RFC-2350

CERT Alior

Metryka dokumentu:

Tytuł:	RFC-2350 CERT Alior
Data wydania pierwszej wersji:	13.05.2019
Data wygaśnięcia dokumentu:	Dokument jest obowiązujący do czasu wydania kolejnej jego wersji.
Właściciel:	Alior Bank S.A.
Obecna wersja:	1.0
Data publikacji obecnej wersji:	13.05.2019

1. Informacje na temat dokumentu

1.1. Data ostatniej aktualizacji

To jest wersja 1.0, wydana 13.05.2019.

1.2. Lista dystrybucyjna powiadomień

Obecnie CERT Alior nie korzysta z żadnej listy dystrybucyjnej mającej na celu powiadamianie o zmianach w tym dokumencie.

1.3. Lokalizacje w których można znaleźć ten dokument

Aktualna wersja dokumentu może być znaleziona na https://www.aliorbank.pl/dodatkowe-informacje/bezpieczenstwo/cert-alior.html

1.4. Uwierzytelnianie tego dokumentu

Ten dokument został podpisany kluczem PGP należącym do CERT Alior. Jego sygnaturę można znaleźć na: https://www.aliorbank.pl/dodatkowe-informacje/bezpieczenstwo/cert-alior.html

2. Dane kontaktowe

2.1. Nazwa zespołu

CERT Alior

2.2. Adres zespołu

CERT Alior
Alior Bank S.A.
Łopuszańska 38 D
02-232 Warszawa
Polska

2.3. Data założenia

CERT Alior został założony w październiku 2010.

2.4. Strefa czasowa

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

2.5. Numer telefonu

+48 22 5552925

2.6. Adres poczty elektronicznej

Wszystkie incydenty powinny być raportowane na cert[at]alior.pl

2.7. Klucze publiczne, informacje dotyczące szyfrowania

Klucz publiczny wraz ze swoją sygnaturą może być znaleziony na
https://www.aliorbank.pl/dodatkowe-informacje/bezpieczenstwo/cert-alior.html

2.8. Członkowie zespołu

Zespół CERT Alior składa się z doświadczonych ekspertów w dziedzinie zagadnień cyberbezpieczeństwa.

2.9. Inne informacje

Więcej informacji na temat zespołu CERT Alior można znaleźć na:
https://www.aliorbank.pl/dodatkowe-informacje/bezpieczenstwo/cert-alior.html

3. Statut

3.1. Misja

Celem zespołu CERT Alior jest podejmowanie działań minimalizujących prawdopodobieństwo wystąpienia incydentów cyberbezpieczeństwa, oraz aktywności minimalizujących skutek ich wystąpienia w grupie swoich użytkowników (w zakresie świadczonych usług).

3.2. Grupa użytkowników

CERT Alior zapewnia wsparcie w zakresie obsługi zdarzeń bezpieczeństwa dla Alior Bank S.A., uniwersalnego banku w Polsce, w tym podmiotów korzystających z infrastruktury sieciowej Banku i systemów informatycznych, a także użytkowników platform serwisowych Banku w zakresie świadczonych usług.

3.3. Sponsoring oraz afiliacje

CERT Alior operuje w ramach Alior Bank S.A.

3.4. Autorytet

CERT Alior działa pod auspicjami i upoważnieniem kierownictwa Alior Banku.

4. Polityki

4.1. Typy incydentów oraz poziom wsparcia

CERT Alior jest upoważniony do obsługi wszystkich rodzajów incydentów związanych z bezpieczeństwem komputerów i sieci, które mogą wystąpić w grupie użytkowników CERT Alior (w zakresie usług świadczonych dla tych użytkowników).

CERT Alior nadaje priorytet incydentom - odpowiednio do ich dotkliwości, zasięgu i przedmiotu sprawy. Incydenty są obsługiwane zgodnie z nadanym priorytetem. Poziom wsparcia udzielanego przez CERT Alior będzie się różnić w zależności od dotkliwości i rodzaju zgłoszenia, a także innych istotnych dla sprawy okoliczności.

4.2. Współpraca, interakcja i ujawnianie informacji

CERT Alior wymienia wszystkie niezbędne do współpracy informacje z innymi zespołami CSIRT, a także z administratorami zainteresowanych stron. Żadne dane osobowe nie są wymieniane, chyba że za wyraźnym upoważnieniem. Wszystkie wrażliwe dane (takie jak dane osobowe, konfiguracje systemu, znane luki w ich lokalizacjach) są szyfrowane, jeśli muszą być przesyłane w niezabezpieczonym środowisku.

CERT Alior uznaje i wspiera protokół Information Sharing Traffic Light Protocol (v1.1). Każda komunikacja z tagami wspieranymi przez TLP będzie odpowiednio obsługiwana.

4.3. Komunikacja i uwierzytelnianie

CERT Alior 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. Odpowiedź na incydenty

Dla incydentów występujących w grupie użytkowników, CERT Alior świadczy szeroki zakres usług, w tym:

5.1.1. Detekcja i analiza incydentów

- Określanie autentyczności zdarzenia
- Określenie początkowej przyczyny zdarzenia
- Definiowanie adekwatnej odpowiedzi
- Ocena dotkliwości
    - Ewaluacja potencjalnego ryzyka wystąpienia prawdziwych efektów
    - Ewaluacja potencjalnej skali incydentu oraz zasobów dotkniętych przez niego.
    - Ustalenie priorytetu incydentu
- Zbieranie dowodów oraz wskaźników kompromitacji
- Analiza złośliwego oprogramowania
- Inżynieria wsteczna

5.1.2. Ograniczenie zagrożenia, plany naprawcze

- Przygotowanie strategii naprawczej post factum
- Tworzenie zaleceń dotyczących ulepszeń 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 wykorzystania w przyszłości.

5.2. Prewencja

- 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) w celu poprawy wydajności zespołu

6. Raportowanie incydentów bezpieczeństwa

Incydenty bezpieczeństwa powinny być raportowane za pośrednictwem poczty szyfrowanej na adres cert[at]alior.pl.

7. Zastrzeżenia

Zastrzega się, że mimo pomimo że wszelkie dostępne środki ostrożności zostaną powzięte podczas przygotowania informacji, notyfikacji oraz alarmów bezpieczeństwa, CERT Alior (oraz Alior Bank S.A.) nie ponosi odpowiedzialności za błędy, pominięcia oraz szkody wynikające z informacji w nich zawartych.