

Informacje o dokumencie:

Tytuł	RFC2350 CSIRT BOŚ
Wersja	1.0
Autor	Daniel Bancer
Recenzent	Krzysztof Trela
Zatwierdzający	Krzysztof Trela
Format dokumentu (elektroniczny/papierowy)	Elektroniczny


Historia zmian:

Status	Data	Wersja	Historia zmian	Autor
Powstanie	2022-12-16	1.0	Utworzenie dokumentu	Daniel Bancer

Podpisy:

	Imię i Nazwisko	KOC	Data	Podpis	Uwagi
Opracował	Daniel Bancer	DCB	2022-12-16		
Recenzował	Krzysztof Trela	DCB	2022-12-16		
Zatwierdził	Krzysztof Trela	DCB	2022-12-16		

Bank Ochrony Środowiska S.A.

 ul. Żelazna 32, 00-832 Warszawa  infolinia 801 355 455 | +48 22 543 34 34  www.bosbank.pl

Sąd Rejonowy dla m.st. Warszawy XIII Wydział Gospodarczy Krajowego Rejestru Sądowego 0000015525 | NIP 527 020 33 13 | Kapitał zakładowy: 929 476 710 zł

1. Informacje o dokumencie

W niniejszym dokumencie zawarto opis zespołu CSIRT BOŚ, zwanego dalej też „CSIRT BOŚ”, bazujący na standardzie RFC2350. Dokument przedstawia informacje na temat CSIRT BOŚ, sposobów komunikacji, a także świadczonych przez ten Zespół usług.

1.1. Data ostatniej aktualizacji

Wersja 1.0 opublikowana 16.12.2022 r.

1.2. Lista dystrybucyjna dla powiadomień

Nie dotyczy

Aktualizacje dostarczane do Trusted Introducer na skrzynkę mailową <ti@trusted-introducer.org>

1.3. Lokalizacja dokumentu

Aktualna wersja dokumentu w języku polskim jest dostępna na stronie:

https://www.bosbank.pl/_data/assets/pdf/file/0011/52202/RFC2350_BOS_PL.pdf

Aktualna wersja dokumentu w języku angielskim jest dostępna na stronie:

https://www.bosbank.pl/_data/assets/pdf/file/0012/52203/RFC2350_BOS_EN.pdf

1.4. Wiarygodność dokumentu

Dokument podpisano kluczem PGP należącym do CSIRT BOŚ. Szczegóły dotyczące sygnatury przedstawiono poniżej (2.8).

2. Informacje kontaktowe

2.1. Nazwa zespołu

CSIRT BOŚ

2.2. Adres

ul. Żelazna 32, 00-832 Warszawa, Polska

2.3. Data utworzenia

16.12.2022 r.

2.4. Strefa czasowa

UTC/GMT +1 godzina – czas środkowoeuropejski od października do marca

UTC/GMT +2 godziny – czas środkowoeuropejski letni od marca do października

2.5. Numer telefonu

+48 22 543 34 34; +48 801 355 455

Bank Ochrony Środowiska S.A.

 ul. Żelazna 32, 00-832 Warszawa  infolinia 801 355 455 | +48 22 543 34 34  www.bosbank.pl

Sąd Rejonowy dla m.st. Warszawy XIII Wydział Gospodarczy Krajowego Rejestru Sądowego 0000015525 | NIP 527 020 33 13 | Kapitał zakładowy: 929 476 710 zł

2.6. Numer faksu

Niedostępny w komunikacji z CSIRT BOŚ

2.7. Pozostałe możliwości komunikacji

Uprzejmie prosimy o kontakt za pośrednictwem formularza dostępnego na stronie https://wnioski.bosbank.pl/ords/f?p=FORMULARZE_WWW:INCYDENT_BEZPIECZENSTWA

2.8. Adres poczty elektronicznej

csirt@bosbank.pl

2.9. Klucze publiczne oraz informacje o szyfrowaniu

Klucz PGP CSIRT BOŚ

Fingerprint: 50B0 82FF 073A FF30 1188 43EA 43A8 BD63 AEF7 06AA

Klucz publiczny jest możliwy do pobrania ze strony:

<https://www.bosbank.pl/wazne-informacje/bezpieczenstwo/csirt-bos-klucz-pgp>

2.10. Członkowie zespołu

Zespół CSIRT BOŚ składa się z analityków cyberbezpieczeństwa będących pracownikami Departamentu Cyberbezpieczeństwa Banku Ochrony Środowiska S.A. (dalej też „BOŚ S.A.”).

2.11. Punkt kontaktowy dla klientów

2.12. Inne informacje

Informacje o najnowszych zagrożeniach można znaleźć na stronie:

<https://www.bosbank.pl/wazne-informacje/bezpieczenstwo>

3. Charakterystyka

3.1. Misja

Misją CSIRT BOŚ jest: koordynowanie oraz zapewnienie adekwatnej odpowiedzi na incydenty bezpieczeństwa teleinformatycznego, prowadzenie aktywnych czynności minimalizujących ryzyko oraz skutki zdarzeń i incydentów bezpieczeństwa teleinformatycznego występujących w obszarze działania (3.2).


3.2. Obszar działania

Obszar działania CSIRT BOŚ obejmuje klientów, pracowników oraz zasoby warunkujące (zapewniające) prawidłowe funkcjonowanie BOŚ S.A.

3.3. Finansowanie i przynależność

CSIRT BOŚ jest finansowany przez BOŚ S.A.

Bank Ochrony Środowiska S.A.

 ul. Żelazna 32, 00-832 Warszawa  infolinia 801 355 455 | +48 22 543 34 34  www.bosbank.pl

Sąd Rejonowy dla m.st. Warszawy XIII Wydział Gospodarczy Krajowego Rejestru Sądowego 0000015525 | NIP 527 020 33 13 | Kapitał zakładowy: 929 476 710 zł

3.4. Umocowanie

CSIRT BOŚ podlega bezpośrednio pod Zarząd BOŚ S.A. i działa bezpośrednio w strukturach Banku.

4. Polityki

4.1. Typy incydentów i poziom wsparcia

CSIRT BOŚ obsługuje wszystkie typy incydentów cyberbezpieczeństwa wykryte w obszarze działania (3.2). W pierwszej kolejności incydenty otrzymują priorytet zależny od dotkliwości, zakresu oraz przedmiotu, co determinuje zaangażowanie odpowiednich zasobów. Kolejny incydent jest klasyfikowany zgodnie z wewnętrznymi procedurami. Analityk CSIRT BOŚ może w oparciu o uzyskiwane informacje podwyższać bądź obniżać priorytet incydentu. Czynności podejmowane przez CSIRT BOŚ warunkujące odpowiedni poziom bezpieczeństwa teleinformatycznego wyznaczają poszczególne polityki i dokumenty wewnętrzne.

4.2. Współpraca, interakcja i ujawnienie informacji

CSIRT BOŚ współpracuje z innymi uczestnikami systemu funkcjonującego w oparciu o Ustawę o Krajowym Systemie Cyberbezpieczeństwa. Przekazuje tylko niezbędne informacje związane z obsługiwanymi incydentami. Wszelkie informacje i inne dane dotyczące poszczególnych incydentów, w tym dowody z nimi związane, są traktowane jako poufne. Komunikacja oraz ujawnienie informacji organom ścigania ma miejsce o ile stanowią o tym odrębne przepisy prawa (przepisy prawa powszechnie obowiązującego). CSIRT BOŚ w pełni wspiera protokół Information Sharing Traffic Light Protocol, o którym szczegółowe informacje są dostępne pod adresem: <https://www.trusted-introducer.org/ISTLP.pdf>. Dane osobowe są przetwarzane zgodnie z obowiązującym prawem. Bazy danych zawierające informacje wrażliwe są szyfrowane.

4.3. Komunikacja i uwierzytelnienie

Komunikacja mailowa jest oznaczana z wykorzystaniem Traffic Light Protocol. Dane w zależności od rodzaju mogą być przekazywane w różny sposób. Dane poufne powinny być dostarczane CSIRT BOŚ w formie zaszyfrowanej protokołem PGP/GPG (2.9). Pozostałe informacje mogą być dostarczane innymi dostępnymi kanałami. Jeśli wystąpią wątpliwości odnośnie do wyboru kanału zachęcamy do uprzedniego kontaktu z CSIRT BOŚ (2.5, 2.6, 2.7, 2.8, 2.9). Uwierzytelnienie przed nawiązaniem kontaktu może nastąpić w oparciu o publicznie dostępne informacje, m.in: portale społecznościowe, sieć Trusted Introducer i inne.

5. Usługi

5.1. Reagowanie na incydenty

W odpowiedzi na pojawiające się zagrożenia bezpieczeństwa teleinformatycznego, CSIRT BOŚ w obszarze działania (3.2) prowadzi czynności zabezpieczające poufność, integralność, dostępność oraz autentyczność informacji zgodnie z krajowymi i międzynarodowymi dokumentami oraz standardami. Poszczególne fazy obsługi incydentu:

Bank Ochrony Środowiska S.A.

 ul. Żelazna 32, 00-832 Warszawa  infolinia 801 355 455 | +48 22 543 34 34  www.bosbank.pl

Sąd Rejonowy dla m.st. Warszawy XIII Wydział Gospodarczy Krajowego Rejestru Sądowego 0000015525 | NIP 527 020 33 13 | Kapitał zakładowy: 929 476 710 zł

- 5.1.1. Detekcja i analiza incydentów
 - obserwacja i analiza zdarzeń występujących w systemach teleinformatycznych,
 - ustalenie autentyczności incyduentu,
 - rejestracja, analiza, klasyfikacja oraz nadanie priorytetu incyduentowi,
 - identyfikacja i zarządzanie ryzykiem w obszarze cyberbezpieczeństwa.
- 5.1.2. Koordynacja obsługi incyduentu
 - określenie początkowej przyczyny zdarzenia,
 - przygotowanie odpowiedzi na incyduent oraz strategii naprawczej,
 - przekazanie stosownych informacji zaangażowanym stronom w oparciu o ustalone kanały komunikacji.
- 5.1.3. Ocena i ewaluacja incyduentów
 - analiza post factum skompromitowanych elementów infrastruktury teleinformatycznej,
 - wyeliminowanie przyczyny oraz skutków incyduentu,
 - gromadzenie dowodów,
 - opracowanie wniosków,
 - przygotowanie rekomendacji,
 - utworzenie procedur i dokumentów obsługi incyduentów w oparciu o pozyskaną wiedzę,
 - stałe doskonalenie procesów i aktualizacja dokumentów.
- 5.2. Czynności prewencyjne
 - ulepszanie narzędzi bezpieczeństwa z uwzględnieniem nowych zagrożeń,
 - okresowa weryfikacja i dostosowanie procedur do zmieniających się wektorów ataku,
 - zewnętrzne i wewnętrzne skany infrastruktury w ramach procesu identyfikacji podatności
- 5.3. Działania proaktywne
 - aktywny monitoring zagrożeń,
 - zarządzanie ujawnionymi podatnościami,
 - okresowe testy i audyty posiadanych zasobów oraz procesów,
 - okresowe szkolenie pracowników,
 - bieżące informowanie uczestników i podmiotów obszaru działania (pkt 3.2)
 - wymiana informacji z podmiotami systemu cyberbezpieczeństwa funkcjonującymi w ramach UKSC.

6. Formularze zgłaszania incyduentów

Uprzejmie prosimy o kontakt z infolinią Banku: +48 22 543 34 34; +48 801 355 455
bądź za pośrednictwem dedykowanego formularza:

https://wnioski.bosbank.pl/ords/f?p=FORMULARZE_WWW:INCYDENT_BEZPIECZENSTWA

Bank Ochrony Środowiska S.A.

 ul. Żelazna 32, 00-832 Warszawa  infolinia 801 355 455 | +48 22 543 34 34  www.bosbank.pl

Sąd Rejonowy dla m.st. Warszawy XIII Wydział Gospodarczy Krajowego Rejestru Sądowego 0000015525 | NIP 527 020 33 13 | Kapitał zakładowy: 929 476 710 zł

7. Zastrzeżenia

CSIRT BOŚ Bank dokłada wszelkiej staranności podczas opracowania informacji, ostrzeżeń i powiadomień. Jednocześnie zastrzega, że nie ponosi odpowiedzialności za błędy, pominięcia lub szkody powstałe wskutek wykorzystania informacji zawartych w niniejszym dokumencie.

RFC2350 CSIRT BOŚ został przygotowany w języku polskim. Tłumaczenie na język angielski może niejednoznacznie oddawać zawarte w dokumencie sformułowania. We wszystkich przypadkach, w których istnieją rozbieżności pomiędzy polskojęzyczną oraz anglojęzyczną wersją dokumentu, obowiązuje wersja polska dokumentu.