CSIRT 5 Wojskowy Szpital Kliniczny z Polikliniką SPZOZ w Krakowie (wersja polska)

1. Informacje o dokumencie

   Dokument zawiera opis zespołu CERT w 5 Wojskowym Szpitalu Klinicznym z Polikliniką SPZOZ w Krakowie zwanym dalej 5 WSzKzP SPZOZ w Krakowie zgodnie z RFC 2350 oraz dostarcza podstawowych informacji o CERT, sposobach kontaktu, opisuje obowiązki zespołu i oferowane usługi.

   1.1 Data ostatniej aktualizacji

   Wersja dokumentu 1.00, opublikowana 2022-11-18.

   1.2 Lista dystrybucyjna powiadomień o zmianach w dokumencie

   CERT w 5 Wojskowym Szpitalu Klinicznym z Polikliniką SPZOZ w Krakowie nie korzysta z żadnej listy dystrybucyjnej mającej na celu powiadamianie o zmianach w tym dokumencie.

   1.3 Miejsce, w którym można znaleźć dokument

   Aktualna wersja tego dokumentu znajduje się na:
   https://5wszk.com.pl/strona/1170-cyberbezpieczenstwo

   1.4 Wiarygodność dokumentu

   Niniejszy dokument został podpisany przy użyciu klucza PGP 5 Wojskowego Szpitala Klinicznego z Polikliniką SPZOZ w Krakowie CERT.

2. Informacje kontaktowe

   2.1 Nazwa zespołu

   W 5 Wojskowym Szpitalu Klinicznym z Polikliniką SPZOZ w Krakowie powołano Zespół ds. Monitorowania Zagrożeń i Utrzymania Polityki Bezpieczeństwa Informacji. Pracami tego Zespołu kieruje Pełnomocnik Komendanta Szpitala ds. Systemu Zarządzania Bezpieczeństwem Informacji.

   Na bazie Działu Informatyki powołano CERT Lokalny Zespół Cyberbezpieczeństwa 5 Wojskowego Szpitala Klinicznego z Polikliniką SPZOZ w Krakowie – nazywany dalej LZC 5WSzKzP.

   2.2 Adres

   LZC 5WSzKzP
   5 Wojskowego Szpitala Klinicznego z Polikliniką SPZOZ w Krakowie
   ul. Wrocławska 1-3
   30-901 Kraków
   Polska

   2.3 Strefa czasowa

   Środkowoeuropejski UTC+01:00 Sarajewo, Skopie, Warszawa, Zagrzeb

   2.4 Numer telefonu

   - +48 126 308 022 w godzinach od 7:00 do 15:00
   - tel. alarmowy + 48 729 316 899

   2.5 Telefaks Numer

   Niedostępny

   2.6 Inne możliwości komunikacji

   Niedostępne

   2.7 Elektroniczny adres e-mail

   incydent@5wszk.com.pl

2.8 Klucze publiczne i inne informacje o szyfrowaniu

LZC 5WSzKzP korzysta z klucza PGP:

Nazwa: Zespół LZC 5WSzKzP
Email: pełnomocnik.szbi@5wszk.com.pl
Identyfikator klucza: CDAD EA8B 3EF0 6B2E
Rozmiar klucza: ed25519 + cv25519
Algorytm: ECDSA/EdDSA + ECDH
Odcisk palca: 3B53 B3CB FC04 4AE0 EC77 9BB0 CDAD EA8B 3EF0 6B2E
Klucz ten można otrzymać bezpośrednio z naszej strony internetowej:
https://5wszk.com.pl/strona/1170-cyberbezpieczenstwo

2.9 Członkowie zespołu

Zespół LZC 5WSzKzP składa się z administratorów Systemów Bezpieczeństwa Systemów Informatycznych odpowiedzialnych za monitorowanie zagrożeń cyberbezpieczeństwa oraz reagowanie na incydenty w systemach teleinformatycznych.

2.10 Inne informacje

Ogólne informacje na temat 5 Wojskowego Szpitala Klinicznego z Polikliniką SPZOZ w Krakowie są zamieszczone na stronie internetowej: https://5wszk.com.pl/ .

2.11 Punkty kontaktu z klientem

Zespół LZC 5WSzKzP preferuje kontakt mailowy.

Użyj powyższego klucza kryptograficznego, aby zapewnić integralność i poufność komunikacji.

W sprawach ogólnych:
Kontakt jest możliwy w godzinach pracy: 07:00-15:00 czasu lokalnego od poniedziałku do piątku z wyjątkiem dni ustawowo wolnych od pracy w Polsce pod numerem telefonu +48 126 308 022.

Zgłoszenia incydentów, sytuacje awaryjne:

Incydenty (zdarzenia) lub podatności należy zgłaszać za pomocą poczty elektronicznej z wykorzystaniem *Formularza zgłaszania zdarzeń i incydentów* na adres e-mail: incydent@5wszk.com.pl

lub telefonicznie na numery +48 126 308 022 w godzinach od 7:00 do 15:00 czasu lokalnego od poniedziałku do piątku z wyjątkiem dni ustawowo wolnych od pracy w Polsce oraz tel. alarmowy + 48 729 316 899.

3. Statut

3.1 Misja

Budowanie kompetencji i zdolności w 5 Wojskowym Szpitalu Klinicznym z Polikliniką SPZOZ w Krakowie w zakresie unikania, identyfikowania i ograniczania cyberzagrożeń.
Wsparcie dla działań krajowych w zakresie bezpieczeństwa cybernetycznego.

3.2 Zakres działania

Zespół LZC 5WSzKzP zapewnia wsparcie w zakresie obsługi zdarzeń cyberbezpieczeństwa dla swoich pacjentów i klientów.

3.3 Finansowanie i przynależność

Nadzór nad działalnością Szpitala sprawuje Minister Obrony Narodowej lub osoby przez niego upoważnione.
Szpital prowadzi gospodarkę finansową na zasadach przewidzianych dla samodzielnego publicznego zakładu opieki zdrowotnej, określonych w ustawie.

3.4. Umocowanie

Organem założycielskim Szpitala jest Minister Obrony Narodowej. Nadzór nad działalnością Szpitala sprawuje Minister Obrony Narodowej lub osoby przez niego upoważnione.

4. Zasady obsługi incydentów (polityki)

4.1 Rodzaje incydentów i poziom wsparcia

Zespół LZC 5WSzKzP jest dedykowany do obsługi wszystkich rodzajów incydentów związanych z bezpieczeństwem komputerowym, które występują lub mogą wystąpić w środowisku teleinformatycznym Szpitala.

Klasyfikacja incydentów i sposób ich obsługi są określone w procesie zarządzania incydentami bezpieczeństwa informacji.

Sposób obsługi incydentów zależy od rodzaju i wagi incydentu lub zdarzenia, elementów, na które oddziałuje incydent, ilości użytkowników, których dotyczy incydent oraz dostępności zasobów. Dla zdarzeń określa się priorytety stosownie do ich dotkliwości i rozmiaru.

4.2 Współpraca, interakcja i ujawnianie informacji

Zespół LZC 5WSzKzP wymienia wszystkie niezbędne do współpracy informacje z innymi zespołami CSIRT, a także z administratorami zainteresowanych stron. Żadne dane osobowe nie są wymieniane, chyba że za wyraźnym upoważnieniem. Wszystkie informacje związane z obsługiwanymi incydentami są traktowane jako chronione. Informacje chronione (takie jak dane osobowe, konfiguracje systemu, znane luki, etc.) są szyfrowane, jeśli muszą być przesyłane w niezabezpieczonym środowisku.

Informacje przesyłane do Zespołu LZC 5WSzKzP mogą być przekazywane zgodnie z potrzebą stronom zaufanym (takim jak dostawcy usług internetowych, inne zespoły CERT) wyłącznie w celu obsługi incydentów.

4.3 Komunikacja i uwierzytelnianie

Zespół LZC 5WSzKzP wykorzystuje szyfrowanie w celu zapewnienia poufności i integralności komunikacji. Wszystkie przesyłane informacje chronione powinny być szyfrowane.

5. Usługi

5.1 Reakcja na incydenty

Szpital ustanowił organizacyjny i techniczny proces reagowania na incydenty. Proces obejmuje pełny cykl reagowania na incydenty:

- obsługę
- zarzadzanie
- rozwiazywanie
- łagodzenie

5.1.1 Ocena incydentów

Ocena incydentów obejmuje analizę wpływu incydentu na bezpieczeństwo informacji przetwarzanych w Szpitalu:

- nadawanie priorytetu stosownie do rodzaju i wagi incydentu,
- określenie zakres incydentu,
- przeprowadzenie badania przyczyn powstania incydentu.

5.1.2 Koordynacja incydentów

Za koordynowanie działań odpowiada Pełnomocnik LZC 5WSzKzP w tym m.in.:

- ułatwianie kontaktu z innymi stronami, które mogą być zaangażowane,
- kontakt z CSIRT MON, NASK i/lub w razie potrzeby z odpowiednimi organami ścigania,
- tworzenie raportów dla innych CSIRT.

5.1.3 Rozwiązywanie incydentów obejmuje:

- powiadamianie zespołu i koordynację odpowiednich działań,
- śledzenie postępów prac zaangażowanego zespołu,
- obsługę żądań raportowania,
- przedstawianie raportów.

5.2 Działania proaktywne

Zespół LZC 5WSzKzP prowadzi działania mające na celu zwiększenie odporności środowiska informatycznego na zdarzenia związane z bezpieczeństwem i minimalizujące potencjalny wpływ tych zdarzeń.

6. Formularze zgłaszania incydentów

Wspomniany powyżej proces zarzadzania incydentami bezpieczeństwa informacji definiuje mailowy (incydent@5wszk.com.pl) kanał zgłaszania incydentów.

W zgłoszeniu incydentu, zgodnie z formularzem, prosimy o przekazanie do Zespołu LZC 5WSzKzP co najmniej następujących informacji:

- dane kontaktowe i informacje organizacyjne:
  - ✓ imię i nazwisko,
  - ✓ nazwa organizacji i adres,
  - ✓ adres e-mail,
  - ✓ numer telefonu,
- adresy IP,
- nazwę domenową oraz wszelkie istotne elementy techniczne i obserwacje:
  - ✓ wyniki skanowania (jeśli istnieją),
  - ✓ wyciąg z rejestru log systemu (jeśli istnieją).

7. Zastrzeżenia

Podczas przygotowywania informacji, powiadomień i alertów zostaną podjęte wszelkie środki ostrożności.
Zespół LZC 5WSzKzP nie ponosi odpowiedzialności za błędy, pominięcia ani za szkody wynikające z wykorzystania informacji zawartych w tym dokumencie.