RFC-2350
SOC SGB-Bank S.A.

1. Informacje o dokumencie

1.1. Lokalizacja dokumentu

Aktualną wersję dokumentu można znaleźć na stronie internetowej:

www.sgb.pl/kontakt

1.2. Uwierzytelnianie dokumentu

Dokument został podpisany kluczem PGP należącym do SGB-Banku S.A., którego sygnaturę można znaleźć na: www.sgb.pl/kontakt

2. Dane kontaktowe

2.1. Nazwa zespołu

SOC SGB-Bank S.A.

2.2. Adres zespołu

SOC SGB-Bank S.A.

SGB-Bank S.A.

ul. Szarych Szeregów 23a

60-462 Poznań

2.3. Strefa czasowa

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

2.4. Adres poczty elektronicznej

Wszystkie incydenty powinny być zgłaszane na adres mailowy: soc[at]sgb.pl

2.5. Klucze publiczne, informacje dotyczące szyfrowania

Klucz PGP SOC SGB-Bank S.A.

Fingerprint: 95BE4234FF79E9591D2DE01029BF0115CE729A1D

Klucz publiczny wraz z sygnaturą można znaleźć na:

https://www.sgb.pl/wp-content/uploads/sgb-bank_cert_pgp_key.txt

2.6. Członkowie zespołu

Zespół SOC SGB-Bank S.A. tworzą doświadczeni eksperci w dziedzinie cyberbezpieczeństwa, którzy dbają o bezpieczeństwo usług świadczonych przez SGB-Bank S.A.

3. Statut

3.1. Misja

Misją SOC SGB-Bank S.A. jest utrzymywanie bezpieczeństwa cyfrowych usług SGB-Banku S.A. na najwyższym poziomie oraz wspieranie Banków Spółdzielczych z Grupy SGB w obsłudze zagrożeń i incydentów z obszaru cyberbezpieczeństwa.

3.2. Grupa użytkowników (zakres działań)

SOC SGB-Bank S.A. wspiera w obsłudze incydentów bezpieczeństwa w sieci spółkę SGB-Bank S.A. oraz podmioty korzystające z jej infrastruktury teleinformatycznej. Pomaga też użytkownikom usług świadczonych przez Bank.

3.3. Finansowanie i przynależność

SOC SGB-Bank S.A. jest finansowany przez SGB-Bank S.A. i działa w ramach jego struktury.

3.4. Umocowanie

SOC SGB-Bank S.A. działa pod auspicjami i upoważnieniem kierownictwa SGB-Banku S.A. i jest związany wewnętrznymi regulacjami SGB-Banku S.A.

4. Polityki

4.1. Rodzaje incydentów oraz poziom wsparcia

SOC SGB-Bank S.A. obsługuje mogące wystąpić w SGB-Banku S.A. incydenty z obszaru cyberbezpieczeństwa.

SOC SGB-Bank S.A. nadaje priorytety incydentom, biorąc pod uwagę ich dotkliwość, zasięg i przedmiot sprawy. Następnie obsługuje je zgodnie z nadanym priorytetem. Poziom wsparcia od SOC SGB-Bank S.A. różni się w zależności od dotkliwości i rodzaju zgłoszenia, a także innych istotnych dla sprawy okoliczności.

4.2. Współpraca, interakcja i ujawnianie informacji

SOC SGB-Bank S.A. wymienia dane w ramach systemu cyberbezpieczeństwa, który funkcjonuje w ramach UKSC, z podmiotami realizującymi zadania z obszaru cyberbezpieczeństwa w dopuszczalnym przez prawo zakresie. Dane osobowe przetwarzane są zgodnie z obowiązującym prawem. Wrażliwe dane (dane osobowe, konfiguracje systemu, znane luki itd.) są szyfrowane, jeśli muszą być przesyłane w niezabezpieczonym środowisku. Wszystkie dane związane z obsługiwanymi incydentami bezpieczeństwa są poufne. Informacje zgromadzone w ramach obsługi incydentu przez SOC SGB-Bank S.A mogą

zostać przekazane podmiotom przewidzianym w ramach innych ustaw i rozporządzeń obowiązujących na terytorium RP.

SOC SGB-Bank S.A. uznaje i wspiera protokół Information Sharing Traffic Light Protocol (v1.1). Każda komunikacja z tagami wspieranymi przez TLP będzie odpowiednio obsługiwana.

Znaczenie kolorów TLP dla odbiorców wiadomości

TLP:RED	Odbiorcy nie mogą dzielić się przekazanymi informacjami z nikim, z wyjątkiem innych odbiorców tych wiadomości.
TLP:AMBER	Odbiorcy mogą dzielić się informacjami jedynie w obrębie swojej organizacji (a także jej klientów) z osobami, które muszą poznać wiadomości, oraz jedynie w zakresie niezbędnym do podjęcia stosownych działań.
TLP:GREEN	Odbiorcy mogą dzielić się informacji ze swoimi współpracownikami, w ramach swojej i partnerskich organizacji oraz w swoim środowisku. Nie można jednak udostępniać tych informacji przez publiczne kanały informacyjne.
TLP:WHITE	Dystrybucja informacji nie podlega żadnym ograniczeniom (z wyjątkiem praw autorskich).

4.3. Komunikacja i uwierzytelnianie

SOC SGB-Bank S.A. jest zobowiązany do przestrzegania przepisów i zasad obowiązujących w Polsce i Unii Europejskiej w sprawach dotyczących informacji wrażliwych.

Wszelkie wiadomości e-mail powinny być oznaczone za pomocą standardów TLP. Dane o niskiej wrażliwości można wysyłać za pomocą niezaszyfrowanych wiadomości e-mail, jednak nie jest to uznawane za bezpieczne. Zalecane jest szyfrowanie PGP, szczególnie w przypadku poufnych danych.

5. Usługi

5.1. Reakcja na incydenty

Dla incydentów występujących w grupie użytkowników, SOC SGB-Bank S.A. świadczy szeroki zakres usług obejmujący m.in:

5.1.1. Wykrywanie i analizę incydentów

- Określenie autentyczności zdarzenia

- Określenie początkowej przyczyny zdarzenia
- Definiowanie adekwatnej odpowiedzi
- Ocena dotkliwości
  - Ewaluacja potencjalnego ryzyka wystąpienia efektów
  - Ewaluacja potencjalnej skali incydentu oraz zasobów dotkniętych przez niego
  - Priorytetyzacja incydentów
- Gromadzenie dowodów oraz wskaźników kompromitacji
- Analiza złośliwego oprogramowania

5.1.2. Ograniczenie zagrożenia, plany naprawcze

- Przygotowanie strategii naprawczej post factum
- Tworzenie zaleceń dotyczących poprawy bezpieczeństwa dla administratorów systemu
- Opracowanie procedur obsługi różnych typów incydentów bezpieczeństwa

5.1.3. Ocena i ewaluacja incydentów

- Korelacja incydentów na podstawie zebranych danych
- Stałe poszukiwanie sposobów na poprawę wydajności zespołu
- Tworzenie raportów i zabezpieczanie ich do późniejszego wykorzystania

5.2. Zapobieganie

- Koordynacja odpowiedzi na zidentyfikowane podatności
- Zbieranie danych dotyczących zagrożeń bezpieczeństwa i znanych wskaźników kompromitacji ze zróżnicowanych źródeł
- Obserwacja aktualnych zagrożeń w technologii i bezpieczeństwie
- Tworzenie i ulepszanie narzędzi i mechanizmów bezpieczeństwa mających na celu ciągłe zwiększanie poziomu bezpieczeństwa

5.3. Czynności proaktywne

- Współtworzenie ogłoszeń o nowych zagrożeniach dla klientów
- Szkolenia oraz inne aktywności (w tym również symulacje rzeczywistych incydentów) przyczyniające się do poprawy wydajności zespołu

6. Zgłaszanie incydentów bezpieczeństwa

Incydenty bezpieczeństwa powinny zostać zgłoszone za pośrednictwem poczty szyfrowanej na adres soc[at]sgb.pl. W celu usprawnienia obsługi incydentu, zgłaszając incydent bezpieczeństwa, należy podać:

- Dane identyfikacyjne i kontaktowe osoby zgłaszającej
- Datę i godzinę wystąpienia i wykrycia zdarzenia
- Opis zdarzenia, opis okoliczności jego wykrycia oraz źródło informacji o zdarzeniu.

7. Zastrzeżenia

SOC SGB-Bank S.A. podczas przygotowania informacji, powiadomień oraz alertów bezpieczeństwa podejmie wszelkie dostępne środki ostrożności.

SOC SGB-Bank S.A. zastrzega, że nie ponosi odpowiedzialności za błędy, pominięcia oraz szkody wynikające z informacji zawartych w tym dokumencie.

Metryka dokumentu

Tytuł:	RFC-2350 SOC SGB-Bank S.A.
Data wygaśnięcia dokumentu:	Dokument jest obowiązujący do czasu wydania kolejnej jego wersji.
Właściciel:	SGB-Bank S.A.
Obecna wersja:	1.1
Data publikacji obecnej wersji:	13.04.2021