Zgłaszanie incydentów przez operatorów usług kluczowych

Spis treści

I. Dlaczego i gdzie zgłaszać incydenty poważne

1. Dlaczego muszę zgłaszać incydenty cyberbezpieczeństwa?

Ponieważ od 2018 roku podmioty wyznaczone przez organy właściwe ds. cyberbezpieczeństwa jako operatorzy usług kluczowych, są częścią Krajowego Systemu Cyberbezpieczeństwa. Ustawa, która weszła w życie 28 sierpnia 2018 roku, nakłada na nie obowiązek raportowania incydentów poważnych.

2. Gdzie zgłosić incydent?

Prześlij zgłoszenie do **CERT Polska (CSIRT NASK)**, 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. Ostatecznie, 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** poważnego. 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 w nim poproszony. Jeśli w chwili zgłaszania incydentu czegoś nie wiesz, po prostu to napisz. Takie zgłoszenie incydentu poważnego również stanowi wypełnienie ustawowego obowiązku.

8. Czym jest incydent poważny?

O incydencie poważnym możemy mówić tylko w przypadku **operatora usługi kluczowej**. Jest to incydent, który powoduje lub może spowodować poważne obniżenie jakości lub przerwanie ciągłości świadczenia usługi kluczowej.

To, czy incydent jest klasyfikowany jako poważny, zależy np. od liczby użytkowników dotkniętych incydentem oraz czasu oddziaływania incydentu na świadczoną usługę. Kryteria dla poszczególnych sektorów określa rozporządzenie Rady Ministrów.

9. 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.

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

Twój podmiot 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].

11. Czy muszę zgłaszać incydent, który nie spełnia kryteriów incydentu poważnego?

Ustawa nie nakłada takiego obowiązku. Zachęcamy jednak do **zgłaszania wszystkich incydentów** cyberbezpieczeństwa, nawet tych, które zostały już rozwiązane. Przekazywane

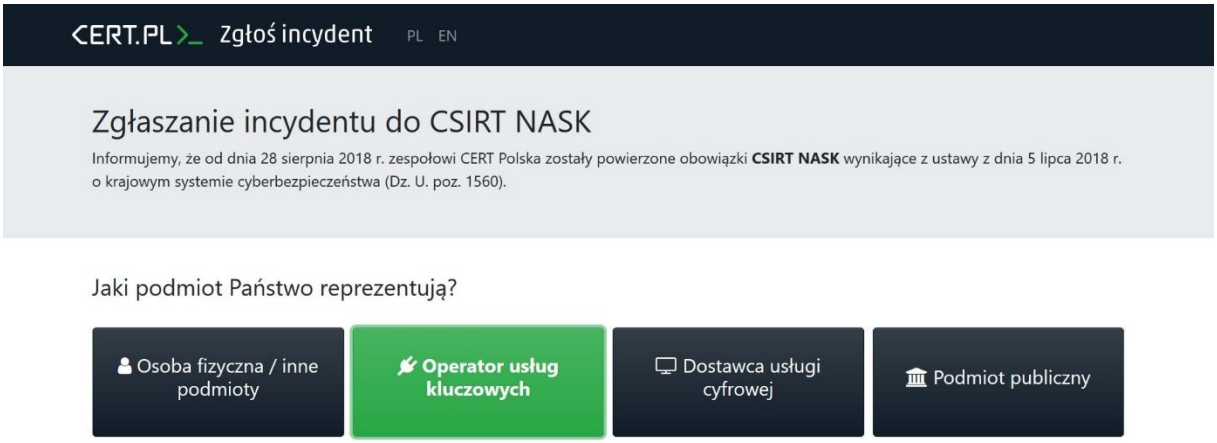
[1] Art. 12 pkt. 3 ustawa o krajowym systemie cyberbezpieczeństwa: „Operator usługi kluczowej przekazuje, w niezbędnym zakresie, w zgłoszeniu, o którym mowa w art. 11 ust. 1 pkt 4, informacje stanowiące tajemnice prawnie chronione, w tym stanowiące tajemnicę przedsiębiorstwa, gdy jest to konieczne do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

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

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. Jeśli organ właściwy ds. cyberbezpieczeństwa wyznaczył cię na operator usługi kluczowej, wybierz pole „**Operator usług kluczowych**" oznaczone ikonką wtyczki.



III. Operator usługi kluczowej – rodzaje incydentów

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

1. **Incydent poważny (obowiązek raportowania)** - 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 (zalecenie raportowania)** - Jeśli incydent, który zgłaszasz nie spełnia kryteriów incydentu poważnego, wybierz opcję „incydent niesklasyfikowany jako poważny".

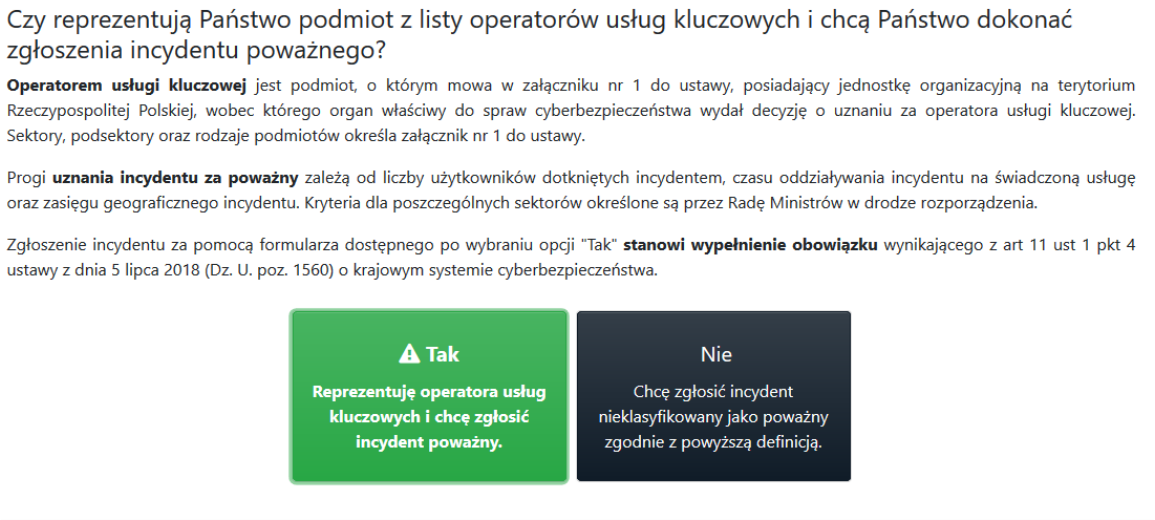
Przykład 1 – sektor energetyki: Dostawca ciepła może być operatorem usługi kluczowej – w tym wypadku organem właściwym będzie minister właściwy ds. energii. Zaatakowany został system informatyczny, którego awaria sprawiła, że przesyłanie ciepła było wstrzymane przez co najmniej 24 godziny. Jeśli w tej sytuacji straty finansowe firmy przekroczą 250 tys. zł lub incydent spowoduje np. ciężki uszczerbek na zdrowiu, to według kryteriów dla tego sektora, będzie to incydent poważny.

Przykład 2 – sektor ochrony zdrowia: Pełniący istotną rolę w regionie szpital również może być operatorem usługi kluczowej – w tym wypadku organem właściwym będzie minister właściwy 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.

a) Zgłaszanie incydentu poważnego przez operatora usługi kluczowej

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 incydent na świadczone usług kluczowe.
    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?

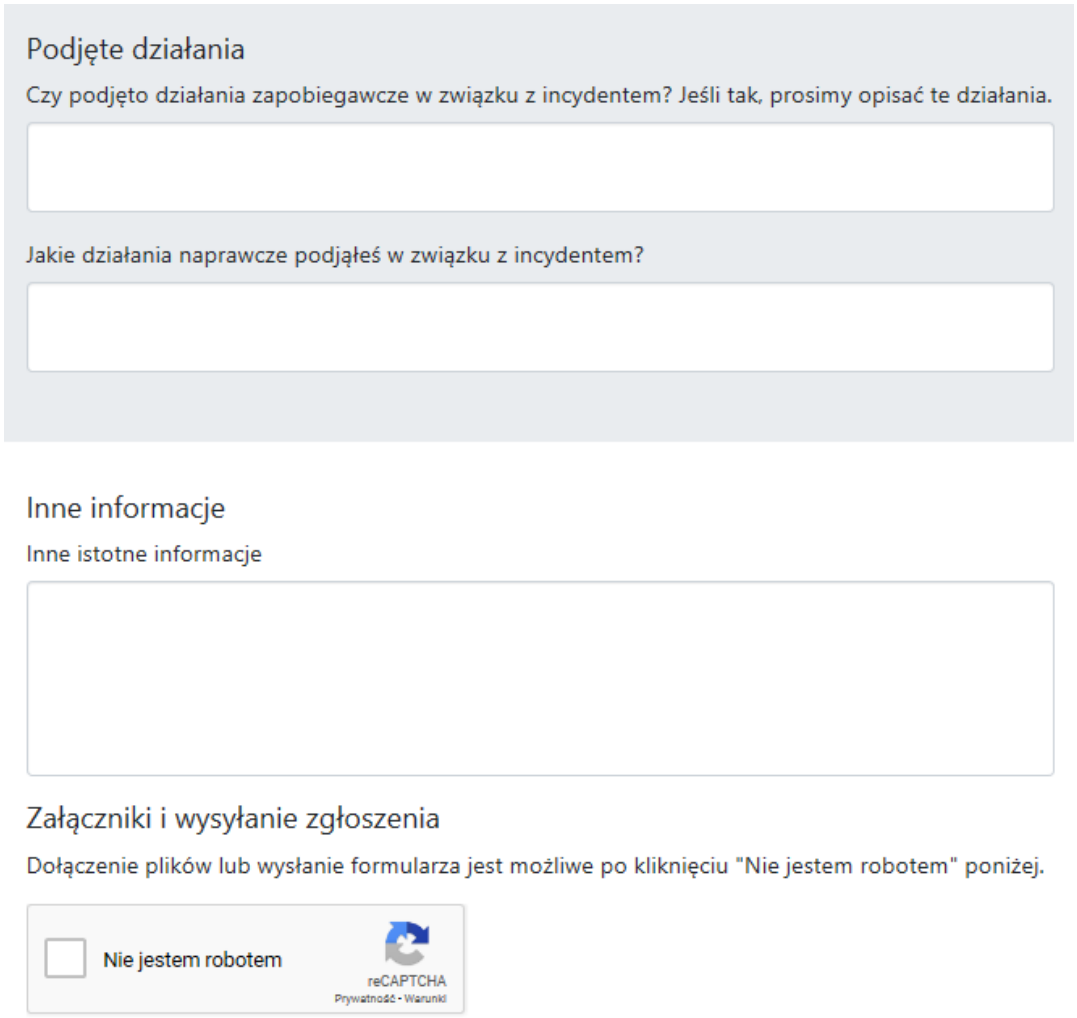
Czy incydent miał wpływ na świadczenie usługi kluczowej przez innych operatorów usług kluczowych i dostawców usług cyfrowych?

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.

IV. Zgłoszenie innego incydentu

Ważne! Pamiętaj, że możesz zgłosić do CERT Polska **każdy incydent cyberbezpieczeństwa**.

Dlaczego warto to robić?

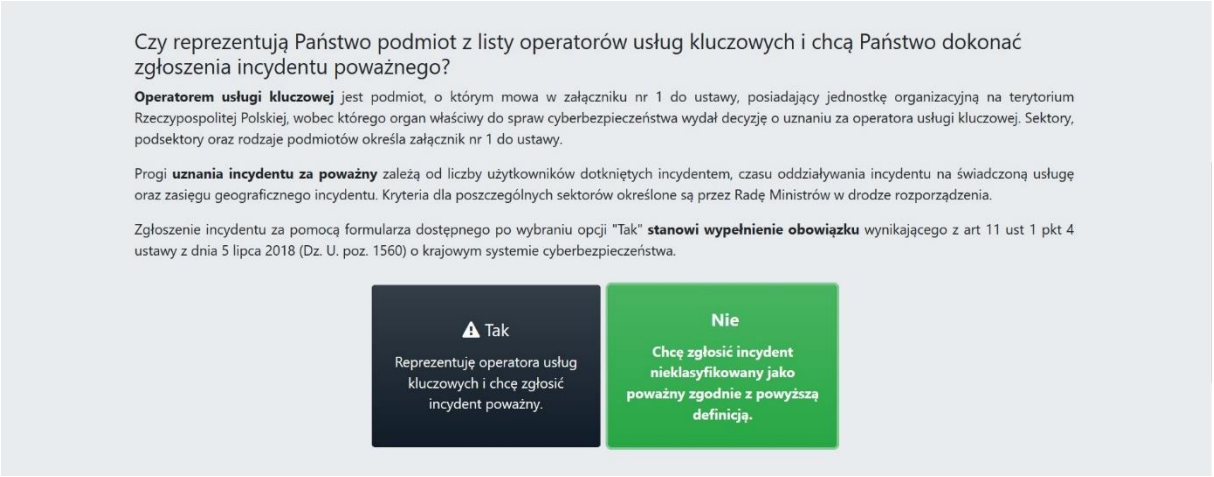
- **Bo dzięki temu mamy więcej informacji na temat poziomu cyberbezpieczeństwa państwa. Możemy też lepiej szacować ryzyko i ostrzegać o potencjalnym zagrożeniu inne podmioty.**
- **Bo CERT Polska analizuje każde zgłoszenie i jeśli okaże się, że to coś istotnego, zawsze uzyskasz od nas wsparcie merytoryczne.**

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.

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 incydent niesklasyfikowany jako poważny zgodnie z powyższą definicją".



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, Paweł Zegarow, Justyna Balcewicz, Magdalena Wrzosek