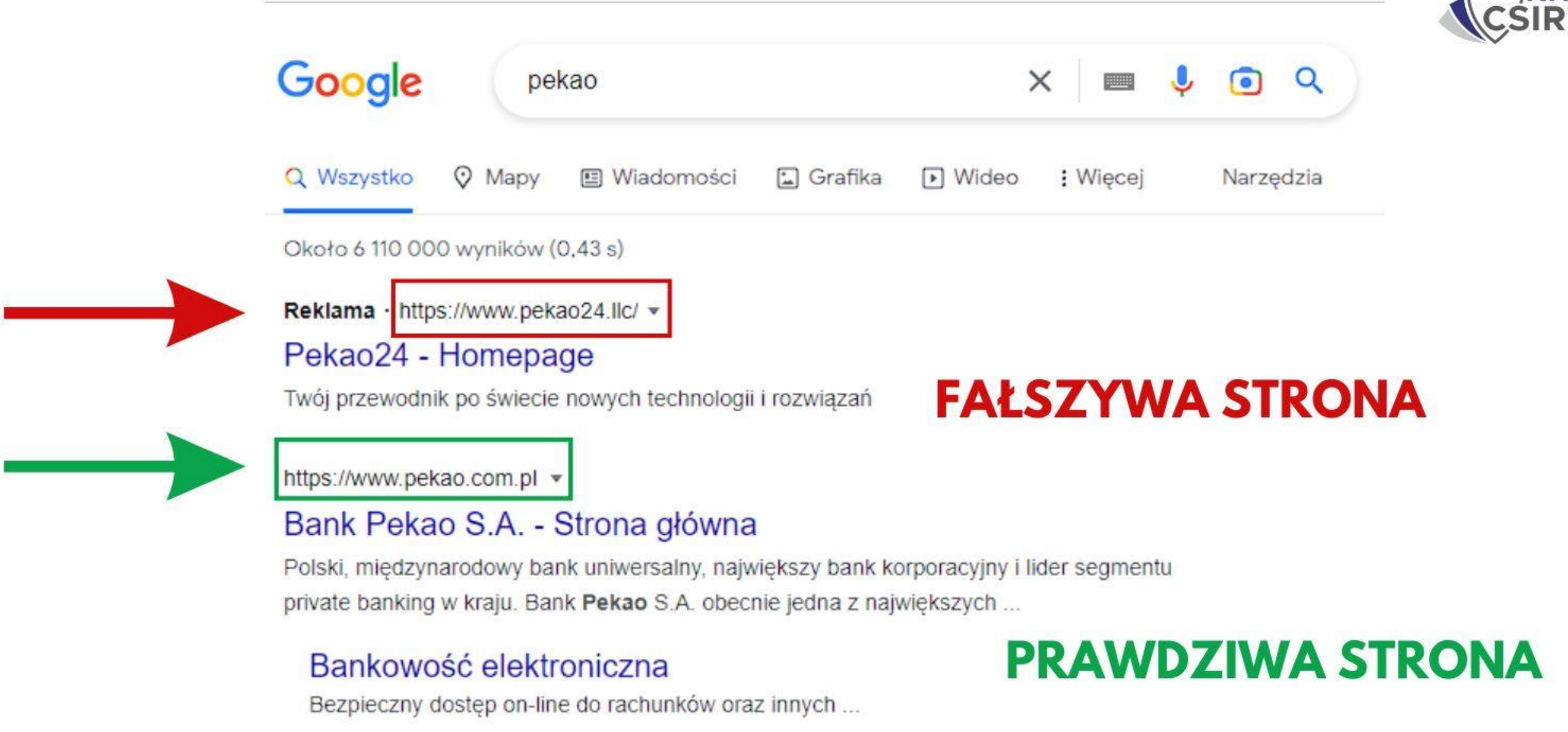
Inne interesujące techniki i metody

Atak na bardziej świadomych - BITB



NASK

JAK ROZPOZNAĆ FAŁSZYWĄ REKLAMĘ W GOOGLE?



Oszustwo w rozmowie telefonicznej

Vishing czyli też phishing

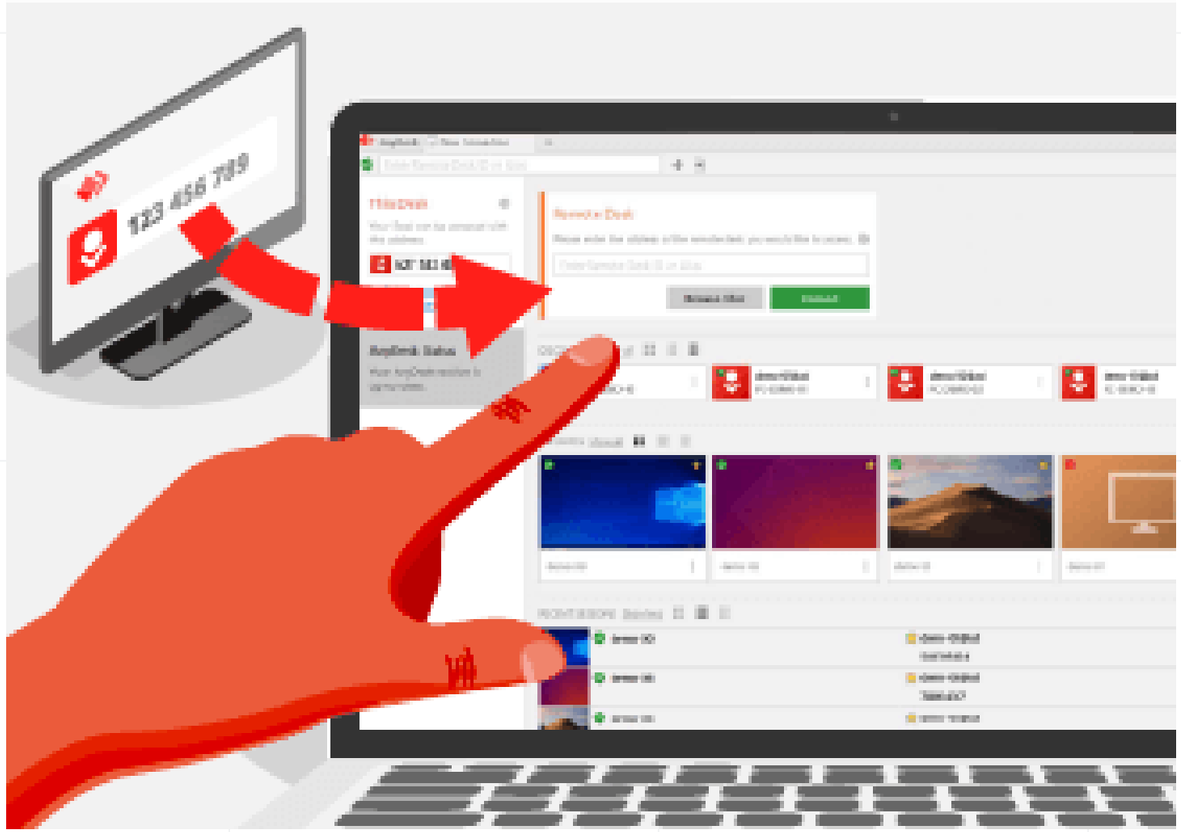
Cele ataku

- Wyłudzenie informacji
- Instalacja oprogramowania
- Wykonanie przelewu/podanie kodów jednorazowych
- Uwaga na **spoofing**,
  podszywanie się pod dowolny numer telefonu!

  (a może już też na Deep Fake?)

NASK

Ataki telefoniczne „na zdalny pulpit”



TeamViewer

AnyDesk

ALPEMIX

NASK

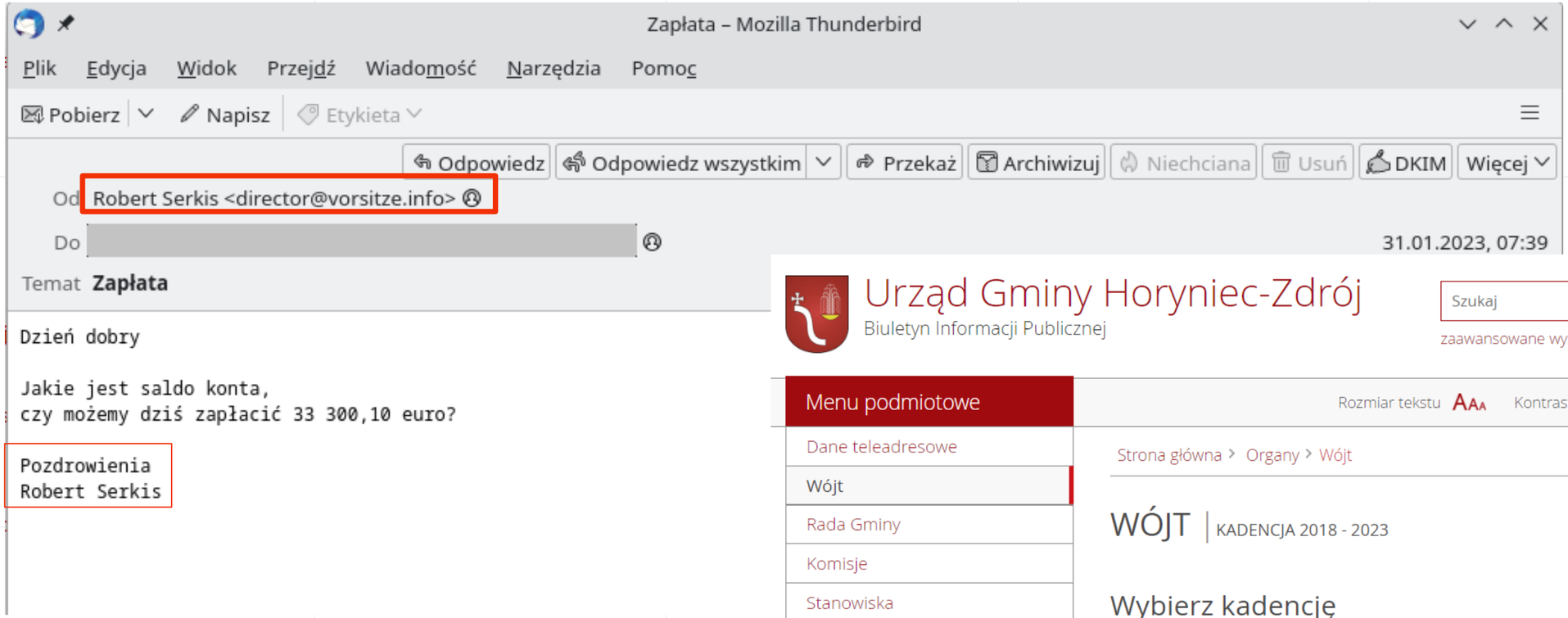
Ataki socjotechniczne na samorządy

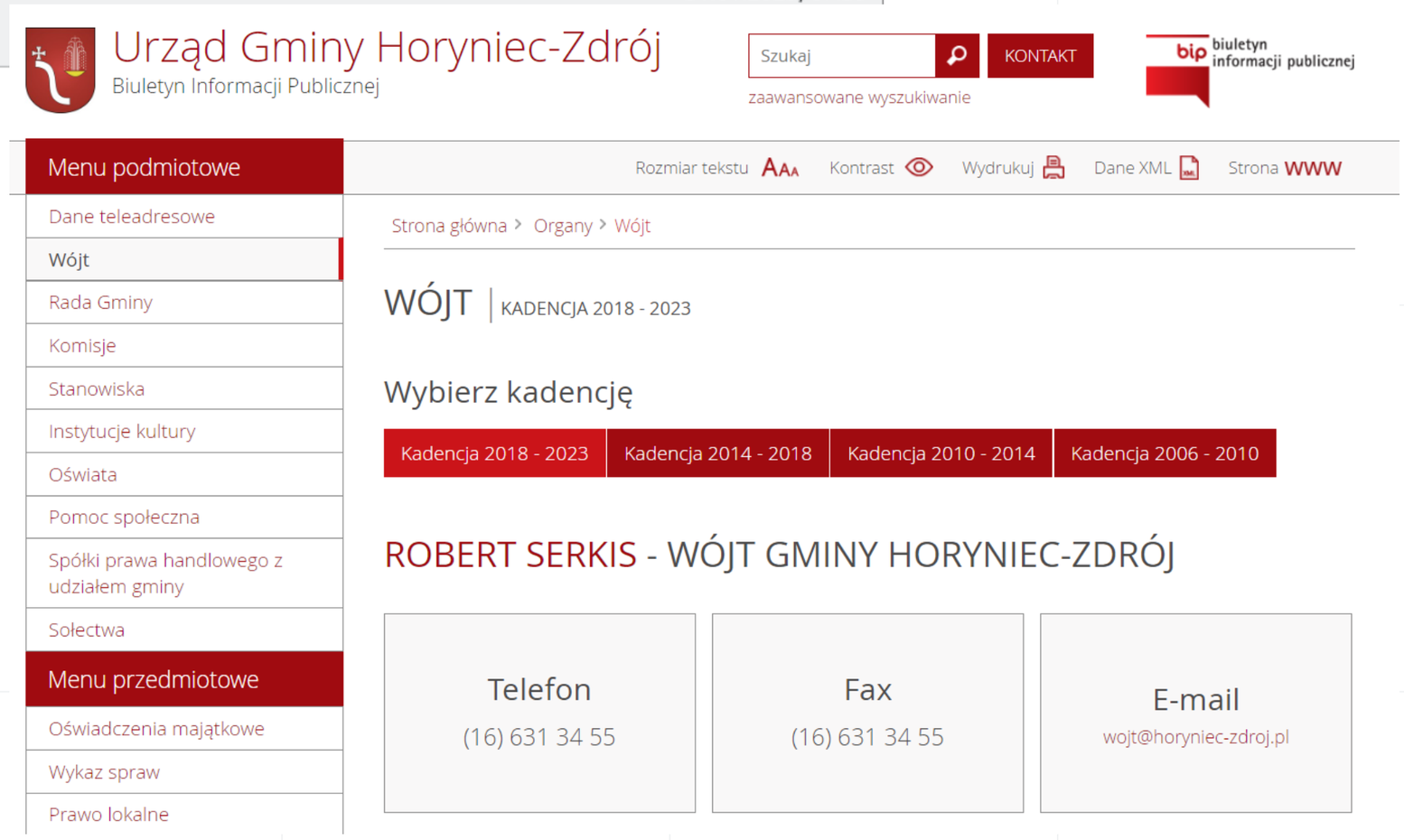
Czyli czy jestem celem?

„Klasyczne”, wysyłane pocztą elektroniczną, elementy personalizacji ataku i rozpoznania celu

Stosunkowo łatwe do rozpoznania

„Oszustwo na dyrektora” – atak na JST





NASK

„Oszustwo na dyrektora” – atak na JST

Temat: Zapłata
Data: Thu, 13 Jul 2023 07:35:24 +0100 (WAT)
Nadawca: Adrian Mateusz [redacted] <office@mailxmailx.online>
Adresat: Bozena. [redacted]

Dzień dobry

Ile wynosi saldo naszego konta?
czy możemy dziś zapłacić 42.000 euro?

Uprzejmie witamy
Adrian Mateusz [redacted]

„Oszustwo na dyrektora” ze spoofingiem

Pilna prośba

Paweł <p. @hospicjum
Do biuro@hospicjum

09:13

PG

Odpowiedz Odpowiedz wszystkim Prześlij dalej Usuń

Mamy dziś pilną płatność, jaki jest stan naszych kont?

Z poważaniem,

Paweł

Przykład oszustwa skierowanego do gminy

Pobierz | Napisz | Etykieta

Odpowiedz | Odpowiedz wszystkim | Przekaż | Archiwizuj | Niechciana | Usuń | DKIM | Więcej

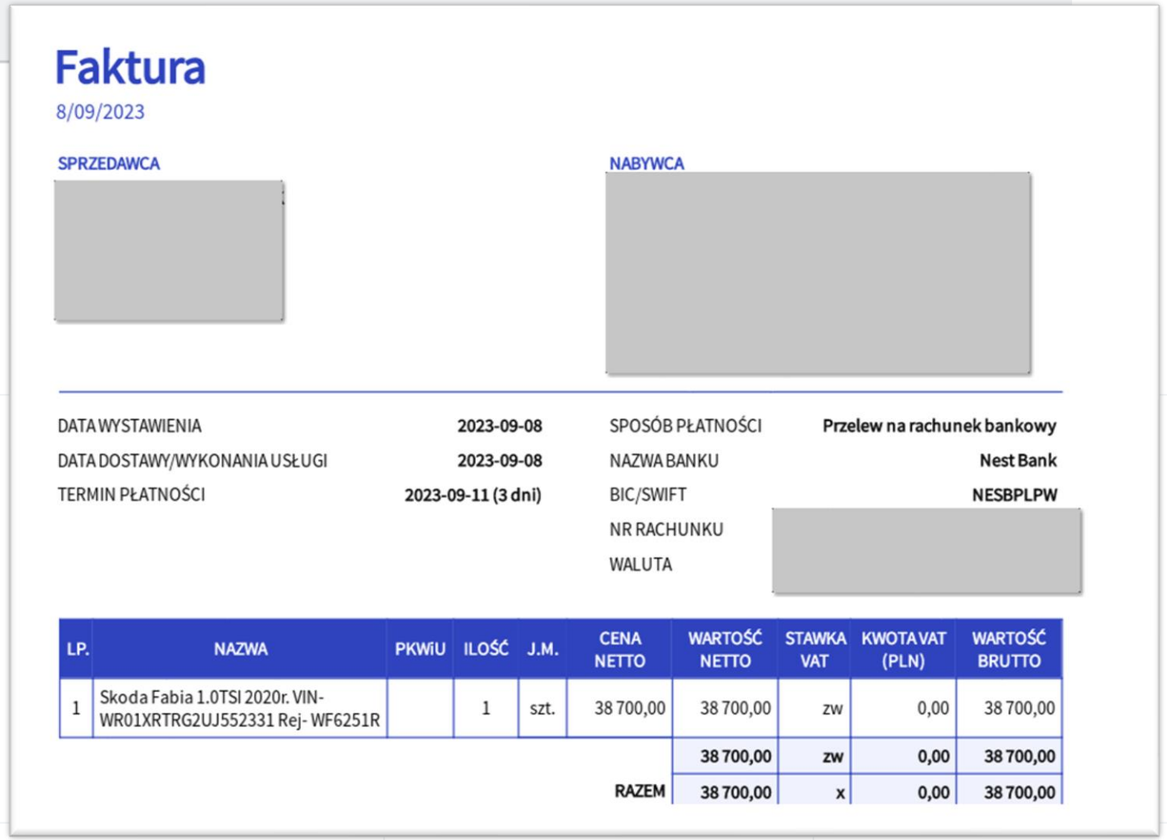
Od j.r[redacted]pl <j.[redacted].com>

Do [redacted] <skarbnik@[redacted].pl>

14.09.2023, 11:26

Temat **Re: RE: Faktura**

W załączniku faktura do opłaty.



Faktura

8/09/2023

SPRZEDAWCA

[redacted]

NABYWCA

[redacted]

DATA WYSTAWIENIA	2023-09-08	SPOSÓB PŁATNOŚCI	Przelew na rachunek bankowy
DATA DOSTAWY/WYKONANIA USŁUGI	2023-09-08	NAZWA BANKU	Nest Bank
TERMIN PŁATNOŚCI	2023-09-11 (3 dni)	BIC/SWIFT	NESBPLPW
		NR RACHUNKU	[redacted]
		WALUTA	

LP.	NAZWA	PKWiU	ILOŚĆ	J.M.	CENA NETTO	WARTOŚĆ NETTO	STAWKA VAT	KWOTA VAT (PLN)	WARTOŚĆ BRUTTO
1	Skoda Fabia 1.0TSI 2020r. VIN-WR01XRTRG2UJ552331 Rej- WF6251R		1	szt.	38 700,00	38 700,00	zw	0,00	38 700,00
						38 700,00	**zw**	**0,00**	**38 700,00**
					RAZEM	**38 700,00**	**x**	**0,00**	**38 700,00**

Z wykorzystaniem telefonu, spersonalizowane

Trudniejsze do rozpoznania: spoofing, rozpoznanie celu, zaniedbania w zabezpieczeniach

Straty bywają wysokie

29.03.2021 Aktualizacja: 29.03.2021, 23:00

Księgowa z radomskiej spółki miejskiej "Rewitalizacja" przelała na konta oszustów ponad 1,5 mln zł.

Śledztwo w tej sprawie prowadzi Prokuratura Okręgowa w Radomiu. W ub. tygodniu organy ścigania zostały powiadomione o oszustwie metodą na policjanta, którego ofiarą padła miejska spółka "Rewitalizacja". Z zawiadomienia wynikało, że z pracownikiem spółki skontaktowała się telefonicznie osoba podająca się za funkcjonariusza Centralnego Biura Śledczego Policji. Rzekomy policjant poinformował, że środki zdeponowane na kontach spółki są zagrożone atakiem hakerskim i należy niezwłocznie podjąć działania udaremniające kradzież pieniędzy.

Gmina padła ofiarą oszustwa, sprawę bada prokuratura

15-07-2021

Gmina Konstancin-Jeziorna w procesie lokowania wolnych środków finansowych na bankowej lokacie terminowej padła ofiarą oszustwa na kwotę 5 mln zł.

Gmina oszukana na 5 milionów złotych

Przez **Redakcja** 7 maja 2021

Skarbnik Urzędu Gminy Rząśnia padła ofiarą oszustwa. Z gminnej kasy wyparowało 5 milionów złotych.

Prokuratura Rejonowa w Wieluniu prowadzi śledztwo w sprawie zuchwałego oszustwa, do jakiego doszło w Urzędzie Gminy w Rząśni. Z nieoficjalnych ustaleń wynika, że ze skarbnik Urzędu Gminy w Rząśni mieli kontaktować się oszuści, którzy skutecznie nakłonili ją do przelania na ich konto zawrotnej kwoty 5 milionów złotych.

NASK

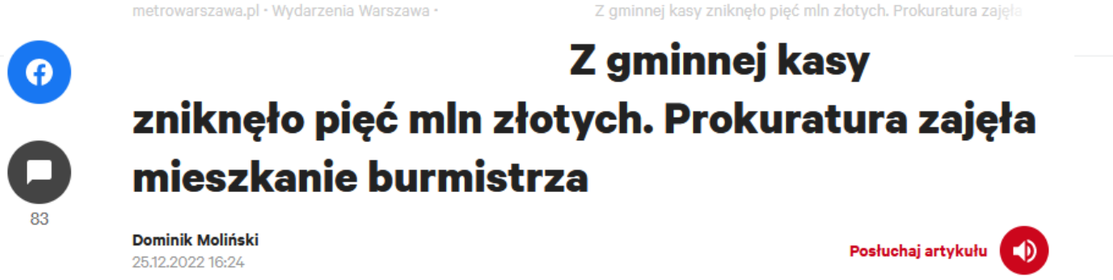
Odpowiedzialność bywa osobista

*„Wobec burmistrza (…) sformułowano zarzut popełnienia przestępstwa polegającego na **nieumyślnym niedopełnieniu ciążących na nim obowiązków** i w związku z tym wyrządzenia szkody w obrocie w wielkich rozmiarach, to jest przestępstwa zagrożonego karą pozbawienia wolności do lat trzech”*

Na podstawie art. 296. KK

*„Burmistrz nie przyznał się do winy. Według prokuratury nie było konieczne zatrzymywanie go, podjęto jednak inne działanie. - Na poczet grożących podejrzanemu - w przypadku uznania go winnym oraz skazania - kary grzywny, orzeczenia obowiązku naprawienia szkody oraz zasądzenia obowiązku zapłaty kosztów sądowych w postępowaniu karnym, **dokonano zajęcia nieruchomości w postaci mieszkania stanowiącej własność podejrzanego**, wchodzącą w skład wspólności ustawowej majątkowej małżeńskiej, poprzez ustanowienie hipoteki przymusowej do kwoty łącznie pięciu milionów i dwudziestu tysięcy złotych.”*

Na podstawie art. 291. KPK



metrowarszawa.pl · Wydarzenia Warszawa · Z gminnej kasy zniknęło pięć mln złotych. Prokuratura zajęła

83

Z gminnej kasy zniknęło pięć mln złotych. Prokuratura zajęła mieszkanie burmistrza

Dominik Moliński
25.12.2022 16:24

Posłuchaj artykułu

Oszukana gmina straciła pięć milionów złotych. Prokuratura zajęła mieszkanie burmistrza

Podobnymi, również kosztownymi atakami padły samorządy miast w (…) i (…). W ich przypadku cyberprzestępcy dokonali **ataku na serwer VoIP** służący do nawiązywania połączeń telefonicznych z wykorzystaniem sieci internetowej. W przypadku (…) hakerzy wykonali prawie 900 połączeń do Zimbabwe, „naciągając” miasto na rachunek w wysokości 49 tys. zł, a (…) na 19,5 tys. zł poprzez telefony do sieci komórkowej w Austrii. (prawo.pl)

NASK

Cecha wspólna: niedochowanie wewnętrznych procedur płatności

Efekt: utrata pieniędzy, zwolnienia dyscyplinarne

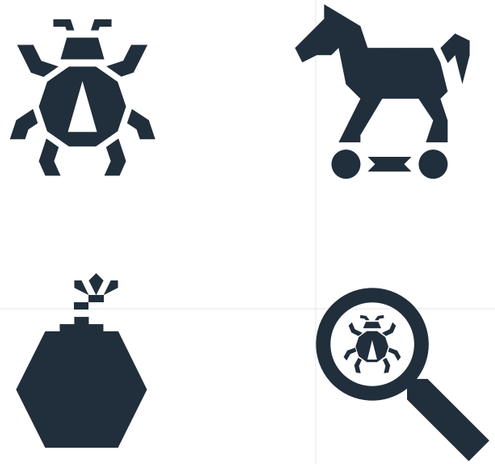
Ransomware

Czyli złośliwe/szkodliwe oprogramowanie

Oprogramowanie wyłudzające okup

Źródła infekcji

- **Maile nakłaniające do pobrania i uruchomienia pliku załączonego lub umieszczonego w linku**
- Luki bezpieczeństwa w publicznie dostępnych usługach
- Niewystarczające zabezpieczenia dostępu do infrastruktury oraz publicznych usług (często zbyt słabe hasło)



Kraków. Ataku hakerskiego na urząd marszałkowski w Krakowie dokonała zagraniczna grupa? Sprawę wyjaśnia policja i prokuratura

Bartosz Dybała 23 lutego 2021, 15:43

KOMUNIKATY

Incydent cyberbezpieczeństwa

Urząd Marszałkowski Województwa Mazowieckiego w Warszawie przy ul. Jagiellońskiej 26 (dalej UMWM), informuje o incydencie cyberbezpieczeństwa w części infrastruktury projektowej "Wrota Mazowsza".

Incydent został stwierdzony 5 grudnia 2022 r. i polegał na **ataku złośliwego oprogramowania szyfrującego pliki** (Ransomware). Na chwilę obecną **nie potwierdzono pozyskania danych osobowych przez osoby trzecie**. Trwają działania mające na celu ustalenie pozostałych okoliczności zdarzenia.

UMWM realizuje ponadto czynności mające na celu odzyskanie danych z istniejących kopii zapasowych oraz zapewnia, że podejmie niezbędne działania, aby podobna sytuacja nie miała miejsca w przyszłości.

CYBERBEZPIECZEŃSTWO

Cyberatak na system biletowy i usług na Śląsku - ŚKUP. [AKTUALIZACJA]: To ransomware

NIKOLA BOCHYŃSKA
10.02.2023 13:11

DRUKUJ PDF

Cashless.pl

Systemy IT Olsztyna zaatakowane przez hakerów. Nie działają biletomaty, tworzą się korki

Sieć informatyczna Zarządu Dróg, Zieleni i Transportu w Olsztynie ma problem z prawidłowym funkcjonowaniem. Prawdopodobnie jest to efekt...

28 cze 2023

Portal Samorządowy

Olsztyn już trzecią dobę walczy z atakiem hakerów. Nie działają ważne systemy

Nie działają systemy sterowania ruchem, biletomaty. Ograniczony jest dostęp do systemu informacji pasażerskiej. To efekty ataku hakerskiego...

28 cze 2023

Interia Motoryzacja

To nie film. Atak hakerski sparaliżował ruch w Olsztynie - Motoryzacja w INTERIA.PL

Awaria systemu zarządzania ruchem, gigantyczne korki, a także zablokowane biletomaty w autobusach, tramwajach i na przystankach.

27 cze 2023

Money.pl

Olsztyn jeździ na gapę. Dwa tygodnie od cyberataku, a paraliż trwa

Cyberatak na systemy Zarządu Dróg Transportu i Zieleni w Olsztynie wciąż odbija się mieszkańcom czkawką. System nie odzyskał pełnej...

7 lip 2023

onet WIADOMOŚCI

enhanced by Google

Niemieckie gminy sparaliżowane przez hakerów. "Nie działają ratusze, urzędy. Konsekwencje dotknęły miliony ludzi"

BENEDIKT FUEST | 16 listopada 2023, 07:11 WELT

"Powodem tego jest cyberatak na Suedwestfalen IT, który dotknął 72 gminy" — wyjaśnia miasto.

Od zeszłego tygodnia w mieście regularnie spotyka się zespół kryzysowy — nie wiadomo, kiedy dostawca usług IT będzie w stanie ponownie uruchomić swoje systemy dla dotkniętych atakiem gmin i miast. **Konsekwencje ataku dotknęły miliony ludzi w całej Nadrenii Północnej-Westfalii.**

https://wiadomosci.onet.pl/

Ransomware – problemy

- **Brak dostępności danych**

- W przypadku ataku ransomware, **atakujący często nie tylko szyfrują dane, ale także wykradają je**, grożąc upublicznieniem w przypadku nie zapłacenia okupu

- Często dochodzi również do **zaszyfrowania kopii zapasowych**

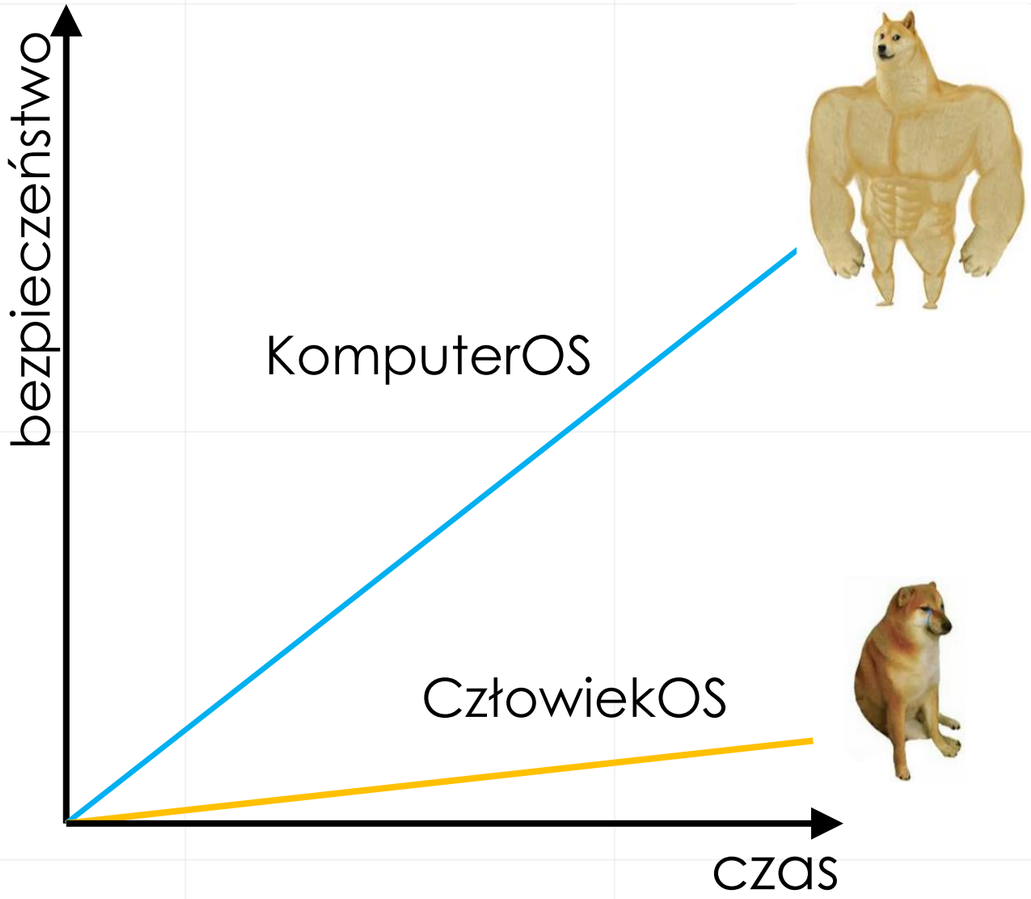
- Warto pamiętać, że **zapłacenie okupu nie gwarantuje odzyskanie danych**

Edukowanie

Dlaczego jest ważne?

Edukowanie, zwiększanie świadomości

- **Stale edukuj siebie i swoich użytkowników**
- Nawet najlepsze techniczne zabezpieczenia nie pomogą, jeśli Twoi użytkownicy nie będą przestrzegać podstawowych zasad bezpieczeństwa
- Atakujący obierają za cel ataku użytkownika – pracownika (socjotechnika działa)



NASK

Edukowanie, zwiększanie świadomości

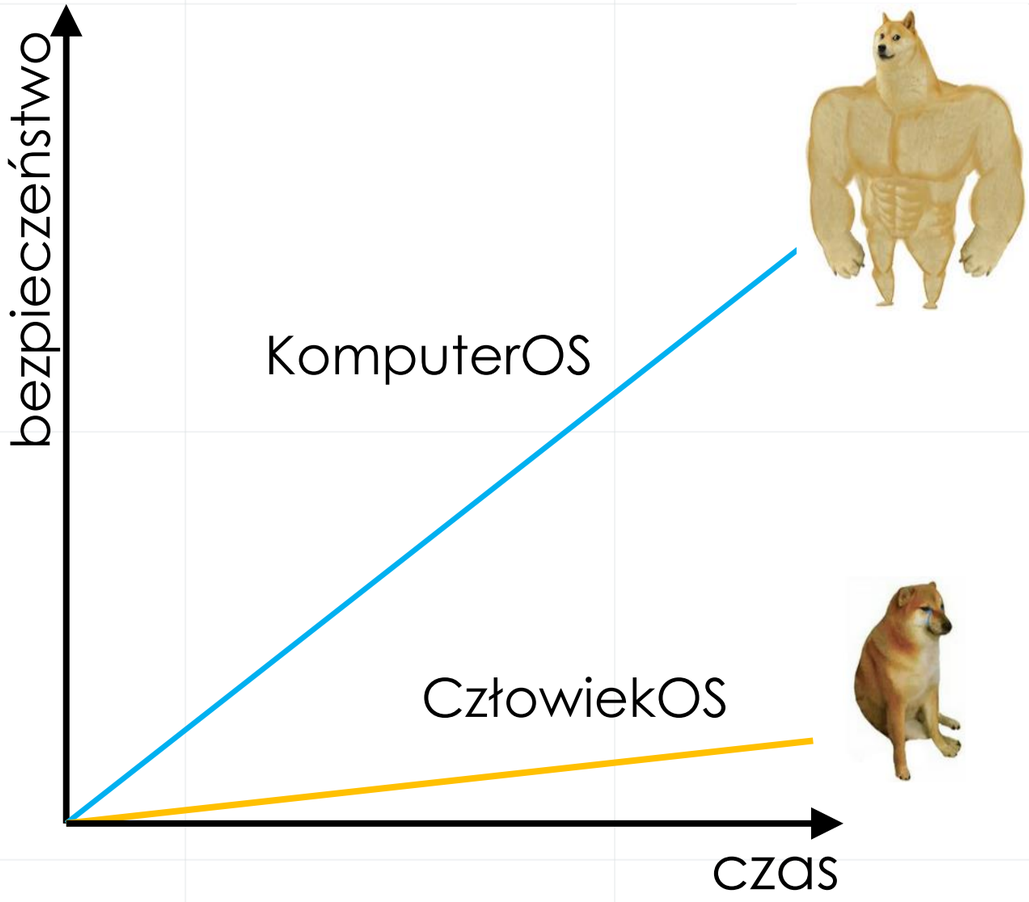
- Zwiększanie świadomości użytkowników o zagrożeniach jest istotnym elementem zapewnienia bezpieczeństwa

ALE

- Nie przerzucamy na niego odpowiedzialności

BO

- **Zgłaszanie przez użytkowników incydentów jest istotnym elementem zapewnienia bezpieczeństwa**



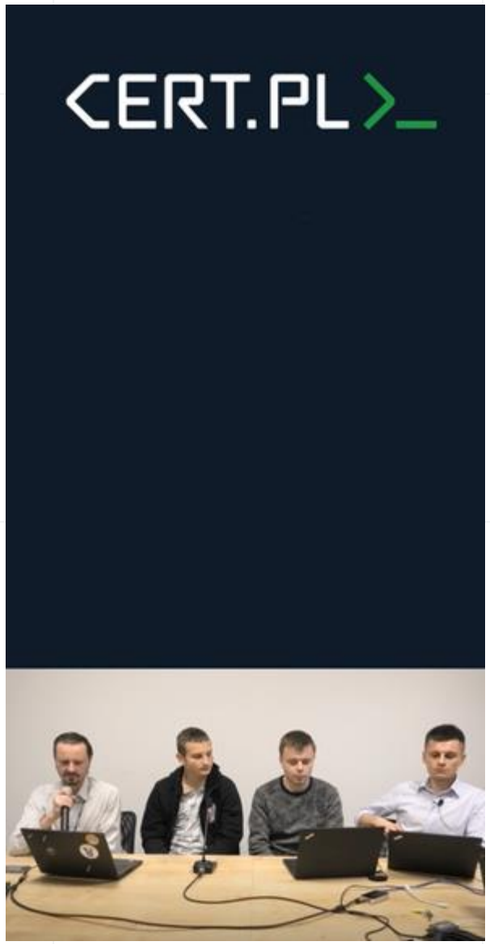
Szkolenia da pracowników

Najważniejsze tematy: **phishing, socjotechnika i cyberhigiena.**

- **Szkolenia wstępne:**
  – podstawowe zagadnienia, polityki i procedury firmowe, zgłaszanie incydentów.
- **Szkolenia przypominające:**
  – uzupełnienie i utrwalenie wiedzy, aktualne kampanie i trendy.
- **Kursy e-learningowe:** w intranetcie, ogólnodostępne lub komercyjne.

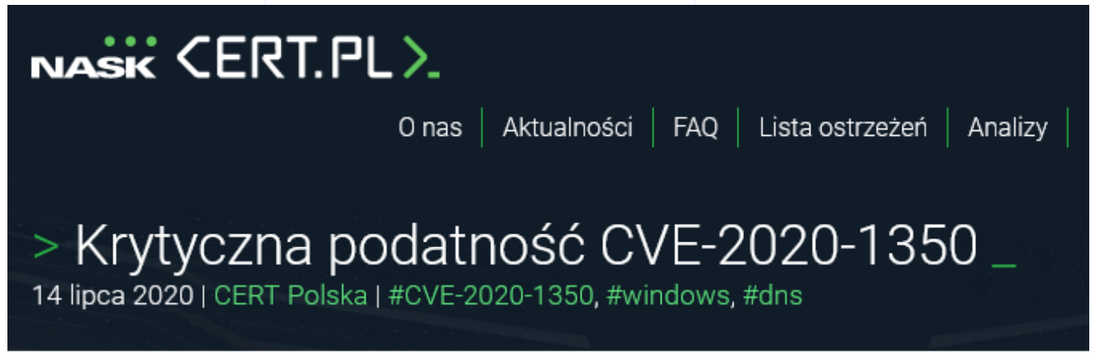
Ćwiczenia dla pracowników

- Ukierunkowane na indywidualnego pracownika.
- Scenariusz realny i aktualny – **phishing/ socjotechnika.**
- Wspierają **wyrobienie dobrych nawyków.**
- Można przeprowadzić samodzielne lub wykupić usługę.
- Zalecane **tylko organizacjom z dojrzałym systemem bezpieczeństwa**, jako element tego systemu.



NASK

Dbamy o bezpieczeństwo? – dbajmy o edukację własną



Różny stopień zaawansowania:

https://cert.pl/news

https://cert.pl/publikacje

Materiały dla pracowników – bazy wiedzy

https://bezpiecznymiesiac.pl/bm/baza-wiedzy

https://www.gov.pl/web/baza-wiedzy/aktualnosci

https://cert.pl/ouch/

„Polityka bezpieczeństwa" w życiu prywatnym – **bezpieczeństwo poczty i mediów społecznościowych.**

https://cert.pl/uploads/docs/CERT_Polska_Bezpieczna_poczta_i_konta_spolecznosciowe.pdf

EUROPEJSKI MIESIĄC CYBER BEZPIECZEŃSTWA

W październiku!

NASK

Wszystko o hasłach i uwierzytelnianiu

https://cert.pl/hasla/

Baza Wiedzy

Materiały

Plakaty informacyjne

A2 | A2 DRUK

Baza polskich haseł

Aktualności w mediach społecznościowych

https://facebook.com/CERT.Polska

https://twitter.com/cert_polska

Komunikaty o **oszustwach finansowych:**

https://www.facebook.com/people/CSIRT-KNF/100065127625555/

https://twitter.com/CSIRT_KNF

NASK

Sprawdzanie własnej wiedzy

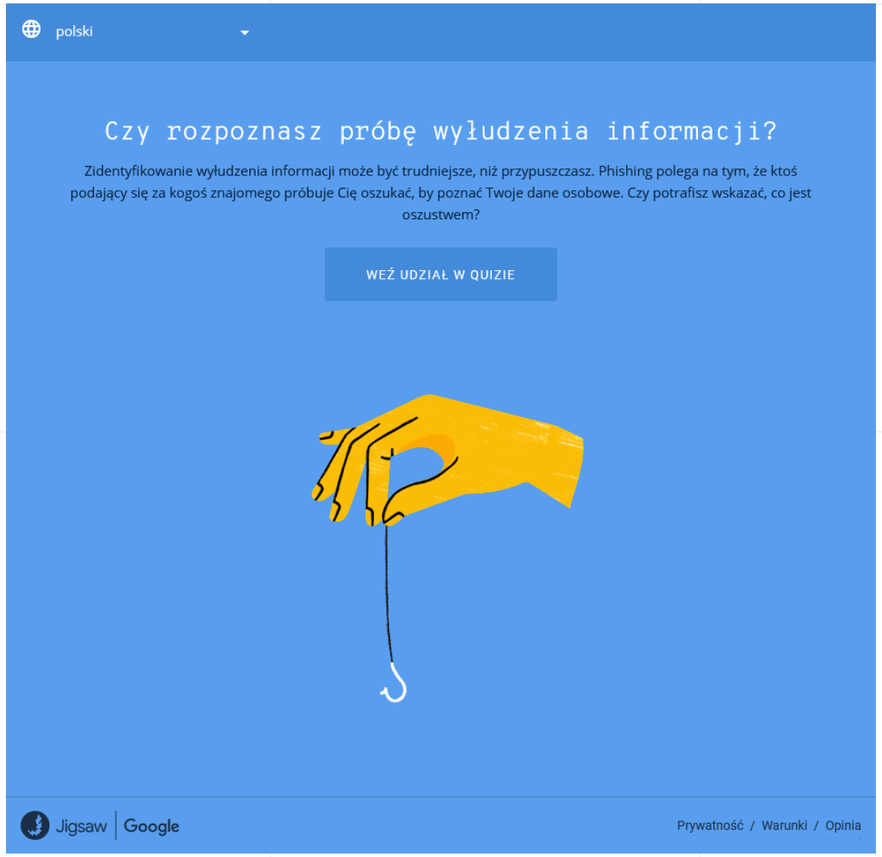
Rozpoznawanie phishingu:

https://phishingquiz.withgoogle.com/

https://quiz.securityinside.pl/

https://phishingstop.aliorbank.pl/

https://www.credit-agricole.pl/quiz/



NASK

Materiały szkoleniowe - bazy wiedzy

https://bezpiecznymiesiac.pl/bm/baza-wiedzy

https://www.gov.pl/web/baza-wiedzy/cyberbezpieczny-samorzad

https://cert.pl/ouch/

https://www.nomoreransom.org/pl/prevention-advice.html

#CyberbezpiecznySamorząd

Wszystko o portalu samorzad.gov.pl - Poradnik PRCyber - 06

Krok po kroku, jak przystąpić do projektu (Grudzień 2020 r.)

Cyberbezpieczne usługi chmurowe dla administracji publicznej - Poradnik PRCyber-05

Środowisko informatyczne dostarczające usługi chmurowe oraz infrastrukturę IT za pośrednictwem Internetu (Listopad 2020 r.)

Jak sobie radzić ze skutkami ataków typu ransomware? – Poradnik PRCyber-04

Ograniczenie skutków ataków typu ransomware (Sierpień 2020 r.)

Jak zapobiegać atakom typu ransomware? – Poradnik PRCyber-03

Wskazówki dotyczące zabezpieczeń przed szkodliwym oprogramowaniem (Lipiec 2020 r.)

Materiały dla profesjonalistów – oficjalne strony CSIRTów

CSIRT GOV: https://csirt.gov.pl

CSIRT NASK: https://www.cert.pl

CSIRT MON: https://csirt-mon.wp.mil.pl/pl/

C:[SIRT/MON

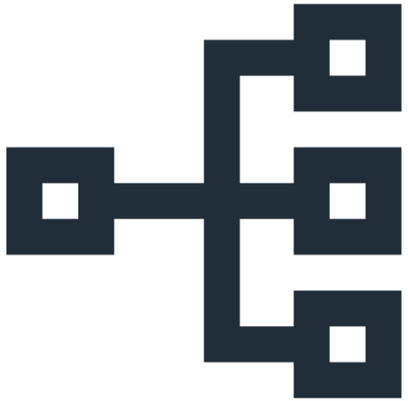
NASK

CERT.PL

Co powinniśmy robić

Czyli obowiązki

Obowiązki ustawowe



uKSC

- incydenty
- osoby konktaktowe

KRI

- SZBI
- wymagania minimalne dla systemów

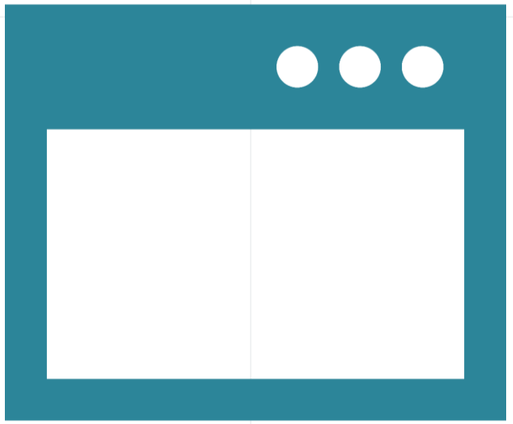
uZNKE

- phishing, smishing
- spoofing
- SPF, DKIM, DMARC

Zgłoszenie incydentu do CSIRT NASK

- Wyznaczona osoba/ zespół bezpieczeństwa
- Incydent należy **zgłosić niezwłocznie, nie później niż w ciągu 24 godzin** od momentu wykrycia do właściwego CSIRT.
- Zgłoszenie przekazywane jest **w postaci elektronicznej**, poprzez uzupełnienie **formularza internetowego** znajdującego się na stronie: **https://incydent.cert.pl**.

24 godz.



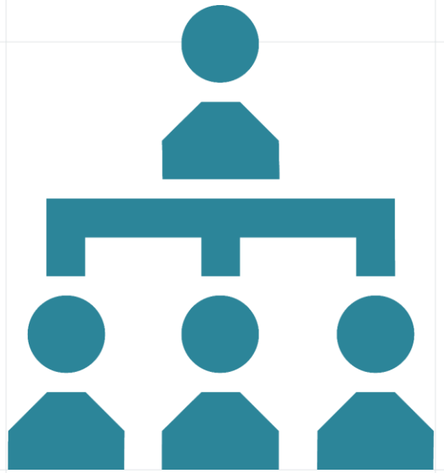
https://incydent.cert.pl

lub

w systemie S46

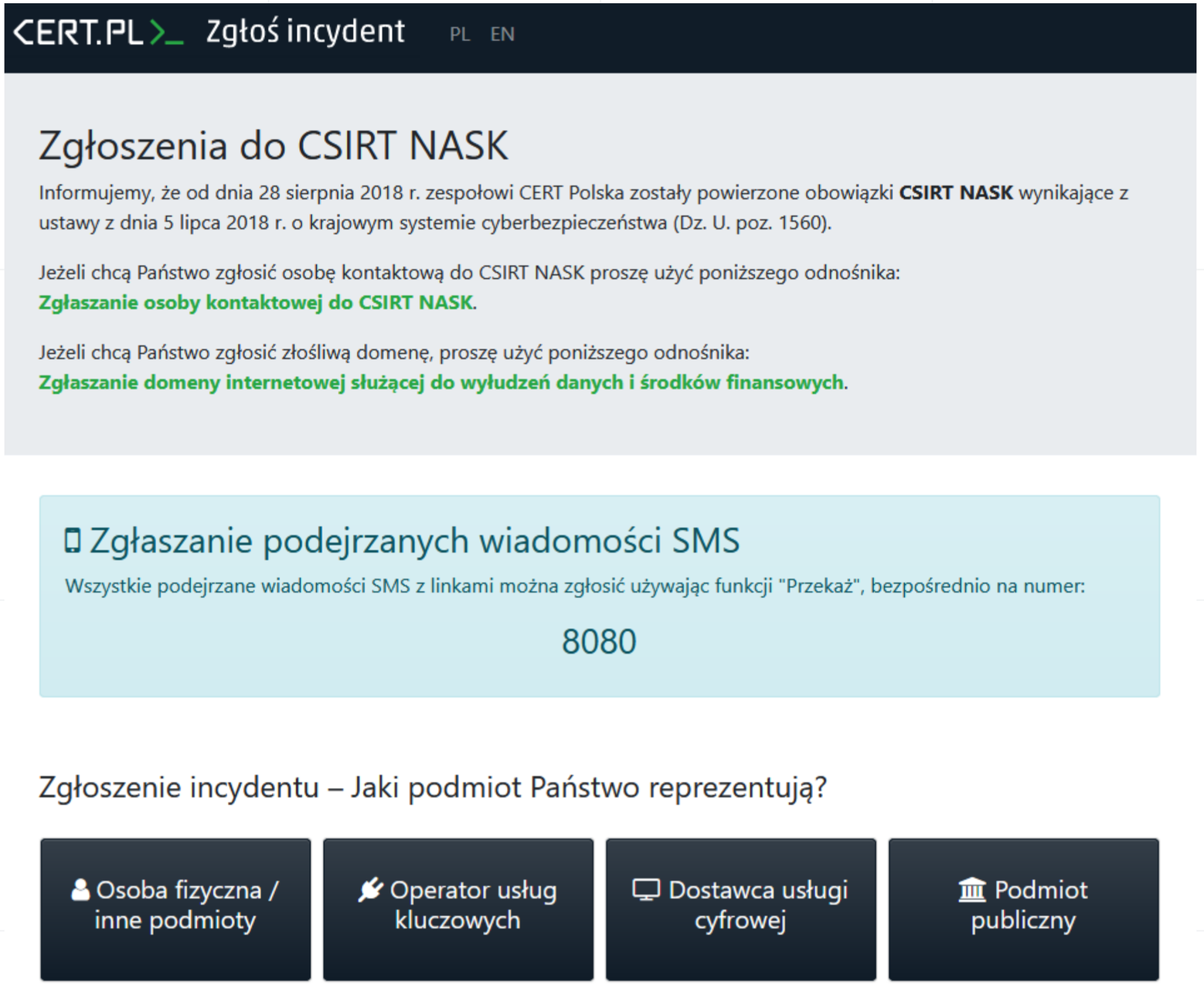
Kto zgłasza incydent w organizacji?

Incydent w środowisku służbowym może i powinna zgłaszać **każda osoba** w organizacji, ale:



Pracownicy zgłaszają do **zespołu bezpieczeństwa/ helpdesku**

Do CSIRT incydent zgłasza **wyznaczona osoba** (lub komórka organizacyjna)


CERT.PL Zgłoś incydent
PL EN
Zgłoszenia do CSIRT NASK
Informujemy, że od dnia 28 sierpnia 2018 r. zespołowi CERT Polska zostały powierzone obowiązki CSIRT NASK wynikające z ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. poz. 1560).
Jeżeli chcą Państwo zgłosić osobę kontaktową do CSIRT NASK proszę użyć poniższego odnośnika:
Zgłaszanie osoby kontaktowej do CSIRT NASK.
Jeżeli chcą Państwo zgłosić złośliwą domenę, proszę użyć poniższego odnośnika:
Zgłaszanie domeny internetowej służącej do wyłudzeń danych i środków finansowych.
Zgłaszanie podejrzanych wiadomości SMS
Wszystkie podejrzane wiadomości SMS z linkami można zgłosić używając funkcji "Przekaż", bezpośrednio na numer:
8080
Zgłoszenie incydentu – Jaki podmiot Państwo reprezentują?
Osoba fizyczna / inne podmioty
Operator usług kluczowych
Dostawca usługi cyfrowej
Podmiot publiczny

Obowiązek informacyjny

- Obsługa incydentu wiąże się również z **obowiązkiem przekazania informacji** osobom, na rzecz których realizuje się zadanie publiczne
- **Osoby mają prawo dostępu do wiedzy pozwalającej na:**

zrozumienie zagrożeń cyberbezpieczeństwa.

stosowanie skutecznych sposobów zabezpieczania się przed tymi zagrożeniami.

Obowiązek informacyjny może zostać spełniony poprzez publikacje stosownego komunikatu na stronie internetowej.

Zgłaszanie osób kontaktowych do CSIRT NASK

Obowiązkowi zgłoszenia osób kontaktowych właściwemu CSIRT podlegają wg ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa (Dz. U. poz. 1560) **operatorzy usług kluczowych** (art 9 ust 1) oraz **podmioty publiczne** (art 22 ust 1 pkt 5).
Jeżeli chcą Państwo zgłosić incydent proszę użyć poniższego odnośnika:
Zgłaszanie incydentu do CSIRT NASK.

Aby zgłosić osoby kontaktowe do CSIRT NASK lub zaktualizować ich dane należy:

- wypełnić poniższy formularz,
- wygenerowane pismo opatrzyć podpisem, elektronicznym lub tradycyjnym kierownika instytucji,
- przesłać pismo na skrzynkę ePUAP (Naukowa i Akademicka Sieć Komputerowa PIB; adres skrzynki: `/NASK-Instytut/SkrytkaESP`, w tytule proszę wpisać "Zgłoszenie osoby kontaktowej do CSIRT NASK") lub na adres NASK-PIB wskazany w dokumencie (w przypadku operatora usługi kluczowej załączając skan decyzji administracyjnej uznającej podmiot za operatora usługi kluczowej).

Przed wypełnieniem poniższego formularza polecamy zapoznać się ze wspólnymi **rekomendacjami CSIRT NASK oraz CSIRT GOV** w zakresie wyznaczania osób kontaktowych.

Zgłoszenie osoby kontaktowej – Jaki podmiot Państwo reprezentują?

Operator usługi kluczowej	Podmiot publiczny	Inny podmiot
Wypełnienie obowiązku wynikającego z art 9 ust 1 ustawy o KSC	Wypełnienie obowiązku wynikającego z art 22 ust 1 pkt 5 ustawy o KSC	Dobrowolne zgłoszenie niezobowiązanego podmiotu

KRI – niezbędne minimum

Rozdział IV rozporządzenia

- Sposoby zapewnienia bezpieczeństwa przy wymianie informacji (**SZBI, normy**)
- Wymagania minimalne (techniczne)

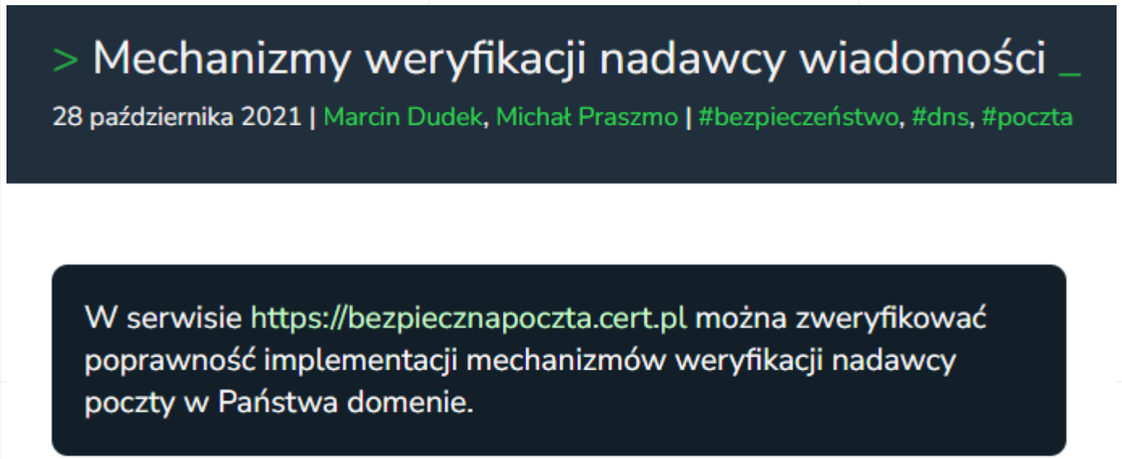
Załączniki do rozporządzenia

- Specyfikacja formatów danych oraz protokołów komunikacyjnych i szyfrujących
- Standardy techniczne zapewniające wymianę informacji
- Sposoby zapewnienia dostępu dla osób niepełnosprawnych

Bezpieczeństwo poczty

https://bezpiecznapoczta.cert.pl/

Narzędzie powstało, by chronić użytkowników poczty elektronicznej i ułatwić instytucjom **sprawdzenie poprawności konfiguracji mechanizmów zapewniających jej bezpieczeństwo**.



CERT.PL Bezpieczna poczta

Zachęcamy do kontaktu pod adresem bezpiecznapoczta@cert.pl jeśli mają Państwo uwagi lub komentarze.

Bezpieczna poczta

Narzędzie bezpiecznapoczta.cert.pl powstało, by chronić użytkowników poczty elektronicznej i ułatwić instytucjom sprawdzenie poprawności konfiguracji mechanizmów zapewniających jej bezpieczeństwo.

Główne funkcjonujące dziś instrumenty weryfikacji nadawcy poczty to: **SPF**, **DMARC** i **DKIM**. Jeżeli instytucja ich nie wykorzystuje, naraża się na znaczące ryzyko. Daje bowiem cyberprzestępcom możliwość wysyłania fałszywych wiadomości, w których mogą oni podszyć się pod dowolnego nadawcę z domeny tego podmiotu. Właśnie dlatego niektórzy dostawcy poczty traktują e-maile przychodzące z domen niewykorzystujących tych mechanizmów jako spam.

Chcesz sprawdzić, czy atakujący mogą łatwo podszyć się pod nadawcę w Twojej domenie? Udostępnione tu narzędzie w tym pomoże.

Wymagania prawne

Ustawa z dnia 28 lipca 2023 r. o zwalczaniu nadużyć w komunikacji elektronicznej nakłada na dostawców poczty elektronicznej obowiązek stosowania mechanizmów SPF, DMARC i DKIM, umożliwiających weryfikację nadawcy wiadomości e-mail. Zapisy te dotyczą dostawców poczty, którzy świadczą usługi dla:

- co najmniej 500 000 użytkowników poczty lub
- dla podmiotu publicznego.

Pełny tekst ustawy znajduje się pod adresem https://isap.sejm.gov.pl/isap.nsf/download.xsp/WDU20230001703/T/D20231703L.pdf.

Chcesz sprawdzić, czy realizujesz poprawnie obowiązek ustawowy? Udostępnione tu narzędzie w tym pomoże.

Sprawdź konfigurację wysyłając wiadomość e-mail

Gdy wyślesz testową wiadomość e-mail na specjalny adres, system zweryfikuje poprawność konfiguracji mechanizmów **SPF**, **DKIM** i **DMARC**.

Ta ścieżka jest przez nas rekomendowana – dzięki niej będziemy w stanie wykonać dokładniejsze sprawdzenie, niż korzystając z domeny.

Wyślij e-mail

Sprawdź domenę

Możesz skorzystać także z opcji weryfikacji konfiguracji podając domenę. W tym wypadku zostaną sprawdzone tylko mechanizmy **SPF** i **DMARC** - dla sprawdzenia DKIM konieczne jest wysłanie testowego e-maila.

Sprawdź domenę

NASK

Profilaktyka

Czyli co możemy zrobić więcej?

Zapewnienie bezpieczeństwa teleinformatycznego – niezbędne elementy

- **Zaangażowanie w proces kierownictwa organizacji**

- **Wyznaczenie komórki organizacyjnej do realizacji wcześniej wymienionych zadań** (dedykowany zespół informatyków, zespół bezpieczeństwa, dedykowana osoba lub wynajęta firma)

S46 w ustawie o KSC (wyróżnik: ten System działa nawet gdy Internet nie działa)

- **S46 został zrealizowany przez NASK PIB na zlecenie Ministra Cyfryzacji w KPRM, jako właściciela systemu**

S46 stworzono na bazie prototypu NPC, w którym m.in. opracowano zintegrowany system monitorowania, obrazowania i ostrzegania o zagrożeniach w cyberprzestrzeni RP.

Został wdrożony z dniem 1 stycznia 2021 r.

- **Zgodnie z art. 46 ustawy o KSC, S46 wspiera**
  1. **współpracę podmiotów** wchodzących w skład **krajowego systemu cyberbezpieczeństwa**
  2. **generowanie** i przekazywanie **rekomendacji** dotyczących działań **podnoszących poziom cyberbezpieczeństwa**
  3. **zgłaszanie i obsługę incydentów**
  4. **szacowanie ryzyka** na poziomie krajowym
  5. **ostrzeganie o zagrożeniach** cyberbezpieczeństwa

! System s46 realizuje wyłącznie zadania określone w art. 46 ustawy o KSC.

! System S46 nie pobiera danych, logów z Państwa systemów.

! Przetwarza tylko te informacje, które Państwo i inni uczestnicy samodzielnie wprowadzają do Systemu S46.

Jest systemem dwukierunkowej bezpiecznej wymiany informacji.

NASK

Cyberbezpieczny Samorząd

Cyberbezpieczny Samorząd” to projekt Ministerstwa Cyfryzacji finansowany z Funduszy Europejskich na Rozwój Cyfrowy 2021-2027 (w skrócie FERC) w ramach Działania 2.2

2.2. Wzmocnienie krajowego systemu cyberbezpieczeństwa

*Interwencja obejmie inwestycje **zwiększające poziom bezpieczeństwa informacji** poprzez wzmacnianie odporności oraz zdolności do skutecznego zapobiegania i reagowania na incydenty w systemach informacyjnych państwa oraz podmiotów mających kluczowe znaczenie dla gospodarki.*

Celem projektu jest zwiększenie bezpieczeństwa informacji w administracji samorządowej poprzez wzmacnianie odporności oraz zdolności do skutecznego zapobiegania i reagowania na incydenty.

NASK

Cyberbezpieczny samorząd

PORADNIK

NASK

Ministerstwo Cyfryzacji

Lista ostrzeżeń

Lista ostrzeżeń zawierająca wykaz witryn stanowiących zagrożenie (aktualizowana co 5 minut):

https://cert.pl/lista-ostrzezen/

https://cert.pl/posts/2020/03/ostrzezenia_phishing/

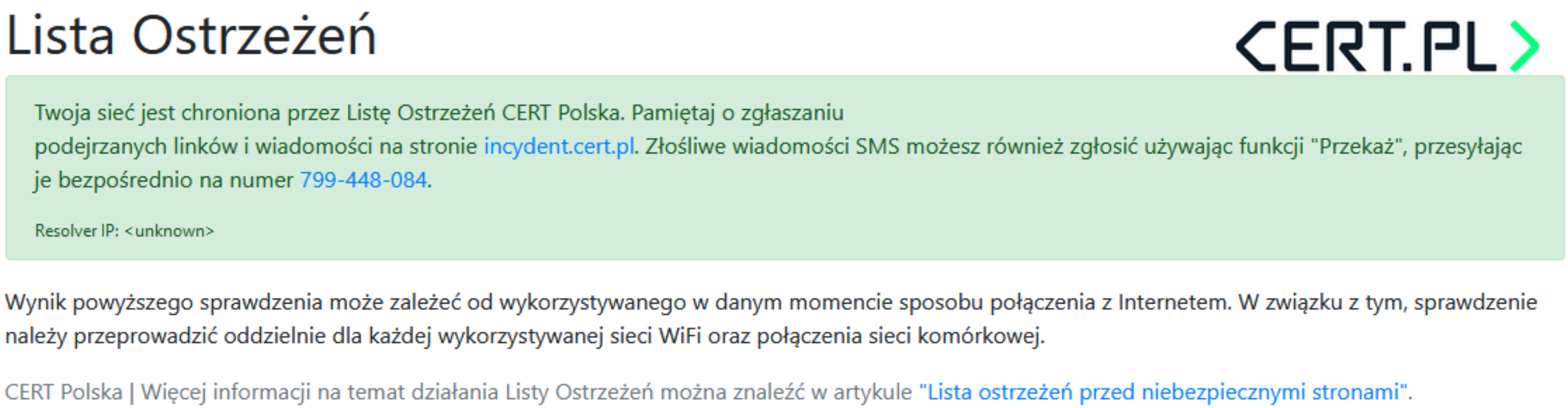
https://hole.cert.pl/domains/

Budowana na podstawnie m.in. zgłoszonych podejrzanych domen
– **obrona przed phishingiem**

Wdrażają operatorzy telekomunikacyjni
– **automatyzacja**

Lista ostrzeżeń

Sprawdzamy czy nasz operator wdrożył listę u siebie: **https://lista.cert.pl**



Obrona przed ransomware

Poradnik dedykowany dla małych organizacji i osób fizycznych

https://cert.pl/uploads/docs/CERT_Polska_Poradnik_ransomware.pdf

Prewencja

Reagowanie

Bezpieczeństwo urządzeń – konieczne minimum

- Weryfikacja procedur wykonywania kopii zapasowych (zasada 3-2-1)
- Regularna aktualizacja oprogramowania
- Segmentacja sieci
- Inwentaryzacja publicznie dostępnych usług
- Zabezpieczenie potencjalnych źródeł infekcji
- Aktywne monitorowanie zdarzeń w sieci

Sprawdzamy
bezpieczeństwo
polskiego internetu

artemis

https://cert.pl/skanowanie/

NASK

Ogólnodostępne rekomendacje

Dostępne w bazie wiedzy KPRM – Cyfryzacja

https://www.gov.pl/web/baza-wiedzy/narodowe-standardy-cyber

Tłumaczenie i przystosowanie do warunków polskich amerykańskiego standardu NIST

Mapowanie środków bezpieczeństwa NSC 800-53 wer. 2 – PN-ISO/IEC 27001:2013

NASK

Zwiększone zagrożenie – stopnie alarmowe

https://cert.pl/posts/2022/02/rekomendacje-cyberprzestrzen-ukraina/

> 24 lutego 2022 | CERT Polska | #rekomendacje | #poradnik | #ransomware | #ukraina |

Rekomendacje w związku ze zwiększonym zagrożeniem w cyberprzestrzeni wywołanym sytuacją na Ukrainie

W związku z obecną sytuacją na Ukrainie oraz ogłoszeniem stopnia alarmowego CHARLIE-CRP, przygotowaliśmy rekomendacje dla obywateli i firm, których wdrożenie uważamy za konieczne.

Czytaj więcej

Zwiększone zagrożenie – stopnie alarmowe

Lista szczególnych działań przypominająca i rozszerzająca poprzednie rekomendacje, m.in.

- sprawdzenie swojej infrastruktury z zewnątrz (Shodan, Artemis, Bezpieczna poczta)
- automatyzacja aktualizacji sygnatur systemów bezpieczeństwa (AV, EDR, IDS, IPS)
- poradniki własne i innych organizacji
- CISA – znane podatności wykorzystywane w atakach
- CSIRT KNF – ochrona DDoS

- **wyznaczenie koordynatora działań**
- **zgłoszenie osoby kontaktowej do NASK**
- **zgłaszanie podejrzanej działalności do CSIRTów**

Uwaga! Jeśli Twoja firma współpracuje z podmiotami na Ukrainie lub ma tam oddziały, dodatkowo:

- Sprawdź reguły dla dostępu sieciowego, ogranicz dozwolony ruch do minimum.
- Monitoruj ruch sieciowy, w szczególności na styku sieci z tymi firmami/oddziałami.
- Obejmij szczególnym monitoringiem hosty, na których jest zainstalowane oprogramowanie, które otrzymuje automatyczne aktualizacje od podmiotów na Ukrainie.
- Ostrzeż pracowników, aby byli szczególnie wyczuleni na informacje nakłaniające ich do podjęcia jakiegoś działania.

Zamiast właściwego podsumowania

Będziemy się mierzyć ze zwiększonym zagrożeniem ze względu na napięcia wojenne, także w internecie, oraz akcje odwetowe na infrastrukturę cyfrową i usługi o strategicznym znaczeniu zależne od tej infrastruktury.

Powinniśmy się przygotować na obronę przed zagrożeniami **w długim okresie**.

https://www.whitehouse.gov/briefing-room/statements-releases/2022/03/21/fact-sheet-act-now-to-protect-against-potential-cyberattacks/

https://www.cisa.gov/shields-up

Przygotuj się

- zadbaj o **wdrożenie wieloskładnikowego uwierzytelniania** w celu utrudnienia atakującym dostępu do swoich systemów
- **używaj nowoczesnych narzędzi monitorowania i wykrywania zagrożeń** na komputerach i innych urządzeniach
- **sprawdź czy wszystkie systemy są zaktualizowane** i chronione przed znanymi podatnościami, a następnie **zmień hasła w całej sieci**, aby ewentualnie skradzione dane uwierzytelniające nie mogły być wykorzystane
- wykonaj kopię zapasową danych i **upewnij się, że istnieje nie podłączona do sieci kopia**, która jest **poza zasięgiem potencjalnego atakującego**

Przygotuj się

- **przećwicz plany awaryjne na wypadek incydentu**, tak żeby być przygotowanym na natychmiastowe reagowanie i zminimalizowanie skutków ataku,
- **szyfruj dane**, aby nie mogły być odczytane, jeżeli zostaną skradzione,
- **edukuj użytkowników** swoich systemów, **wskazuj im typowe sposoby ataków** poprzez maile, strony internetowe oraz **zachęć ich do zgłaszania wszelkiego nietypowego działania** komputerów czy telefonów, np. zawieszania, awarii czy spowolnienia,
- **nawiąż kontakt i ustal sposoby komunikacji z organami ścigania i cyberbezpieczeństwa na wypadek incydentu przed jego wystąpieniem.**

NASK

NASK

Dziękuję

zbsc@nask.pl

nask.pl