CSIRT CEZ

Reagowanie na incydenty

w ramach zaleceń w zakresie podstaw bezpieczeństwa i ochrony danych dla użytkowników w sektorze ochrony zdrowia

01. Rozpoznanie nietypowych objawów

- Zwracaj uwagę na niecodzienne komunikaty, spowolnione działanie komputera lub inne niepokojące zachowania systemu.
- Bądź wyczulony na podejrzane wiadomości e-mail, prośby o hasło czy nieoczekiwane alerty antywirusowe.
- Stosuj się do zasady, że w przypadku wątpliwości zawsze lepiej zgłosić podejrzane zdarzenie, niż przeoczyć zagrożenie.

02. Wstępne działania

- Jeżeli podejrzewasz atak (np. wirus, ransomware) lub zauważysz nieautoryzowaną aktywność, bezzwłocznie wyłącz Wi-Fi lub odłącz kabel sieciowy, aby zatrzymać ewentualne rozprzestrzenianie się zagrożenia.
- Zapisz dokładny czas wystąpienia niepokojących zdarzeń, które zwróciły Twoją uwagę, oraz podjęte czynności przed pojawieniem się incydentu i w trakcie jego trwania.
- Unikaj samodzielnego usuwania plików czy formatowania dysku, możesz zatrzeć ślady istotne dla analizy incydentu. Nie otwieraj ponownie podejrzanych plików.
- Unikaj dalszych działań, które mogłyby zatrzeć istotne informacje potrzebne do ustalenia przyczyny incydentu.
- Jeśli to możliwe utrwal dowody, błędy systemu (zrzuty ekranu), aby pomóc w analizie.
- Ustal, czy problem dotyczy jedynie Twojego stanowiska, czy ma szerszy zasięg.

03. Zgłaszanie incydentu

- Skontaktuj się z przełożonym i/lub działem IT w celu zgłoszenia incydentu.
- Przekaż krótki opis zdarzenia – co się stało, kiedy wystąpiło i jakie zauważyłeś/łaś symptomy.
- Ostrzeż współpracowników, żeby nie otwierali podobnych wiadomości czy plików.

CSIRT CEZ