RFC 2350

1. Informacje o dokumencie

Ten dokument zawiera opis zespołu bezpieczeństwa - Działu Zarządzania Bezpieczeństwem Giełdy Papierów Wartościowych w Warszawie (DZB GPW) - zgodnie z RFC 2350.

Dostarcza podstawowych informacji o DZB GPW, sposobach kontaktu, opisuje obowiązki zespołu i oferowane usługi.

1.1 Data ostatniej aktualizacji

To jest wersja 1.0, opublikowana 2023-07-12

1.2 Lista dystrybucyjna dla powiadomień

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

1.3 Miejsca, w których można znaleźć niniejszy dokument

Aktualna wersja dokumentu jest dostępna pod adresem:
https://www.gpw.pl/pub/GPW/RFC2350_PL_GPW.txt
An English version of this document is also available:
https://www.gpw.pl/pub/GPW/RFC2350_EN_GPW.txt
Upewnij się, że używasz najnowszej wersji.

1.4 Uwierzytelnienie niniejszego dokumentu

Zarówno polska, jak i angielska wersja tego dokumentu została podpisana kluczem PGP zespołu DZB GPW.

2. Dane kontaktowe

2.1 Nazwa zespołu

Dział Zarządzania Bezpieczeństwem Giełdy Papierów Wartościowych w Warszawie - DZB GPW

2.2 Adres

GPW
Giełda Papierów Wartościowych w Warszawie S.A. / The Warsaw Stock Exchange
ul. Książęca 4
00-498 Warszawa
Polska

2.3 Strefa czasowa

UTC +0100 - Czas środkowoeuropejski (CET)
UTC +0200 - Czas środkowoeuropejski letni (CEST - od ostatniej niedzieli marca do ostatniej niedzieli października)

2.4 Numer telefonu

+48 22 53 777 08
+48 669 55 1111

2.5 Numer faksu

Niedostępne

2.6 Inne środki komunikacji

Niedostępne

2.7 Adres poczty elektronicznej

security@gpw.pl

2.8 Klucze publiczne i informacje o szyfrowaniu

Klucz PGP używany przez DZB GPW:

KeyID: 0x4941A9E7

Fingerprint: 49F2 6339 2259 0E47 DE3B 97F6 F174 3269 4941 A9E7

Klucz publiczny można znaleźć pod adresem:

https://www.gpw.pl/pub/GPW/RFC2350_klucz_PGP.txt

2.9 Członkowie zespołu

Zespół DZB GPW składa się z doświadczonych ekspertów w dziedzinie zagadnień cyberbezpieczeństwa.

2.10 Pozostałe informacje

Ogólne informacje o dotyczące zasad cyberbezpieczeństwa GPW można znaleźć na stronie https://www.gpw.pl/zasady-cyberbezpieczenstwa

3. Statut

3.1 Misja

DZB GPW ma za zadanie budować kompetencje i zdolności w zakresie unikania, identyfikowania i ograniczania cyberzagrożeń, w szczególności ma za zadanie zapobiegać wystąpieniu incydentów cyberbezpieczeństwa poprzez wdrażanie odpowiednich procesów, narzędzi, polityk w celu poprawy reaktywności w przypadku incydentu, a także zapewnienia wsparcia operacyjnego przy obsłudze poważnych incydentów cyberbezpieczeństwa, które mogą mieć wpływ na majątek i interesy Spółek Grupy Kapitałowej GPW

3.2 Finansowanie i powiązania

DZB GPW jest powiązane z Grupą Kapitałową GPW.

3.3 Autorytet

DZB GPW działa w zgodzie ze standardami zarządzania bezpieczeństwem Giełdy Papierów Wartościowych w Warszawie i podlega zwierzchnictwu Dyrektora Działu Zarządzania Bezpieczeństwem GPW.

4. Polityki

4.1 Rodzaje incydentów i poziom wsparcia

DZB GPW jest upoważniony do obsługi wszystkich rodzajów incydentów cyberbezpieczeństwa, które mają miejsce lub mogą wystąpić w jego obszarze działania. Wszystkie zgłoszenia incydentów otrzymywane przez DZB GPW są analizowane, klasyfikowane i priorytetyzowane zgodnie z wewnętrznymi regulacjami, tak aby zapewnić sprawny i odpowiedni poziom obsługi.

4.2 Współpraca, współdziałanie i ujawnianie informacji

DZB GPW zobowiązuje się do otwartej i przejrzystej współpracy z naszymi zaufanymi partnerami, w tym międzynarodową społecznością CERT, zgodnie z prowadzoną polityką Giełdy Papierów Wartościowych. Z tego powodu wszystkie zespoły CERT na całym świecie mogą kontaktować się

z DZB GPW (security@gpw.pl) w celu ustalenia zasad współpracy, pytań lub inicjatyw wymiany informacji, jeśli jest to konieczne.

4.3 Komunikacja i uwierzytelnianie

Preferowaną metodą kontaktu z DZB GPW jest poczta elektroniczna. Podstawowy adres e-mail: security@gpw.pl

Zachęcamy naszych klientów do korzystania z narzędzi kryptograficznych PGP/GPG podczas wysyłania poufnych informacji do DZB GPW.

Jeśli korzystanie z poczty elektronicznej nie jest możliwe (lub nie jest wskazane ze względów bezpieczeństwa), z DZB GPW można skontaktować się telefonicznie w regularnych godzinach pracy na numery telefonów wskazane w sekcji 2.4.

Godziny pracy DZB GPW są ograniczone do regularnych godzin pracy (08:00-16:00 od poniedziałku do piątku z wyjątkiem dni ustawowo wolnych od pracy w Polsce).

5. Usługi

5.1 Reagowanie na incydenty

Ta usługa ma na celu prowadzenie rozpoznania i koordynację reagowanie na incydenty cyberbezpieczeństwa . Działania wspierające i koordynujące incydent obejmują ocenę dostępnych informacji, ich walidację i weryfikację, zebranie dodatkowych dowodów, komunikację z odpowiednimi stronami, a na końcu zaproponowanie rozwiązań w celu rozwiązania incydentu.

5.2 Monitoring

Ta usługa ma na celu wykrywanie zdarzeń cyberbezpieczeństwa wraz z ich analizą mającą na celu określenie autentyczności, przyczyny, dotkliwości oraz adekwatnej reakcji dotyczącej zdarzenia.

5.3 Działania prewencyjne

Działania prewencyjne obejmują identyfikację istniejących podatności cyberbezpieczeństwa systemów informatycznych oraz bieżące poszerzanie posiadanych danych dotyczących zagrożeń.

5.4 Działania proaktywne

DZB GPW prowadzi szkolenia oraz sporządza okresowe raporty informujące o potencjalnych zagrożeniach.

6. Formularze zgłaszania incydentów

Zgłaszanie incydentów bezpieczeństwa odbywa się za pomocą szyfrowanej poczty elektronicznej na adres security@gpw.pl z wykorzystaniem klucza PGP. W zgłoszeniu należy w miarę możliwości podać następujące informacje:

- Informacje kontaktowe
  - Imię i nazwisko osoby zgłaszającej, adres email i numer telefonu.
- Data i czas zdarzenia.
- Opis incydentu bezpieczeństwa.
  - Rodzaj incydentu
    - Utrata danych/narażenie danych
    - Uszkodzenie systemu
    - Strata finansowa
    - Naruszenie regulaminu
    - Naruszenie polityki bezpieczeństwa informacji lub procedury

        - Obecnie nieznany
        - Podejrzany email (Spam/phishing, link bądź załącznik)
        - Inne
    - Lokalizacja osoby bądź systemu, którego incydent dotyczy.
    - Ilość osób/systemów, których incydent dotyczy.
    - Dane techniczne
        - Adres(y) IP,
        - FQDN(y),
        - Logi systemowe,
        - Podejrzany email wraz z jego załącznikami,
        - Inne dane, które mogą pomóc w analizie incydentu.
    - Dotychczas podjęte działania w reakcji na incydent

7. Zastrzeżenia

Pomimo zachowania wszelkich środków ostrożności przy opracowywaniu informacji, powiadomień i alertów, DZB GPW nie ponosi odpowiedzialności za błędy lub pominięcia, ani za szkody wynikające z wykorzystania zawartych w nich informacji.

-----BEGIN PGP PUBLIC KEY BLOCK-----

mDMEZV8+rhYJKwYBBAHaRw8BAQdA52uyX4SpLF6RaXGa4qY4gPmojv2EWZ444vCC

IcSrpJ20HlNlY3VyaXR5IEdQVyA8c2VjdXJpdHlAZ3B3LnBsPoiZBBMWCgBBFiEE

nxnuJ/iKkWPgeSPXy/BoMSidOdAFAmVfPq4CGwMFCQ0q/YIFCwkIBwICIgIGFQoJ

CAsCBBYCAwECHgcCF4AACgkQy/BoMSidOdBDxwEAoAmJBaGOWEaLR05NZJmOvMHg

hCA97X6Bfpv9uOFb6VkA/0dAqcbimgiQP1/w/Sxlz354LmVqcENPIuICEhZNdgED

uDgEZV8+rhIKKwYBBAGXVQEFAQEHQJ4Xx5p+IWLQDPobwsUsq7tWVQT/PZ2D6ale

cMnTidt7AwEIB4h+BBgWCgAmFiEEnxnuJ/iKkWPgeSPXy/BoMSidOdAFAmVfPq4C

GwwFCQ0q/YIACgkQy/BoMSidOdDt2QEA5EODaqx5sdPnQyLFC4g/qP2CjqLMLvH6

uHDhG2cMHMIBAN5bpeEoRFCb4a42nwRFcisty4cdZMRCnK81Tqex85MH

=W1wz

-----END PGP PUBLIC KEY BLOCK-----