FORMULARZ ZGŁOSZENIA INCYDENTU CSIRT MON

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

DANE ADRESOWE

1. Nazwa instytucji / firmy*: Uniwersytet Warmińsko-Mazurski w Olsztynie

2. Adres*: ul. Oczapowskiego 9

3. Kod pocztowy: 10-900

4. Miasto*: Olsztyn

5. REGON / NIP / KRS:

ZGŁASZAJĄCY INCYDENT

6. Imię i nazwisko*: Kasia Basia

7. Stanowisko*: Pracownik UWM

8. Tel.*: 123-456-789

dostępność ○ 8-16 ○ 8-22 ◉ 24h

9. E-mail*: kasia.basia22@o2.pl

OSOBA UPRAWNIONA DO SKŁADANIA WYJAŚNIEŃ W SPRAWIE INCYDENTU

10. Imię i nazwisko*: Asia Basia

11. Stanowisko*: Pracownik UWM

12. Tel.*: 987-654-321

dostępność ○ 8-16 ○ 8-22 ◉ 24h

13. E-mail*: asia.basia89@gmail.com

OPIS INCYDENTU

14. Data wystąpienia incydentu*.: 12:30

15. Czas trwania incydentu [m, h, dni, m-ce, lata]*: 2 h

16. Data wykrycia incydentu*.: 12:45

17. Zadanie publiczne, na które incydent miał wpływ*.	Szkolnictwo.
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
- [x] Przełamywanie zabezpieczeń | np.: Włamanie na konto, do aplikacji, do systemu, do infrastruktury
- [x] Niepożądane treści | np.: Treści obraźliwe, spam
- [ ] Gromadzenie informacji | np.: Skanowanie, podsłuch, inżynieria społeczna
- [ ] Dostępność zasobów | np.: Utrata dostępności usługi, DoS, DDoS, sabotaż, awaria, zaniedbanie
- [x] 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
- [x] Utrata poufności danych / usług
- [ ] Utrata integralności danych / usług
- [ ] Podejrzenie infekcji oprogramowaniem złośliwym
- [x] Podejrzenie możliwości uzyskania nieuprawnionego dostępu
- [ ] Inne

Dodatkowe informacje.	
25. Przebieg incydentu oraz możliwa przyczyna jego wystąpienia*.	Otrzymałam wiadomość e-mail z adresu podszywającego się pod MBank. Wiadomość zawierała link prowadzący do fałszywej strony logowania oraz prośbę o podanie danych dostępowych. W treści pojawiły się błędy językowe oraz fałszywy numer telefonu kontaktowego. W link nie kliknęłam i nie wprowadziłam danych.
26. Podjęte działania zapobiegawcze*.	Szkolenia pracowników i edukacja, ANTYWIRUSY.
27. Podjęte działania naprawcze*.	Sprawdzono system pod kątem złośliwego oprogramowania, przeanalizowano aktywność konta e-mail, zmieniono hasła w systemach, zablokowano dostęp nadawcy phishingu oraz przywrócono normalne funkcjonowanie konta

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

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.