

# Zgłaszanie incydentów cyberbezpieczeństwa przez podmioty sektora ochrony zdrowia

(Wydanie 1 - Kwiecień 2020 r.)

## Spis treści

I. Dlaczego i gdzie zgłaszać incydenty.....	1
II. Jak zgłosić incydent do CSIRT NASK.....	5
III. Raportuję, jako podmiot publiczny, czyli nie jestem jednocześnie operatorem usługi kluczowej.....	7
a) Zgłaszanie incydentu w podmiocie publicznym.....	7
IV. Jestem operatorem usługi kluczowej .....	12
a) Zgłaszanie incydentu poważnego przez operatora usługi kluczowej .....	12
V. Zgłoszenie innego incydentu .....	17
VI. Zgłaszanie phishingu.....	19

## I. Dlaczego i gdzie zgłaszać incydenty?

### 1. Dlaczego muszę zgłaszać incydenty cyberbezpieczeństwa?

Ponieważ od 2018 roku podmioty publiczne, w tym wszystkie zakłady opieki zdrowotnej, które realizują zadania publiczne zależne od systemów informacyjnych, są częścią Krajowego Systemu Cyberbezpieczeństwa. Ustawa, która weszła w życie 28 sierpnia 2018 roku, nakłada na nie obowiązek raportowania incydentów.

### 2. Dlaczego CHCĘ zgłosić incydent?

Liczba incydentów bezpieczeństwa, w tym także celowych ataków przestępców, ma stałą tendencję rosnącą. Szpitale, przychodnie oraz inne podmioty w sektorze zdrowia także są celem cyberprzestępców. Każdy zgłoszony incydent do zespołu reagowania na incydenty bezpieczeństwa komputerowego CSIRT NASK<sup>1</sup> (CERT Polska) to m.in.:

- Możliwość ostrzeżenia innych podmiotów przed zaraportowanym typem incyduentu;
- Uzyskanie wsparcia ze strony ekspertów ds. cyberbezpieczeństwa;
- Przygotowanie mechanizmów umożliwiających poradzenie sobie z incyduentem np. opracowanie dekryptorów do zaszyfrowanych przez przestępcę danych;

### 3. Jak zgłosić osobę kontaktową do CSIRT NASK?

Ustawa nakłada także obowiązek wyznaczenia specjalnej osoby do utrzymywania kontaktów z zespołem reagowania na incydenty komputerowe. Podmioty publiczne z sektora zdrowia muszą przekazać dane takiej osoby do CSIRT NASK. Aby zgłosić osoby kontaktowe do CSIRT NASK lub zaktualizować ich dane należy: wypełnić formularz, wygenerowane pismo przedstawić do podpisu kierownikowi instytucji, przesłać pismo na wskazany w nim adres (w przypadku operatora usługi kluczowej załączając skan decyzji administracyjnej uznającej podmiot za operatora usługi kluczowej). Formularz zgłoszeniowy dostępny jest pod adresem:

<https://incydent.cert.pl/osoba-kontaktowa>.

### 4. Kto jeszcze, poza podmiotami publicznymi, może zgłaszać osobę do kontaktu?

Przepisy ustawy o ksc nakładają na podmioty publiczne obowiązek zgłoszenia osoby kontaktowej oraz raportowania o incyduentach. Natomiast pozostałe placówki zdrowia m.in. prywatne szpitale, kliniki, przychodnie zdrowia **mogą na zasadzie dobrowolności** przekazać taką informację do zespołu CSIRT NASK. Ponadto, podmioty te mogą także zgłaszać wszelkie incydenty cyberbezpieczeństwa. Ministerstwo Cyfryzacji oraz zespół CSIRT NASK wspólnie zachęcają do przekazywania informacji o osobach do kontaktu oraz o zaobserwowanych incyduentach.

### 5. Kto może być osobą kontaktową?

---

<sup>1</sup> CSIRT NASK działa w strukturach nadzorowanej przez Ministra Cyfryzacji Naukowej i Akademickiej Sieci Komputerowej – Państwowym Instytucie Badawczym.

Rekomenduje się, aby ta osoba była na stałe zatrudniona w urzędzie/przedsiębiorstwie/szpitalu. Osoba taka powinna być dyspozycyjna, decyzyjna, o technicznym rozumieniu tematu oraz mająca rozwinięte kontakty w swojej organizacji. Rola osoby do kontaktów może być pełniona równolegle z innymi, takimi jak np. pełnomocnik ds. bezpieczeństwa informacji, czy Inspektor Ochrony Danych Osobowych. Rekomendacje dotyczące osoby kontaktowej są dostępne pod adresem: <https://incydent.cert.pl/osoba-kontaktowa/rekomendacje>

## **6. Gdzie zgłosić incydent?**

Prześlij zgłoszenie do **CSIRT NASK**, który jest jednym z trzech zespołów reagowania na incydenty cyberbezpieczeństwa poziomu krajowego.

## **7. Jak przekazać zgłoszenie?**

Prześlij zgłoszenie w formie elektronicznej. Najlepiej zrobić to za pośrednictwem formularza online na stronie <https://incydent.cert.pl>, który podpowie jakie informacje powinienś zawierać w zgłoszeniu. Alternatywnie, można wysłać zgłoszenie pocztą elektroniczną na adres [cert@cert.pl](mailto:cert@cert.pl).

**Uwaga:** Formularz do wydruku znajdziesz na [BIP NASK](#).)

## **8. W jakim czasie zgłosić incydent?**

Jak najszybciej. Czas reakcji na zgłoszenie jest bardzo ważny i może wpłynąć na rozwiązanie problemu.

## **9. Co jeśli nie mam wszystkich potrzebnych informacji?**

Przełącz informacje, które znasz w chwili zgłoszenia. Zespół CERT Polska, w toku badania sprawy, może poprosić cię o dalsze informacje, które nie zostały przekazane w pierwszym zgłoszeniu.

## **10. Czy muszę przekazać informacje prawnie chronione?**

Tak, poprosimy cię o przesłanie takich informacji, jeśli jest to niezbędne do obsługi incydentu<sup>2</sup>. Dzięki tej wiedzy będziemy mogli lepiej zrozumieć problem i udzielić ci adekwatnego wsparcia. Nie musisz obawiać się o bezpieczeństwo przekazanych informacji, co trafia do CSIRT NASK zostaje w CSIRT NASK!

**Ważne!** Zaznacz w zgłoszeniu, które informacje stanowią tajemnice prawnie chronione.

### **11. Jakie informacje muszę przekazać, aby spełnić obowiązek ustawowy?**

Zostaniesz poprowadzony przez formularz. Formularz jest prosty i intuicyjny. Podaj wszystkie informacje, o które zostaniesz w nim poproszony. Jeśli w chwili zgłaszania incydentu czegoś nie wiesz, po prostu to napisz. Takie zgłoszenie incydentu stanowi wypełnienie ustawowego obowiązku.

### **12. Czym jest incydent w podmiocie publicznym?**

Incydent w podmiocie publicznym to incydent, który powoduje lub może spowodować obniżenie jakości lub przerwanie realizacji zadania publicznego.

### **13. Czym jest incydent poważny?**

O incydencie poważnym możemy mówić tylko w przypadku, gdy **jednostka ochrony zdrowia jest jednocześnie operatorem usług kluczowej**. To, czy incydent jest uznawany za poważny, zależy np. od liczby użytkowników dotkniętych incydem oraz czasu oddziaływania incydentu na świadczoną usługę. Kryteria dla poszczególnych sektorów określa [rozporządzenie Rady Ministrów](#).

### **14. Gdzie znajdę kryteria incydentu poważnego?**

Kryteria dla poszczególnych sektorów znajdziesz m.in. w naszej analizie [Rozporządzenia Rady Ministrów w sprawie progów uznania incydentu za poważny](#).

### **15. Skąd mam wiedzieć, czy zostałem wyznaczony na operatora usługi kluczowej?**

---

<sup>2</sup> Art. 12 pkt. 3 [ustawa o krajowym systemie cyberbezpieczeństwa](#): „Operator usługi kluczowej przekazuje, w niezbędnym zakresie, w zgłoszeniu, o którym mowa w art. 11 ust. 1 pkt 4, informacje stanowiące tajemnice prawnie chronione, w tym stanowiące tajemnicę przedsiębiorstwa, gdy jest to konieczne do realizacji zadań właściwego CSIRT MON, CSIRT NASK lub CSIRT GOV oraz sektorowego zespołu cyberbezpieczeństwa”

Otrzymaś decyzję administracyjną wydaną przez ministra, który nadzoruje dany sektor gospodarki. Wymienieni w ustawie ministrowie oraz Komisja Nadzoru Finansowego to tzw. organy właściwe do spraw cyberbezpieczeństwa<sup>3</sup>.

### **16. Czy muszę zgłaszać incydent, który nie jest incydem w podmiocie publicznym, ani nie spełnia kryteriów incydemu poważnego?**

Ustawa nie nakłada takiego obowiązku. Zachęcamy jednak do **zgłaszania wszystkich incydentów** cyberbezpieczeństwa, nawet tych, które zostały już rozwiązane. Przekazywane informacje pomagają nam zapobiegać podobnym sytuacjom w przyszłości oraz pozwalają budować całościowy obraz polskiego cyberbezpieczeństwa.

## **II. Jak zgłosić incydent do CSIRT NASK**

1. Wejdź na stronę <https://incydent.cert.pl>.
2. Wybierz, jaki podmiot reprezentujesz. Jako szpital wskaż „Podmiot publiczny” oznaczony ikonką budynku.

### **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 incydemu – Jaki podmiot Państwo reprezentują?



<sup>3</sup> Art. 41 [ustawa o krajowym systemie cyberbezpieczeństwa](#).

## 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.

### III. Raportuję, jako podmiot publiczny, czyli nie jestem jednocześnie operatorem usługi kluczowej

Jeśli reprezentujesz podmiot publiczny, który **nie jest** jednocześnie operatorem usługi kluczowej, wybierz pole „**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".

<p><b>Podmiot publiczny</b> Reprezentowany przeze mnie podmiot nie jest operatorem usługi kluczowej.</p>	<p><b>⚠ Podmiot publiczny będący operatorem usługi kluczowej</b> Reprezentowany przeze mnie podmiot publiczny jest równocześnie operatorem usługi kluczowej.</p>
--	--

Jako podmiot publiczny możesz zgłosić dwa rodzaje incydentów:

1. **Incydent w podmiocie publicznym** - incydent, który powoduje lub może spowodować obniżenie, jakości lub przerwanie realizacji zadania publicznego.
2. **Inny incydent** - są to wszystkie inne incydenty cyberbezpieczeństwa, które nie wpłynęły na obniżenie, jakości ani nie przerwały realizacji zadania publicznego. Zachęcamy do ich zgłaszania! Pomoże nam to właściwie szacować ryzyko wystąpienia podobnych zagrożeń w przyszłości, także u innych podmiotów.

#### a) Zgłaszanie incydentu w podmiocie publicznym

Incydent w podmiocie publicznym to incydent, który powoduje lub może spowodować obniżenie, jakości lub przerwanie realizacji zadania publicznego.

**Przykład 1:** Lekarz posiadający dostęp do systemu informacyjnego niezbędnego do np. rejestracji pacjenta, czy wypisania e-recepty padł ofiarą złośliwego oprogramowania typu *ransomware*, które zablokowało mu dostęp do systemu komputerowego. Jeśli taki incydent może znacząco przedłużyć lub przerwać możliwości leczenia pacjentów, będzie incydem w podmiocie publicznym.

**Przykład 2:** Szpital/przychodnia oferują możliwość zdalnej rejestracji wizyty pacjenta poprzez dedykowany formularz dostępny na stronie internetowej placówki. Jeśli

strona ta przestanie działać w wyniku incydentu cyberbezpieczeństwa (np. atak DDoS), a pacjenci przez dłuższy czas nie będą mogli dokonać rejestracji, należy potraktować taki atak, jako incydent w podmiocie publicznym. Nawet, jeśli istnieje alternatywna możliwość rejestrowania np. osobiście lub telefonicznie, wciąż jest to obniżenie jakości usług świadczonych przez podmiot publiczny.


Aby zgłosić incydent w podmiocie publicznym:

1. Wybierz pole „**Tak**” oznaczone wykrzyknikiem wpisanym w trójkąt.

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.

 <b>Tak</b> Chcę zgłosić incydent w podmiocie publicznym.	<b>Nie</b> Chcę zgłosić inny incydent.
---	---

2. Zostaniesz przekierowany do formularza. **Wypełnij go.**
  - a. **Podaj dane** podmiotu zgłaszającego, osoby zgłaszającej i osoby uprawnionej do składania wyjaśnień.
  - b. **Opisz incydent** i odpowiedz na pytania, które pozwolą nam zobaczyć, jaki wpływ wywarł on na Twój podmiot publiczny.
  - c. **Opisz działania zapobiegawcze i naprawcze**, które podjęto w związku z incydemtem.

Pamiętaj, że będziesz mógł dostać istotne aktualizacje pocztą elektroniczną.

Wystarczy, że podasz numer zgłoszenia, który nadamy po otrzymaniu formularza.



**Ważne!** Oznacz kwadratowymi nawiasami informacje prawnie chronione, w tym stanowiące tajemnicę przedsiębiorstwa. Poniżej możesz zobaczyć, jakie pola należy obowiązkowo uzupełnić, wysyłając zgłoszenie do CSIRT NASK:

### Prosimy o wypełnienie poniższego formularza

#### Dane podmiotu zgłaszającego

Pełna nazwa firmy

Numer REGON/NIP/KRS

Adres siedziby (ulica, numer budynku, numer lokalu)

Kod pocztowy siedziby

Miasto siedziby

#### Dane osoby dokonującej zgłoszenia

Imię i nazwisko osoby zgłaszającej

Numer telefonu osoby zgłaszającej

Adres e-mail osoby zgłaszającej

### Dane osoby uprawnionej do składania wyjaśnień

Imię i nazwisko osoby do kontaktu w sprawie

Numer telefonu osoby do kontaktu w sprawie

Adres e-mail osoby do kontaktu w sprawie

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

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

Czy znasz dokładny lub przybliżony czas wystąpienia oraz wykrycia incydentu?

Czy możesz geograficznie określić obszar, którego dotyczy incydent?

Czy ustaliłeś przyczynę incydentu?

Czy ustaliłeś skutki oddziaływania incydentu na twoje systemy informacyjne?

Opisz najdokładniej jak potrafisz przebieg incydentu

## Podjęte działania

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


Jakie działania naprawcze podjąłeś w związku z incydem?

## Inne informacje

Inne istotne informacje

## Załączniki i wysyłanie zgłoszenia

Dołączenie plików lub wysłanie formularza jest możliwe po kliknięciu "Nie jestem robotem" poniżej.

 Nie jestem robotem   
reCAPTCHA  
Prywatność - Warunki

**Uwaga:** Będziesz mógł dodać załączniki oraz wysłać zgłoszenie dopiero po kliknięciu pola „Nie jestem robotem” na samym dole formularza.

## IV. Jestem operatorem usługi kluczowej

Jeśli reprezentujesz podmiot publiczny – szpital/hurtownię farmaceutyczną, który **jest** jednocześnie operatorem usługi kluczowej, wybierz odpowiednie pole oznaczone wykrzyknikiem wpisanym w trójkąt.

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.

Jako operator usług kluczowej możesz zgłosić **dwa rodzaje incydentów**:

1. **Incydent poważny** - Masz wrażenie, że incydent, który chcesz zgłosić jest poważny? Możesz to sprawdzić. Każdy sektor ma swoje kryteria, które wpływają na to, kiedy możemy mówić o incydencie poważnym. Wpływa na to np. liczba użytkowników dotkniętych incydem lub też jego czas oddziaływania na świadczoną usługę. **Ważne:** Sprawdź kryteria dla twojego sektora: [Rozporządzenie Rady Ministrów w sprawie progów uznania incydem za poważny](#)
2. **Inny incydent** - Jeśli incydent, który zgłaszasz nie spełnia kryteriów incydem poważnego, wybierz opcję „incydent niesklasyfikowany, jako poważny”.

### a) Zgłaszanie incydem poważnego przez operatora usługi kluczowej

O incydemie poważnym możemy mówić w przypadku, jeżeli szpital/hurtownia farmaceutyczna został wyznaczony na **operatora usługi kluczowej**. To, czy incydent jest uznawany za poważny, zależy np. od liczby użytkowników dotkniętych incydem oraz czasu oddziaływania incydem na świadczoną usługę.

**Przykład:** Szpital został wyznaczony przez Ministra Zdrowia na operatora usługi kluczowej. Zaatakowany został system informatyczny, którego awaria sprawiła, że znacząco utrudnione jest lub wręcz uniemożliwione jest najważniejsze zadanie

placówki, czyli świadczenie opieki zdrowotnej powyżej 24 godzin. Co więcej, w wyniku tego ataku doszło nie tylko do zagrożenia życia i zdrowia pacjentów, ale np. efektem był „wyciek” poufnych danych medycznych.

**Przykład 2:** Pełniący istotną rolę w regionie szpital (operator usługi kluczowej z jedynym w regionie specjalistycznym centrum urazowym) w wyniku ataku typu *ransomware* ma zablokowany dostęp do komputerów w placówce, co uniemożliwiło np. przyjmowanie nowych pacjentów przez ponad 24 godziny i skutkowało koniecznością przekierowywania chorych do innych placówek. Według kryteriów ustalonych w sektorze zdrowia, będzie to incydent poważny.

Aby zgłosić incydent poważny:


1. Wybierz pole „**Tak**” oznaczone wykrzyknikiem wpisanym w trójkąt.

Czy reprezentują Państwo podmiot z listy operatorów usług kluczowych i chcą Państwo dokonać zgłoszenia incydentu poważnego?

**Operatorem usługi kluczowej** jest podmiot, o którym mowa w załączniku nr 1 do ustawy, posiadający jednostkę organizacyjną na terytorium Rzeczypospolitej Polskiej, wobec którego organ właściwy do spraw cyberbezpieczeństwa wydał decyzję o uznaniu za operatora usługi kluczowej. Sektory, podsektory oraz rodzaje podmiotów określa załącznik nr 1 do ustawy.

Progi **uznania incydentu za poważny** zależą od liczby użytkowników dotkniętych incydem, czasu oddziaływania incydentu na świadczoną usługę oraz zasięgu geograficznego incydentu. Kryteria dla poszczególnych sektorów określone są przez Radę Ministrów w drodze rozporządzenia.

Zgłoszenie incydentu za pomocą formularza dostępnego po wybraniu opcji „**Tak**” **stanowi wypełnienie obowiązku** wynikającego z art 11 ust 1 pkt 4 ustawy z dnia 5 lipca 2018 (Dz. U. poz. 1560) o krajowym systemie cyberbezpieczeństwa.

 <b>Tak</b> Reprezentuję operatora usług kluczowych i chcę zgłosić incydent poważny.	<b>Nie</b> Chcę zgłosić incydent nieklasyfikowany jako poważny zgodnie z powyższą definicją.
--	---

2. Zostaniesz przekierowany do formularza. **Wypełnij go.**
  - a. **Podaj dane** podmiotu zgłaszającego, osoby zgłaszającej i osoby uprawnionej do składania wyjaśnień.
  - b. **Opisz incydent** i odpowiedz na pytania, które pozwolą nam zobaczyć, jaki wpływ wywarł on na Twój podmiot publiczny.
  - c. **Opisz działania zapobiegawcze i naprawcze**, które podjęto w związku z incydem.

Pamiętaj, że będziesz mógł dostać istotne aktualizacje pocztą elektroniczną. Wystarczy, że podasz numer zgłoszenia, który nadamy po otrzymaniu formularza.

**Ważne!** Oznacz kwadratowymi nawiasami informacje prawnie chronione, w tym stanowiące tajemnicę przedsiębiorstwa. Poniżej możesz zobaczyć, jakie pola należy uzupełnić, wysyłając zgłoszenie do CSIRT NASK.

## Prosimy o wypełnienie poniższego formularza

### Dane podmiotu zgłaszającego

Pełna nazwa firmy

Sektor i podsektor

(wybierz z listy)



Numer REGON/NIP/KRS

Adres siedziby (ulica, numer budynku, numer lokalu)

Kod pocztowy siedziby

Miasto siedziby

### Dane osoby dokonującej zgłoszenia

Imię i nazwisko osoby zgłaszającej

Numer telefonu osoby zgłaszającej

Adres e-mail osoby zgłaszającej

### Dane osoby uprawnionej do składania wyjaśnień

Imię i nazwisko osoby do kontaktu w sprawie

Numer telefonu osoby do kontaktu w sprawie

Adres e-mail osoby do kontaktu w sprawie

Usługi kluczowe zgłaszającego, na które incydent poważny miał wpływ

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

Czy znasz dokładny lub przybliżony czas wystąpienia oraz wykrycia incydu?

Czy możesz geograficznie określić obszar, którego dotyczy incydent?

Czy incydent miał wpływ na świadczenie usługi kluczowej przez innych operatorów usług kluczowych i dostawców usług cyfrowych?

Czy ustaliłeś przyczynę incydu?

Czy ustaliłeś skutki oddziaływania incydu na twoje systemy informacyjne?

Opisz najdokładniej jak potrafisz przebieg incydu

Czy incydent ma charakter międzynarodowy? Jeśli tak, jakich innych krajów Unii Europejskiej dotyczył?

## Podjęte działania

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


Jakie działania naprawcze podjąłeś w związku z incydem?

## Inne informacje

Inne istotne informacje

## Załączniki i wysyłanie zgłoszenia

Dołączenie plików lub wysłanie formularza jest możliwe po kliknięciu "Nie jestem robotem" poniżej.

 Nie jestem robotem   
reCAPTCHA  
Prywatność - Warunki

**Uwaga:** Będziesz mógł dodać załączniki oraz wysłać zgłoszenie dopiero po kliknięciu pola „Nie jestem robotem” na samym dole formularza.



## V. Zgłoszenie innego incydentu

**Ważne!** Pamiętaj, że możesz zgłosić do CSIRT NASK **każdy incydent cyberbezpieczeństwa**.

**Dlaczego warto to robić?**

- **Bo dzięki temu mamy więcej informacji na temat poziomu cyberbezpieczeństwa państwa. Możemy też lepiej szacować ryzyko i ostrzegać o potencjalnym zagrożeniu inne podmioty.**
- **Bo CSIRT NASK analizuje każde zgłoszenie i jeśli okaże się, że to coś istotnego, zawsze uzyskasz od nas wsparcie merytoryczne.**

**Przykład:** Otrzymałeś na służbową skrzynkę e-mail podejrzaną wiadomość, w której zostałeś poproszony o podanie swoich danych logowania lub ściągnięcie dziwnie wyglądającego załącznika? A może planując zakupy dla podmiotu publicznego, natknąłeś się na fałszywy sklep internetowy? **Możesz zgłosić te incydenty do CSIRT NASK**, nawet, jeśli nie spełniają wymogów incydentu poważnego oraz incydentu w podmiocie publicznym.

Twoje zgłoszenie musi zawierać informację o nazwie podmiotu lub systemu informacyjnego, w którym wystąpił incydent. Poprosimy cię również o dane kontaktowe, które mogą pomóc nam w prawidłowej reakcji na zgłaszany incydent. Podanie ich jest jednak dobrowolne.

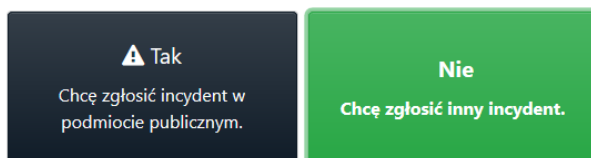
Aby wysłać takie zgłoszenie, musisz w menu wyboru wskazać pole z napisem „Nie. Chcę zgłosić inny incydent”.

---

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.



Następnie wybierz kategorię, w której chcesz zgłosić incydent i postępuj według poleceń na ekranie. Do dyspozycji masz sześć opcji:

Prosimy o wybranie odpowiedniej kategorii:

 <b>Podjęrzana wiadomość e-mail</b> Podjęrzane załączniki, phishing, szantaż	 <b>Próba oszustwa</b> Fałszywe sklepy internetowe i inne próby podszywania się	 <b>Złośliwe oprogramowanie</b> Próbki wirusów lub pliki zaszyfrowane ransomware	 <b>Podatności</b> Błędy w oprogramowaniu lub aplikacjach internetowych
 <b>Nielegalne treści</b> Zgłoszenia przeznaczone dla zespołu Dyżurnet.pl	<b>Inne</b> Wszystkie inne incydenty niepasujące do poprzednich kategorii		

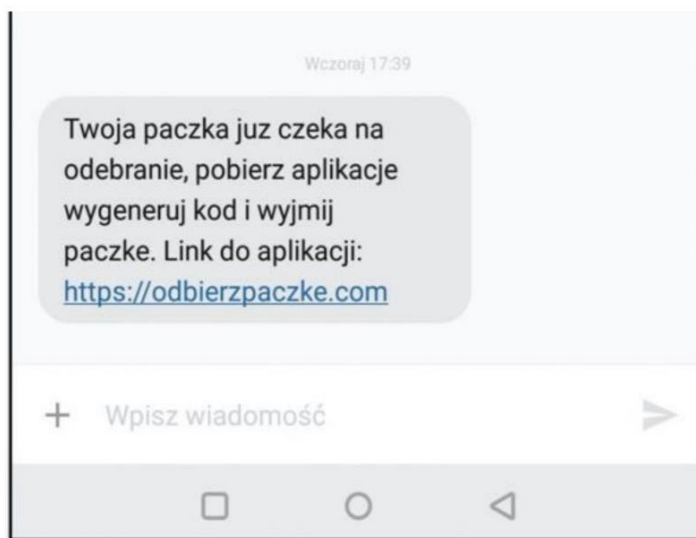
1. **Podjęrzana wiadomość e-mail** - zapisz podejrzaną wiadomość do pliku.eml i dołącz go do formularza. Jeżeli zawiera załączniki, pod żadnym pozorem ich nie otwieraj!
2. **Próba oszustwa** - zamieść wszelkie informacje na temat oszustwa. Napisz nam skąd dowiedziałeś się np. o fałszywym sklepie, prześlij korespondencję i numer konta, na który miałyś przelać pieniądze. Jeśli zgłosiłeś sprawę policji, prześlij numer sprawy i podaj jednostkę, która ją prowadzi.
3. **Złośliwe oprogramowanie** - spakuj podejrzany plik do archiwum np. w formacie .rar, .zip, .7z. Zabezpiecz archiwum hasłem infected. Jeżeli ktoś zaszyfrował pliki na Twoim urządzeniu, załącz plik tekstowy z żądaniem okupu lub przykładowy zaszyfrowany plik.
4. **Podatności** – podaj dokładne techniczne wyjaśnienie charakteru zgłaszanej podatności. Poinformuj również o ewentualnych próbach kontaktu z podmiotem, którego podatność dotyczy.
5. **Nielegalne treści**, – jeśli chcesz zgłosić nielegalne treści w Internecie związane z przemocą w stosunku do dzieci i młodzieży, skorzystaj z [formularza zespołu Dyżurnet.pl](#).
6. **Inne** – naciśnij to pole, jeśli nie wiesz, którą z kategorii wybrać. Jeśli zdarzenie dotyczy zdarzeń sieciowych (skanowanie, atak DDoS, nieuprawnione próby logowania), dołącz do zgłoszenia logi z tych zdarzeń.

**Uwaga:** Będziesz mógł dodać załączniki oraz wysłać zgłoszenie dopiero po kliknięciu pola „Nie jestem robotem” na samym dole formularza.

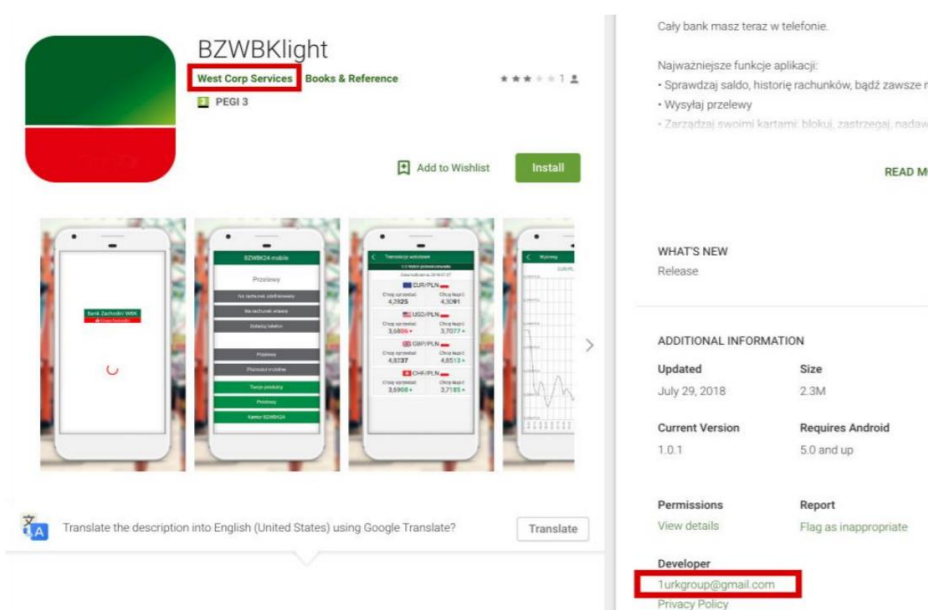
## VI. Zgłaszanie phishingu

Każdy może zgłosić stronę, która może wyludzać dane osobowe, dane uwierzytelniające do kont bankowych lub serwisów społecznościowych, za pomocą formularza dostępnego na <https://incydent.cert.pl/phishing>. Poniżej przykładowe próby wyludzeń informacji::

### Przykład 1. SMS



### Przykład 2. Fałszywa aplikacja banku

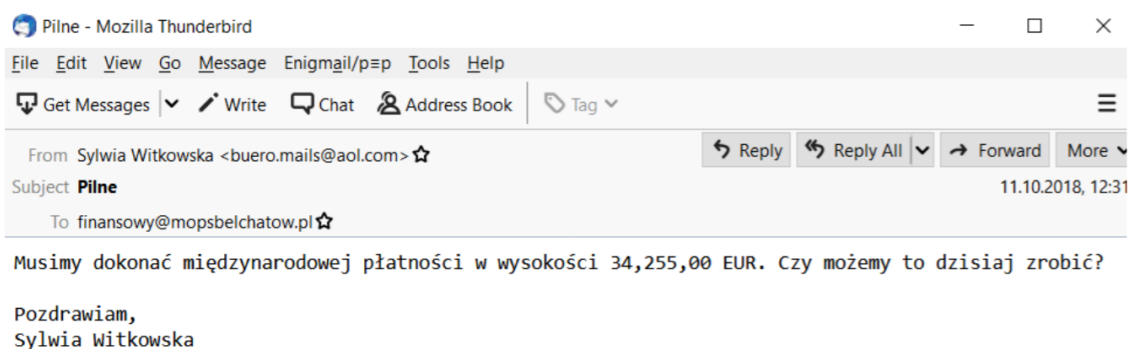


The image shows a screenshot of a Google Play Store listing for an application named 'BZWBKlight'. The app icon is a vertical rectangle with a green top half and a red bottom half. The listing includes the following information:

- Developer:** West Corp Services (Books & Reference)
- Category:** Books & Reference
- Age Rating:** PEGI 3
- Buttons:** 'Add to Wishlist' and 'Install'
- App Preview:** Four screenshots showing the app's interface, including a login screen, a menu, a transaction list, and a graph.
- Description:** 'Cały bank masz teraz w telefonie.' (The whole bank is now in your phone.)
- Key Features:**
  - Najważniejsze funkcje aplikacji:
    - Sprawdzaj saldo, historię rachunków, bądź zawsze n
    - Wysyłaj przelewy
    - Zarządzaj swoimi kartami: blokuj, zastrzeżaj, nadaw
- WHAT'S NEW:** Release
- ADDITIONAL INFORMATION:**

<b>Updated:</b> July 29, 2018	<b>Size:</b> 2.3M
<b>Current Version:</b> 1.0.1	<b>Requires Android:</b> 5.0 and up
- Permissions:** View details
- Report:** Flag as inappropriate
- Developer:** 1urkgroupp@gmail.com (highlighted with a red box), Privacy Policy

### Przykład 3. E-mail dotycząca pilnego przelewu



Następnie korzystając z niniejszego formularza, możecie zgłosić domeny internetowe, które za podstawowy cel swojego działania mają wprowadzenie w błąd użytkowników Internetu i w ten sposób umożliwienie kradzieży pieniędzy z konta albo do wyłudzenia danych osobowych.

Jeżeli chcą Państwo zgłosić innego rodzaju incydent proszę użyć poniższego odnośnika:

[Zgłaszanie incydentu \(innego niż złośliwa domena\) do CSIRT NASK.](#)

#### Prosimy o wypełnienie poniższego formularza

##### Złośliwe domeny

W ramach zgłoszenia można wskazać maksymalnie 50 złośliwych domen.

Złośliwe domeny lub adresy URL (po jednym w linii)

Uzasadnienie zgłoszenia

### Zgłaszający (pola nieobowiązkowe)


Podane dane mogą zostać wykorzystane w celu kontaktu ze zgłaszającym w celu wyjaśnienia ewentualnych wątpliwości. Podanie ich jest dobrowolne.

E-mail zgłaszającego

Numer telefonu zgłaszającego

### Wysyłanie zgłoszenia

Wysłanie formularza jest możliwe po kliknięciu "Nie jestem robotem" poniżej.

 Nie jestem robotem   
reCAPTCHA  
Prywatność · Warunki

**Uwaga:** Będziesz mógł dodać załączniki oraz wysłać zgłoszenie dopiero po kliknięciu pola „Nie jestem robotem” na samym dole formularza.

*Opracowanie:*

*Rafał Babraj, Justyna Balcewicz, Magdalena Wrzosek – CSIRT NASK*

*Aktualizacja:*

*Monika Pieniek, Tomasz Właż, Łukasz Magdziak – Ministerstwo Cyfryzacji*