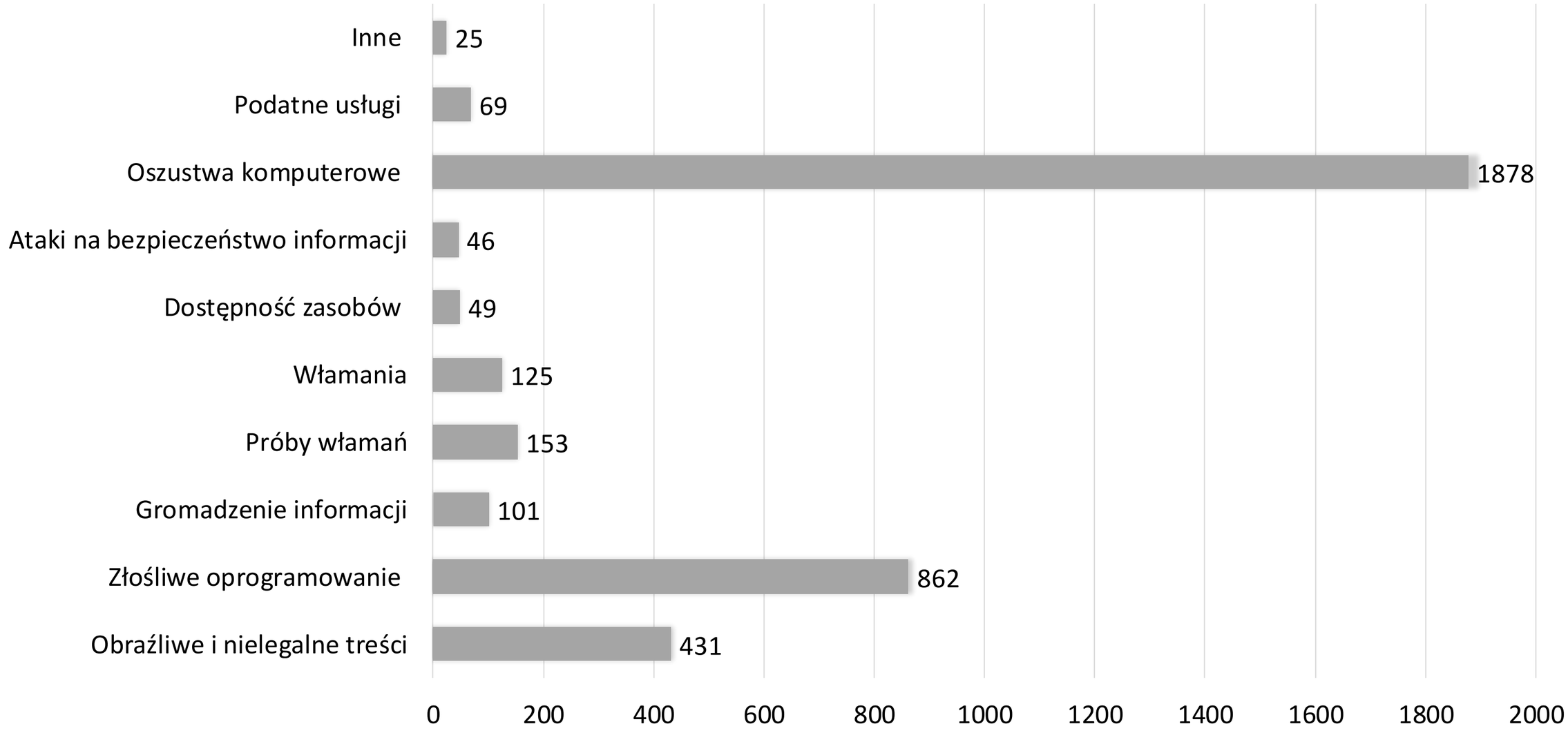
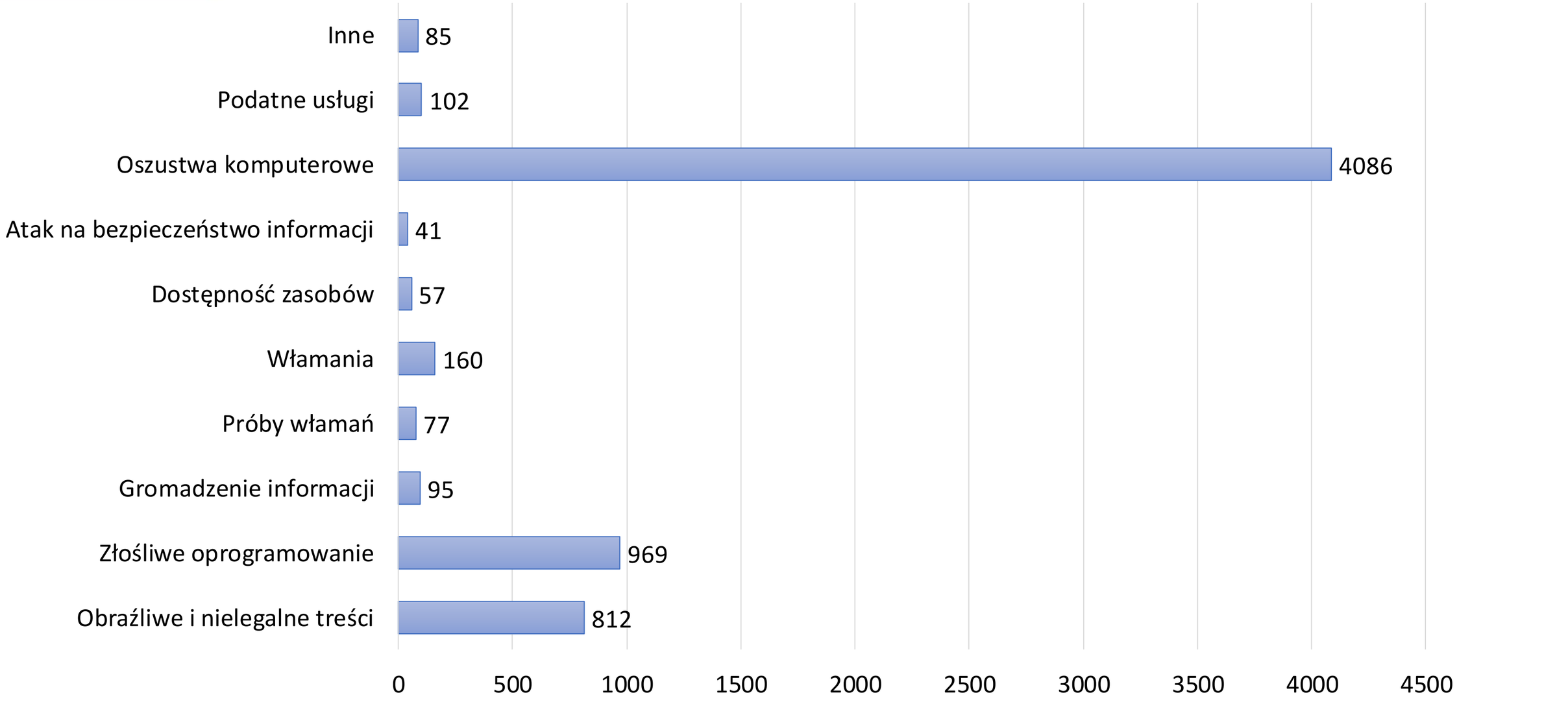
Najczęściej zgłaszane incydenty do CERT Polska w latach 2017-2020

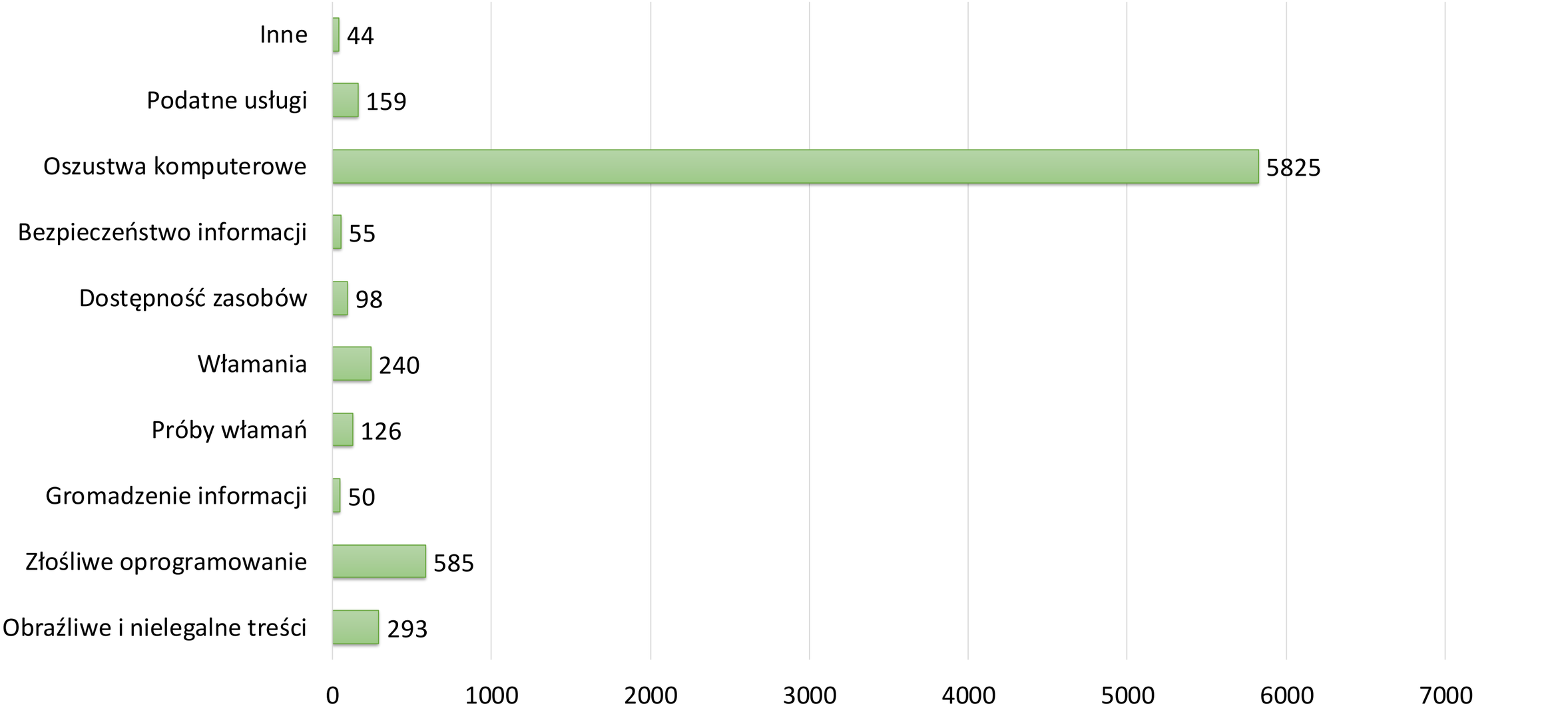
Statystyki - Incydenty w roku 2018



Statystyki - Incydenty w roku 2019



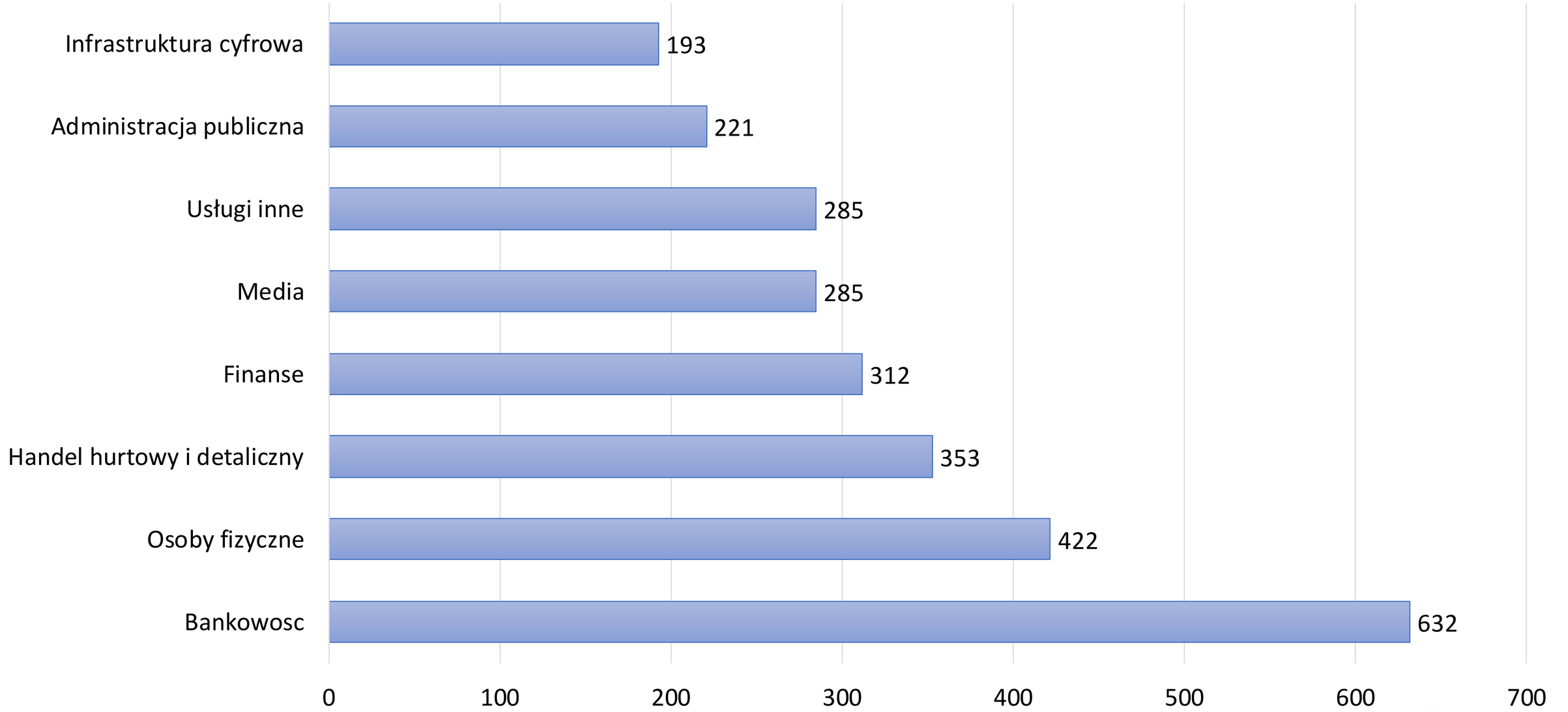
Statystyki - Incydenty w roku 2020 (stan na 30.09.2020)



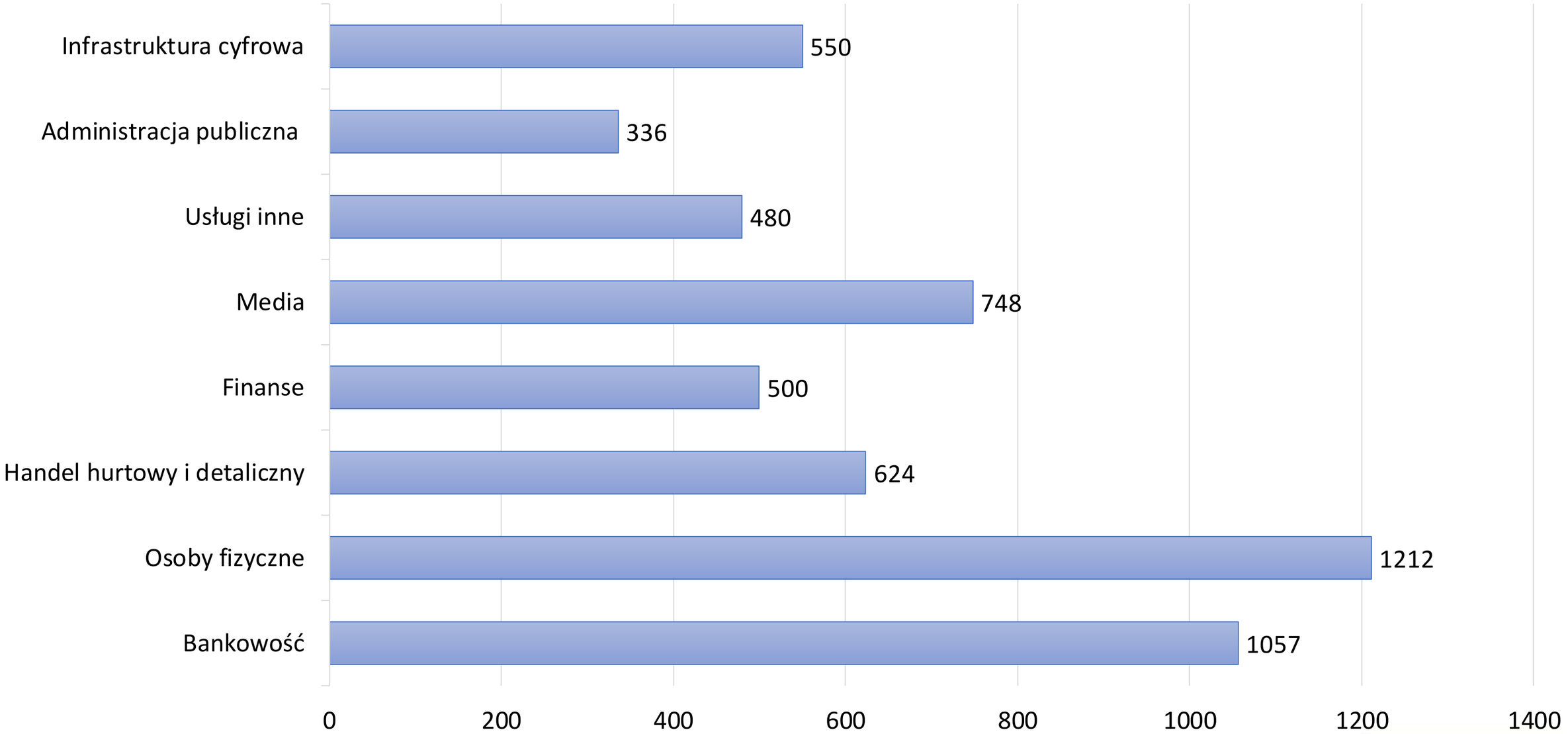
Statystyki – Liczba zarejestrowanych incydentów w latach 2017-2020

Incydent	2017	2018	2019	2020
Oszustwa komputerowe	1439	1878	4086	5825
Obraźliwe i nielegalne treści	195	431	812	293
Złośliwe oprogramowanie	854	862	969	585
Próby włamań	262	153	77	126
Inne	52	46	85	44
Gromadzenie informacji	157	101	95	50
Włamania	118	125	160	240
Dostępność zasobów	53	69	57	98
Ataki na bezpieczeństwo informacji	28	49	41	55
Podatne usługi	24	25	102	159

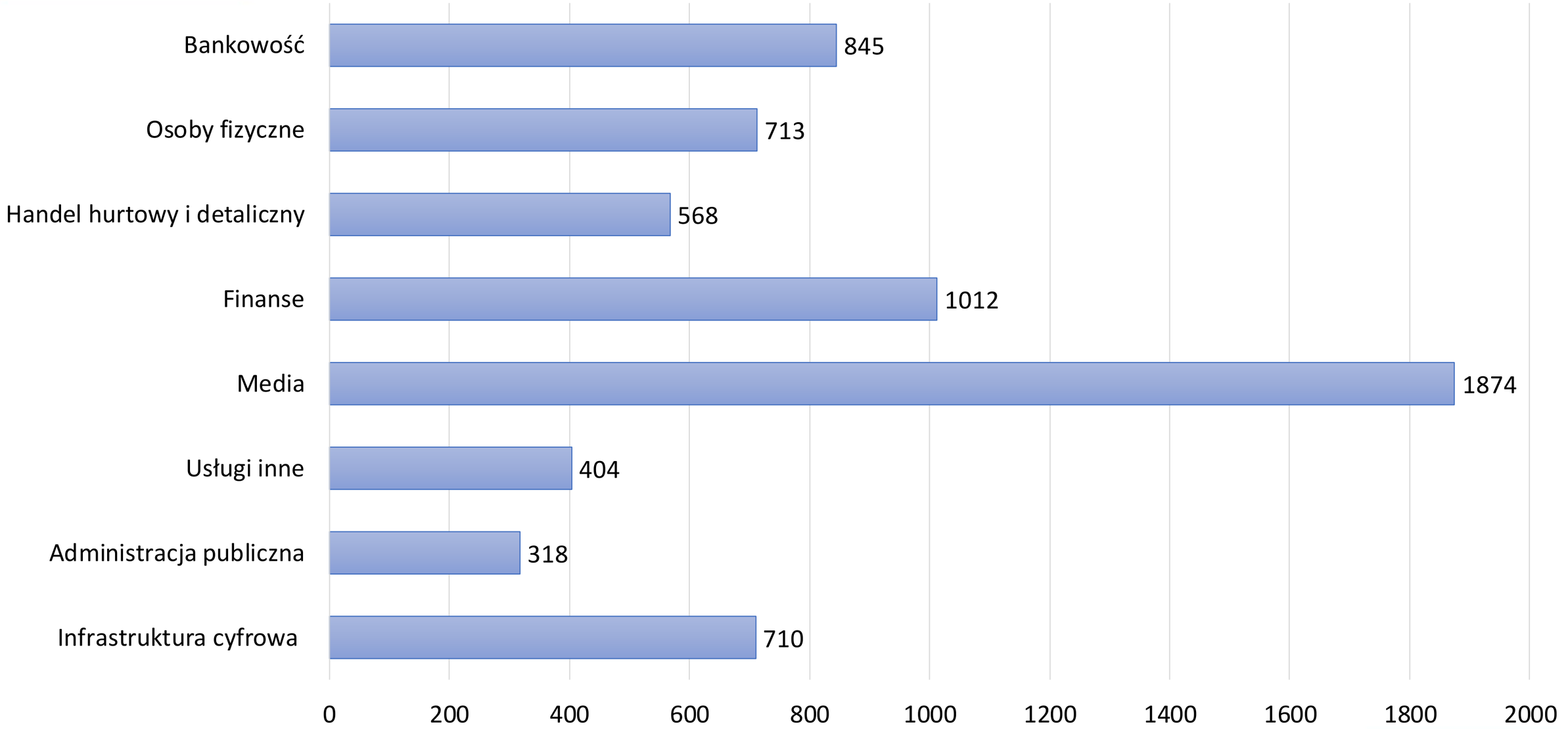
Klasyfikacja zarejestrowanych incydentów w podziale na sektory gospodarki w 2018 roku



Klasyfikacja zarejestrowanych incydentów w podziale na sektory gospodarki w 2019 roku



Klasyfikacja zarejestrowanych incydentów w podziale na sektory gospodarki w 2020 roku (stan na 30.09.2020)



Obsługa incydentów

Obsługa incydentów

Zgodnie z ustawą o krajowym systemie cyberbezpieczeństwa NASK-PIB został jest jednym z trzech CSIRTów poziomu krajowego, który koordynuje obsługę incydentów zgłaszanych przez operatorów usług kluczowych, dostawców usług cyfrowych, samorząd terytorialny. Do CSIRT NASK incydenty mogą także zgłaszać wszyscy użytkownicy.

Obsługa incydentów

Operator Usługi Kluczowej, Dostawca Usługi Cyfrowej, Podmiot publiczny bądź osoba prywatna zgłasza incydent wypełniając formularz stronie https://incydent.cert.pl/ lub wysyłając e-mail na adres cert@cert.pl. Po otrzymaniu zgłoszenia w CERT Polska następuje analiza, która ma na celu skategoryzowanie go (określenie, czy mamy do czynienia ze złośliwym oprogramowaniem, wyłudzeniem, szantażem, fałszywym sklepem...).

Obsługa incydentów

1. Otrzymanie zgłoszenia od Operatora Usługi Kluczowej, Dostawcy Usługi Cyfrowej, Podmiotu Publicznego, osoby prywatnej.
2. Po otrzymaniu zgłoszenia w CERT Polska następuje analiza, która ma na celu skategoryzowanie go.
    1. Sprawdzane jest czy zgłoszony incydent należy do znanej złośliwej kampanii bądź czy IP/domena już wcześniej zostały przeanalizowane.
    2. Jeżeli zgłoszone zagrożenie nie było do tej pory znane, informowane są inne podmioty zajmujące się cyberbezpieczeństwem, takie jak: abuse (hostingodawca), partner DNS, podmioty, które dotknął incydent.
3. W przypadku złośliwego oprogramowania (malware) dochodzi do analizy próbki.
4. W przypadku incydentu dotyczącego sklepów internetowych dochodzi do analizy zarówno technicznej jak i wizualnej.
5. W przypadku wykrycia podatności w organizacji, instytucji czy przedsiębiorstwie CERT kontaktuje się z danym podmiotem i przekazuje mu informacje o danej podatności oraz rekomendacje zmiany konfiguracji, która załata podatność.

Zgłoszenie incydentu

Zgłoszenie incydentu

Incydent powinien zostać zgłoszony 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.

Dane osobowe i tajemnice prawnie chronione

Poszczególne zespoły CSIRT mają prawo przetwarzać dane osobowe, w tym także tajemnice prawnie chronione, które są niezbędne do obsługi incydentów i zagrożeń cyberbezpieczeństwa. Ustawodawca skorzystał w tym przypadku z art. 23 RODO, umożliwiającego wyłączenie niektórych podmiotów z części przepisów rozporządzenia.

Dane osobowe i tajemnice prawnie chronione

Zgłoszenie incydentu powinno zawierać zarówno dane osobowe, a także tajemnice prawnie chronione (w tym tajemnice przedsiębiorstwa), jeżeli jest to konieczne do realizacji zadań CSIRT. W zgłoszeniu należy oznaczyć informacje, które są prawnie chronione.

Dane osobowe i tajemnice prawnie chronione

CSIRT może zwrócić się do podmiotu publicznego o uzupełnienie zgłoszenia o informacje, które stanowią tajemnice prawnie chronione.

Właściwy CSIRT, publikując informacje o incydentach nie może naruszać przepisów o ochronie danych osobowych, przepisów o ochronie informacji niejawnych oraz innych tajemnic prawnie chronionych.

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 i stosowanie skutecznych sposobów zabezpieczania się przed tymi zagrożeniami.

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

Zgłoszenie incydentu przez Podmiot Publiczny

Najszybszą formą zgłoszenia incydentu jest przesłanie zgłoszenia elektronicznego do **CISRT NASK** za pomocą formularza online na stronie https://incydent.cert.pl, który krok po kroku podpowie jakie informacje zawrzeć w zgłoszeniu.
Przed nami wyświetli się okienko jak na poniższym slajdzie.

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.

Zgłoszenie incydentu – Jaki podmiot Państwo reprezentują?

Osoba fizyczna / inne podmioty | Operator usług kluczowych | Dostawca usługi cyfrowej | Podmiot publiczny

CERT Polska | Polityka prywatności

Zgłoszenie incydentu – Jaki podmiot Państwo reprezentują?

Osoba fizyczna / inne podmioty | Operator usług kluczowych | Dostawca usługi cyfrowej | **Podmiot publiczny**

Czy reprezentowany przez Państwa podmiot publiczny jest jednocześnie operatorem usługi kluczowej?

Zgodnie z art 25 ustawy z dnia 5 lipca 2018 (Dz. U. poz. 1560) o krajowym systemie cyberbezpieczeństwa, podmioty, wobec których wydana została odpowiednia decyzja podlegają pod tryb zgłaszania przewidziany dla operatorów usług kluczowych.

Jeśli reprezentowany przez Państwa podmiot publiczny nie figuruje w wykazie operatorów usług kluczowych, prosimy o wybranie opcji "Podmiot publiczny".

Podmiot publiczny
Reprezentowany przeze mnie podmiot nie jest operatorem usługi kluczowej.

⚠ Podmiot publiczny będący operatorem usługi kluczowej
Reprezentowany przeze mnie podmiot publiczny jest równocześnie operatorem usługi kluczowej.

Czy reprezentowany przez Państwa podmiot publiczny jest jednocześnie operatorem usługi kluczowej?

Zgodnie z art 25 ustawy z dnia 5 lipca 2018 (Dz. U. poz. 1560) o krajowym systemie cyberbezpieczeństwa, podmioty, wobec których wydana została odpowiednia decyzja podlegają pod tryb zgłaszania przewidziany dla operatorów usług kluczowych.

Jeśli reprezentowany przez Państwa podmiot publiczny nie figuruje w wykazie operatorów usług kluczowych, prosimy o wybranie opcji "Podmiot publiczny".

Podmiot publiczny

Reprezentowany przeze mnie podmiot nie jest operatorem usługi kluczowej.

⚠ Podmiot publiczny będący operatorem usługi kluczowej

Reprezentowany przeze mnie podmiot publiczny jest równocześnie operatorem usługi kluczowej.

Czy chcą Państwo zgłosić incydent w podmiocie publicznym?

Incydent w podmiocie publicznym to incydent, który powoduje lub może spowodować obniżenie jakości lub przerwanie realizacji zadania publicznego realizowanego przez podmiot publiczny, o którym mowa w art. 4 pkt 7–15 ustawy z dnia 5 lipca 2018 (Dz. U. poz 1560) o krajowym systemie cyberbezpieczeństwa.

Zgłoszenie incydentu za pomocą formularza dostępnego po wybraniu opcji "Tak" **stanowi wypełnienie obowiązku** wynikającego z art 22 ust 1 pkt 2 ustawy z dnia 5 lipca 2018 (Dz. U. poz. 1560) o krajowym systemie cyberbezpieczeństwa.

⚠ Tak

Chcę zgłosić incydent w podmiocie publicznym.

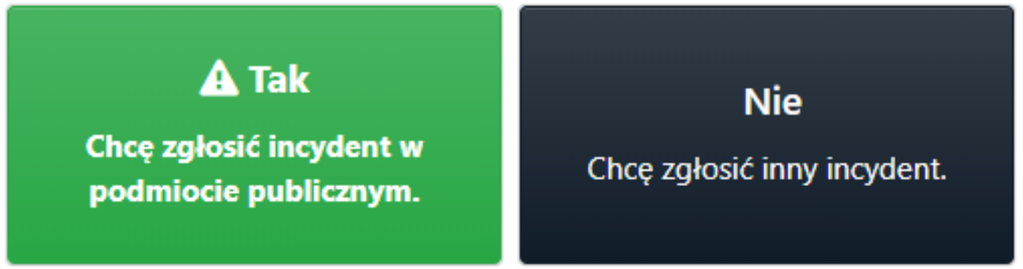
Nie

Chcę zgłosić inny incydent.

Czy chcą Państwo zgłosić incydent w podmiocie publicznym?

Incydent w podmiocie publicznym to incydent, który powoduje lub może spowodować obniżenie jakości lub przerwanie realizacji zadania publicznego realizowanego przez podmiot publiczny, o którym mowa w art. 4 pkt 7–15 ustawy z dnia 5 lipca 2018 (Dz. U. poz 1560) o krajowym systemie cyberbezpieczeństwa.

Zgłoszenie incydentu za pomocą formularza dostępnego po wybraniu opcji "Tak" **stanowi wypełnienie obowiązku** wynikającego z art 22 ust 1 pkt 2 ustawy z dnia 5 lipca 2018 (Dz. U. poz. 1560) o krajowym systemie cyberbezpieczeństwa.



Prosimy o wypełnienie poniższego formularza

Dane podmiotu zgłaszającego

Pełna nazwa firmy

Gmina XYZ

Numer REGON/NIP/KRS

000000000000

Adres siedziby (ulica, numer budynku, numer lokalu)

Ul. Adresowa 1

Kod pocztowy siedziby

00-000

Miasto siedziby

QWERTY

Dane osoby dokonującej zgłoszenia

Imię i nazwisko osoby zgłaszającej

Jan Kowalski

Numer telefonu osoby zgłaszającej

513 579 032

Adres e-mail osoby zgłaszającej

jan.kowalski@gminaxyz.pl

Dane osoby uprawnionej do składania wyjaśnień

Imię i nazwisko osoby do kontaktu w sprawie

Adam Nowak

Numer telefonu osoby do kontaktu w sprawie

513 456 123

Adres e-mail osoby do kontaktu w sprawie

adam.nowak@gminaxyz.pl

Opis wpływu incydentu w podmiocie publicznym

Wypełnij poniższy formularz zgodnie z wiedzą, którą posiadasz w chwili zgłoszenia. Istotne aktualizacje będziesz mógł wysłać później przez pocztę elektroniczną. Wystarczy, że podasz numer zgłoszenia, który nadamy po otrzymaniu tego formularza.

Pamiętaj, aby wysyłając zgłoszenie **oznaczyć informacje prawnie chronione**, w tym stanowiące tajemnicę przedsiębiorstwa. Aby to zrobić, użyj nawiasów kwadratowych, na przykład: `[Incydent w systemie bankowym miał wpływ na 10 tysięcy użytkowników końcowych.]`

Uwaga: Nieuzasadnione użycie oznaczeń może wydłużyć czas odpowiedniej reakcji.

Czy incydent miał wpływ na realizację zadań publicznych? Jeśli tak, na jakie?

Tak, wypłacanie świadczeń socjalnych dla obywateli gminy

Czy możesz określić dokładną lub przybliżoną liczbę osób, na które ma wpływ incydent?

10 000 osób

Czy znasz dokładny lub przybliżony czas wystąpienia oraz wykrycia incydentu?

10:24

Czy możesz geograficznie określić obszar, którego dotyczy incydent?

Gmina XYZ

Czy ustaliłeś przyczynę incydentu?

Prawdopodobnie wiadomość phishingowa zawierająca malware

Czy ustaliłeś skutki oddziaływania incydentu na twoje systemy informacyjne?

4 zaszyfrowane stacje robocze

Opisz najdokładniej jak potrafisz przebieg incydentu

Zauważono, że nie można było podejrzeć wniosków dot. wypłacania świadczeń socjalnych. Okazało się, że chwilę później ten sam problem dotyczy kolejnych stacji roboczych. po jakimś czasie nie można skorzystać z komputera. komputer nie odpowiadał, w takim wypadku zostawiliśmy je włączone, ale odłączyliśmy od sieci wew. i internetu.

Podjęte działania

Czy podjęto działania zapobiegawcze w związku z incydentem? Jeśli tak, prosimy opisać te działania.

Odłączenie zaszyfrowanych stacji roboczych od internetu i sieci wewnętrznej

Jakie działania naprawcze podjąłeś w związku z incydentem?

Brak

Inne informacje

Inne istotne informacje

Załączniki

Maksymalny rozmiar załączanego pliku to 12 MB.

Kliknij tutaj lub przeciągnij plik, aby dodać nowy załącznik.

Wysyłanie zgłoszenia

Prosimy o sprawdzenie, czy wszystkie pola zostały wypełnione prawidłowo i kliknięcie przycisku "Wyślij zgłoszenie".

Spodziewaj się odpowiedzi od nas niezwłocznie, nie później niż w ciągu 24 godzin.

Przyjmuję do wiadomości, że:

- administratorem ww. danych osobowych jest CSIRT NASK działający w strukturach Naukowej i Akademickiej Sieci Komputerowej - Państwowego Instytutu Badawczego z siedzibą przy ul. Kolskiej 12 w Warszawie;
- mam prawo żądania wglądu do swoich danych, ich poprawiania, ograniczenia przetwarzania oraz zażądania ich usunięcia; realizacja tych obowiązków może być ograniczona w przypadku, gdy uniemożliwiałoby to realizację zadań ustawowych CSIRT NASK;
- ww. dane kontaktowe mogą zostać udostępnione innym CSIRT-om poziomu krajowego, tj. CSIRT MON i CSIRT GOV, oraz sektorowym zespołom cyberbezpieczeństwa w celu realizacji ich zadań określonych przepisami prawa, jak również administratorom sieci, innym zespołom reagującym na naruszenia bezpieczeństwa w sieci lub organom ścigania;
- podanie ww. danych osobowych jest wymagane odpowiednio art. 12, art. 19 i art. 23 ustawy z dnia 13 sierpnia 2018 roku o krajowym systemie cyberbezpieczeństwa (Dz. U. 2018, poz. 1560);
- ww. dane osobowe będą przetwarzane przez okres niezbędny do skutecznej obsługi zgłoszenia incydentu, lecz nie dłużej niż przez okres 5 lat od zakończenia obsługi incydentu;
- przysługuje mi prawo do przeniesienia ww. danych osobowych do innego administratora;
- przysługuje mi prawo do wniesienia skargi do Urzędu Ochrony Danych Osobowych;
- z wykorzystaniem ww. danych osobowych nie są podejmowane decyzje w sposób zautomatyzowany.

Dane kontaktowe Inspektora Ochrony Danych w NASK: inspektorochronydanych@nask.pl.

Wyślij zgłoszenie