CERT.GOV.PL

http://cert.gov.pl/cer/faq/22,FAQ-NAJCZESCIEJ-ZADAWANE-PYTANIA.html
2018-06-20, 14:50

FAQ - NAJCZĘŚCIEJ ZADAWANE PYTANIA

1.Co to jest CERT.GOV.PL?
2.Jaka jest misja zespołu CERT.GOV.PL?
3.Jakie są zadania CERT.GOV.PL?
4.Jaki jest obszar działania CERT.GOV.PL?
5.Kto finansuje działalność zespołu?
6.Jak skontaktować się z CERT.GOV.PL?
7.Co można zgłaszać do CERT.GOV.PL?
8.Po co zgłaszać incydenty?
9.Jak zgłaszać incydenty?
10.Jak zapewnić poufność przesyłanych informacji?
11.Czy będę poinformowany o przebiegu zgłoszonej sprawy?
12.Gdzie są wykorzystywane dane o zgłoszeniu?

---

1. Co to jest CERT.GOV.PL?
CERT.GOV.PL – jest Rządowym Zespołem Reagowania na Incydenty Komputerowe. Zespół został powołany w dniu 1 lutego 2008 roku na mocy porozumienia Ministra Spraw Wewnętrznych i Administracji oraz Szefa Agencji Bezpieczeństwa Wewnętrznego.

2. Jaka jest misja zespołu CERT.GOV.PL?
Misją zespołu jest zapewnianie i rozwijanie zdolności jednostek organizacyjnych administracji publicznej Rzeczypospolitej Polskiej do ochrony przed cyberzagrożeniami, ze szczególnym uwzględnieniem ataków ukierunkowanych na infrastrukturę obejmującą systemy i sieci teleinformatyczne, których zniszczenie lub zakłócenie może stanowić zagrożenie dla życia, zdrowia ludzi, dziedzictwa narodowego oraz środowiska w znacznych rozmiarach, albo spowodować poważne straty materialne, a także zakłócić funkcjonowanie państwa.

3. Jakie są zadania CERT.GOV.PL?

Do podstawowych zadań CERT.GOV.PL należy:

- koordynacja reagowania na incydenty
- publikacja alertów i ostrzeżeń
- obsługa i analiza incydentów (w tym gromadzenie dowodów realizowane przez zespół biegłych sądowych)
- publikacja powiadomień (biuletynów zabezpieczeń)
- koordynacja reagowania na luki w zabezpieczeniach
- obsługa zdarzeń w sieciach objętych ochroną przez system ARAKIS-GOV
- przeprowadzanie testów bezpieczeństwa

Więcej informacji dotyczącej działalności zespołu dostępna jest w menu O Nas.

4. Jaki jest obszar działania CERT.GOV.PL?
Obszarem działania CERT.GOV.PL oraz podstawowymi „odbiorcami" usług (ang. constituency) oferowanych przez zespół są użytkownicy systemów teleinformatycznych administracji państwowej (domena *.gov.pl), a także podmioty należące do tzw. krytycznej infrastruktury teleinformatycznej państwa.

5. Kto finansuje działalność zespołu?
CERT.GOV.PL jest zespołem działającym w strukturze Departamentu Bezpieczeństwa Teleinformatycznego ABW i jest finansowany z budżetu państwa.

6. Jak skontaktować się z CERT.GOV.PL?
Preferowanym sposobem kontaktu z CERT.GOV.PL jest wysłanie maila na adres cert@cert.gov.pl . Pozostałymi kanałami komunikacji z CERT.GOV.PL jest telefon, faks oraz poczta tradycyjna. Pełne dane kontaktowe znajdziesz tutaj.

7. Co można zgłaszać do CERT.GOV.PL?

Do zespołu CERT.GOV.PL należy zgłaszać informacje dotyczące wszelkich działań zagrażających i/lub naruszających bezpieczeństwo sieciowe systemów teleinformatycznych w domenie gov.pl a także podmiotów należących do tzw. krytycznej infrastruktury teleinformatycznej państwa. Każdy przypadek nadużycia będzie traktowany z należytą powagą. W szczególności zajmujemy się zdarzeniami dotyczącymi:
• włamań lub prób włamań
• ograniczania dostępności zasobów sieciowych (np. ataki typu DoS - denial of service)
• działań z użyciem złośliwych kodów (np. rozsyłanie wirusów)
• skanowania
• innych ważnych przypadków naruszenia bezpieczeństwa teleinformatycznego

8. Po co zgłaszać incydenty?
Każdy zgłoszony incydent przyczynia się do poprawy bezpieczeństwa teleinformatycznego. Przesyłając zgłoszenia o incydentach do CERT.GOV.PL dostarczasz nam wielu informacji, które możemy 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 służymy 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.

9. Jak zgłaszać incydenty?
Incydenty należy zgłaszać na adres cert@cert.gov.pl poprzez wypełnienie i wysłanie formularza znajdującego się na stronie. W celu zachowania poufności przesyłanych danych należy w kontaktach z CERT.GOV.PL szyfrować przesyłki korzystając w opublikowanego na witrynie klucza PGP.
W przypadku braku dostępu do poczty elektronicznej prosimy dzwonić pod numer:
+48 22 58 59 373,
lub skorzystać z faksu
+48 22 58 58 833

10. Jak zapewnić poufność przesyłanych informacji?
Aby zapewnić poufność przesyłanych informacji zalecamy skorzystanie z szyfrowania PGP/GPG (standard ten jest używany przez wszystkie zespoły CERT 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 CERT.GOV.PL, który dostępny jest tutaj.

11. Czy będę poinformowany o przebiegu zgłoszonej sprawy?
Jeśli zgłoszony incydent dotyczy bezpośrednio zainteresowanej osoby to jak najbardziej informujemy o przebiegu sprawy. Zwracamy się również do osoby zgłaszającej incydent, jeżeli potrzebujemy dalszych informacji związanych z incydentem.
W większości przypadków sprawę uważamy za rozwiązaną, po przekazaniu informacji do właściwej osoby lub instytucji zaangażowanej w incydent (np. innego zespołu w kraju lub zagranicą) W związku z powyższym należy zauważyć, że brak reakcji na zgłoszony incydent nie świadczy o tym, że nie zajmujemy się nim.

12. Gdzie są wykorzystywane dane o zgłoszeniu?
Dane osobowe przechowujemy i przetwarzamy w sposób zgodny z wymogami prawa polskiego, a w szczególności w zgodzie z ustawą o ochronie danych osobowych. Nie przekazujemy i nie użyczamy zgromadzonych danych osobowych użytkowników innym osobom lub instytucjom. Dane osobowe znajdujące się w posiadaniu CERT.GOV.PL są objęte ochroną.
Dane odnośnie zgłoszenia wykorzystywane są tylko w sposób zbiorczy w statystykach i raportach pokazujących stan bezpieczeństwa w polskich instytucjach. Nie są publikowane informacje, które mogłyby wskazywać lub pomóc ustalić poszkodowanego.