Formularz zgłaszania incydentów do CSIRT GOV

DANE PODMIOTU ZGŁASZAJĄCEGO

1. Nazwa podmiotu*
2. Adres*
3. Miejscowość*
4. Kod pocztowy*
5. NIP/REGON/KRS*

Należy podać ogólne dane zgłaszającego podmiotu. Dostarczone dane powinny być jednoznacznymi identyfikatorami podmiotu.

DANE OSOBY ZGŁASZAJĄCEJ INCYDENT

6. Imię i Nazwisko*
7. Stanowisko / Funkcja
8. e-mail*
9. nr. tel.* Dostępność ◯ 8-16 ◯ 8-22 ◯ 24h

DANE OSOBY UPRAWNIONEJ DO SKŁADANIA WYJAŚNIEŃ W SPRAWIE INCYDENTU

10. Imię i Nazwisko*
11. Stanowisko / Funkcja
12. e-mail*
13. nr. tel.* Dostępność ◯ 8-16 ◯ 8-22 ◯ 24h

OPIS INCYDENTU

14. Klasyfikacja incydentu*

◯ POWAŻNY ◯ ISTOTNY ◯ W PODMIOCIE PUBLICZNYM ◯ INNY

15. Czas trwania incydentu*
16. Data i godzina wykrycia incydentu*
17. Data i godzina wystąpienia incydentu*
18. Usługi kluczowe / usługi cyfrowe / zadania publiczne i systemy informacyjne, na które incydent miał wpływ*

* - Pola wymagane w przypadku incydentów dot. odpowiednio: usług kluczowych, usług cyfrowych i zadań publicznych.
Pola stanowiące tajemnice prawnie chronione, w tym stanowiące tajemnicę przedsiębiorstwa należy oznaczyć kwadratowymi nawiasami, na przykład: [PRZEKAZYWANA INFORMACJA].

Formularz zgłaszania incydentów do CSIRT GOV

19. Liczba osób, na które incydent miał wpływ*

- ◯ 1 – 50
- ◯ 51 – 100
- ◯ 101 – 200
- ◯ 201 – 300
- ◯ > 300
- ◯ Brak wpływu
- ◯ Brak danych

20. Czy incydent dotyczy innych państw członkowskich Unii Europejskiej? (należy podać jakich)*

21. Zasięg geograficzny obszaru, którego dotyczy incydent*

- ◯ Instytucja
- ◯ Polska
- ◯ Unia Europejska
- ◯ Świat
- ◯ Brak danych

22. Rodzaj zdarzenia*

- ◯ Celowe
- ◯ Niecelowe
- ◯ Brak danych

23. Skutki incydentu*

- ☐ Utrata dostępności danych / usług
- ☐ Utrata poufności danych / usług
- ☐ Utrata integralności danych / usług
- ☐ Inne

23.1 Dodatkowe informacje

24. Przebieg incydentu oraz możliwa przyczyna jego wystąpienia*

* - Pola wymagane w przypadku incydentów dot. odpowiednio: usług kluczowych, usług cyfrowych i zadań publicznych.
Pola stanowiące tajemnice prawnie chronione, w tym stanowiące tajemnicę przedsiębiorstwa należy oznaczyć kwadratowymi nawiasami, na przykład: [PRZEKAZYWANA INFORMACJA].

25. Kategoria zdarzenia

- [ ] Niepożądane treści | np. treści obraźliwe, dezinformacja, spam
- [ ] Oprogramowanie złośliwe | np. wirus, trojan, ransomware, dialer, botnet
- [ ] Zbieranie informacji | np. skanowanie, podsłuch, inżynieria społeczna
- [ ] Próby włamania | np. próby wykorzystania znanych błędów, próby logowania
- [ ] Włamanie | np. włamanie: na konto, do aplikacji, do systemu, do infrastruktury
- [ ] Utrata dostępności usługi | np. DoS, DDoS, sabotaż, awaria, zaniedbanie, prace techniczne
- [ ] Bezpieczeństwo informacji | np. nieuprawniony dostęp do informacji, nieuprawniona zmiana informacji, jej zastosowanie lub usunięcie
- [ ] Oszustwo | np. nieuprawnione wykorzystanie zasobów, naruszenie praw autorskich, podszywanie się, kradzież tożsamości, phishing
- [ ] Podatność | np. błędna konfiguracja, wykrycie podatności
- [ ] Cyberterroryzm | zdarzenie o charakterze terrorystycznym popełnione w cyberprzestrzeni
- [ ] Inne | zdarzenia niemieszczące się w powyższych kategoriach

26. Podjęte działania naprawcze*

27. Podjęte działania zapobiegawcze*

28. Inne istotne informacje

* - Pola wymagane w przypadku incydentów dot. odpowiednio: usług kluczowych, usług cyfrowych i zadań publicznych.
Pola stanowiące tajemnice prawnie chronione, w tym stanowiące tajemnicę przedsiębiorstwa należy oznaczyć kwadratowymi nawiasami, na przykład: [PRZEKAZYWANA INFORMACJA].

Formularz zgłaszania incydentów do CSIRT GOV

INFORMACJE DODATKOWE

WYPEŁNIĆ TYLKO W PRZYPADKU INCYDENTU DOTYCZĄCEGO USŁUGI KLUCZOWEJ

29. Czy incydent miał wpływ na świadczenie usługi kluczowej przez innych Operatorów Usług Kluczowych i/lub Dostawców Usług Cyfrowych (należy opisać w przypadku odpowiedzi twierdzącej)*

WYPEŁNIĆ TYLKO W PRZYPADKU INCYDENTU DOTYCZĄCEGO USŁUGI CYFROWEJ

30. Zakres wpływu incydentu istotnego na działalność gospodarczą i społeczną*

31. Źródło incydentu istotnego*

32. Zakres zakłócenia funkcjonowania usługi cyfrowej*

WYPEŁNIĆ TYLKO W PRZYPADKU INCYDENTU DOTYCZĄCEGO ZADANIA PUBLICZNEGO

33. Źródło incydentu w podmiocie publicznym*

PRZESŁANIE FORMULARZA

Wypełniony formularz należy wysłać w postaci załącznika do wiadomości e-mail na adres:
incydent@csirt.gov.pl

W przypadku braku możliwości przekazania incydentu w postaci elektronicznej incydent należy zgłosić poprzez przesłanie wypełnionego formularza incydentu faksem na numer: **+48-22-58-58-833**

---

* - Pola wymagane w przypadku incydentów dot. odpowiednio: usług kluczowych, usług cyfrowych i zadań publicznych.
Pola stanowiące tajemnice prawnie chronione, w tym stanowiące tajemnicę przedsiębiorstwa należy oznaczyć kwadratowymi nawiasami, na przykład: [PRZEKAZYWANA INFORMACJA].