CSIRT Powiatowego Centrum Zdrowia Sp. z o.o. CERT (wersja polska)

1. Informacje o dokumencie

Dokument zawiera opis zespołu CERT w Powiatowym Centrum Zdrowia Sp. z o.o. 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 2022-11-23.

1.2 Lista dystrybucyjna powiadomień o zmianach w dokumencie

CERT w Powiatowe Centrum Zdrowia Sp. z o.o. 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://www.pczkartuzy.pl/cyberbezpieczenstwo.html

1.4 Wiarygodność dokumentu

Niniejszy dokument został podpisany przy użyciu klucza PGP Powiatowego Centrum Zdrowia Sp. z o.o. CERT.
Więcej szczegółów w rozdziale 2.8.

2. Informacje kontaktowe

2.1 Nazwa zespołu

" Powiatowe Centrum Zdrowia Sp. z o.o. CERT ": Zespół ds. Reagowania na incydenty cyberbezpieczeństwa - nazywany dalej jako Zespół Cyberbezpieczeństwa

2.2 Adres

Zespół Cyberbezpieczeństwa
Powiatowe Centrum Zdrowia w Kartuzach
ul. Floriana Ceynowy 7
83-300 Kartuzy
Polska

2.3 Strefa czasowa

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

2.4 Numer telefonu

+48 58 685 49 05

2.5 Telefaks Numer

Niedostępny

2.6 Inne możliwości komunikacji

Niedostępne

2.7 Elektroniczny adres e-mail

incydent@pczkartuzy.pl

2.8 Klucze publiczne i inne informacje o szyfrowaniu

Zespół Cyberbezpieczeństwa korzysta z klucza PGP:
Nazwa: PCZ Zespół Cyberbezpieczeństwa
Email: incydent@pczkartuzy.pl
Identyfikator klucza: 699C F941 C9D5 4B04
Rozmiar klucza: 4096
Algorytm: RSA
Odcisk palca: B0066DFF85D6992119EE060A969CF941C9D54B04

Klucz ten można otrzymać bezpośrednio z naszej strony internetowej:
https://www.pczkartuzy.pl/cyberbezpieczenstwo.html

2.9 Członkowie zespołu

Zespół Cyberbezpieczeństwa składa się z ekspertów w dziedzinie zagadnień Cyberbezpieczeństwa.

2.10 Inne informacje

Ogólne informacje na temat Powiatowym Centrum Zdrowia Sp. z o.o. są zamieszczone na stronie internetowej
https://www.pczkartuzy.pl/cyberbezpieczenstwo.html

2.11 Punkty kontaktu z klientem

Zespół Cyberbezpieczeństwa preferuje kontakt mailowy.
Użyj powyższego klucza kryptograficznego, aby zapewnić integralność i poufność komunikacji.
W sprawach ogólnych:
Kontakt jest możliwy w godzinach pracy: 07:00-14:35 czasu lokalnego od poniedziałku do piątku z wyjątkiem dni ustawowo wolnych od pracy w Polsce.

Zgłoszenia incydentów, sytuacje awaryjne:
Kontakt telefoniczny z Zespołem Cyberbezpieczeństwa oraz / lub wiadomość e-mail zawierająca szczegóły podane telefonicznie.
Telefon Zespołu Cyberbezpieczeństwa jest dostępny w godzinach pracy: 07:00-14:35 czasu lokalnego od poniedziałku do piątku z wyjątkiem dni ustawowo wolnych od pracy w Polsce.

3. Statut

3.1 Misja

Budowanie kompetencji i zdolności Powiatowym Centrum Zdrowia Sp. z o.o. w zakresie unikania, identyfikowania i ograniczania cyberzagrożeń.
Wsparcie dla działań krajowych w zakresie bezpieczeństwa cybernetycznego.

3.2 Zakres działania

Zespół Cyberbezpieczeństwa zapewnia wsparcie w zakresie obsługi zdarzeń cyberbezpieczeństwa dla swoich pacjentów i klientów.

3.3 Finansowanie i przynależność

Nadzór nad działalnością Spółki sprawuje Rada Nadzorcza i Zgromadzenie Wspólników.
Spółka prowadzi gospodarkę finansową na zasadach określonych w obowiązujących przepisach prawa polskiego.

3.4. Umocowanie

Powiat Kartuski w całości posiada udziały Spółki.

4. Zasady obsługi incydentów (polityki)

4.1 Rodzaje incydentów i poziom wsparcia

Zespół Cyberbezpieczeństwa jest dedykowany do obsługi wszystkich rodzajów incydentów związanych z bezpieczeństwem komputerowym, które występują lub mogą wystąpić w środowisku teleinformatycznym Spółki.
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 Cyberbezpieczeństwa 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 Cyberbezpieczeństwa 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 Cyberbezpieczeństwa wykorzystuje szyfrowanie w celu zapewnienia poufności i integralności komunikacji. Wszystkie przesyłane informacje chronione powinny być szyfrowane.

5. Usługi

5.1 Reakcja na incydenty

Spółka 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 Spółce
- 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 ds. Cyberbezpieczeństwa 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 Cyberbezpieczeństwa 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@pczkartuzy.pl) kanał zgłaszania incydentów.
W zgłoszenia incydentu prosimy o przekazanie do Zespołu Cyberbezpieczeństwa 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 Cyberbezpieczeństwa nie ponosi odpowiedzialności za błędy, pominięcia ani za szkody wynikające z wykorzystania informacji zawartych w tym dokumencie.