RFC 2350

Spis treści

1. Informacje o dokumencie

Dokument ten zawiera informacje dotyczące zespołu reagowania na incydenty bezpieczeństwa komputerowego Flowberg IT SOC. Dokument jest zgodny z RFC 2350.

1.1 Data ostatnie aktualizacji

Wersja: 1.1 z dnia 3.07.2023 r.

1.2 Lokalizacja dokumentu

Aktualna wersja dokumentu jest dostępna:

Wersja PL – https://flowbergit.pl/cyberbezpieczenstwo/soc/

Wersja ENG – https://flowbergit.pl/cyberbezpieczenstwo/soc/

1.3 Wiarygodność dokumentu

Ten dokument został podpisany przy użyciu podpisu kwalifikowanego Prezesa spółki Flowberg IT sp. z o.o..

Sygnatura znajduje się pod adresem: https://flowbergit.pl/cyberbezpieczenstwo/soc/

2. Informacje kontaktowe

2.1 Nazwa zespołu

Flowberg IT SOC

2.2 Adres zespołu

Flowberg IT Sp. z o.o.
SOC
ul. Borowska 283b
50-556 Wrocław
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 71 728 10 80

2.5 Adres skrzynki pocztowej

Powiadomienia, zgłoszenia incydentów i kwestie operacyjne prosimy kierować na adres: soc@flowbergit.pl

Pytania dot. oferty, zakresu świadczonych usług i kwestii biznesowych prosimy kierować na adres biuro@flowbergit.pl

2.6 Klucze publiczne i inne informacje o szyfrowaniu

Dla zabezpieczenia poufnych danych stosujemy technologię szyfrowania PGP.

Klucz publiczny: 0535E92182D5C22669A97E6A25AC42757E9C1733
Autor: Flowberg IT Security Operations Center (soc@flowbergit.pl)

Klucz publiczny znajduje się pod adresem: https://flowbergit.pl/cyberbezpieczenstwo/soc/

2.7 Członkowie zespołu

Zespół Flowberg IT SOC tworzą ludzie mocno zaangażowani w ideę promowania świadomości w obszarze cyberbezpieczeństwa. Stale monitorujemy aktywność w przestrzeni cyfrowej, obserwujemy rynek rozwiązań i technologii bezpieczeństwa teleinformatycznego, podnosimy kompetencje.

2.8 Punkty kontaktu z klientem

Preferowaną metodą kontaktu z Flowberg IT SOC jest e-mail.

3. Statut

3.1 Misja

Misją Flowberg IT SOC jest utrzymywanie bezpieczeństwa IT na najwyższym poziomie. Misją Flowberg IT SOC jest wspieranie zarówno spółki Flowberg IT i klientów biznesowych Flowberg IT w reagowaniu i w obsłudze incydentów bezpieczeństwa komputerowego.

3.2 Obszar działania

Obszar działania Flowberg IT SOC obejmuje wszystkich użytkowników systemów spółki Flowberg IT oraz klientów z sektora publicznego oraz prywatnego.

3.3 Finansowanie i przynależność

Flowberg IT SOC jest wewnętrzną jednostką Flowberg IT Sp. Z o.o. i jest ona finansowana przez Flowberg IT Sp. Z o.o. działając w ramach jej struktury.

3.4 Umocowanie

Flowberg IT SOC działa pod auspicjami i upoważnieniem kierownictwa Flowberg IT Sp. Z o.o.

Flowberg IT SOC działa na podstawie wewnętrznych regulacji, warunków umów z klientami, przepisów prawnych oraz przyjętych standardów i zasad.

4. Polityki

4.1 Typy incydentów i poziom wsparcia

Domyślnym priorytetem dla wszystkich zgłoszonych incydentów jest priorytet normalny. Inna klasyfikacja może mieć zastosowanie na podstawie zapisów umów. O ewentualnej zmianie priorytetu decyduje zespół Flowberg IT SOC.

4.2 Współpraca, interakcja i ujawnianie informacji

Wszystkie informacje dotyczące obsługi incydentów traktowane są jako poufne. Zalecamy, aby przy zgłaszaniu incydentów i podawaniu informacji poufnych, korzystać z szyfrowania PGP lub ewentualnie ustalić z Flowberg IT SOC innego bezpieczny kanał komunikacyjny.

Flowberg IT SOC deklaruje pełne wsparcie dla Information Sharing Traffic Light Protocol (FIRST TLP v1.0, https://www.trusted-introducer.org/ISTLP.pdf). Informacje wysłane i oznaczone zgodnie z ISTLP będą przetwarzane w odpowiedni sposób.

Informacje przekazane Flowberg IT SOC mogą być przekazane do zainteresowanych stron, takich jak inne zespoły CSIRT / CERT, właściciele lub administratorzy dotkniętych incydentem zasobów, na zasadzie „niezbędnej wiedzy”, wyłączenie w celu obsługi incydentów (w zakresie niezbędnym do identyfikacji i ograniczenia zagrożenia).

Flowberg IT SOC samodzielnie nie zgłasza incydentów do organów ścigania, o ile nie wynika to z przepisów prawa. Jednakże w przypadku postępowań prowadzonych przez uprawnione organy, możemy przekazać informacje na ich wniosek.

Flowberg IT SOC samodzielnie nie zgłasza incydentów do organów ścigania, o ile nie wynika to z przepisów prawa. Jednakże w przypadku postępowań prowadzonych przez uprawnione organy, możemy przekazać informacje na ich wniosek.

4.3 Komunikacja i uwierzytelnianie

Flowberg IT SOC zabezpiecza wrażliwe informacje zgodnie z odpowiednimi przepisami prawa i wewnętrznymi zasadami.

W szczególności respektujemy oznaczenia poufności zdefiniowane przez autorów informacji przekazanych do Flowberg IT SOC.

W przypadku informacji o niskiej wrażliwości możliwy jest kontakt z Flowberg IT SOC przy użyciu nieszyfrowanej wiadomości e-mail lub drogą telefonicznąWszystkie wrażliwe informacje, które są przesyłane, powinny być szyfrowane.

W celu weryfikacji autentyczności otrzymanej informacji lub jej źródła czy uwierzytelnienia osoby nawiązującej kontakt, możliwe jest użycie ogólnodostępnych źródeł informacji jak np. baza WHOIS, serwisy społecznościowe, rejestry. W uzasadnionych przypadkach może być stosowane potwierdzenie telefoniczne bądź spotkanie.

5. Usługi

Flowberg IT oferuje swoim Klientom m.in. usługi Security Operations Center (SOC) w modelu as-a-service obejmujące usługi reagowania na incydenty. Ponadto świadczymy szereg usług profesjonalnych z obszaru cyberbezpieczeństwa.

5.1 Usługi reaktywne

- analiza zdarzeń w systemach SIEM
- analiza i kwalifikacja podejrzeń incydentów
- obsługa incydentów
- obsługa podatności
- analiza IoC (Indication of Compromise)

5.2 Usługi proaktywne

- wsparcie w tworzeniu strategii rozwoju bezpieczeństwa
- wdrażanie rozwiązań bezpieczeństwa
- utrzymywanie i rozwój rozwiązań bezpieczeństwa
- ostrzeżenia o nowych podatnościach i zagrożeniach
- testy podatności
- budowanie świadomości bezpieczeństwa

6. Formularze zgłaszania incydentów

Incydenty powinny być zgłaszane e-mail na adres SOC@flowbergit.pl, najlepiej zaszyfrowane naszym publicznym kluczem PGP.

Kontaktując się z Flowberg IT SOC, prosimy o przekazanie poniższych informacji:

1. Dane kontaktowe i informacje organizacyjne — imię i nazwisko osoby, nazwa i adres organizacji, adres e-mail, numer telefonu,
2. Rodzaj i krótkie podsumowanie incydentu/zdarzenia,
3. Źródło zdarzenia/incydentu - w jakim systemie zostało zaobserwowane, publiczne adresy IP źródłowe i docelowe itp.,
4. Dotknięte podmioty lub systemy,
5. Szacowany wpływ - np. utrata dostępności usług),
6. Dodatkowe informacje i obserwacje, które doprowadziły do wykrycia incydentu — wyniki skanowania (jeśli występują), wyciąg z dziennika przedstawiający problem itp.

W przypadku przekazania podejrzanego e-maila, prosimy o upewnienie się, że wszystkie nagłówki, treść i załączniki są zawarte.

7. Zastrzeżenia

Pomimo, że podczas przygotowywania informacji, powiadomień i ostrzeżeń dokładamy wszelkiej staranności, Flowberg IT SOC nie ponosi odpowiedzialności za błędy lub pominięcia, ani za szkody powstałe w wyniku wykorzystania zawartych informacji w nich zawartych.