Zgłaszanie incydentów przez samorządy

Spis treści

I. Dlaczego i gdzie zgłaszać incydenty cyberbezpieczeństwa

1. Dlaczego muszę zgłaszać incydenty cyberbezpieczeństwa?

Ponieważ od 2018 roku podmioty publiczne, 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. Gdzie zgłosić incydent?

Prześlij zgłoszenie do **CERT Polska**, który jest jednym z trzech CSIRT poziomu krajowego.

3. 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 powinieneś zawrzeć w zgłoszeniu. Alternatywnie, można wysłać zgłoszenie pocztą elektroniczną na adres cert@cert.pl.

Uwaga: Formularz do wydruku znajdziesz na BIP NASK.)

4. W jakim czasie zgłosić incydent?

Jak najszybciej, przy czym nie później niż w ciągu 24 godzin od momentu wykrycia incydentu. Czas reakcji na zgłoszenie jest bardzo ważny i może wpłynąć na rozwiązanie problemu.

5. Co jeśli nie mam wszystkich potrzebnych informacji?

Przekaż 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.

6. Czy muszę przekazać informacje prawnie chronione?

Tak, poprosimy cię o przesłanie takich informacji, jeśli jest to niezbędne do obsługi incydentu[1]. Dzięki tej wiedzy będziemy mogli lepiej zrozumieć problem i udzielić ci adekwatnego wsparcia. Nie musisz obawiać się o bezpieczeństwo przekazanych informacji, co trafia do CERT Polska zostaje w CERT Polska!

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

7. Jakie informacje muszę przekazać, aby spełnić obowiązek ustawowy?

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

8. Czym jest incydent w podmiocie publicznym?

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

9. Czym jest incydent poważny?

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

10. 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.

11. Skąd mam wiedzieć, czy zostałem wyznaczony na operatora usługi kluczowej?

Twój podmiot publiczny otrzyma 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[2].

[1] 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”

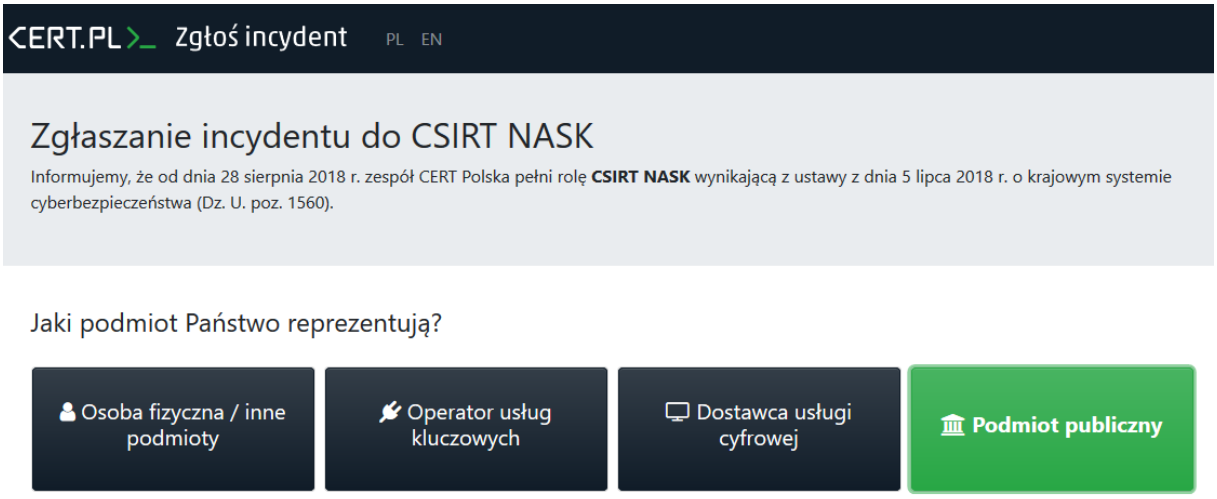
[2] Art. 41 ustawa o krajowym systemie cyberbezpieczeństwa.

12. Czy muszę zgłaszać incydent, który nie jest incydentem w podmiocie publicznym, ani nie spełnia kryteriów incydentu 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.

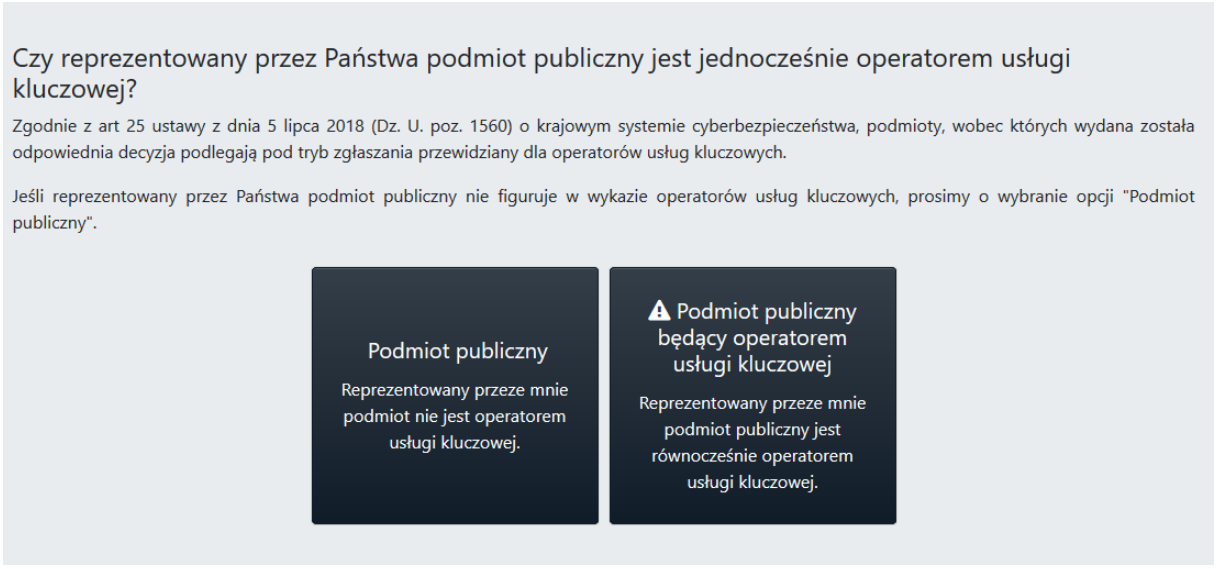
II. Jak zgłosić incydent do CSIRT NASK (CERT Polska)

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



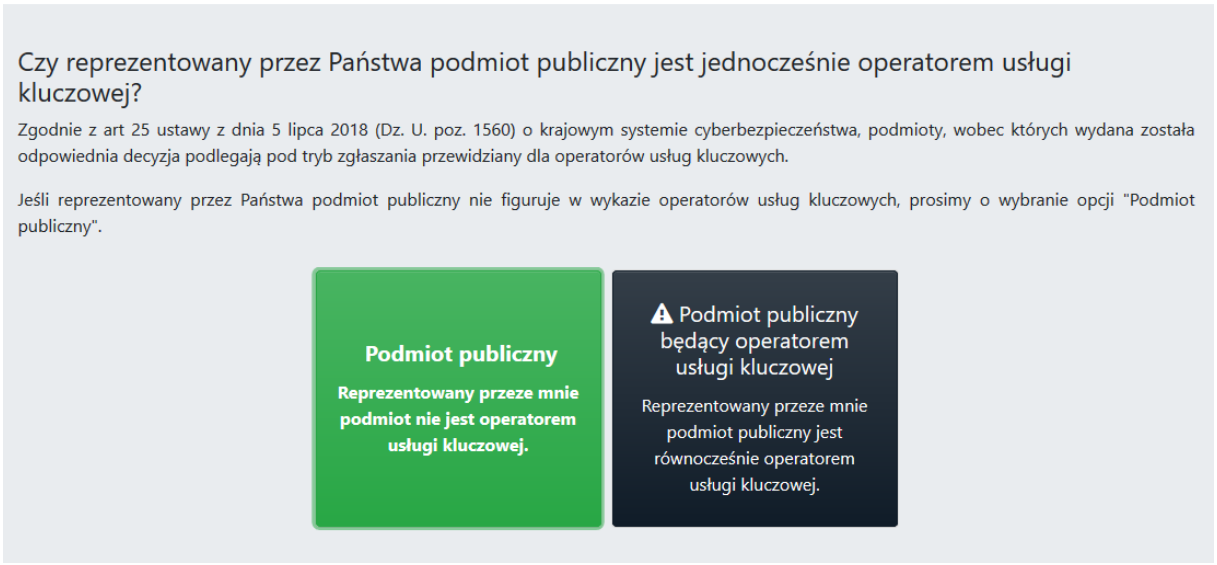
3. Odpowiedz na pytanie, czy podmiot publiczny, w którym pracujesz, jest jednocześnie operatorem usługi kluczowej. Dalszy przebieg zgłoszenie będzie zależał od tego, którą opcję wybierzesz.

Uwaga: Twój podmiot publiczny otrzyma decyzję administracyjną wydaną przez organ właściwy, nadzorujący dany sektor gospodarki.



III. Podmiot publiczny, który nie jest operatorem usługi kluczowej

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



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

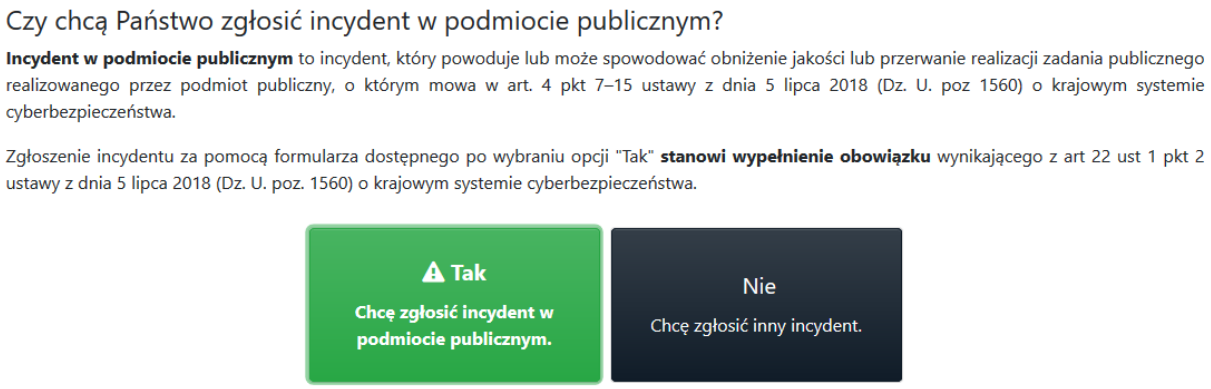
Incydent w podmiocie publicznym to incydent, który powoduje lub może spowodować obniżenie jakości lub przerwanie realizacji zadania publicznego.

Przykład 1: Pracownik urzędu gminy zajmujący się wypłatą świadczeń (np. 500 plus) padł ofiarą złośliwego oprogramowania typu ransomware, które zablokowało mu dostęp do systemu komputerowego. Jeśli taki incydent może znacząco przedłużyć lub przerwać proces wypłaty świadczeń mieszkańcom, będzie incydentem w podmiocie publicznym.

Przykład 2: Miasto oferuje swoim mieszkańcom zniżki na komunikację miejską. Mieszkaniec może złożyć odpowiedni wniosek drogą elektroniczną, logując się na dedykowanej stronie internetowej. Jeśli strona ta przestanie działać w wyniku incydentu cyberbezpieczeństwa (np. atak DDoS), a mieszkańcy przez dłuższy czas nie będą mogli składać wniosków elektronicznych, należy potraktować taki atak jako incydent w podmiocie publicznym. Nawet jeśli istnieje alternatywna możliwość składania wniosków papierowych, wciąż jest to obniżenie jakości świadczonych przez podmiot publiczny usług.

Aby zgłosić incydent w podmiocie publicznym:

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



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 incydentem.

Pamiętaj, że będziesz mógł dosłać 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:

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?

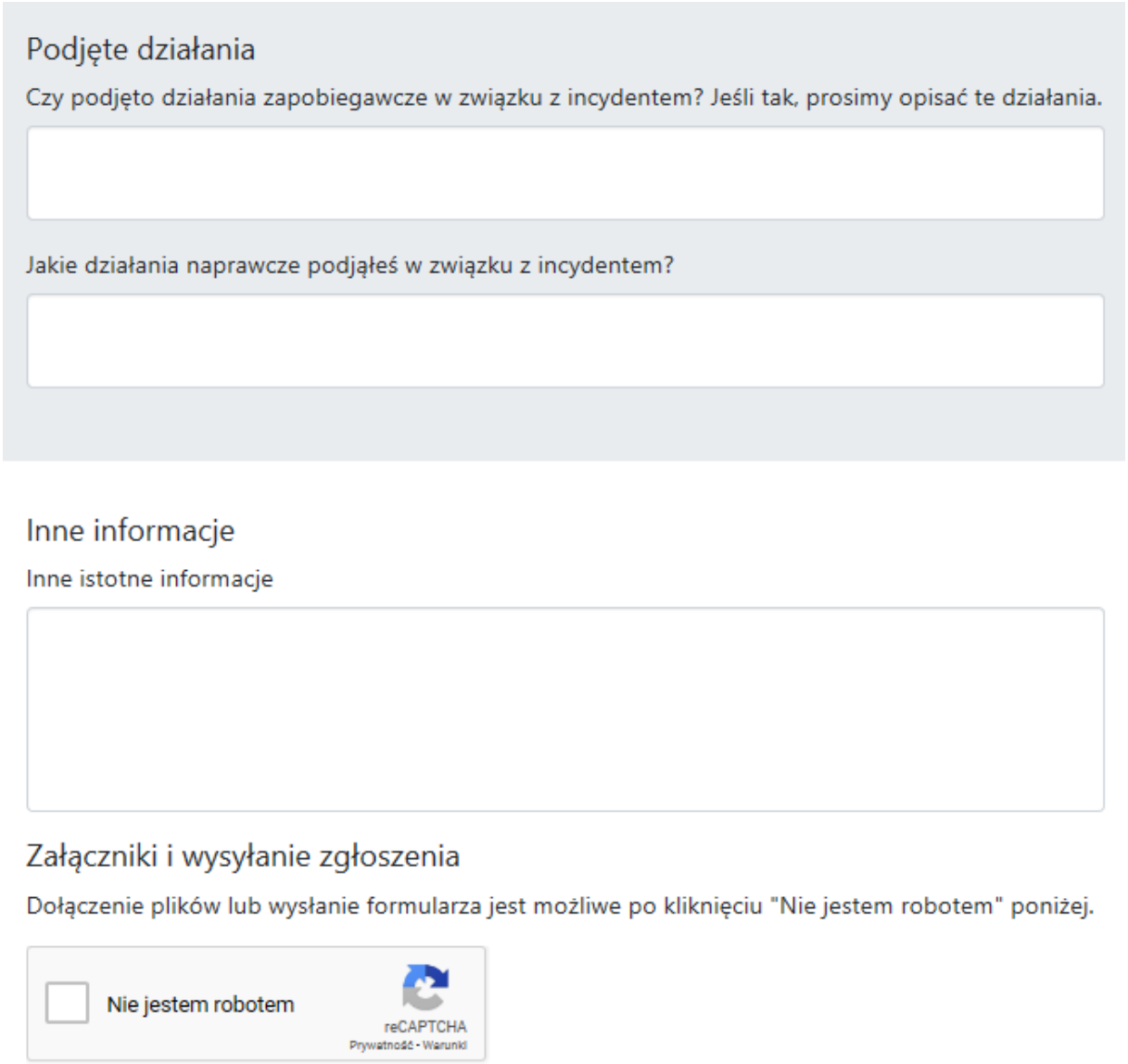
Czy znasz dokładny lub przybliżony czas wystąpienia oraz wykrycia incydentu?

Czy możesz geograficznie określić obszar, którego dotyczy incydent?

Czy ustaliłeś przyczynę incydentu?

Czy ustaliłeś skutki oddziaływania incydentu na twoje systemy informacyjne?

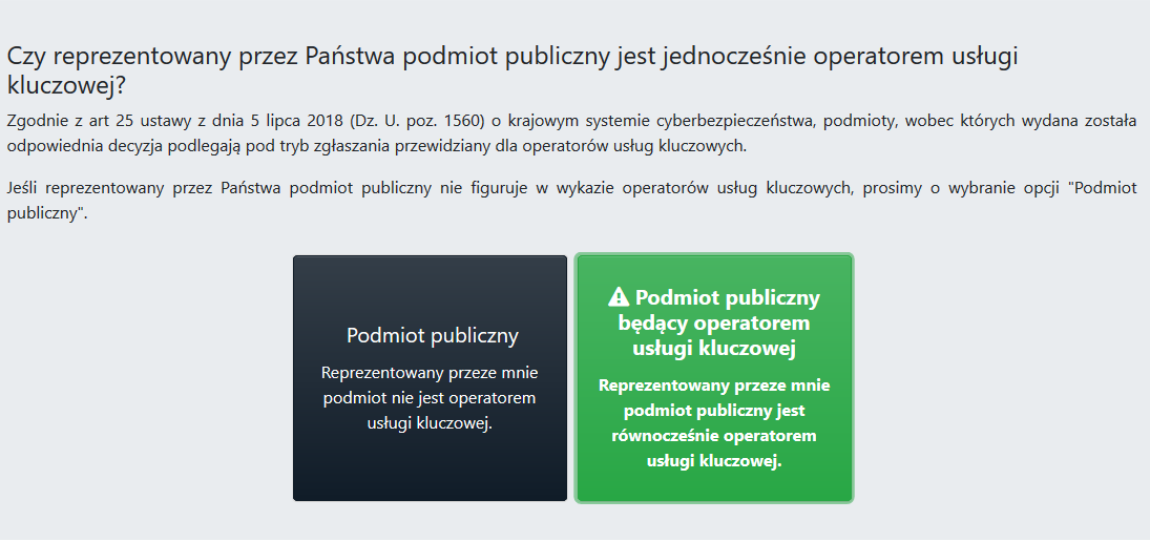
Opisz najdokładniej jak potrafisz przebieg incydentu



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

IV. Podmiot publiczny, który jest operatorem usługi kluczowej

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



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 incydentem lub też jego czas oddziaływania na świadczoną usługę. **Ważne:** Sprawdź kryteria dla twojego sektora: Rozporządzenie Rady Ministrów w sprawie progów uznania incydentu za poważny
2. **Inny incydent** - Jeśli incydent, który zgłaszasz nie spełnia kryteriów incydentu poważnego, wybierz opcję „incydent niesklasyfikowany jako poważny”.

a) Zgłaszanie incydentu poważnego przez operatora usługi kluczowej

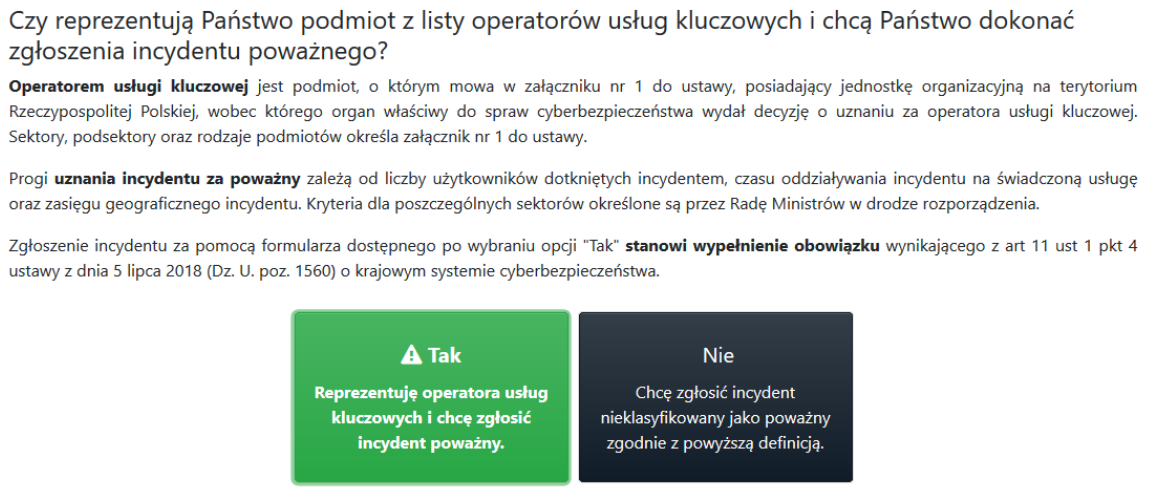
O incydencie poważnym możemy mówić w przypadku, gdy **samorząd jest jednocześnie operatorem usług kluczowej**. To, czy incydent jest uznawany za poważny, zależy np. od liczby użytkowników dotkniętych incydentem oraz czasu oddziaływania incydentu na świadczoną usługę.

Przykład: Miejskie przedsiębiorstwo wodno-kanalizacyjne może być jednocześnie podmiotem publicznym, a także znaleźć się w wykazie operatorów usług kluczowych – w tym wypadku organem właściwym będzie minister właściwy ds. gospodarki wodnej. Zaatakowany został system informatyczny, którego awaria sprawiła, że bez dostaw wody przez co najmniej 8 godzin znalazło się ponad 100 tys. użytkowników. Według kryteriów dla tego sektora, będzie to incydent poważny.

Przykład 2: Pełniący istotną rolę w regionie szpital, którego organem założycielskim jest samorząd, również może trafić na wykaz operatorów usług kluczowych – będzie nadzorowany przez ministra właściwego ds. zdrowia. Atak ransomware zablokował 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 tego sektora, będzie to incydent poważny.

Aby zgłosić incydent poważny:

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



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 incydentem.

Pamiętaj, że będziesz mógł dosłać 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 CERT Polska.

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 incydentu?

Czy możesz geograficznie określić obszar, którego dotyczy incydent?

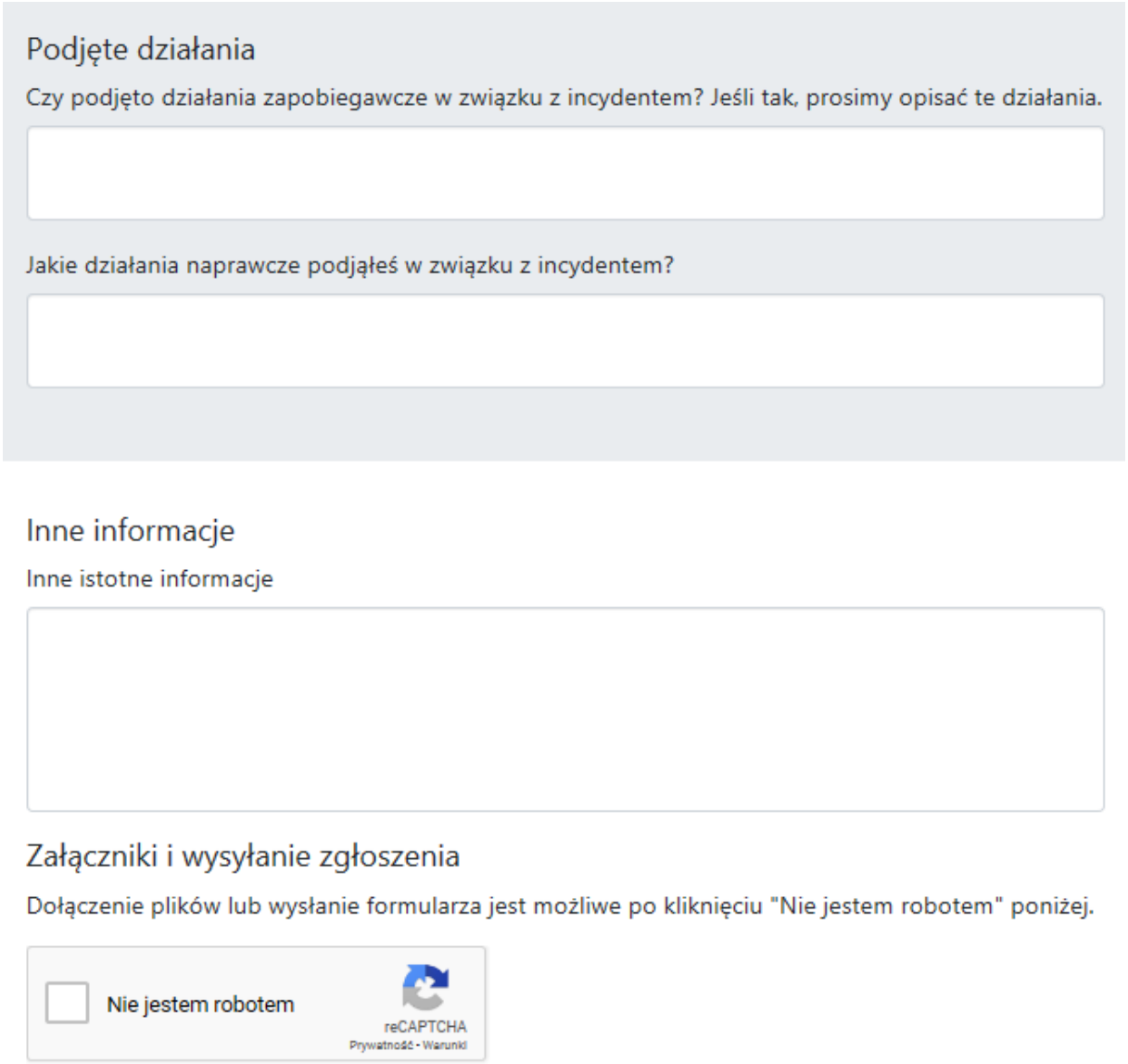
Czy incydent miał wpływ na świadczenie usługi kluczowej przez innych operatorów usług kluczowych i dostawców usług cyfrowych?

Czy ustaliłeś przyczynę incydentu?

Czy ustaliłeś skutki oddziaływania incydentu na twoje systemy informacyjne?

Opisz najdokładniej jak potrafisz przebieg incydentu

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



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 CERT Polska **każdy incydent cyberbezpieczeństwa**.

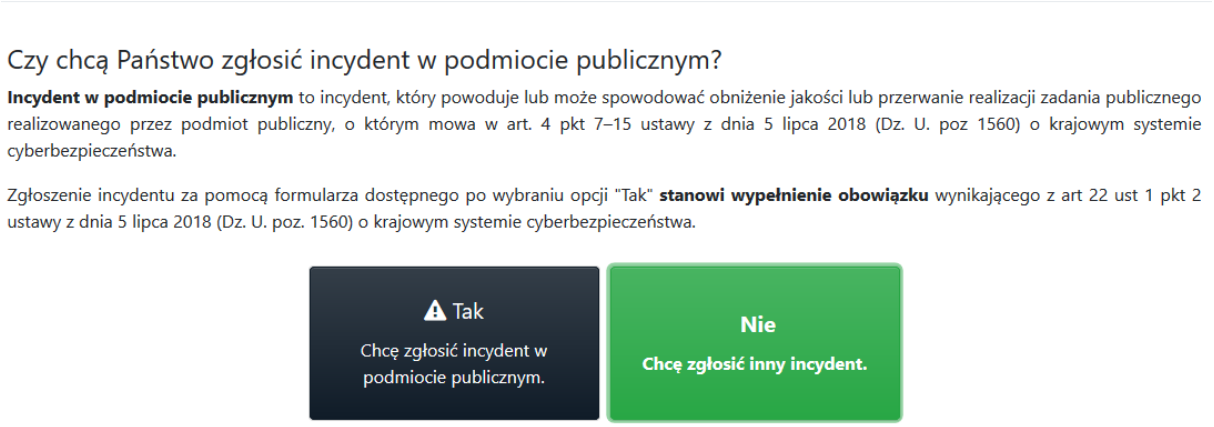
Dlaczego warto to robić?

- **Bo dzięki temu mamy więcej informacji na temat poziomu cyberbezpieczeństwa państwa. Możemy też lepiej szacować ryzyko i ostrzegać o potencjalnym zagrożeniu inne podmioty.**
- **Bo CERT Polska 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 CERT Polska**, 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”.



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

1. **Podejrzana 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, przekaż korespondencję i numer konta, na który miałeś przelać pieniądze. Jeśli zgłosiłeś sprawę policji, przekaż numer sprawy i podaj jednostkę, która ją prowadzi.
3. **Złośliwe oprogramowanie** - spakuj podejrzany pliku 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, 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.

Opracowali:

Rafał Babraj, Justyna Balcewicz, Magdalena Wrzosek.