CSIRT Talex

RFC-2350

Informacje o dokumencie

Tytuł:	Wersja:	Data publikacji:
RFC-2350 CSIRT Talex	1.0	17.03.2020

1. **Informacje o dokumencie**
   - **1.1. Data ostatniej aktualizacji**
     To jest wersja 1.0 opublikowana 17 Marca 2020 roku.
   - **1.2. Lista dystrybucyjna powiadomień**
     W chwili obecnej informacje o zmianach w dokumencie nie są publikowane za pomocą list dystrybucyjnych.
   - **1.3. Miejsce składowania dokumentu**
     Najnowsza wersja niniejszego dokumentu jest dostępna na stronie WWW Talex S.A. pod adresem *https://www.talex.pl/pl/CSIRT*.
   - **1.4. Wiarygodność dokumentu**
     Ten dokument został podpisany kluczem PGP Talex S.A. Sygnaturę klucza PGP można znaleźć na stronie *https://www.talex.pl/pl/CSIRT*.
2. **Dane kontaktowe**
   - **2.1. Nazwa zespołu**
     CSIRT Talex
   - **2.2. Adres**
     CSIRT Talex
     Talex S.A.
     ul. Karpia 27d
     61-619 Poznań
     Polska
   - **2.3. Data utworzenia**
     CSIRT Talex został utworzony w grudniu 2017 roku.
   - **2.4. Strefa Czasowa**
     Central European Time (CET)
     GMT +0100 od listopada do marca
     GMT +0200 od kwietnia do października
   - **2.5. Numer Telefonu**
     +48 61 827 55 00
   - **2.6. Numer Faksu**
     +48 61 827 55 99
   - **2.7. Pozostałe możliwości komunikacji**
     Brak.
   - **2.8. Adres poczty elektronicznej**
     Informacje o incydentach prosimy przesyłać na adres <csirt(at)talex.pl>.

2.9. Klucze publiczne oraz informacje o szyfrowaniu

Do szyfrowania przesyłanej komunikacji e-mail wykorzystywany jest mechanizm PGP (Pretty Good Privacy).

Klucz publiczny CSIRT Talex oraz jego sygnatura są dostępne pod następującym adresem:
https://www.talex.pl/pl/CSIRT

2.10. Członkowie Zespołu

Zespół CSIRT Talex tworzą dedykowani specjaliści z zakresu cyberbezpieczeństwa z wieloletnim doświadczeniem w w/w obszarze i pokrewnych obszarach IT.

2.11. Punkt kontaktowy dla klientów

Preferowaną formą kontaktu jest kontakt poprzez pocztę elektroniczną na adres <csirt(at)talex.pl>. Prosimy o przesyłanie wiadomości szyfrowanych z użyciem podanego w dokumencie klucza PGP. W sytuacjach wymagających pilnego kontaktu prosimy o kontakt telefoniczny na numer +48 827 55 00. Dyżur prowadzony jest w godzinach roboczych obowiązujących w Polsce.

3. Statut

3.1. Misja

Zespół CSIRT Talex postrzega swoją misję jako działalność na rzecz zapewnienia przyjaznych kosztowo usług cyberbezpieczeństwa oraz zapobiegania i reagowania na incydenty bezpieczeństwa IT dla Spółki oraz jej klientów.

3.2. Obszar działania

CSIRT Talex zapewnia wsparcie dla Spółki oraz jej klientów.

3.3. Finansowanie i afiliacja

CSIRT Talex jest podmiotem komercyjnym działającym w ramach spółki Talex S.A.

3.4. Autoryzacja działania

CSIRT Talex działa z upoważnienia i pod patronatem Zarządu spółki Talex S.A.

4. Polityki

4.1. Typy incydentów oraz poziom wsparcia

CSIRT Talex jest upoważniony do obsługi wszystkich incydentów cyberbezpieczeństwa występujących w środowiskach IT Spółki i jej klientów (w zakresie wskazanym w umowach).

Zgłoszenia przekazywane do CSIRT Talex są analizowane, klasyfikowane i nadawane są im priorytety zgodnie z przyjętymi regułami. Poziom wsparcia jest uzależniony od dotkliwości incydentu, jego zasięgu oraz dostępnych zasobów. Poziom wsparcia oraz czas obsługi incydentu w przypadku zgłoszeń przekazanych w ramach usług świadczonych przez CSIRT dla klientów Spółki wynika z zapisów zamieszczonych w umowach dotyczących tych usług.

4.2. Współpraca, interakcja i ujawnianie informacji

CSIRT Talex deklaruje wolę współpracy z innymi CERT/CSIRT oraz pracownikami klientów Spółki. Dane przekazane do CSIRT Talex są chronione zgodnie z polskimi i europejskimi aktami prawnymi. Żadne dane osobowe nie są wymieniane bez jednoznacznej zgody zainteresowanej strony. Informacje przekazywane dalej są anonimizowane.

4.3. Komunikacja i uwierzytelnianie

Przesyłanie danych wrażliwych podlega szyfrowaniu. Zaleca się użycie mechanizmu PGP. Miejsce składowania kluczy PGP CSIRT Talex wskazano w punkcie 2.9. Do komunikacji operacyjnej o niskim poziomie wrażliwości akceptuje się użycie kanałów nieszyfrowanych.

Uwierzytelnienie nadawcy przed nawiązaniem kanału komunikacji odbywa się poprzez weryfikację klucza PGP lub z użyciem dostępnych metod potwierdzenia tożsamości (np. kontakt bezpośredni).

CSIRT Talex wspiera komunikację z użyciem zbioru reguł TLP (Traffic Light Protocol). Wiadomości elektroniczne zawierające dane wrażliwe powinny być oznaczane zgodnie ze standardem TLP.

5. Usługi

5.1. Odpowiedź na incydenty

CSIRT Talex świadczy usługi dla administratorów Spółki i jej klientów w następującym zakresie:

5.1.1. Ocena incydentu

- analiza autentyczności danego zdarzenia,
- klasyfikacja oraz określenie priorytetu incydentu.

5.1.2. Koordynacja obsługi incydentu

- określenie przyczyn zdarzenia i zasięgu oddziaływania,
- zebranie danych do analizy oraz ich kategoryzacja,
- powiadomienie stron zaangażowanych w obsługę incydentu,
- przygotowanie komunikacji do użytkowników końcowych,
- przygotowanie raportów.

5.1.3. Obsługa incydentu

- usunięcie przyczyny incydentu,
- wsparcie likwidacji skutków incydentu,
- zabezpieczenie i zebranie dowodów na potrzeby ewentualnego śledztwa,
- przegotowanie zaleceń „Lesson learning” dla administratorów.

5.2. Działania prewencyjne

Zespół CSIRT Talex dokłada starań aby aktywnie przeciwdziałać incydentom poprzez następujące działania prewencyjne:

- ulepszanie reguł korelacyjnych w celu poprawienia wykrywania danego typu incydentu w przyszłości,

- akcje informacyjne i e-learningi kierowane do pracowników Spółki i klientów podnoszące świadomość w zakresie cyberbezpieczeństwa,
- zbieranie i analiza informacji oraz powiadamianie o wykrytych zagrożeniach dla administratorów Spółki i jej klientów,
- konsultacje w zakresie technologii, organizacji pracy IT oraz cyberbezpieczeństwa,
- skanowanie podatności.

6. Raportowanie incydentów bezpieczeństwa

Prosimy o przesyłanie raportów o incydentach bezpieczeństwa na adres poczty elektronicznej podany w punkcie 2.11. Zgłoszenia kierowane do CSIRT Talex powinny zawierać jako minimum informacje o systemach, których dotyczą, datę i godzinę wystąpienia, opis zdarzenia oraz wskazanie czy dotyczą one spółki Talex S.A. czy jej klientów.

7. Zastrzeżenia

CSIRT Talex dokłada wszelkich starań aby przygotowywane informacje, powiadomienia i alarmy były prawidłowe i adekwatne, jednakże nie ponosi odpowiedzialności za ewentualne błędy lub pominięcia oraz szkody wynikające z wykorzystania informacji w nich zawartych.