Zgłaszanie incydentów

Sposoby zgłaszania incydentów bezpieczeństwa

csirt
Centrum e-Zdrowia

Centrum e-Zdrowia

Spis treści

I. Sposób zgłaszania incydentów

01. W przypadku incydentu poważnego należy:

- zgłosić incydent bezpieczeństwa niezwłocznie, nie później niż w ciągu 24 godzin od momentu wykrycia do sektorowego zespołu CSIRT w Centrum e-Zdrowia (CSIRT CeZ) i właściwego CSIRT poziomu krajowego, ustalonym kanałem komunikacyjnym:
  - w przypadku możliwości wykorzystania systemu S46, należy z niego skorzystać,
  - za pomocą dedykowanego formularza kontaktowego dostępnego na stronie cez.gov.pl,
  - w przypadku niedostępności formularza lub braku potwierdzenia przyjęcia zgłoszenia - za pośrednictwem poczty elektronicznej (incydent@csirt.cez.gov.pl) lub telefonicznie (**+48 573 205 962**).
- prawidłowe wpłynięcie do CSIRT CeZ e-maila zgłoszeniowego potwierdzane jest automatycznie drogą mailową z adresu incydent@csirt.cez.gov.pl. Wyjątkiem jest zgłoszenie incydentu za pomocą systemu S46,
- w przypadku stwierdzenia zdarzenia typu false-positive, zgłaszający informowany jest o wyniku analizy, a zgłoszenie jest zamykane,
- w przypadku zaistnienia zdarzenia, które ma wpływ na bezpieczeństwo, kontynuowana jest komunikacja do czasu, aż zidentyfikowane zostaną oznaki naruszenia bezpieczeństwa (IoC), zagrożenia zostaną zmitygowane, a podmiot odzyska ciągłość świadczenia usług.

II. Wymogi zgłoszenia incydentu

01. Zgłoszenie incydentu z art. 11 ust. 1 pkt 4 UKSC, zgodnie z art. 12 ust. 1 UKSC, zawiera:

- → dane podmiotu zgłaszającego, w tym nazwę firmy, numer we właściwym rejestrze, siedzibę i adres,
- → imię i nazwisko, numer telefonu oraz adres poczty elektronicznej osoby dokonującej zgłoszenia,
- → imię i nazwisko, numer telefonu oraz adres poczty elektronicznej osoby uprawnionej do składania wyjaśnień dotyczących zgłaszanych informacji,
- → opis wpływu incydentu. Natomiast w przypadku wystąpienia **incydentu poważnego** na świadczenie usługi kluczowej, niezbędne są informacje:
  - usługi kluczowe zgłaszającego, na które zgłaszany incydent miał wpływ,
  - liczba użytkowników usługi kluczowej, na których zgłaszany incydent miał wpływ,
  - moment wystąpienia i wykrycia incydentu oraz czas jego trwania,
  - zasięg geograficzny obszaru, którego dotyczy incydent,
  - wpływ incydentu na świadczenie usługi kluczowej przez innych operatorów usług kluczowych i dostawców usług cyfrowych,
  - przyczynę zaistnienia incydentu i sposób jego przebiegu oraz skutki,
  - jego oddziaływania na systemy informacyjne lub świadczone usługi kluczowe,
- → w przypadku incydentu, który mógł mieć wpływ na świadczenie usługi kluczowej, opis przyczyn tego incydentu, sposób jego przebiegu oraz prawdopodobne skutki oddziaływania na systemy informacyjne,
- → informacje o podjętych działaniach zapobiegawczych,
- → informacje o podjętych działaniach naprawczych,
- → inne istotne informacje.

III. Inne incydenty oraz zdarzenia

01. Podmioty z sektora zdrowia mogą dodatkowo przekazywać informacje:

- → o innych incydentach,
- → o zagrożeniach cyberbezpieczeństwa,
- → dotyczące szacowania ryzyka,
- → o wykorzystywanych technologiach.

IV. Kanały komunikacji i publikacje - CSIRT CeZ

Sektorowy zespół CSIRT CeZ publikuje zalecenia oraz informacje o zagrożeniach na stronie: cez.gov.pl w zakładce CSIRT.

Mailowo wysyłane są również ostrzeżenia z adresu: ostrzezenia@csirt.cez.gov.pl.

Komunikację, która nie dotyczy incydentów, należy kierować na adres: info@csirt.cez.gov.pl.