FAQ - NAJCZĘŚCIEJ ZADAWANE PYTANIA

---

1. Co to jest CSIRT GOV?

CSIRT GOV – jest jednym z trzech krajowych Zespołów Reagowania na Incydenty Bezpieczeństwa Komputerowego wraz z CSIRT MON oraz CSIRT NASK. Zespół został powołany w dniu 1 lutego 2008 roku na mocy porozumienia Ministra Spraw Wewnętrznych i Administracji oraz Szefa Agencji Bezpieczeństwa Wewnętrznego i do wejścia w życie ustawy z dnia 5 lipca 2018 r. funkcjonował jako CERT.GOV.PL tj. Rządowy Zespół Reagowania na Incydenty Komputerowe.

2. Jakie są zadania CSIRT GOV?

Do wybranych podstawowych zadań CSIRT GOV należy:

- monitorowanie zagrożeń cyberbezpieczeństwa i incydentów na poziomie krajowym;
- szacowanie ryzyka związanego z ujawnionym zagrożeniem cyberbezpieczeństwa oraz zaistniałymi incydentami,w tym prowadzenie dynamicznej analizy ryzyka;
- przekazywanie informacji dotyczących incydentów i ryzyk podmiotom krajowego systemu cyberbezpieczeństwa;
- wydawanie komunikatów o zidentyfikowanych zagrożeniach cyberbezpieczeństwa;
- reagowanie na zgłoszone incydenty;
- prowadzenie i koordynacja systemu wczesnego ostrzegania o zagrożeniach występujących w sieci Internet;
- przeprowadzanie oceny bezpieczeństwa systemów teleinformatycznych.

3. Jaki jest obszar działania CSIRT GOV?

Obszarem działania CSIRT GOV oraz podstawowymi „odbiorcami” usług (ang. constituency) oferowanych przez zespół są użytkownicy systemów teleinformatycznych:
1) Jednostek sektora finansów publicznych, o których mowa w art. 9 pkt 1, 8 i 9 ustawy z dnia 27 sierpnia 2009 r. o finansach publicznych, z wyjątkiem wymienionych w ust. 5 i 6;
2) jednostki podległe Prezesowi Rady Ministrów lub przez niego nadzorowane;
3) Narodowy Bank Polski;
4) Bank Gospodarstwa Krajowego;
5) Systemy sieci teleinformatycznych objętych jednolitym wykazem obiektów, instalacji, urządzeń i usług wchodzących w skład infrastruktury krytycznej, a także systemy teleinformatyczne właścicieli i posiadaczy obiektów, instalacji lub urządzeń infrastruktury krytycznej, o których mowa w art. 5b ust. 7 pkt 1 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym.

4. Co można zgłaszać do CSIRT GOV?

Do zespołu CSIRT GOV należy zgłaszać zdarzenia, które mają lub mogą mieć niekorzystny wpływ na działania naruszające poufność, integralność, dostępność autentyczność przetwarzanych danych lub związanych z nimi usług oferowanych przez systemypodmiotów, o których mowa w art. 26 ust 7 ustawy z dnia 5 lipca 2018 roku o krajowym systemie cyberbezpieczeństwa)a także na systemy sieci teleinformatycznych objętych jednolitym wykazem obiektów, instalacji, urządzeń i usług wchodzących w skład infrastruktury krytycznej, a także systemy teleinformatyczne właścicieli i posiadaczy obiektów, instalacji lub urządzeń infrastruktury krytycznej, o których mowa w art. 5b ust. 7 pkt 1 ustawy z dnia 26 kwietnia 2007 r. o zarządzaniu kryzysowym.

5. Po co zgłaszać incydenty do CSIRT GOV?

Każdy zgłoszony incydent przyczynia się do poprawy bezpieczeństwa teleinformatycznego. Przesyłając zgłoszenia o incydentach do CSIRT GOV dostarczane są informacje, które można wykorzystać wiążąc je z innymi zgłoszeniami z całego świata dla lepszego wsparcia ze strony zespołu oraz podwyższenia świadomości innych użytkowników Internetu.
W miarę dostępności zasobów CSIRT GOV służy wsparciem i pomocą m. in. w odnalezieniu źródła incydentu, skierowaniu informacji bezpośrednio do innych miejsc zaangażowanych w incydent, dostarczeniu wskazówek odnośnie poprawy bezpieczeństwa systemu komputerowego.

6. Jak zgłaszać incydenty do CSIRT GOV?

Zgłaszać incydenty teleinformatyczne do CSIRT GOV mogą podmioty wskazane w art. 26 ust 7 ustawy z dnia 5 lipca 2018 r. o krajowym systemie cyberbezpieczeństwa poprzez wypełnienie formularza dostępnego na stronie:
www.csirt.gov.pl w zakładce zgłaszanie incydentu oraz przesłania:
- E-mailem na adres: {mailto(incydent@csirt.gov.pl,encode = secure)}

W celu zachowania poufności przesyłanych danych można w kontaktach z CSIRT GOV używać szyfrowania przesyłek elektronicznych. Do tego celu używać można systemu PGP/GPG. Aktualnie obowiązujący klucz publiczny PGP zespołu CSIRT GOV dostępny jest na stronie www.csirt.gov.pl w zakładce klucz PGP,
W przypadku braku możliwości dokonania zgłoszenia albo przekazania ich w postaci elektronicznej zgłosić incydent można poprzez przesłanie wypełnionego formularza:
- Faksem na numer: +48 22 58 58 833,

Lub
- Pocztą tradycyjną na adres:

CSIRT GOV
Ul. Rakowiecka 2A

00-993 Warszawa

W przypadku konieczności pilnego kontaktu prosimy o kontakt telefoniczny do Dyżurnego CSIRT GOV pod nr +48 22 58 59 373.

7. Jak zapewnić poufności przesyłanych informacji?

Aby zapewnić poufność przesyłanych informacji zalecamy skorzystanie z szyfrowania PGP/GPG (standard ten jest używany przez wszystkie zespoły CSIRT na świecie). Oprogramowanie wspomagające szyfrowanie PGP dostępne jest za darmo dla celów niekomercyjnych, na praktycznie wszystkie platformy sprzętowe. Do wysłania zaszyfrowanej wiadomości potrzebny będzie klucz publiczny CSIRT GOV, który dostępny jest w zakładce klucz PGP.

8. Czy będę poinformowany o przebiegu zgłoszonej sprawy?
Zgłaszający incydent będzie oczywiście informowany o przebiegu sprawy. CSIRT GOV zwraca się również do osoby zgłaszającej incydent, jeżeli potrzebne jest uzupełnienie informacji związanych z incydentem. W przypadku, gdy CSIRT GOV nie jest właściwy do koordynacji obsługi zgłoszonego incydentu, zgłoszenie niezwłocznie jest przekazywane do właściwego CSIRT wraz z otrzymanymi informacjami, jednocześnie informując o tym fakcie osobę zgłaszającą.

9. Gdzie są wykorzystwane dane o zgłoszeniu?

Dane osobowe CSIRT GOV przechowuje i przetwarzaw sposób zgodny z wymogami obowiązującego prawa.
Dane odnośnie zgłoszenia wykorzystywane są główne w sposób zbiorczy w statystykach i raportach pokazujących stan bezpieczeństwa w cyberprzestrzeni. Nie są publikowane informacje, które mogłyby wskazywać lub pomóc ustalić poszkodowanego.

10. Jak zgłosić osoby wyznaczone do kontaktów z CSIRT GOV?

Wyznaczone osoby do kontaktów z CSIRT GOV należy zgłosić poprzez wypełnienie formularza dostępnego na stronie www.csirt.gov.pl w zakładce zgłoszenie osób do kontaktów z CISRT GOV i przesłanie go na adres {mailto(incydent@csirt.gov.pl,encode = secure)} wpisując w temacie wiadomości:

<formularz zgłoszenia osób wyznaczonych do kontaktów z CSIRT GOV + skrócona nazwa instytucji>, której zgłoszenie dotyczy.