OPIS CSIRT/SOC DLA BANK POLSKIEJ SPÓŁDZIELCZOŚCI S.A.

1. O tym dokumencie

1.1. Data ostatniej aktualizacji

To jest wersja 1.0, opublikowana dnia 20 listopada 2020 r.

1.2. Lista dystrybucyjna dla powiadomień

Obecnie CSIRT/SOC nie używa list dystrybucyjnych do powiadamiania o zmianach w tym dokumencie.

1.3. Lokalizacje, w których można znaleźć ten dokument

Aktualna wersja tego opisu CSIRT/SOC jest dostępna na stronie internetowej Banku Polskiej Spółdzielczości S.A. Jego adres URL to https://www.bankbps.pl/

2. Informacje kontaktowe

2.1. Skrócona nazwa zespołu

SOC BPS

2.2. Nazwa zespołu

Security Operations Center Bank BPS

2.3. Adres CERT/SOC BPS

Bank Polskiej Spółdzielczości SA

ul. Grzybowska 81

00-844 - Warszawa

Polska

2.4. Strefa czasowa

Czas środkowoeuropejski (GMT+0100, GMT+0200 od kwietnia do października)

2.5. Numer telefonu

801 321 456 (opłata za połączenie wg taryfy operatora)

(+48) 86 215 50 00 (z telefonów komórkowych lub z zagranicy, opłata wg taryfy operatora)

2.6. Numer faksu

(+48) 86 215 50 01

2.7. Adres mailowy incydent@bankbps.pl

2.8. Klucze publiczne i inne informacje o szyfrowaniu

Aktualnie niedostępny

2.9. Inne informacje

Brak dostępu

2.10. Punkty kontaktu z Klientem

Preferowaną metodą kontaktu z SOC BPS jest e-mail na adres incydent@bankbps.pll

E-mail wysłany na ten adres będzie obsługiwany przez odpowiedzialnego człowieka.

Jeśli korzystanie z poczty elektronicznej nie jest możliwe (lub nie jest wskazane ze względów bezpieczeństwa), z SOC BPS można skontaktować się telefonicznie przez infolinię 24/7

Godziny pracy SOC BPS są zwykle ograniczone do zwykłych godzin pracy (07:00 - 19:00 CET / CEST od poniedziałku do piątku z wyjątkiem świąt).

3. Statut

3.1. Opis misji

Główną rolą SOC BPS jest obsługa operacyjna globalnych incydentów bezpieczeństwa teleinformatycznego z wczesnym ostrzeganiem, wykrywaniem zagrożeń, analizą złośliwego oprogramowania, wydawaniem komunikatów bezpieczeństwa, ocenami bezpieczeństwa i audytami, a także konsultacjami w dziedzinie bezpieczeństwa IT.

3.2. Domena

Domena SOC BPS to:

- ASN: AS21280
- IP: 193.30.160/24;
- Domeny: bankbps.pl

3.3. Sponsoring i/lub Przynależność

SOC BPS jest finansowo utrzymywany przez Bank Polskiej Spółdzielczości S.A., którego formalnie jest częścią.

3.4. Autorytet

SOC BPS działa pod patronatem i pod nadzorem delegowanym przez Bank Polskiej Spółdzielczości S.A.

SOC BPS oczekuje współpracy z administratorami systemu i użytkownikami (Klientami) w sieci Banku Polskiej Spółdzielczości. Jednakże, jeśli uzasadniają to okoliczności, SOC BPS jest uprawniony do podjęcia środków, które uzna za właściwe, aby odpowiednio obsłużyć incydent związany z bezpieczeństwem informacji.

4. Polityki

4.1. Rodzaje incydentów i poziom wsparcia

SOC BPS jest upoważniony do reagowania na wszelkiego rodzaju incydenty związane z bezpieczeństwem informacji, które występują lub mogą wystąpić w sieciach Banku Polskiej Spółdzielczości S.A.

Poziom wsparcia udzielanego przez SOC BPS będzie się różnić w zależności od rodzaju i wagi incydentu lub problemu, rodzaju elementu, ilości użytkowników, której dotyczy problem, oraz zasobów SOC BPS w tym czasie.

Zdarzenia będą traktowane priorytetowo według wagi i ważności.

4.2. Współpraca, interakcja i ujawnianie informacji

SOC BPS wymienia wszystkie niezbędne informacje z innymi zespołami CSIRT/SOC, a także z administratorami zainteresowanych stron. Żadne dane osobowe lub inne dane ogólne nie są wymieniane, chyba że wyraźnie to wskazano.

Wszystkie wrażliwe dane (takie jak dane osobowe, konfiguracje systemu, znane luki w zabezpieczeniach związane z ich lokalizacjami) są szyfrowane, jeśli muszą zostać przesłane przez niezabezpieczone środowisko.

4.3. Komunikacja i uwierzytelnianie

Nieszyfrowane wiadomości e-mail nie będą uważane za szczególnie bezpieczne, ale wystarczą do transmisji danych o niskiej czułości. Jeśli konieczne będzie przesłanie bardzo wrażliwych danych pocztą e-mail, zostanie użyte GPG. Sieciowe transfery plików zostaną uznane za podobne do poczty elektronicznej do tych celów: wrażliwe dane powinny być szyfrowane w celu transmisji.

5. Usługi

5.1. Reagowanie na incydenty

SOC BPS pomoże administratorom systemu w obsłudze technicznych i organizacyjnych aspektów incydentów. W szczególności zapewni pomoc lub poradę w odniesieniu do następujących aspektów zarządzania incydentami:

5.1.1. Analiza incydentu

- Badanie, czy rzeczywiście miał miejsce incydent,
- Określenie zakresu incydentu.

5.1.2. Koordynacja incydentów

- Ustalenie pierwotnej przyczyny incydentu (wykorzystana luka),
- Ułatwienie kontaktu z innymi stronami, które mogą być zaangażowane,
- W razie potrzeby ułatwianie kontaktu z odpowiednimi funkcjonariuszami organów ścigania,
- Robienie raportów do innych zespołów CSIRT/SOC,
- Redagowanie ogłoszeń dla użytkowników, jeśli dotyczy.

5.1.3. Rozwiązywanie incydentów

- Usunięcie podatności.
- Zabezpieczenie systemu przed skutkami incydentu.
- Zbieranie dowodów zdarzenia.

Ponadto SOC BPS będzie gromadzić statystyki dotyczące przetwarzanych incydentów i powiadomi społeczność w razie potrzeby, aby pomóc jej w ochronie przed znanymi atakami.

SOC BPS udziela porad, ale nie zapewnia fizycznego wsparcia klientom w zakresie rozwiązywania incydentów.

5.2. Usługi proaktywne

SOC BPS koordynuje i utrzymuje następujące usługi w możliwym zakresie, w zależności od zasobów:

- Usługi informacyjne za pośrednictwem następujących kanałów:
- strona internetowa: https://bankbps.pl
- Usługi szkoleniowe i edukacyjne

6. Formularze zgłaszania incydentów

SOC BPS obsługuje tylko incydenty zgłoszone e-mailem lub telefonicznie. Dane kontaktowe są dostępne na stronie: https://www.bankbps.pl/kontakt

7. Zastrzeżenia

Przy przygotowywaniu informacji, powiadomień i alertów zostaną podjęte wszelkie środki ostrożności. W związku z tym SOC BPS nie ponosi żadnej odpowiedzialności za błędy lub pominięcia, ani za szkody wynikające z wykorzystania informacji zawartych w raporcie.