NASK

Krajobraz cyberbezpieczeństwa z perspektywy CSIRT NASK

Krzysztof Silicki
Zastępca Dyrektora NASK PIB
Dyrektor ds. Cyberbezpieczeństwa i Innowacji

Konferencja Miasta w Internecie
23 czerwca 2023 r.

Agenda

- Wprowadzenie: kilka słów o CSIRT NASK oraz o obowiązkach podmiotów publicznych (uKSC)
- Statystyki CSIRT NASK, trendy, najczęstsze zagrożenia
- Badania bezpieczeństwa stron informacyjnych gmin, placówek oświatowych
- Cyfrowa Gmina a cyberbezpieczeństwo
- Budowanie świadomości cyberzagrożeń

Kilka słów o CSIRT NASK

- **CSIRT NASK jest elementem krajowego systemu cyberbezpieczeństwa** (ustawa z dnia 5 lipca 2018r. o KSC)

  Krajowy system cyberbezpieczeństwa obejmuje:
  operatorów usług kluczowych, dostawców usług cyfrowych, CSIRT MON, **CSIRT NASK**, CSIRT GOV, sektorowe zespoły cyberbezpieczeństwa, **jednostki sektora finansów publicznych**, o których mowa w art. 9 pkt 1–6, 8, 9, 11 i 12 ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych, […] (**art. 4**)

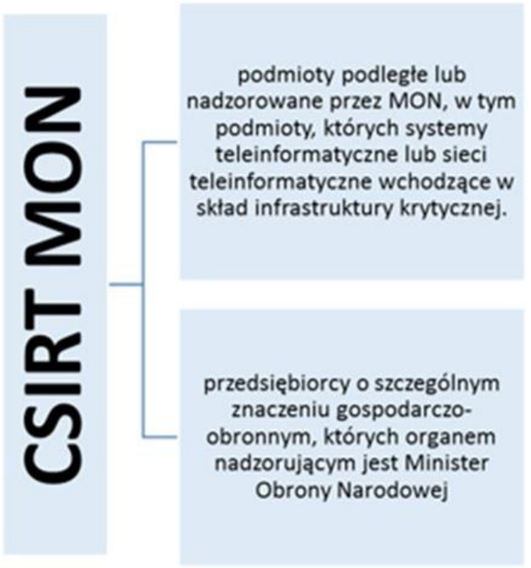
  CSIRT NASK – Zespół Reagowania na Incydenty Bezpieczeństwa Komputerowego działający na poziomie krajowym, prowadzony przez Naukową i Akademicką Sieć Komputerową – Państwowy Instytut Badawczy (**art. 2 ust. 3**)

Parę słów o CSIRT NASK

- **Zadania CSIRT NASK (główne)**
  (ustawa z dnia 5 lipca 2018r. o KSC)
  - ✓ Monitorowanie zagrożeń cyberbezpieczeństwa i incydentów na poziomie krajowym
  - ✓ Szacowanie ryzyka związanego z ujawnionym zagrożeniem cyberbezpieczeństwa (…)
  - ✓ Przekazywanie informacji dotyczących incydentów i ryzyk podmiotom krajowego systemu cyberbezpieczeństwa
  - ✓ Wydawanie komunikatów o zidentyfikowanych zagrożeniach cyberbezpieczeństwa
  - ✓ Reagowanie na zgłoszone incydenty
  - ✓ Koordynacja zgłoszonych incydentów

Parę słów o CSIRT NASK

- **Obszar odpowiedzialności CSIRT NASK**
  (ustawa z dnia 5 lipca 2018r. o KSC)



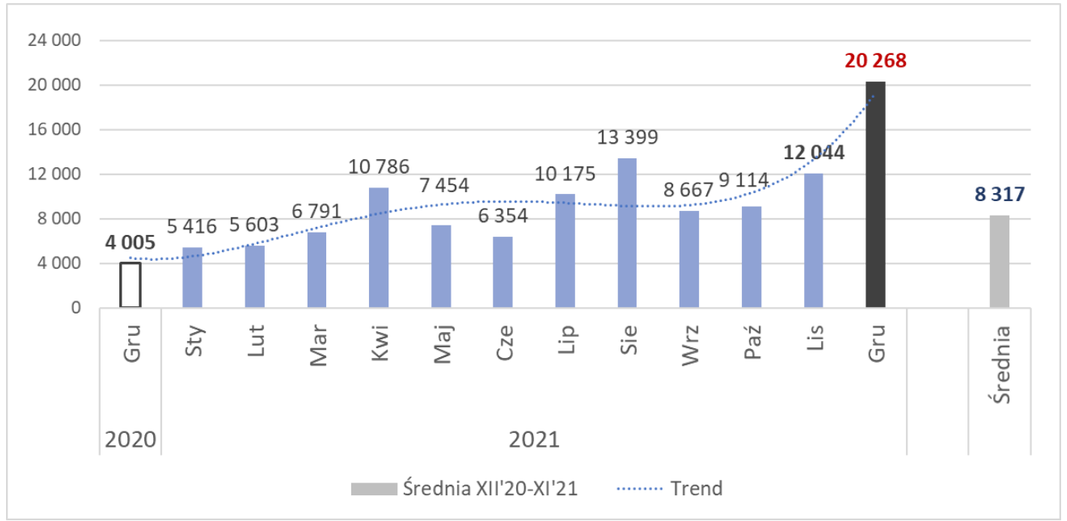
Kilka słów o obowiązkach podmiotów publicznych (uKSC)

Podmiot publiczny realizujący zadanie publiczne zależne od systemu informacyjnego:

- **wyznacza osobę odpowiedzialną za utrzymywanie kontaktów** z podmiotami krajowego systemu cyberbezpieczeństwa (rekomendacje: https://incydent.cert.pl/osoba-kontaktowa/rekomendacje)
- **zapewnia zarządzanie incydentem** w podmiocie publicznym;
- **zgłasza incydent** niezwłocznie, nie później niż w ciągu 24 godzin od momentu wykrycia, do właściwego CSIRT (poradnik: https://www.gov.pl/attachment/4f2ace9b-5bc8-4d49-accb-8205a49c1c9c)
- zgłoszenie przekazywane jest w postaci elektronicznej, a w przypadku braku możliwości przekazania w postaci elektronicznej, przy użyciu innych dostępnych środków komunikacji
- **zapewnia obsługę incydentu** w podmiocie publicznym i incydentu krytycznego we współpracy z właściwym CSIRT, przekazując niezbędne dane, w tym dane osobowe.

Statystyki CSIRT NASK

Liczba zagrożeń cyberbezpieczeństwa	2020	2021	Zmiana w stosunku do 2020 r.
Zarejestrowane zgłoszenia	34 555	116 071	236%
w tym obsłużone incydenty	10 420	29 483	183%



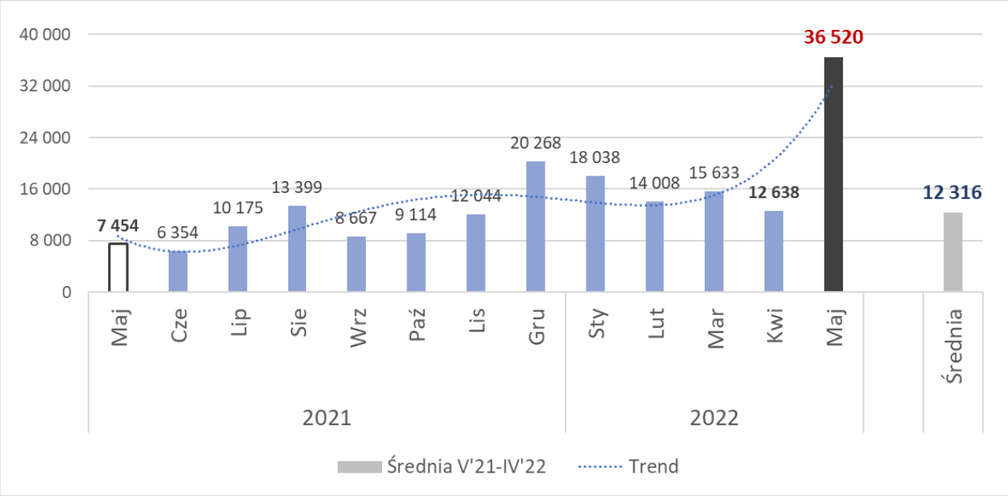
Liczba zarejestrowanych zgłoszeń od 01.12.2020 do 31.12.2021.

NASK

Incydenty zgłaszane obowiązkowo z ustawy od I do XII 2021

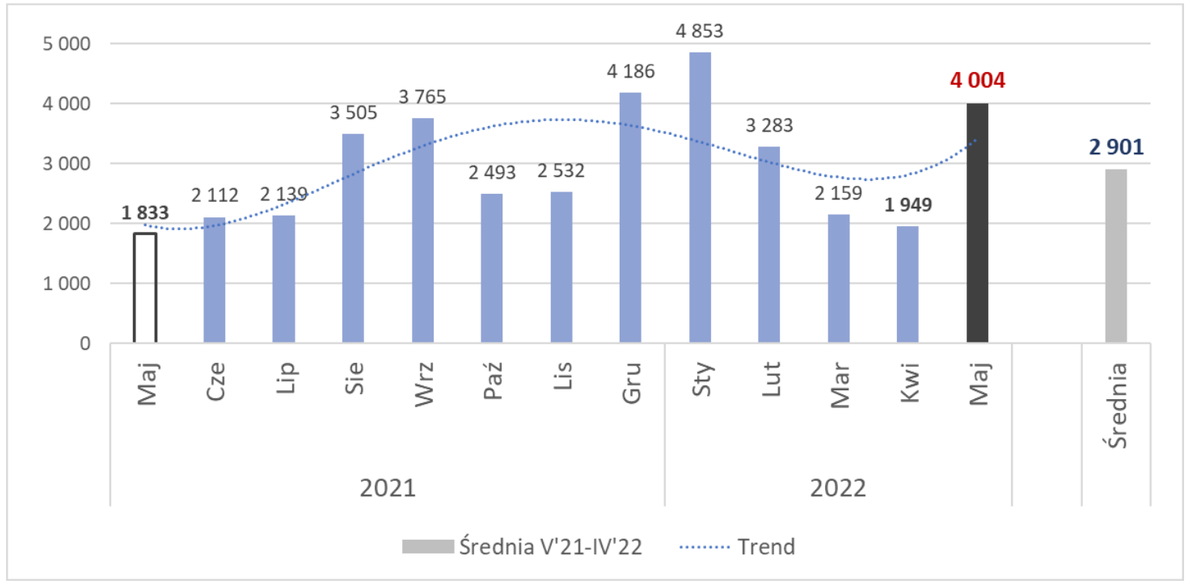
Rodzaj incydentu	2021												
	I	II	III	IV	V	VI	VII	VIII	IX	X	XI	XII	Razem
Incydenty poważne	2	2	2	1	3	3	1	1	11	5	4	1	36
Incydenty istotne	0	0	0	0	0	0	0	0	0	0	0	0	0
Incydenty w podmiotach publicznych	24	56	59	66	51	31	38	43	37	45	26	36	512

Statystyki i trendy

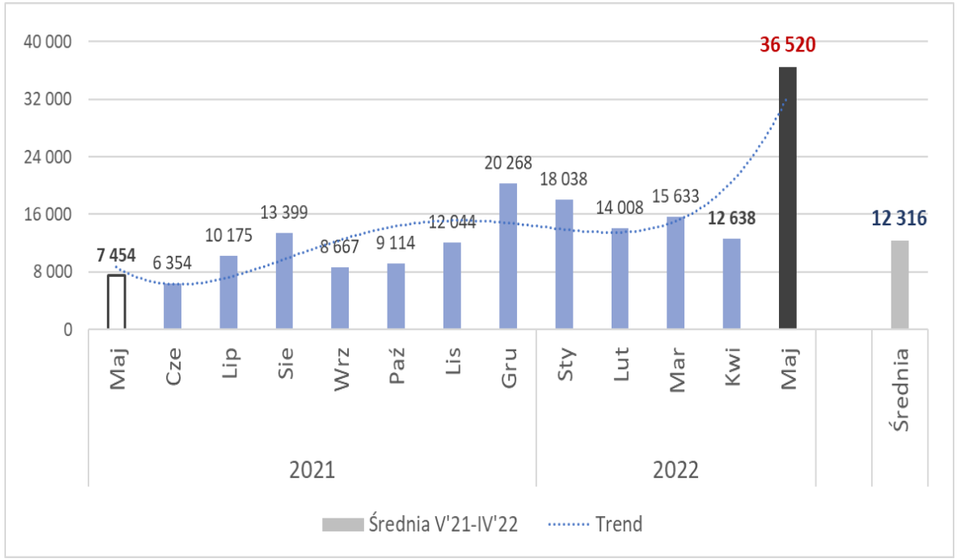


Rośnie także liczba incydentów co jest efektem wprowadzania nowych metod i technik przez atakujących.

Systematycznie rosnąca liczba zgłoszeń jest odzwierciedleniem rosnącej świadomości podmiotów i użytkowników indywidualnych.

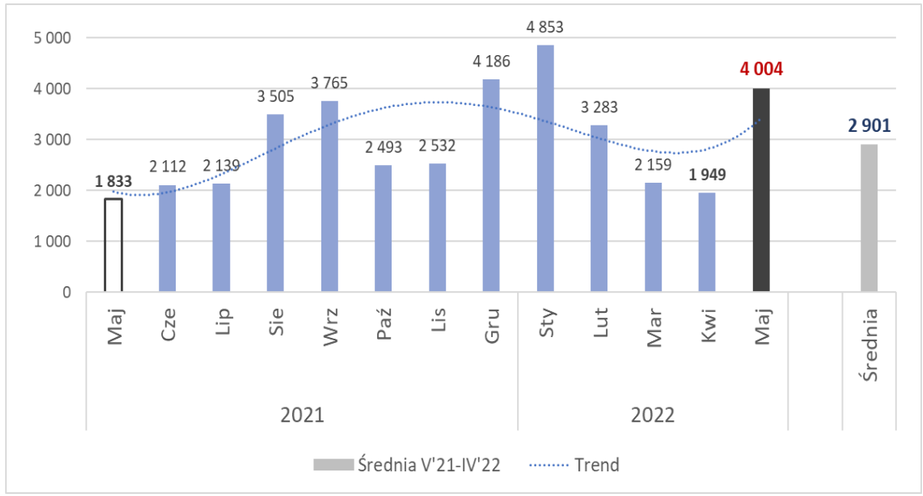


Statystyki i trendy



Wykres: Liczba zarejestrowanych zgłoszeń od 01.05.2021 do 31.05.2022.

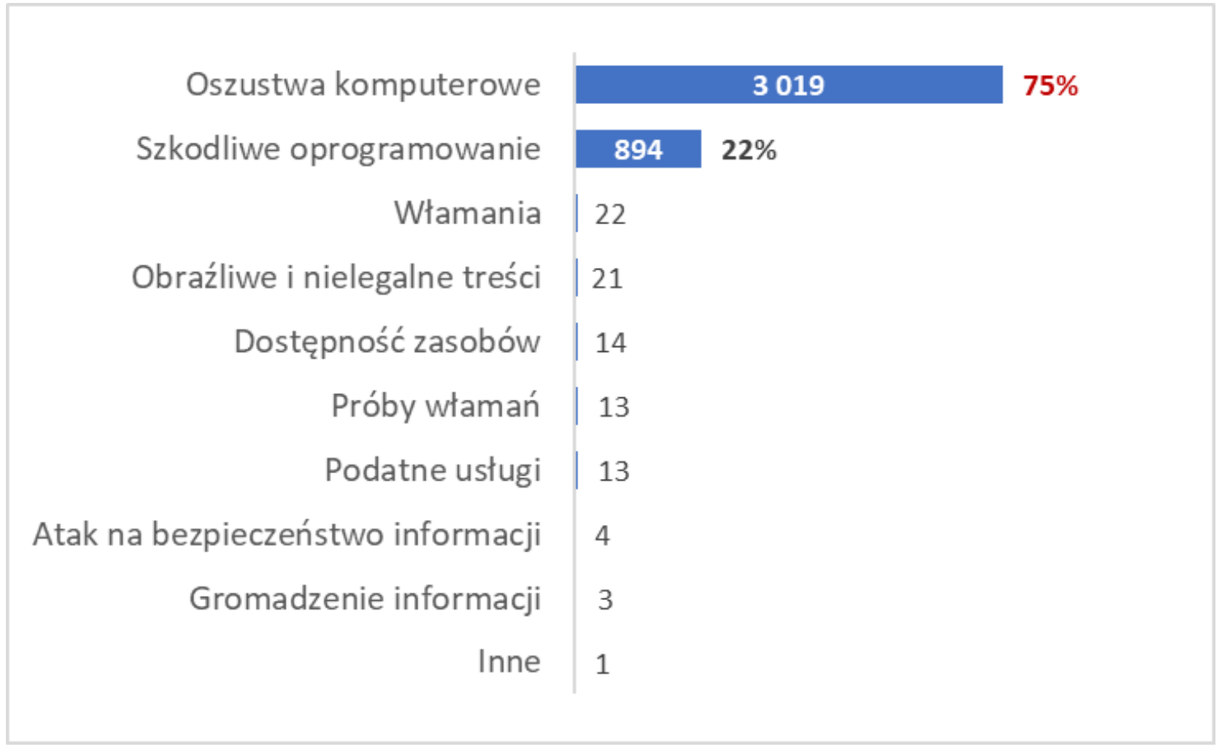
Systematycznie rosnąca liczba zgłoszeń jest odzwierciedleniem rosnącej świadomości podmiotów i użytkowników indywidualnych.



Wykres: Liczba zarejestrowanych incydentów od 01.05.2021 do 31.05.2022.

Rośnie także liczba incydentów co jest efektem wprowadzania nowych metod i technik przez atakujących.

Statystyki i trendy (maj 2022)



Wykres: Liczba zarejestrowanych incydentów wg rodzaju od 1 do 31 maja 2022 r.

- **Oszustwa komputerowe**: rozpowszechnione próby wyłudzania poufnych danych, np. loginu i hasła do poczty, strony banku, portalu społecznościowego czy innej usług online (ang. phishing)
- **Szkodliwe oprogramowanie** (w tym ransomware) jest szczególnie dotkliwe dla firm i instytucji
- **Ataki na dostępność zasobów** są jednymi z najprostszych, ale przy tym mają duże odziaływanie na wizerunek

NASK

Bezpieczeństwo stron informacyjnych gmin (Przebadano 2806 stron internetowych)

- 2,3% domen zarejestrowanych na osoby fizyczne
- W 210 przypadkach dane w rejestrze nie wskazywały w żaden sposób na JST
- Tylko w przypadku 38% domen w rejestrze znajdował się nr telefonu ułatwiający kontakt
- 95,2% stron miała ustawiony certyfikat SSL
  - ale 41,8% było wystawionych na inną nazwę domenową
  - a w 11,3% przypadków certyfikat był wygasły
  - ponadto 62,6% nie miało przekierowania z transmisji nieszyfrowanej na szyfrowaną

- Zostało znalezionych 1993 podatności
- Znaleziono 120 plików logów, prywatne repozytorium git, 10 plików konfiguracyjnych zawierających hasła lub skróty haseł do panelu administracyjnego lub bazy danych
- Innych informacji nie możemy ujawnić

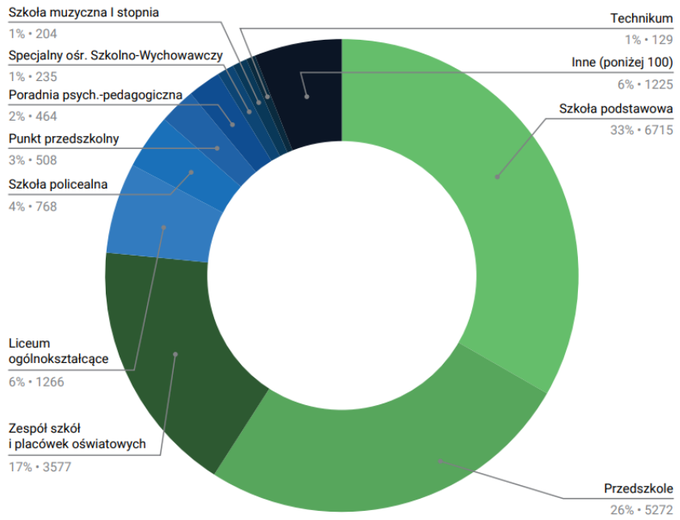
- 4 zgłoszenia typu abuse
- tylko 4/10 incydentów zgłoszonych do instytucji było naprawianych w rozsądnym czasie

Na podstawie badania CSIRT NASK z lutego 2020 roku.

Bezpieczeństwo stron informacyjnych placówek oświatowych

- 11,7% domen zarejestrowanych na osoby fizyczne
- 47,1% kontaktowych adresów email było z usług darmowych
- Znaleziono 5175 podatności na 2873 stronach z systemem Joomla
- Znalezion 9210 podatności na 6602 stronach z systemem Wordpress
- W pojedynczych przypadkach natrafiono także na kopie zapasowe czy logi
- 94% stron miały jakiś certyfikat SSL, ale 50,1% było dla złych domen, 5,1% wygasłych, a 11,5% nie było podpisanych przez zaufane centrum

Rys. 1. Rozkład typów placówek oświatowych poddanych badaniu



Na podstawie badania CSIRT NASK z sierpnia 2020 roku.
Przebadano: **22.354 strony**
Pełny raport dostępny na: https://www.cert.pl/publikacje/

Projekt Cyfrowa Gmina

- **Konkurs Grantowy Cyfrowa Gmina** realizowany dzięki Funduszom Europejskim - REACT-EU (Działanie 5.1 Rozwój cyfrowy JST oraz wzmocnienie cyfrowej odporności na zagrożenia).

- **Instytucja Pośrednicząca:** Centrum Projektów Polska Cyfrowa
- **Operator konkursu grantowego:** Politechnika Łódzka

- **Cel:**
  Wsparcie rozwoju cyfrowego instytucji samorządowych oraz zwiększenie cyberbezpieczeństwa.

- **Dofinansowanie na:**
  Cyfryzację urzędów JST
  Zakup sprzętu IT dla szkół i placówek specjalnych
  Edukację cyfrową JST
  Cyberbezpieczeństwo -> obligatoryjna Diagnoza Cyberbezpieczeństwa JST

- **Dla kogo:**
  Gminy w Polsce (miejskie, miejsko-wiejskie, wiejskie)

Program Cyfrowa Gmina

- **Harmonogram konkursu:**
  I runda: 18.10 - 17.11.2021
  II runda: 22.11 - 22.12.2021
  III runda: 11.01 - 10.02.2022

- **Jak aplikować:**
  Każda gmina miała wyznaczoną dla siebie rundę do ubiegania się o dofinansowanie.
  Wnioski o przyznanie grantu należało wypełnić za pomocą Generatora Wniosków Grantowych.

- **Wyniki naboru:**
  I runda: **718**
  II runda: **1053**
  III runda: **668**

- **Okres realizacji Projektu:**
  Maksymalnie 18 miesięcy od dnia wejścia w życie Umowy, ale nie dłużej niż do 30.09.2023 r.

Program Cyfrowa Gmina

- **Diagnoza Cyberbezpieczeństwa:**
  - Powinna zostać przeprowadzona w terminie do 6 miesięcy od dnia zawarcia Umowy o powierzenie Grantu.
  - Powinna zostać przeprowadzona przez osobę posiadająca uprawnienia wykazane w Rozporządzeniu Ministra Cyfryzacji z dnia 12 października 2018 r. w sprawie wykazu certyfikatów uprawniających do przeprowadzenia audytu.
  - Wypełniony formularz diagnozy cyberbezpieczeństwa należy przesłać do NASK.

- **Analiza:**
  Na podstawie przesłanych danych będą prowadzone badania ankietowe, które pozwolą zdiagnozować kluczowe problemy w zakresie cyberbezpieczeństwa dotyczące gmin.

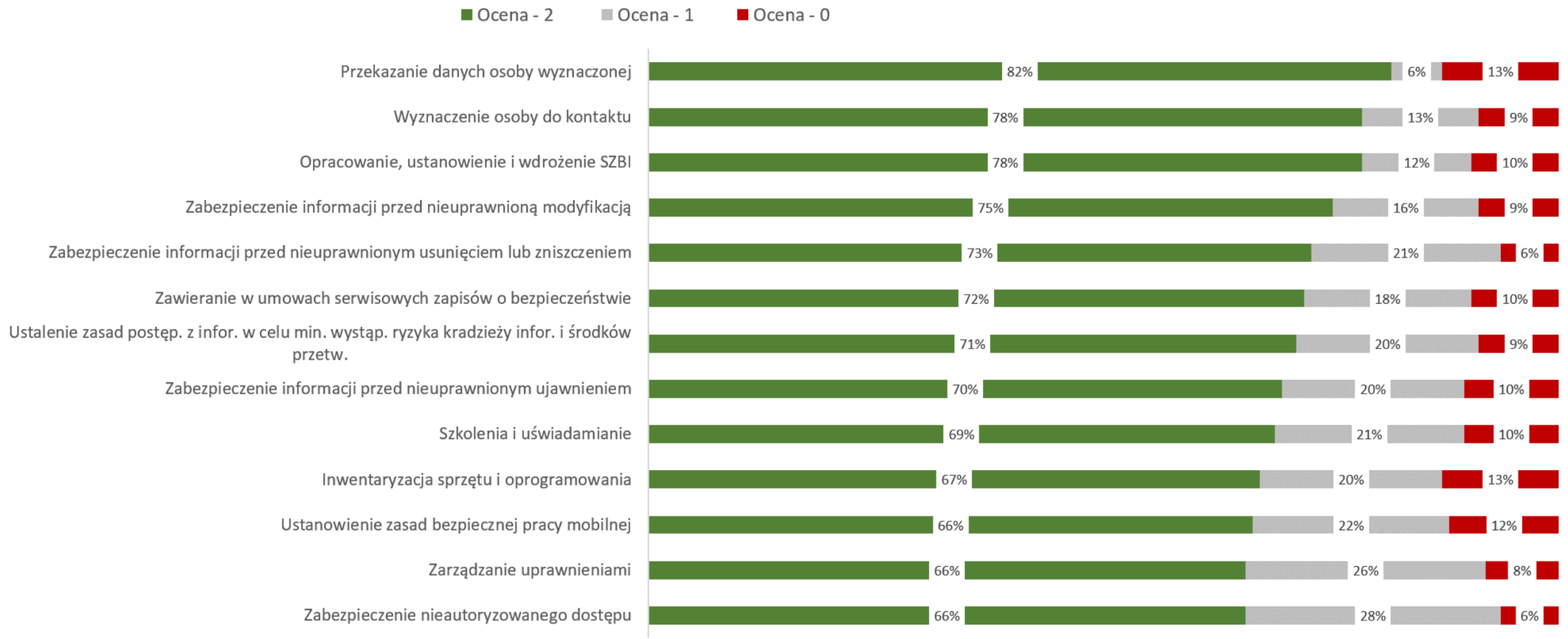
Wymiary analizy pod kątem m.in. wymagań KRI

1. Monitorowanie dostępu do informacji.
2. Zapewnienie dostępu do wiedzy.
3. **Zgłaszanie incydentu**.
4. Monitorowanie nieautoryzowanych zmian.
5. Stosowanie mechanizmów kryptograficznych w systemach.
6. Doskonalenie Systemu Zarządzania Bezpieczeństwem Informacji (SZBI).
7. Aktualizowanie regulacji wewnętrznych.
8. Ochrona systemu przed błędami.
9. Zapewnienie bezpieczeństwa plików systemowych.
10. Zapewnienie zarządzania incydentem.
11. **Postępowanie z ryzykiem.**
12. **Zarządzanie podatnościami systemów.**
13. **Zapewnienie audytu bezpieczeństwa informacji (nie rzadziej niż raz na rok).**
14. Zapewnienie obsługi incydentu.
15. Ustanowienie zasad bezpiecznej pracy mobilnej.
16. Zabezpieczenie nieautoryzowanego dostępu.
17. Minimalizowanie ryzyka utraty informacji w wyniku awarii systemu.
18. **Kontrola zgodności systemów z regulacjami.**
19. Wyznaczenie osoby do kontaktu.
20. Przekazanie danych osoby wyznaczonej.
21. Monitorowanie i przegląd Systemu Zarządzania Bezpieczeństwem Informacji (SZBI).
22. **Zarządzanie uprawnieniami.**
23. **Zabezpieczenie informacji przed nieuprawnionym ujawnieniem.**
24. Zabezpieczenie informacji przed nieuprawnioną modyfikacją.
25. Ustalenie zasad postępowania z informacjami w celu minimalizacji wystąpienia ryzyka kradzieży informacji i środków przetwarzania.
26. **Aktualizowanie oprogramowania.**
27. **Opracowanie, ustanowienie i wdrożenie Systemu Zarządzania Bezp. Informacji (SZBI).**
28. **Przeprowadzanie okresowych analiz ryzyka.**
29. Szkolenia i uświadamianie.
30. Zawieranie w umowach serwisowych zapisów o bezpieczeństwie.
31. Inwentaryzacja sprzętu i oprogramowania.

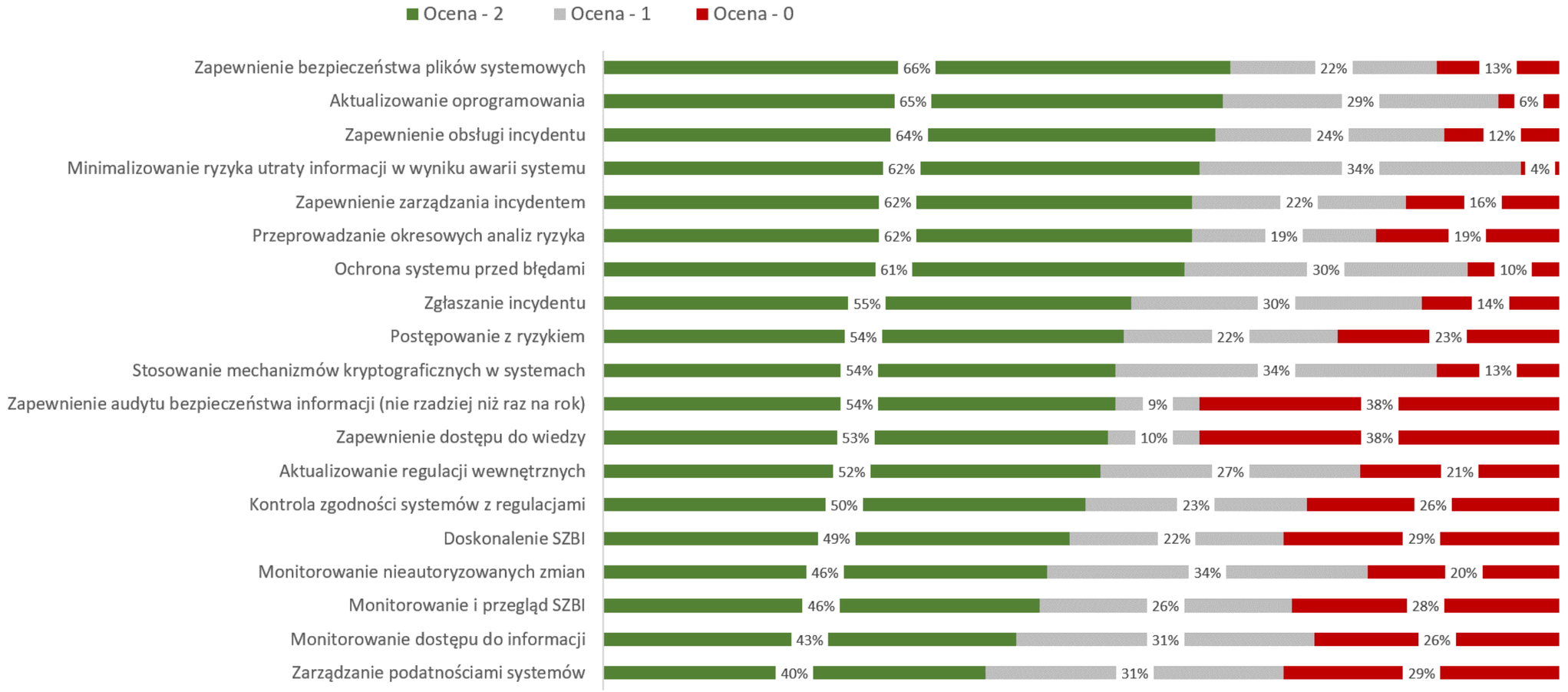
NASK

Analiza wstępna aspektów bezpieczeństwa związanych m.in. z KRI (próbka n=125)

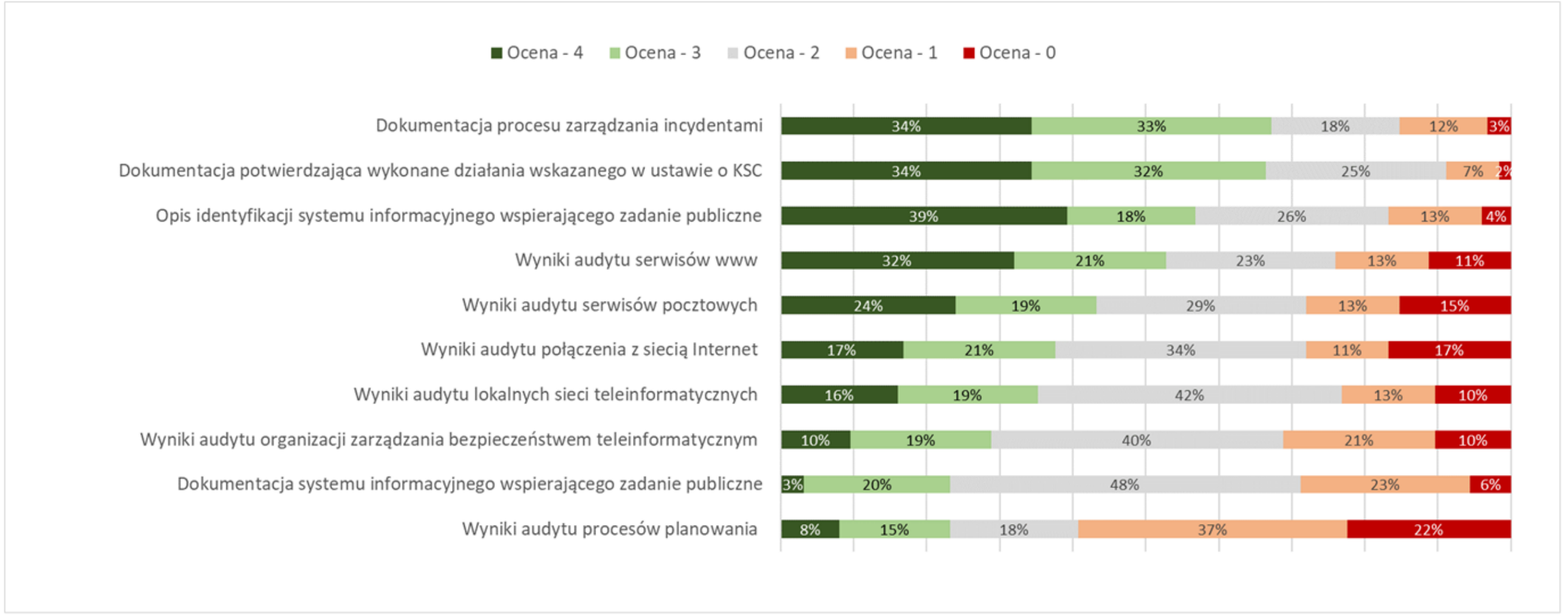
Analiza wstępna aspektów bezp. związanych m.in. z KRI GÓRNA POŁOWA



Analiza wstępna aspektów bezp. związanych m.in. z KRI DOLNA POŁOWA



Analiza wstępna aspektów bezpieczeństwa związanych min. z uKSC (próbka n=125)



Budowanie świadomości cyberzagrożeń

Szkolenia Cyber JST od 2019 roku

- Aktualne regulacje prawne z zakresu cyberbezpieczeństwa na poziomie krajowym
- Wytyczne i standardy dla JST w zakresie bezpieczeństwa teleinformatycznego
- Procedury reagowania w przypadku wystąpienia incydentów cyberbezpieczeństwa, w tym współpraca z CSIRT NASK

Szkolenia SecurV-JST zadanie zlecone z KPRM

- Pilotaż w województwie podlaskim
- Do przeprowadzenia 570 szkoleń
- Szkolenia indywidualne, prezentujące jak realne ataki w sposób praktyczny
- Wyposażanie uczestników w tokeny 2FA

Zachęcam do udziału, w przyszłym roku także inne województwa!

Program CPPC - Cyfrowa Gmina

- Ankiety w wielu formatach
- Na razie mała liczba ankiet
- Bardzo interesujące informacje statystyczne i merytoryczne do zbudowania obrazu cyberbezpieczeństwa w przyszłości

Dziękuję

Krzysztof Silicki@nask.pl

NASK