

**FORMULARZ ZGŁOSZENIA INCYDENTU CSIRT MON**

Formularz pozwala na edycję i zapisanie treści w oprogramowaniu obsługującym zawartość interaktywną

**DANE ADRESOWE**

1. Nazwa instytucji / firmy\*

2. Adres\*

3. Kod pocztowy

4. Miasto\*

5. REGON / NIP / KRS

**ZGŁASZAJĄCY INCYDENT**

6. Imię i nazwisko\*

7. Stanowisko\*

8. Tel.\*

dostępność

☐

8-16

☐

8-22

☐

24h

9. E-mail\*

**OSOBA UPRAWNIONA DO SKŁADANIA WYJAŚNIEŃ 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\*.

15. Czas trwania incydentu

[m, h, dni, m-ce, lata]\*

16. Data wykrycia incydentu\*.

17. Zadanie publiczne, na które incydent miał wpływ\*.

18. Usługi kluczowe, na które incydent miał wpływ\*.

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

20. Liczba osób, na które incydent miał wpływ\*.

☐

1-50

☐

51-100

☐

101-200

☐

201-300

☐

>300

☐

Brak danych

21. Zasięg geograficzny obszaru, którego dotyczy incydent\*.

☐

Instytucja

☐

Polska

☐

Unia Europejska

☐

Świat

☐

Brak danych

22. Rodzaj działania\*.

☐

Celowe

☐

Niecelowe

☐

Brak danych

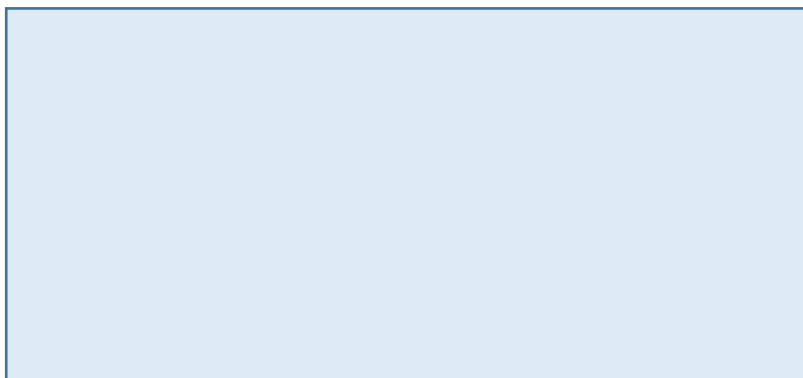
23. Kategoria zdarzenia  
(proszę zaznaczyć  
wszystkie właściwe  
pola)\*.

- ☐ Złośliwe oprogramowanie | np.: Wirus, trojan, ransomware, dialer, botnet
- ☐ Przelamywanie zabezpieczeń | np.: Włamanie na konto, do aplikacji, do systemu, do infrastruktury
- ☐ Niepożądane treści | np.: Treści obraźliwe, spam
- ☐ Gromadzenie informacji | np.: Skanowanie, podsłuch, inżynieria społeczna
- ☐ Dostępność zasobów | np.: Utrata dostępności usługi, DoS, DDoS, sabotaż, awaria, zaniedbanie
- ☐ Bezpieczeństwo informacji | np.: Nieuprawniony dostęp do informacji, nieuprawniona zmiana informacji lub jej usunięcie
- ☐ Naruszenie przepisów prawa | np.: Obrażanie, pornografia dziecięca, przemoc, działania noszące znamiona ataku terrorystycznego w cyberprzestrzeni, rozpowszechnianie plików niezgodnie z klauzulami tajności
- ☐ Inne | np.: Awarie, inne incydenty komputerowe.
- ☐ Zgłoszenie podatności | np.: Błędna konfiguracja, wykrycie podatności, zagrożenia

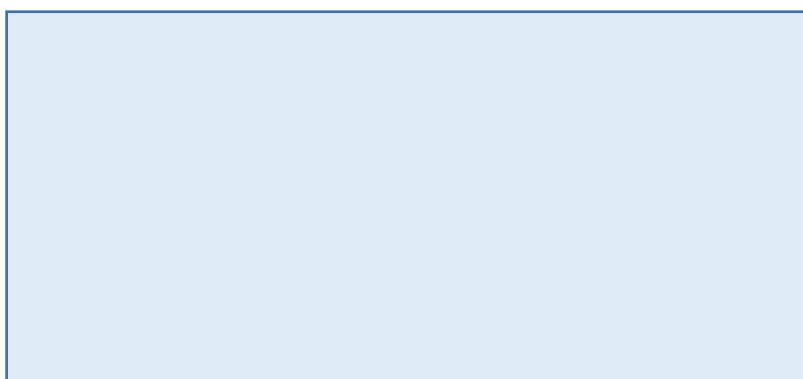
24. Skutki incydentu\*.

- ☐ Utrata dostępności danych / usług
- ☐ Utrata poufności danych / usług
- ☐ Utrata integralności danych / usług
- ☐ Podejrzenie infekcji oprogramowaniem złośliwym
- ☐ Podejrzenie możliwości uzyskania nieuprawnionego dostępu
- ☐ Inne

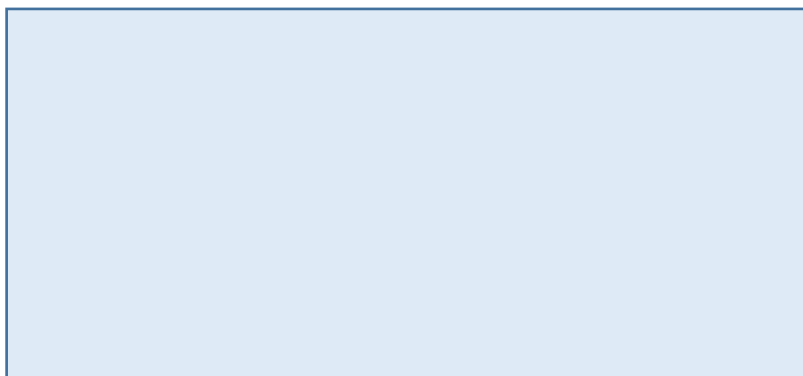
Dodatkowe informacje.



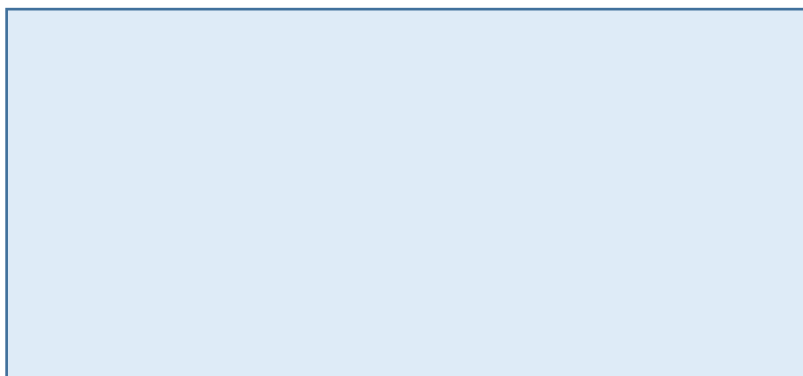
25. Przebieg incydentu  
oraz możliwa przyczyna  
jego wystąpienia\*.



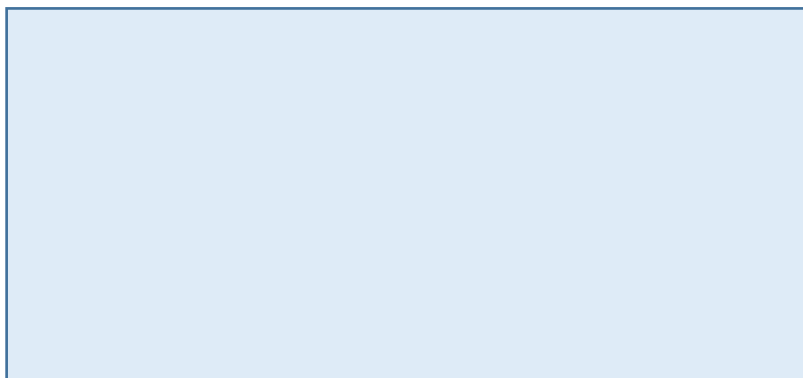
26. Podjęte działania  
zapobiegawcze\*.



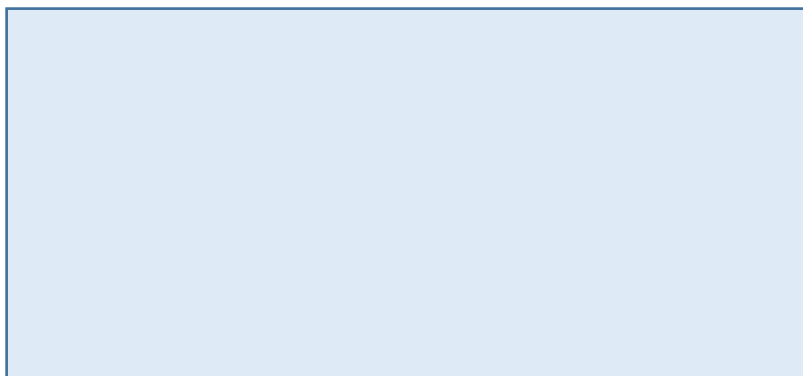
27. Podjęte działania  
naprawcze\*.



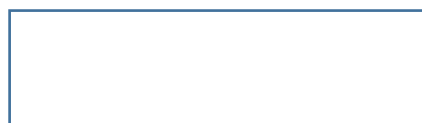
28. Inne istotne informacje.



29. Wymień numery pól zawierających tajemnice prawnie chronione oddzielając je przecinkami.



30. Data i podpis (pieczęć) osoby zgłaszającej (w przypadku przekazania wydruku lub jego skanu).



\* Pola wymagane

Pola nr 18. - 19. wypełniają wyłącznie operatorzy usług kluczowych

---

## Instrukcja przekazania formularza do CSIRT MON:

### INCYDENT W SYSTEMIE JAWNYM:

Niniejszy formularz należy przesłać na podany poniżej adres e-mail:

[csirt-mon@ron.mil.pl](mailto:csirt-mon@ron.mil.pl)

### INCYDENT W SYSTEMIE NIEJAWNYM:

Incydenty w systemach NIEJAWNYCH należy zgłaszać zgodnie z zapisami dokumentacji bezpieczeństwa systemu w którym stwierdzono incydent komputerowy, wyłącznie poprzez NIEJAWNE, dedykowane kanały komunikacji.