Zespół Cyberbezpieczeństwa dla Szpitala Powiatowego w Zawierciu (wersja polska)

1. Informacje o dokumencie

Niniejszy dokument zawiera informacje na temat Zespołu Cyberbezpieczeństwa dla Szpitala Powiatowego w Zawierciu. Dokument został sporządzony według RFC 2350.

1.1 Data ostatniej aktualizacji

To jest wersja 1.2, opublikowana 11.08.2024.

1.2 Rozpowszechnianie powiadomień o zmianach w dokumencie

Zespół Cyberbezpieczeństwa nie korzysta z listy dystrybucyjnej.

1.3 Miejsce, gdzie można znaleźć dokument

Aktualne wersje dokumentów są dostępne na stronie internetowej Szpitala pod odnośnikami: polska wersja językowa i angielska wersja językowa.
Proszę zawsze upewnić się, że używacie Państwo najnowszej wersji dokumentu.

1.4 Poświadczenie dokumentu

Zarówno polska jak i angielska wersja językowa zostały podpisane kluczem PGP Zespołu Cyberbezpieczeństwa. Pliki dokumentów, pliki podpisów oraz sumy kontrolne wygenerowane za pomocą algorytmu sha256 są dostępne na stronie internetowej Szpitala pod odnośnikiem dokumenty RFC.

2. Informacje kontaktowe

2.1 Nazwa zespołu

Pełna nazwa: Zespół ds. monitorowania poziomu Cyberbezpieczeństwa Szpitala Powiatowego w Zawierciu.
Skrócona nazwa: Zespół Cyberbezpieczeństwa.

2.2 Adres

Zespół ds. monitorowania poziomu Cyberbezpieczeństwa
Szpital Powiatowy w Zawierciu
ul. Miodowa 14
42-400 Zawiercie
Polska

2.3 Strefa czasowa

Czas Środkowoeuropejski UTC+1.
Czas Środkowoeuropejski letni UTC+2 (od ostatniej niedzieli marca do ostatniej niedzieli października).

2.4 Numer telefonu

+48 32 67-40-371
+48 885-999-138

2.5 Numer faksu

Niedostępne

2.6 Pozostała telekomunikacja

Niedostępne

2.7 Adres e-mail

incydent@szpitalzawiercie.pl

2.8 Klucz publiczny i inne informacje o szyfrowaniu

Klucz PGP używany przez Zespół Cyberbezpieczeństwa:
Odcisk klucza: 5152 3F73 0B49 F813 32DD 372E 3FB9 CAF9 904E 5A35
Klucz publiczny można pobrać ze strony internetowej Szpitala pod odnośnikiem klucz PGP

2.9 Członkowie zespołu

W skład Zespołu Cyberbezpieczeństwa wchodzą osoby posiadające praktyczną wiedzę oraz doświadczenie w zakresie zapewnienia bezpieczeństwa fizycznego i teleinformatycznego.

2.10 Inne informacje

Informacje na temat cyberbezpieczeństwa są zamieszczone w bieżącym dokumencie oraz opublikowane na stronie internetowej Szpitala pod odnośnikiem cyberbezpieczeństwo.

2.11 Dodatkowe informacje kontaktowe

Preferowaną metodą kontaktu z Zespołem Cyberbezpieczeństwa jest poczta elektroniczna. Dla zapewnienia bezpieczeństwa (poufności) korespondencji zalecane jest jej zaszyfrowanie przy użyciu klucza PGP o którym mowa w punkcie 2.8. W przypadku konieczności ustalenia innego bezpiecznego kanału komunikacji prosimy o kontakt bezpośrednio z Zespołem Cyberbezpieczeństwa.
Kontakt telefoniczny z Zespołem Cyberbezpieczeństwa jest możliwy od poniedziałku do piątku z wyjątkiem dni ustawowo wolnych od pracy w Polsce, w godzinach od 08:00 do 15:30 czasu lokalnego.
W sytuacjach pilnych (np. w celu zgłoszenie cyberzagrożenia) informacje można przekazać telefonicznie na podany w punkcie 2.4 numer telefonu komórkowego. Zgłoszenie następnie powinno być przekazane również drogą e-mail wraz ze wszystkimi szczegółami podanymi uprzednio telefonicznie.

3. Statut

3.1 Misja

Misją Zespołu Cyberbezpieczeństwa jest stałe podnoszenie odporności zasobów informatycznych Szpitala Powiatowego w Zawierciu poprzez identyfikowanie, unikanie oraz przeciwdziałanie potencjalnym zagrożeniom zarówno fizycznym jak i teleinformatycznym.

3.2 Zakres działania

Zespół Cyberbezpieczeństwa obejmuje swoim zakresem działania systemy oraz usługi teleinformatyczne działające w Szpitalu Powiatowym w Zawierciu.

3.3 Finansowanie i przynależność

Zespół Cyberbezpieczeństwa jest utrzymywany finansowo przez Szpital Powiatowy w Zawierciu. Szpital prowadzi gospodarkę finansową na zasadach określonych w obowiązujących przepisach polskiego prawa.

3.4. Umocowanie

Nadzór nad działalnością Zespołu Cyberbezpieczeństwa sprawuje Dyrektor Szpitala.

4. Zasady obsługi incydentów (polityki)

4.1 Rodzaje incydentów i poziom wsparcia

Zespół Cyberbezpieczeństwa bierze czynny udział w obsłudze wszystkich rodzajów incydentów bezpieczeństwa teleinformatycznego, które występują lub mogą wystąpić w Szpitalu. Klasyfikacja incydentów i sposób ich obsługi będzie zróżnicowany w zależności od: wagi incydentu, rodzaju incydentu, elementów na które on oddziałuje, ilości użytkowników, których dotyczy oraz inne czynniki.

4.2 Współpraca, interakcja i ujawnianie informacji

Zespół Cyberbezpieczeństwa wymienia wszelkie niezbędne informacje z zespołami CERT, CSIRT oraz innymi podmiotami wchodzącymi w skład Krajowego Systemu Cyberbezpieczeństwa a także z administratorami stron poszkodowanych.

Wszystkie informacje dotyczące obsługi incydentów są poufne, dlatego też przekazywane nam informacje zalecamy zaszyfrować przy użyciu klucza PGP Zespołu Cyberbezpieczeństwa lub skorzystać z innego ustalonego wspólnie kanału komunikacji.

Żadne dane osobowe nie są udostępniane do współpracujących ze Szpitalem podmiotów, chyba że zostaną one do tego wyraźnie upoważnione.

4.3 Komunikacja i uwierzytelnianie

Zespół Cyberbezpieczeństwa wykorzystuje szyfrowanie kluczem PGP w celu zapewnienia poufności, integralności oraz uwierzytelnieniu prowadzonej komunikacji.

5. Usługi

5.1 Reakcja na incydenty

Szpital ustanowił organizacyjny i techniczny proces reagowania na incydenty.

5.1.1 Segregacja incydentów

Ocena incydentów obejmuje:

- analiza i klasyfikacja zdarzenia, jako incydent bezpieczeństwa lub fałszywy alarm,
- jeżeli zdarzenie zostało zaklasyfikowane jako incydent to następuje określenie jego rozmiaru oraz wpływu na bezpieczeństwo informacji przetwarzanych w Szpitalu,
- nadawanie priorytetu stosownie do rodzaju i wagi incydentu.

5.1.2 Koordynacja incydentów

Za koordynowanie działań odpowiada Inspektor Ochrony Danych przy współpracy Administratora Systemów Informatycznych. Do podstawowych zadań koordynatora należy:

- analiza artefaktów i dowodów wystąpienia incydentu w celu ustalenia pierwotnej przyczyny jego powstania (luki w zabezpieczeniach),
- powiadomienie CSIRT NASK, CSIRT CeZ oraz w razie potrzeby odpowiednich służb i organów ścigania,
- zapewnienia skutecznej komunikacji z innymi stronami, które mogą być zaangażowane w incydent,
- jeśli ma to zastosowanie przekazanie informacji do wiadomości użytkowników.

5.1.3 Rozwiązywanie incydentów

Obejmuje:

- usunięcie przyczyny powstanie incydentu,
- przywrócenie normalnego funkcjonowania systemów objętych incydentem,
- gromadzenie materiału dowodowego z zaistniałego incydentu,
- przekazanie wniosków i zaleceń powstałych po analizie zaistniałego incydentu.

5.2 Działania proaktywne

Zespół Cyberbezpieczeństwa prowadzi działania mające na celu zwiększenie odporności środowiska informatycznego oraz minimalizujące potencjalny wpływ wystąpienia takich zdarzeń na bezpieczeństwo zasobów teleinformatycznych Szpitala.

6. Formularze zgłaszania incydentów

Nie ma jeszcze opracowanych gotowych formularzy do zgłaszania incydentów.

Wspomniany powyżej proces zarządzania incydentami bezpieczeństwa informacji definiuje kanał zgłaszania incydentów pocztą e-mail (incydent@szpitalzawiercie.pl). W zgłoszeniu incydentu prosimy o przekazanie do Zespołu Cyberbezpieczeństwa jak największej ilości informacji, które są możliwe do zebrania, w szczególności:

- dane kontaktowe i informacje o zgłaszającym: imię i nazwisko, adres e-mail, numer telefonu oraz nazwa i adres organizacji,
- obserwacje i wyniki analiz,
- wszelkie istotne elementy techniczne (adresy IP, nazwę domenową itp),
- wyniki skanowania (jeśli istnieją),
- wyciąg z rejestru log systemu (jeśli istnieje),
- wszelkie inne dostępne informacje mogące mieć związek ze zgłoszeniem a które przyspieszą jego rozwiązanie i pomogą w jego dogłębnej analizie.

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.