CSIRT Szpital Powiatowy w Zawierciu
(wersja polska)

1. Informacje o dokumencie

Dokument zawiera opis Zespołu ds. monitorowania poziomu Cyberbezpieczeństwa w Szpitalu Powiatowym w Zawierciu zgodnie z RFC 2350 oraz dostarcza podstawowych informacji , sposobach kontaktu, opisuje obowiązki zespołu i oferowane usługi.

1.1 Data ostatniej aktualizacji
Wersja dokumentu 1.00, opublikowana 2024-05-17.

1.2 Lista dystrybucyjna powiadomień o zmianach w dokumencie Zespół ds. monitorowania poziomu Cyberbezpieczeństwa nie korzysta z żadnej listy dystrybucyjnej mającej na celu powiadamianie o zmianach w tym dokumencie.

1.3 Miejsce, w którym można znaleźć ten dokument
Aktualna wersja tego dokumentu znajduje się na:
www.szpitalzawiercie.pl/RFC-2350-PL – Polska wersja
www.szpitalzawiercie.pl/RFC-2350-ENG – Angielska wersja

1.4 Wiarygodność dokumentu
Niniejszy dokument został podpisany przy użyciu klucza PGP Zespółu ds. monitorowania poziomu Cyberbezpieczeństwa Szpitala Powiatowego w Zawierciu. Więcej szczegółów w rozdziale 2.8.

2. Informacje kontaktowe

2.1 Nazwa zespołu
Szpital Powiatowy w Zawierciu „Zespół ds. monitorowania poziomu Cyberbezpieczeństwa" – nazywany dalej w skrócie jako „Zespół ZMPC".

2.2 Adres
Zespół ZMPC
Szpital Powiatowy w Zawierciu
Ul. Miodowa 14
42-400 Zawiercie
Polska

2.3 Strefa czasowa
Środkowoeuropejski (GMT+0100, GMT+0200 od kwietnia do października)

2.4 Numer telefonu
+48 32 67 40 350

2.5 Numer faksu
+48 32 67 40 350

2.6 Inne możliwości komunikacji
Niedostępne.

2.7 Adres e-mail
incydent@szpitalzawiercie.pl

2.8 Klucze publiczne i inne informacje o szyfrowaniu
Zespół ZMPC korzysta z klucza PGP:
Adres email: incydent@szpitalzawiercie.pl
Identyfikator klucza: 51523F730B49F81332DD372E3FB9CAF9904E5A35
Rozmiar klucza: 3072
Algorytm: RSA
Odcisk klucza: 5152 3F73 0B49 F813 32DD 372E 3FB9 CAF9 904E 5A35
Klucz ten można otrzymać bezpośrednio z naszej strony internetowej: www.szpitalzawiercie.pl/rfc

2.9 Członkowie zespołu
Zespół ZMPC składa się z ekspertów w dziedzinie zagadnień Cyberbezpieczeństwa.

2.10 Inne informacje
Ogólne informacje na temat Szpitala Powiatowego w Zawierciu są zamieszczone na stronie internetowej www.szpitalzawiercie.pl

2.11 Punkty kontaktu z klientem
Preferowaną metodą kontaktu jest e-mail. Rekomendujemy wykorzystanie PGP w celu zapewnienia integralności i poufności.

W sprawach ogólnych:
Kontakt jest możliwy w godzinach pracy: 08:00-15:35 czasu lokalnego od poniedziałku do piątku z wyjątkiem dni ustawowo wolnych od pracy w Polsce.

Zgłoszenia incydentów, sytuacje awaryjne:
Kontakt telefoniczny z Zespołem ZMPC i/lub wiadomość e-mail zawierająca szczegóły podane wcześniej telefonicznie. Telefon Zespołu ZMPC jest dostępny w godzinach pracy: 08:00-15:35 czasu lokalnego od poniedziałku do piątku z wyjątkiem dni ustawowo wolnych od pracy w Polsce.

3. Statut
3.1 Misja
Misją jest budowanie kompetencji i zdolności Szpitala Powiatowego w Zawierciu w zakresie unikania, identyfikowania i ograniczania cyberzagrożeń. Wsparcie dla działań krajowych w zakresie bezpieczeństwa cybernetycznego.

3.2 Zakres działania
Zespół ZMPC zapewnia wsparcie w zakresie obsługi zdarzeń cyberbezpieczeństwa dla swoich pacjentów i klientów.

3.3 Finansowanie i przynależność
Nadzór nad działalnością Szpitala sprawuje Powiat Zawierciański. Szpital prowadzi gospodarkę finansową na zasadach określonych w obowiązujących przepisach prawa polskiego.

3.4. Umocowanie
Podmiotem tworzącym i nadzorującym Szpital jest Powiat Zawierciański.

4. Zasady obsługi incydentów (polityki)

4.1 Rodzaje incydentów i poziom wsparcia

Zespół ZMPC 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 ZMPC 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 ZMPC 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 ZMPC 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:

- analizę,
- obsługę,
- zarządzanie,
- rozwiązywanie,
- 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 ZMPC w tym m.in.:

- ułatwianie kontaktu z innymi stronami, które mogą być zaangażowane,
- kontakt z CSIRT 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 ZMPC 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 zarządzania incydentami bezpieczeństwa informacji definiuje mailowy (incydent@szpitalzawiercie.pl) kanał zgłaszania incydentów. W zgłoszenia incydentu prosimy o przekazanie do Zespołu ZMPC 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 ZMPC nie ponosi odpowiedzialności za błędy, pominięcia ani za szkody wynikające z wykorzystania informacji zawartych w tym dokumencie.