

## DANE ADRESOWE

1. Nazwa instytucji / firmy\*
2. Adres\*
3. Kod pocztowy
4. Miasto\*
5. NIP

## ZGŁASZAJĄCY INCYDENT

6. Imię i Nazwisko\*
7. Stanowisko\*
8. tel. \*

dostępność	8-16	8-22
	24h	
9. e-mail\*

## OSOBA UPRAWNIONA DO SKŁADANIA WYJAŚNIENI W SPRAWIE INCYDENTU

10. Imię i Nazwisko\*
11. Stanowisko\*
12. tel. \*

dostępność	8-16	8-22
	24h	
13. e-mail\*

## OPIS INCYDENTU

14. Data wystąpienia incydentu\*

Czas trwania incydentu
------------------------
15. Data wykrycia incydentu\*
16. Pola stanowiące tajemnice prawnie chronione, w tym stanowiące tajemnicę przedsiębiorstwa (podaj nr pól po przecinku lub w przedziale np. 4. - 8.)
17. Zadanie publiczne na które incydent miał wpływ\*
18. liczba osób, na które incydent miał wpływ\*

1 - 50	51 - 100	101 - 200
201 - 300	> 300	Brak danych
19. Zasięg geograficzny obszaru, którego dotyczy incydent\*

Instytucja	Polska	Unia Europejska
Świat	Brak danych	

20. Rodzaj działania*	Celowe	Niecelowe
21. Kategoria zdarzenia*	<p>Treści obraźliwe   np. obrażanie, pornografia dziecięca, przemoc</p> <p>Oprogramowanie złośliwe   np. wirus, trojan, ransomware, dialer, botnet</p> <p>Zbieranie informacji   np. skanowanie, podsłuch, SPAM, inżynieria społeczna</p> <p>Próby włamania   np. próby wykorzystania znanych błędów, próby logowania</p> <p>Włamanie   np. włamanie na konto, do aplikacji, do systemu, do infrastruktury</p> <p>Utrata dostępności usługi   np. DoS, DDoS, sabotaż, awaria, zaniedbanie, prace techniczne</p> <p>Bezpieczeństwo informacji   np. nieuprawniony dostęp do informacji, nieuprawniona zmiana informacji lub jej skasowanie</p> <p>Oszustwo   np. nieuprawnione wykorzystanie zasobów, naruszenie praw autorski, podszywanie się, kradzież tożsamości, phishing</p> <p>Podatność   np. błędna konfiguracja, wykrycie podatności</p> <p>Cyberterroryzm   zdarzenie o charakterze terrorystycznym popełnione w cyberprzestrzeni</p> <p>Inne   zdarzenia niemieszczące się w powyższych kategoriach</p> <p>Test   kategoria ćwiczebna</p>	

22. Skutki incydentu*	<p>utrata dostępności danych / usługi</p> <p>utrata poufności danych / usługi</p> <p>utrata integralności danych / usługi</p> <p>próba infekcji oprogramowaniem złośliwym</p> <p>próba uzyskania nieuprawnionego dostępu</p> <p>inne</p>
-----------------------	--

dodatkowe informacje

23. Przebieg incydentu oraz  
możliwa przyczyna jego  
wystąpienia\*

24. Podjęte działania  
zapobiegawcze\*

25. Podjęte działania  
naprawcze\*

26. Inne istotne informacje

---

Wypełniony formularz należy wysłać w postaci załącznika do wiadomości e-mail na  
adres: [csirt@knf.gov.pl](mailto:csirt@knf.gov.pl) Pola oznaczone\* są polami wymaganymi.