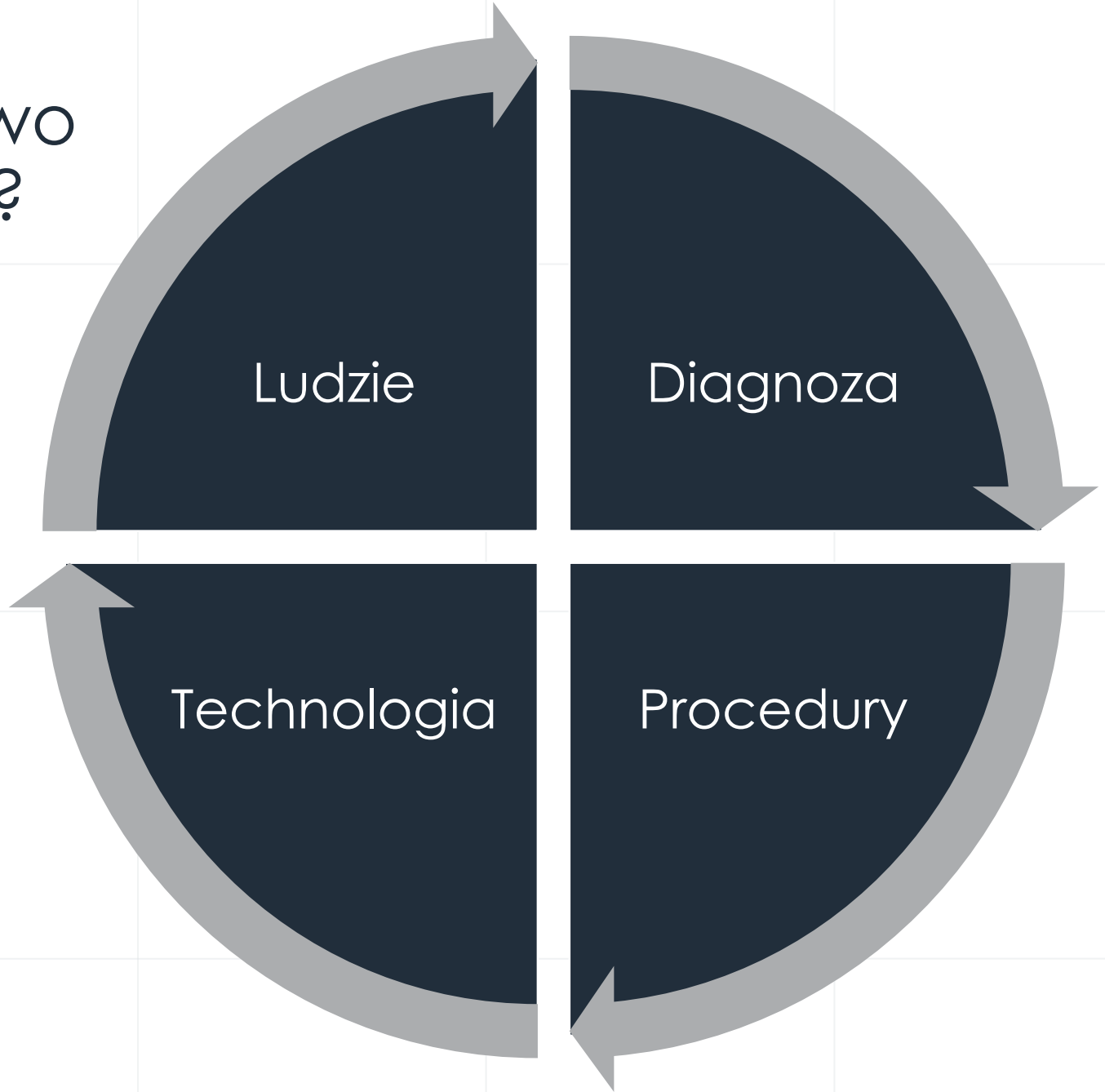
NASK

4 kroki do zbudowania podstaw cyberbezpieczeństwa w JST

Zuzanna Polak

nask.pl

Jak zadbać o cyberbezpieczeństwo w 4 prostych krokach?



NASK

Diagnoza sytuacji

Diagnoza sytuacji

- Brak systemowego podejścia do zapewnienia bezpieczeństwa informacji
- Brak analiz ryzyka i nieprowadzenie audytów bezpieczeństwa informacji
- Nieprzestrzeganie ustanowionych wymogów w zakresie bezpieczeństwa informacji
- Brak poprawy w zapewnieniu bezpieczeństwa informacji w urzędach j.s.t.

Wyniki kontroli NIK opublikowane w 2019 r.

-

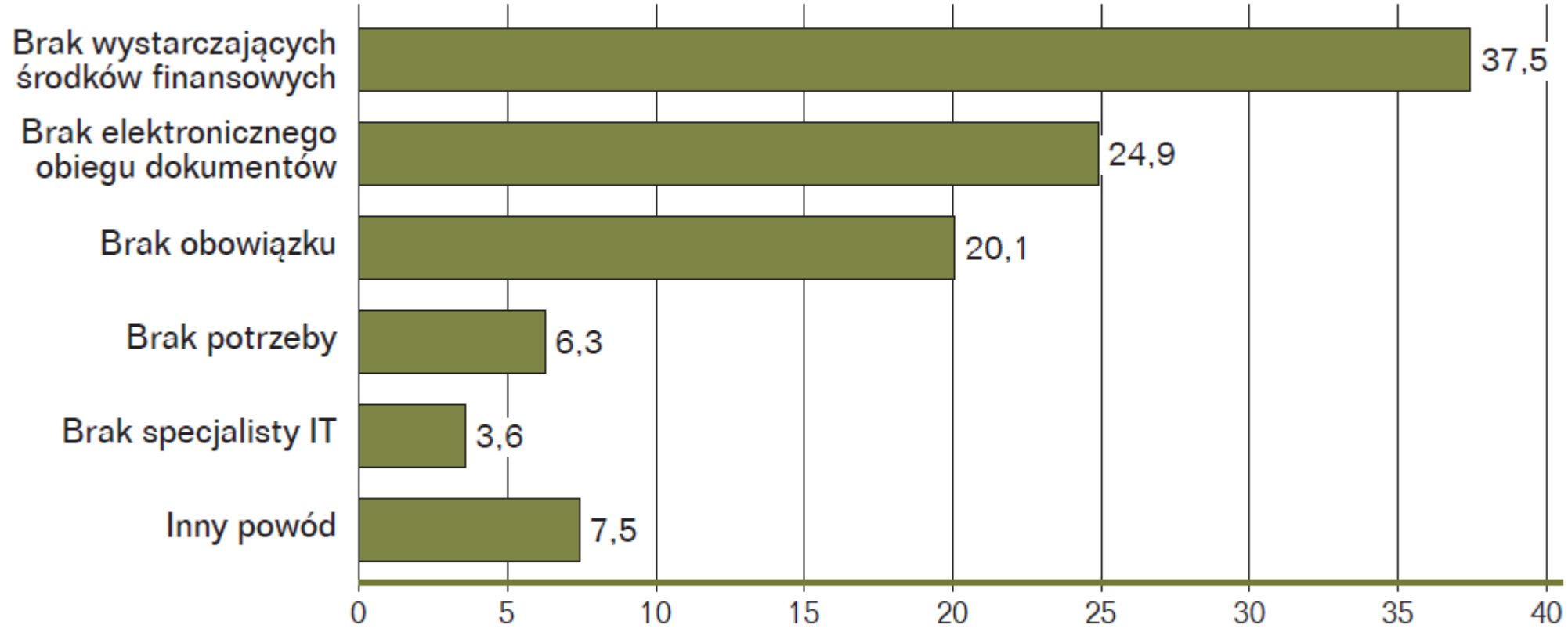
Diagnoza sytuacji

- 2477 gmin w Polsce. Według stanu na dzień badania były to: 1532 gminy wiejskie, 643 miejsko-wiejskie oraz 302 miejskie, w tym 66 będących miastami na prawach powiatu.
- Wdrożenie systemu zarządzania bezpieczeństwem informacji: **76,9% gmin.**
- **66% gmin** identyfikuje cyberprzestępczość jako duże lub bardzo duże zagrożenie dla urzędu
- Tylko w **połowie gmin** uczestniczących w badaniu przeprowadzane są szkolenia urzędników z zakresu cyberbezpieczeństwa, w 9% przeszkolono tylko kadrę kierowniczą

NASK

ANETA CHODAKOWSKA, SŁAWOMIRA KAŃDUŁA, JOANNA PRZYBYLSKA: Jak polskie gminy radzą sobie z cyberbezpieczeństwem – wyniki badań własnych. Kontrola Państwowa, 1/2022.

Rysunek 3. Przyczyny niewdrożenia w gminie systemu zarządzania bezpieczeństwem informacji (odsetek odpowiedzi, N=413)



Źródło: Opracowanie na podstawie badań własnych.

ANETA CHODAKOWSKA, SŁAWOMIRA KAŃDUŁA, JOANNA PRZYBYLSKA: Jak polskie gminy radzą sobie z cyberbezpieczeństwem – wyniki badań własnych. Kontrola Państwowa, 1/2022.

Diagnoza sytuacji

Projekt Cyfrowa Gmina – wyniki badań cząstkowych (n=1500)

- Zapewnia zarządzanie incydentem: **59%** (art. 22 pkt. 1)
- Zgłaszanie incydentu: 50% z oceną „2", **22% z oceną „0"** (art. 22 pkt. 2)
- Zapewnia obsługę incydentu: **58%** (art. 22 pkt. 3)
- Zapewnia (*mieszkańcom*) dostęp do wiedzy pozwalającej na zrozumienie zagrożeń cyberbezpieczeństwa **45% nie zapewnia!** (art. 22 pkt. 4):
- Przekazywanie danych osoby wyznaczonej do kontaktu KSC: **80%** (art. 21 i 22 pkt. 5)

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
Wypełnienie obowiązku wynikającego z art 9 ust 1 ustawy o KSC

Podmiot publiczny
Wypełnienie obowiązku wynikającego z art 22 ust 1 pkt 5 ustawy o KSC

Inny podmiot
Dobrowolne zgłoszenie niezobowiązanego podmiotu

Procedury, standardy, normy

NASK

Procedury: Ramy prawne

Wymagania minimalne dla systemów teleinformatycznych podmiotów publicznych określone są w tzw**. Krajowych Ramach Interoperacyjności**.

- Rozporządzenie Rady Ministrów z dnia 12 kwietnia 2012 r. w sprawie Krajowych Ram Interoperacyjności, minimalnych wymagań dla rejestrów publicznych i wymiany informacji w postaci elektronicznej oraz minimalnych wymagań dla systemów teleinformatycznych (tj. Dz.U.2017.0.2247)

KRI

- Rozwiązania na poziomie organizacyjnym, semantycznym i technologicznym

- dobór środków, metod i standardów wykorzystywanych w systemach teleinformatycznych
- dobór norm, standardów i rekomendacji na wszystkich poziomach interoperacyjności
- zachowanie zasady neutralności technologicznej

- Podsumowując: standaryzacja, informowanie, efektywność kosztowa.

- Powinny je stosować wszystkie **podmioty realizujące zadania publiczne z użyciem systemów teleinformatycznych**

KRI

1) dokumentacja – SZBI inne regulacje wewnętrzne – ważna aktualizacja!

2) inwentaryzacja systemów IT – sprzęt, oprogramowanie i inne aktywa, np. pomieszczenia)

3) analizy ryzyka;

4) uprawnienia personelu;

5) szkolenia;

6) ochrona i zabezpieczenie informacji;

7) praca mobilna/praca zdalna (!);

8) umowy;

9) odpowiedni poziom bezpieczeństwa w systemach teleinformatycznych;

10) reagowanie na incydenty;

11) audyt.

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

Zgłaszanie incydentu

NASK

Zgłoszenie incydentu

Incydent powinien zostać zgłoszony **niezwłocznie, nie później niż w ciągu 24 godzin** od momentu wykrycia do właściwego CSIRT. https://incydent.cert.pl

Poszczególne zespoły CSIRT mają prawo przetwarzać dane osobowe, w tym także tajemnice prawnie chronione, które są niezbędne do obsługi incydentów i zagrożeń cyberbezpieczeństwa.

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 i stosowanie skutecznych sposobów zabezpieczania się przed tymi zagrożeniami.

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

KOMUNIKATY

Incydent cyberbezpieczeństwa

Urząd Marszałkowski Województwa Mazowieckiego w Warszawie przy ul. Jagiellońskiej 26 (dalej UMWM) informuje o incydencie cyberbezpieczeństwa w infrastrukturze Węzła Regionalnego.

W jego ramach funkcjonują systemy informatyczne wykorzystywane przez partnerów projektów, realizowanych przez urząd („Rozwój elektronicznej administracji w samorządach województwa mazowieckiego wspomagającej niwelowanie dwudzielności potencjału województwa", „Przyspieszenie wzrostu konkurencyjności województwa mazowieckiego, przez budowanie społeczeństwa informacyjnego i gospodarki opartej na wiedzy poprzez stworzenie zintegrowanych baz wiedzy o Mazowszu", „Regionalne partnerstwo samorządów Mazowsza dla aktywizacji społeczeństwa informacyjnego w zakresie e-administracji i geoinformacji", „Informatyzacja bibliotek pedagogicznych na Mazowszu").

Incydent został stwierdzony **5 grudnia 2022 r.** i polegał na **ataku złośliwego oprogramowania** szyfrującego pliki (**Ransomware**). Zgodnie z posiadanymi informacjami

Technologia

NASK

Technologia: Kopie zapasowe

Wykonuj regularnie kopię zapasową istotnych danych

Reguła 3-2-1

- co najmniej 3 kopie istotnych danych (oryginał i 2 zapasowe)
- co najmniej 2 różne nośniki (zabezpieczenie przed awariami)
- **co najmniej jedna kopia w innej lokalizacji** (niedostępna z maszyn, których kopie przechowuje)

- **Weryfikuj regularnie wykonywane kopie**

Technologia: Architektura sieci

Zadbaj o odpowiednią architekturę sieci

- wyodrębnij odpowiednie segmenty
- **przeprowadź inwentaryzację usług sieciowych i upewnij się czy:**
  1. dana usługa rzeczywiście powinna być dostępna z poziomu internetu,
  2. oprogramowanie udostępniające usługę jest odpowiednio zaktualizowane lub czy są zaaplikowane najnowsze łatki bezpieczeństwa,
  3. zastosowana jest odpowiednia polityka haseł

- atakowane są usługi wystawione do sieci (np. RDP), błędnie skonfigurowane, w nieaktualnych wersjach
- dostęp poprzez VPN dla usług, które nie muszą być wystawione na zewnątrz

Technologia: Aktualizacje

Na bieżąco aktualizuj system operacyjny oraz oprogramowanie

- **stare wersje mają znane wszystkim podatności**

- Dodatkowe rozwiązania (do rozważenia):

- konfiguracja Access Control List (ACL) w celu zapewnienia jak najmniejszych, niezbędnych uprawnień dla użytkowników
- wyłączenie obsługi makr w oprogramowaniu biurowym
- wykorzystanie Software Restriction Policies (SRP) w celu zdefiniowania dozwolonych aplikacji, ale również zablokowania wykonania programów z lokalizacji popularnych wśród ransomware:
  1. foldery tymczasowe
  2. foldery `AppData` oraz lokalne `LocalAppData`
  3. foldery `ProgramData` oraz `UserProfile`

Technologia: oprogramowanie antywirusowe

Używaj aktualnego oprogramowania antywirusowego na serwerze poczty oraz stacjach roboczych

- **dodatkowa linia obrony, ale nie daje 100% pewności**
- zabezpiecz także każdą maszynę widoczną z internetu
- pozostaw włączone funkcje heurystyczne (wykrywanie pojedynczych atrybutów plików lub usług, które wskazują na złośliwość programu)

Zwiększone zagrożenie – stopnie alarmowe

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

https://cert.pl/hasla/

NASK

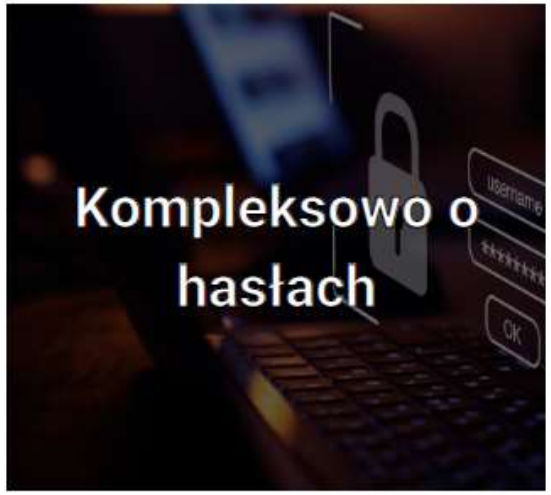
CERT.PL NASK

O nas | Aktualności | FAQ | Lista ostrzeżeń | Zagrożenia | Publikacje | Raporty roczne | Praca | Kontak

> Hasła _

W dzisiejszym świecie haseł używa każdy człowiek. Ich rola jest jednak często niedoceniana, a używane przez nas sekrety często pozostawiają wiele do życzenia. Ma to bezpośredni wpływ na nasze bezpieczeństwo w świecie wirtualnym, ale nie tylko. Utrata hasła bądź jego wykradnięcie może nieść za sobą poważne konsekwencje dla każdego. Wiele się mówi o tym, że hasła używane w różnych serwisach powinny być unikalne. Jednak na przestrzeni lat specjaliści rekomendowali metody tworzenia haseł i zarządzania nimi, które przestały być aktualne. Poniżej prezentujemy zbiór materiałów, kierowany do wielu grup odbiorców. Ich celem jest poprawa ogólnej świadomości i usystematyzowane przedstawienie współczesnych zaleceń dotyczących zarządzania hasłami.

Baza Wiedzy



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

Poradnik ransomware (2021)

NASK

https://cert.pl/uploads/docs/RAPORT_CERT_badanie-stron-oswiatowych.pdf

Raport dotyczący stanu bezpieczeństwa stron placówek oświatowych w Polsce (2020)

NASK

Strona główna
Rada Ministrów
Kancelaria Premiera
Ministerstwa
Urzędy, instytucje i placówki RP

Usługi dla obywatela
Usługi dla przedsiębiorcy
Usługi dla urzędnika
Usługi dla rolnika

Koronawirus: informacje i zalecenia
Załóż Profil zaufany
Baza wiedzy

I oś Powszechny dostęp do szybkiego Internetu
II oś E-administracja i otwarty rząd
III oś Cyfrowe kompetencje społeczeństwa
IV oś Pomoc Techniczna
V oś Rozwój cyfrowy JST - REACT EU
VI oś Pomoc Techniczna REACT-EU
Projekty realizowane w ramach POPC
Dokumenty do pobrania
Przeciwdziałanie nadużyciom
Kontrola zamówień
Kontrola projektów
Raporty ewaluacyjne
Listy kandydatów na ekspertów

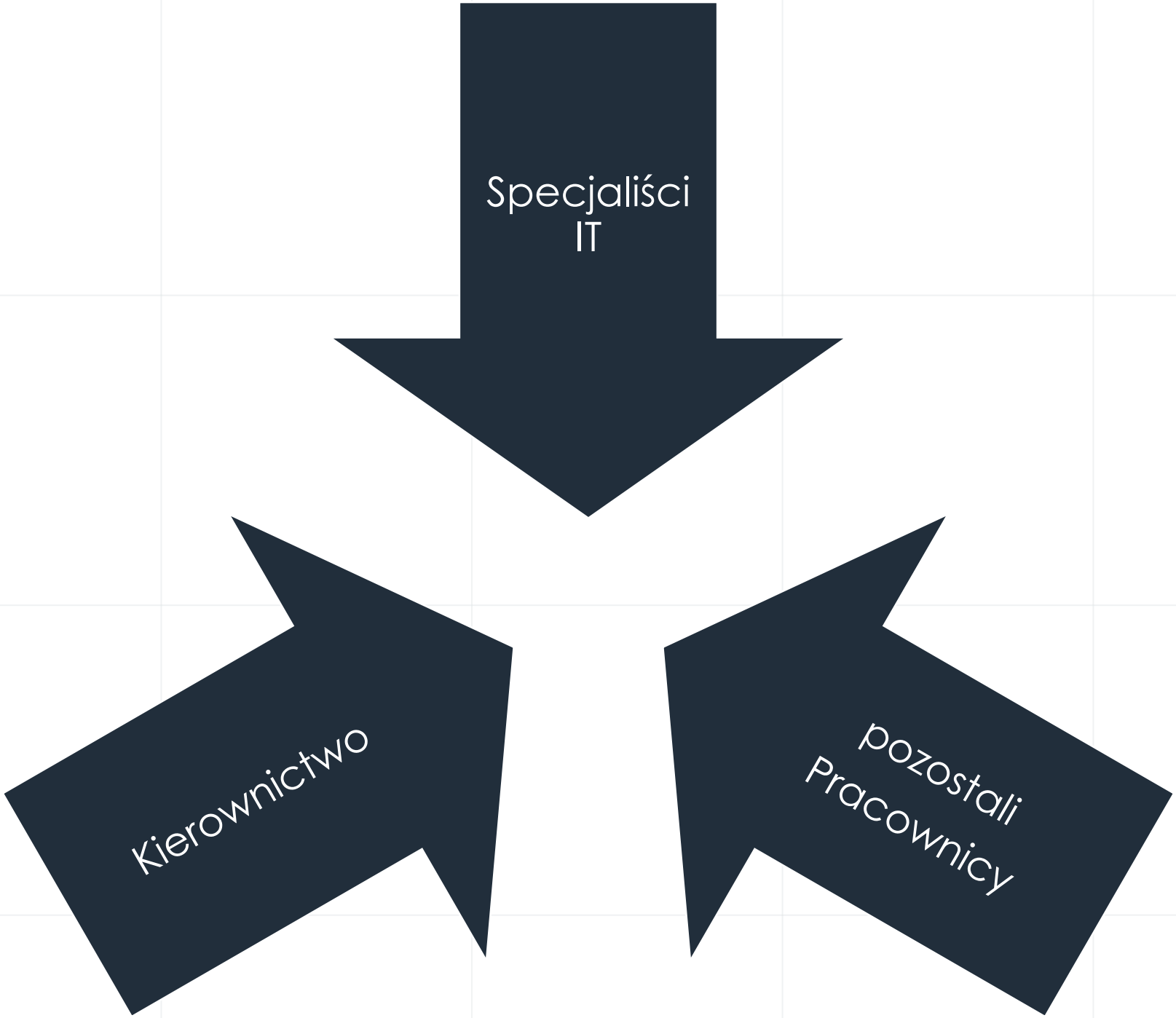
V oś Rozwój cyfrowy JST - REACT EU

> Cyfrowy Powiat
> Cyfrowa Gmina
> Granty PPGR - Wsparcie dzieci i wnuków byłych pracowników PGR w rozwoju cyfrowym

V oś. Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia - REACT-EU

Ludzie

NASK



NASK

Szkolenia – jakie?

- Szkolenia wstępne – podstawowe zagadnienia, polityki i procedury firmowe (lista), zgłaszanie incydentów
- Szkolenia przypominające – uzupełnienie i utrwalenie wiedzy, aktualne trendy
- Warsztaty – element dodatkowy szkoleń
- Szkolenia specjalistyczne – dla wybranych grup zawodowych
- Kursy online – intranet, internet, usługi komercyjne

Najważniejsze tematy: phishing i socjotechnika

Zespoły CSIRT

C:[SIRT/MON

- CSIRT GOV: https://csirt.gov.pl
- CSIRT NASK: https://www.cert.pl
- CSIRT MON: https://csirt-mon.wp.mil.pl/pl/

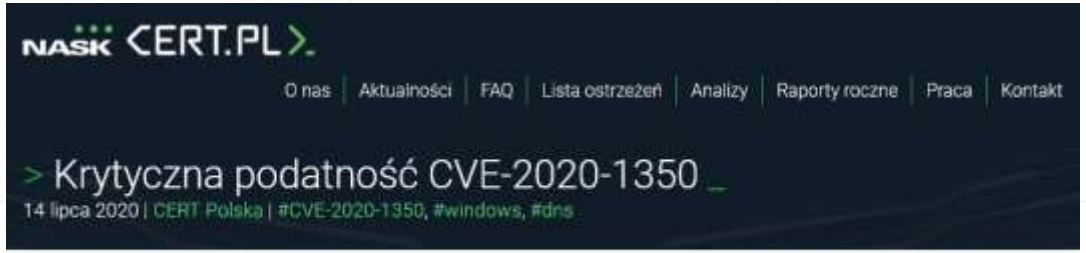
NASK
CERT.PL>_

- CSIRT KNF: https://www.knf.gov.pl/dla_rynku/CSIRT_KNF
- https://twitter.com/CSIRT_KNF

KNF CSIRT

Dbamy o bezpieczeństwo? - edukujemy siebie

- https://cert.pl/news
- https://cert.pl/zagrozenia
- https://facebook.com/CERT.Polska
- https://twitter.com/cert_polska



Zespół CERT Polska rekomenduje administratorom systemów Windows Server, w każdej jego wersji, niezwłocznie zaaplikować poprawkę naprawiającą krytyczną podatność CVE-2020-1350 (CVSS 10/10).

Podatność

Podatność w usłudze DNS systemów Windows Server polega na błędnym mechanizmie parsowania odpowiedzi z rekordami DNS. Odpowiednio spreparowany rekord DNS może spowodować nadpisanie pamięci procesu z usługą DNS.

Windows Server

Skutki

Pomyślne wykorzystanie podatności pozwala atakującemu na wykonanie kodu w systemie z uprawnieniami użytkownika *Local System*. Powoduje to, że atakujący łatwo może uzyskać kontrolę nad całym systemem. Często ten sam serwer jest również kontrolerem domeny, co będzie wiązać się z uzyskaniem przez atakującego praw administratora domeny.

W momencie wydania tego zalecenia nie jest znany publicznie dostępny exploit wykorzystujący tę podatność, jednak należy spodziewać się, że może się on pojawić już nawet w ciągu kilkunastu następnych godzin lub kilku dni. Potencjalny exploit, jak zaznacza sama firma Microsoft, może mieć charakter samorozprzestrzeniającego się robaka.

Wektor ataku

Do przeprowadzenia ataku wystarczy, aby podatny serwer spróbował rozwiązać nazwę domenową z

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

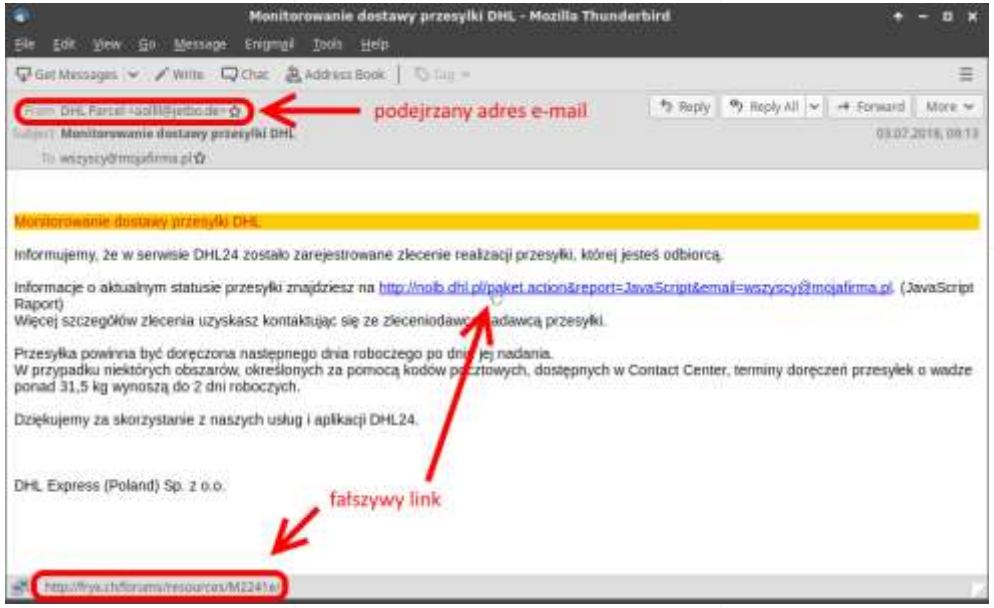
Ograniczenie skutków ataków typu ransomware (Sierpień 2020 r.)

Jak zapobiegać atakom typu ransomware? – Poradnik PRCyber-03

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

Materiały szkoleniowe - quizy

- https://phishingquiz.withgoogle.com/
- https://quiz.securityinside.pl/
- https://phishingstop.aliorbank.pl/
- https://www.credit-agricole.pl/quiz/



NASK

Dziękuję

Zuzanna.polak@nask.pl

nask.pl