COIG S.A.

ul. Mikołowska 100, 40-065 Katowice
tel. 32 757 33 50 | fax 32 757 41 98
coig@coig.pl | www.coig.pl

WASKO®
GRUPA KAPITAŁOWA

„Informacja o działaniu CSIRT COIG”

RFC-2350

Polska wersja językowa

NIP 634-013-42-05
KRS 00000 92497
ING Bank Śląski S.A. w Katowicach
nr konta: 97 1050 1214 1000 0007 0005 5510

Sąd Rejonowy Katowice-Wschód w Katowicach
Wydział VIII Gospodarczy Krajowego Rejestru Sądowego
Kapitał zakładowy w kwocie 5.400.000 zł
w całości wniesiony

1. Informacje o dokumencie

Dokument ten zawiera formalny opis CSIRT COIG oparty na RFC 2350. Dostarcza on informacji o zespole CSIRT, jego kanałach komunikacji i usługach.

1.1. Data ostatniej aktualizacji

Jest to wersja 1.1, wydana w marcu 2023 roku.

1.2. Lista dystrybucyjna powiadomień

Obecnie CSIRT COIG 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 http://www.coig.pl/wp-content/uploads/2022/05/COIG-RFC-2350-PL.pdf

1.4. Uwierzytelnienie niniejszego dokumentu

Ten dokument został podpisany kluczem PGP należącym do CSIRT COIG. Jego sygnaturę można znaleźć na: https://www.coig.pl/download/Klucz%20publiczny%20zespo%c5%82u%20CSIRT%20COIG.asc

2. Informacje kontaktowe

2.1. Nazwa zespołu

CSIRT COIG

2.2. Adres

CSIRT COIG

COIG S.A. (dalej: COIG)
ul. Mikołowska 100
40-065 Katowice, Polska

2.3. Strefa czasowa

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

2.4. Numer telefonu

+48 32 757-44-44, +48 32 338-27-00

2.5. Numer faksu

N/A

2.6. Inne drogi kontaktu

N/A

2.7. Adres mailowy

helpdesk@gk.wasko.pl

2.8. Klucze publiczne i inne informacje dotyczące szyfrowania

Informacja oraz klucz publiczny znajduje się na stronie: https://www.coig.pl/modul-cb-csirt/

2.9. Członkowie zespołu

Zespół CSIRT COIG składa się z ekspertów w dziedzinie zagadnień Cyberbezpieczeństwa.

2.10. Inne informacje

CSIRT COIG jest jednostką komercyjną świadczącą usługi cyberbezpieczeństwa podmiotom które podpisały odpowiednią umowę o świadczenie takich usług. Obecnie nie przewiduje się obsługi innych zgłoszeń od osób fizycznych oraz innych podmiotów niż wymienione.

Więcej informacji na temat zespołu CSIRT COIG można znaleźć na: https://www.coig.pl/modul-cb-csirt/

2.11. Punkty kontaktu dla klientów

helpdesk@gk.wasko.pl

3. Statut

3.1. Główne cele

Misją zespołu CSIRT COIG jest identyfikacja, analiza i ograniczenie zagrożeń występujących w całej infrastrukturze grupy kapitałowej WASKO jak i dla wszystkich klientów obsługiwanych przez Grupę Kapitałową WASKO.

3.2. Ustanowienie

SOC NSZW zapewnia wsparcie w zakresie obsługi zdarzeń bezpieczeństwa dla swoich klientów oraz na potrzeby własne.

3.3. Sponsorowanie i/lub powiązanie

Działalność CSIRT COIG finansowana jest z środków Grupy Kapitałowej WASKO.

3.4. Władze

CSIRT COIG działa pod auspicjami i upoważnieniem kierownictwa COIG S.A. i jest związany z jego wewnętrznymi regulacjami.

4. Zasady

4.1. Rodzaje incydentów i poziom wsparcia

CSIRT COIG dedykowany jest do reagowania na wszystkie incydenty występujące w infrastrukturze Grupy Kapitałowej WASKO oraz podmiotów o których mowa w punkcie 2.10 . Poziom wsparcia w razie

wystąpienia incydentów bezpieczeństwa zależny jest od jego charakteru, czasu trwania, wielkości oraz dostępnych środków. Niezależnie od konkretnego przypadku, czas podjęcia reakcji przez zespół CSIRT COIG nie jest dłuższy niż 1 dzień roboczy. Zdarzenia będą traktowane priorytetowo zgodnie z przypisaną do nich wagą. Szczegóły regulują umowy zawarte z konkretnym podmiotem.

4.2. Współpraca, interakcja i ujawnienie informacji

CSIRT COIG wymienia informacje z pozostałymi zespołami CSIRT oraz zainteresowanymi stronami. Wszystkie wymieniane informacje, nie zawierają wrażliwych danych. Wrażliwe dane, jeśli zajdzie taka konieczność, takie jak dane osobowe, konfiguracja systemu operacyjnego, informacje o znalezionych podatnościach są szyfrowane jeżeli przesyłane są nieszyfrowanym kanałem komunikacji.

4.3. Komunikacja i uwierzytelnienie

Wszystkie informacje przekazane drogą telefoniczną do CSIRT COIG, uważane są za wystarczająco bezpieczne nawet jeżeli będą one niezaszyfrowane. Niezaszyfrowane informacje przesyłane drogą mailową, będą uważane za wystarczająco bezpieczne do transmisji danych o niskiej wrażliwości. W przypadku przesyłania wrażliwych danych drogą elektroniczną będzie ona dodatkowo szyfrowana z wykorzystaniem PGP.

5. Usługi

5.1. Reagowanie na incydent

CSIRT COIG zapewnia możliwość reagowania na incydenty bezpieczeństwa w poniższych obszarach:

5.1.1. Ocena incydentu

1. Ocena autentyczności zdarzenia
2. Korelacja incydentów na podstawie zebranych danych
3. Stałe poszukiwanie sposobów na poprawę wydajności zespołu
4. Określenie zakresu incydentu

5.1.2. Koordynacja incydentu

1. Ustalenie źródła incydentu (wykorzystana podatność)
2. Ułatwienie kontaktu ze stronami, które mogą być zainteresowane aktualnym incydentem
3. Ułatwienie kontaktu z odpowiednimi organami ścigania
4. Utworzenie raportów do innych zainteresowanych zespołów CSIRT
5. Tworzenie ogłoszeń dla użytkowników, jeżeli incydent jest z nimi bezpośrednio związany

5.1.3.Analiza incydentu

Zakres wsparcia zależny jest od rodzaju, wagi incydentu oraz rodzaju podmiotu, którego dotyczy incydent. Działaniami podstawowymi są

- Ocena potencjalnego ryzyka wystąpienia prawdziwych efektów
- Ocena potencjalnej skali incydentu oraz zasobów dotkniętych przez niego.
- Ustalenie priorytetu incydentu
- Określenie początkowej przyczyny zdarzenia
- Definiowanie adekwatnej odpowiedzi
- Zbieranie dowodów oraz wskaźników kompromitacji.

5.2. Działania proaktywne

1. CSIRT COIG udostępnia na swojej stronie informacje o nowych zagrożeniach o których wiedza nie jest powszechna

2. CSIRT COIG zamieszcza na swojej stronie materiały edukacyjne dotyczące zachowania użytkowników, potencjalnych zagrożeń globalnych i lokalnych, prowadzenie szkoleń oraz skanowania zagrożeń w zasobach podległych.

3. Tworzenie i ulepszanie narzędzi i mechanizmów bezpieczeństwa mających na celu ciągłe zwiększanie poziomu bezpieczeństwa.

6. Formy zgłaszania incydentu

Incydenty należy zgłaszać drogą mailową na adres: helpdesk@gk.wasko.pl

7. Zastrzeżenia

Wszelkiego rodzaju roszczenia kierowane do CSIRT COIG mogą być formułowane wyłącznie przez podmioty mające ważną umowę z COIG S.A. o świadczenie usług które są bezpośrednią domeną CSIRT COIG.

Zastrzega się, że pomimo powzięcia wszelkich dostępnych środków ostrożności podczas przygotowania informacji, notyfikacji oraz alarmów bezpieczeństwa, CSIRT COIG (oraz COIG S.A.) nie ponosi odpowiedzialności za błędy, pominięcia oraz szkody wynikające z informacji w nich zawartych.