CERT mBANK

RFC 2350

Kontrola Dokumentu

Zatwierdzenie

	Imię i nazwisko	Data
Przygotowany przez:	Jarosław Stasiak	2017.10.20
Zatwierdzony przez:	Jarosław Górski	2017.10.26

Historia

Data	Wydanie	Autor	Zmiana
2017.10.20	1.0	Jarosław Stasiak	Wersja inicjalna

Spis Treści:

1. Informacje o dokumencie

Dokument zawiera opis CERT mBank bazujący na standardzie RFC2350. Przedstawione są tutaj informacje na temat zespołu CERT mBank, sposobów komunikacji oraz świadczonych przez zespół usług.

1.1. Data ostatniej aktualizacji

Wersja 1.0 wydana 20 października 2017

1.2. Lista dystrybucyjna dla powiadomień

Nie jest prowadzona lista dystrybucyjna dla powiadomień.

1.3. Lokalizacja dokumentu

Aktualna wersja tego dokument jest dostępna w formacie PDF na stronie mBanku. URL do dokumentu: https://www.mbank.pl/pdf/inne/cert-mbank-rfc2350.pdf

1.4. Wiarygodność dokumentu

Tekstowa wersja dokumentu została podpisana kluczem PGP CERT mBank. Klucz można znaleźć na stronie mBanku:
https://www.mbank.pl/pomoc/info/certyfikat/cert-mbank.asc

2. Informacje kontaktowe

2.1. Nazwa zespołu

CERT mBank
Pełna nazwa: Cyber Security Response Team of mBank S.A.

2.2. Adres

mBank S.A.
CERT mBank
ul. Kilińskiego 74
90-257 Łódź
Polska

2.3. Data utworzenia

CERT mBank został utworzony w grudniu 2016

2.4. Strefa Czasowa

GMT +0100 - Central European Time (CET)
GMT +0200 - Daylight Saving Time (from last Sunday in March to last Sunday in October)

2.5. Numer Telefonu

+48 42 218 67 67

2.6. Numer Faksu

+48 42 218 67 24

2.7. Pozostałe możliwości komunikacji

Brak

2.8. Adres poczty elektronicznej

Wszystkie zgłoszenia prosimy kierować na adres <cert(at)mbank.pl>

2.9. Klucze publiczne oraz informacje o szyfrowaniu

Informacje o kluczu PGP CERT mBank:

ID klucza: 0x873D6686
Odcisk palca: 9E9D11C6D3B85233D3E7FFD1038048FE873D6686

Klucz publiczny można znaleźć na stronie CERT mBank:

https://www.mbank.pl/bezpieczenstwo/certyfikaty/

2.10. Członkowie Zespołu

Menedżerem zespołu jest Jarosław Stasiak. Zespół składa się z kilku Analityków Bezpieczeństwa IT.

2.11. Punkt kontaktowy dla klientów

Preferowaną metodą kontaktu jest wysłanie wiadomości e-mail. Pytania prosimy kierować na adres:

<cert(at)mbank.pl>

Dyżurny Analityk odpowiada na maile w godzinach pracy zespołu (24/7/365). W uzasadnionych pilnych sytuacjach możliwy jest bezpośredni kontakt telefoniczny pod numerem telefonu (+48 42 218 67 67). Dyżur telefoniczny prowadzony jest w polskich godzinach roboczych.

3. Charakterystyka

3.1. Misja

Główne cele CERT mBank:

- zapobiegać oraz przewidywać incydentom cyberbezpieczeństwa poprzez implementację odpowiednich procesów, narzędzi i polityk.
- Dostarczać odpowiednie wsparcie operacyjne w celu obsługi incydentów cyberbezpieczeństwa (w trybie 24x7x365) dotyczących klientów, pracowników, partnerów i akcjonariuszy.
- Wspierać pracowników w implementacji proaktywnych środków minimalizujących ryzyko wystąpienia incydentów cyberbezpieczeństwa. Także w ramach konsultacji i szkoleń.

3.2. Obszar działania

CERT mBank wspiera pracowników oraz klientów mBank.

3.3. Finansowanie

CERT mBank to prywatny podmiot w sektorze finansowym. Jest finansowany przez mBank S.A.
CERT mBank jest członkiem stowarzyszenia Trusted Introducer https://www.trusted-introducer.org/directory/teams/cert-mbank.html . Komunikuje się także z innymi zespołami CERT.

3.4. Kompetencje

CERT mBank pracuje z polecenia i pod patronatem Chief Security Officer mBank S.A. (CSO). CERT mBank koordynuje incydentami bezpieczeństwa Pracowników oraz Klientów.

4. Polityki

4.1. Typy incydentów i poziom wparcia

CERT mBank jest upoważniony do obsługi wszystkich typów incydentów cyberbezpieczeństwa oraz cyber ataków występujących w obszarze działania (sekcja 3.2)

Wszystkie zgłoszenia otrzymane przez CERT mBank są analizowane, klasyfikowane i priorytetyzowane zgodnie z wewnętrznymi wytycznymi tak by utrzymać odpowiedni poziom usług.

Zasoby zostaną przypisane w szczególności do następujących zagadnień:

- Zagrożenie bezpieczeństwa fizycznego ludzi
- Ataki na poziomie root lub systemu operacyjnego w dowolnej części sieci lub usługi banku

- kompromitacja kont serwisowych lub aplikacji, w szczególności używanych w krytycznych aplikacjach przetwarzających poufne informacje
- ataki na odmowę usługi lub inne próby ograniczenia dostępności usług lub przetwarzania informacji w krytycznych systemach
- wysoko skalowane ataki dowolnego typu, np. inżynieria społeczna celowana w pracowników, klientów banku, dystrybucja złośliwego oprogramowania, wyciek danych
- groźby i inne przestępstwa dotyczące indywidualnych użytkowników
- kompromitacja indywidualnych kont użytkowników, kompromitacja stacji roboczych
- fałszerstwo lub inne naruszenia związane z bezpieczeństwem lokalnych regulacji

Pozostałe typy incydentów będą priorytetyzowane według poziomu, stopnia i zasięgu zagrożenia.

4.2. Współpraca, interakcja i ujawnianie informacji

CERT mBank współpracuje z innymi zespołami CERT. Współpraca polega między innymi na wymianie informacji o incydentach, zagrożeniach i podatnościach. Niemniej jednak CERT mBank działa zgodnie z wymaganiami polskiego prawa oraz tajemnicy bankowej.

Na mocy zobowiązania o ochronie prywatności obszaru chronionego (sekcja 3.2) CERT mBank w standardowych okolicznościach przekazuje dane zanonimizowane.

4.3. Komunikacja i uwierzytelnienie

CERT mBank chroni dane wrażliwe zgodnie z Polskimi i Europejskimi regulacjami.

Dla standardowej komunikacji CERT mBank może używać standardowej komunikacji takiej jak nieszyfrowana poczta elektroniczna lub telefon.

Do bezpiecznej komunikacji CERT mBank używa poczty szyfrowanej PGP. W celu uwierzytelnienia osoby przed nawiązaniem kanału komunikacji możliwe jest użycie istniejących stron społeczności takich jak Trusted Introducer, FIRST itp, ewentualnie innych metod taki jak oddzwonienie czy spotkanie jeśli jest to wymagane.

CERT mBank deklaruje pełne wsparcie dla ISTLP (Information Sharing Traffic Light Protocol).

5. Usługi

5.1. Reagowanie na incydenty

CERT mBank wspiera administratorów systemów w obsłudze i zarządzaniu incydentami. W szczególności prowadzi wsparcie na poszczególnych następujących fazach obsługi incydentu:

5.1.1 Ocena incydentu

- weryfikacja czy incydent jest autentyczny
- wycena, klasyfikacja i priorytetyzacja incydentu

5.1.2 Koordynacja obsługi incydentu

- określanie początkowej przyczyny incydentu
- ułatwianie kontaktu z innymi stronami objętymi incydentem
- ułatwienie kontraktu z innymi odpowiednimi zespołami cyberbezpieczeństwa
- przygotowywanie ogłoszeń dla użytkowników
- przygotowywanie raportów

5.1.3 Rozwiązywanie incydentu

- wparcie techniczne przy dochodzeniu, włączając analizę skompromitowanego systemu
- likwidacja i eliminacja przyczyny incydentu oraz skutków incydentu
- zbieranie dowodów w celu wszczęcia śledztwa (jeśli wymagane)
- rekomendacja ulepszeń bezpieczeństwa dla administratorów i managerów biznesowych

Dodatkowo CERT mBank zbiera statystyki dotyczące incydentów w obszarze działania. Na podstawie tych danych przygotowywane są powiadomienia dla odbiorców oraz opracowywane metody odpierania znanych ataków.

5.2. Proaktywne aktywności

CERT mBank dokłada starań aby ograniczyć liczbę oraz skutki incydentów. Prowadzone są następujące zadania:

- obserwacja aktualnych trendów technologicznych oraz trendów bezpieczeństwa
- kampanie uświadamiające (np. o aktualnych zagrożeniach)
- szkolenia i symulacje dla użytkowników i klientów
- wparcie z zakresu cyberbezpieczeństwa
- skanowanie podatności
- analiza dowodowa
- raportowanie wywiadowcze

6. Formularze zgłaszania incydentów

Poprzez email lub telefon.

7. Zastrzeżenia

Podczas przygotowywania wszelkich informacji, powiadomień i alertów zostaną podjęte wszelkie środki ostrożności, jednak CERT mBank nie ponosi odpowiedzialności za błędy lub pominięcia oraz szkody wynikające z wykorzystania informacji zawartych w tym dokumencie.