netia.pl t +48 22 352 20 00 Netia SA, ul. Puławska 464
f +48 22 330 23 23 02-884 Warszawa

RFC 2350

Wersja: 1.0

9 czerwca 2022

TLP:WHITE | PUBLIC

TLP:WHITE informacja może być dowolnie dystrybuowana.

NETIA SOC

1 Informacje na temat dokumentu

Dokument ten zawiera informacje na temat zespołu reagowania na incydenty bezpieczeństwa komputerowego (CSIRT) Netia SOC w formacie zgodnym z RFC 2350.

1.1 Data ostatniej aktualizacji

Wersja: 1.0 z dnia 9 czerwca 2022.

1.2 Lista dystrybucyjna powiadomień

Nie dotyczy

1.3 Lokalizacje, w których można znaleźć ten dokument

Aktualna wersja dokumentu publikowana jest na stronie:

https://www.netia.pl/pl/csirt/rfc - wersja w jęz. polskim,

https://www.netia.pl/en/csirt/rfc - wersja w jęz. angielskim

1.4 Uwierzytelnianie tego dokumentu

Dokument został podpisany kluczem PGP należącym do Netia SOC. Sygnaturę można znaleźć na:

https://www.netia.pl/pl/csirt/rfc

2 Informacje kontaktowe

2.1 Nazwa zespołu

Netia SOC

2.2 Adres

Netia S.A.
Netia SOC
ul. Poleczki 13
02-822 Warszawa
Polska

2.3 Strefa czasowa

Czas środkowoeuropejski UTC+1

Czas środkowoeuropejski letni UTC+2 (od ostatniej niedzieli marca do ostatniej niedzieli października)

2.4 Numer telefonu

+48 22 352 25 55

2.5 Numer faksu

Niedostępne.

2.6 Inna komunikacja

Niedostępne.

2.7 Adres poczty elektronicznej

Powiadomienia, zgłoszenia incydentów i kwestie operacyjne prosimy kierować na adres csirt@netia.pl

Pytania dot. oferty, zakresu świadczonych usług i kwestii biznesowych prosimy kierować na adres biznes@netia.pl

2.8 Klucze publiczne i inne informacje o szyfrowaniu

W celu ochrony informacji wrażliwych korzystamy z szyfrowania PGP.

```
E-mail: csirt@netia.pl
Odcisk klucza: 2777 F603 4CCF 1596 A22A  FBFF DE20 21B7 2A76 31D1
```

Klucz publiczny publikowany jest na stronie https://www.netia.pl/pl/csirt/rfc

2.9 Członkowie zespołu

Zespół Netia SOC tworzą ludzie mocno zaangażowani w ideę promowania świadomości w obszarze cyberbezpieczeństwa. Stale monitorujemy aktywność w przestrzeni cyfrowej, obserwujemy rynek rozwiązań i technologii bezpieczeństwa teleinformatycznego, podnosimy kompetencje.

2.10 Inne informacje

Dodatkowe informacje można znaleźć na stronie https://www.netia.pl/pl/csirt/rfc

2.11 Punkty kontaktu z Klientem

Preferowaną metodą kontaktu z Netia SOC jest e-mail. Rekomendujemy wykorzystanie PGP w celu zapewnienia integralności i poufności.

Standardowe godziny obsługi zgłoszeń to 9:00-17:00 od poniedziałku do piątku z wyłączeniem świąt. Jednak zespół Netia SOC pracuje całodobowo i w pilnych kwestiach możliwy jest kontakt poza ww. wskazanymi godzinami.

3 Statut

3.1 Misja

Misją Netia SOC jest wspieranie zarówno podmiotów z Grupy Netia jak i klientów biznesowych Netia w reagowaniu i w obsłudze incydentów bezpieczeństwa komputerowego.

Netia SOC świadczy usługi cyberbezpieczeństwa klientom prywatnym oraz podmiotom publicznym.

3.2 Obszar działania

Obszar działania Netia SOC obejmuje spółki Grupy Netia:

- Netia S.A.
- TK Telekom Sp. z o.o.

oraz klientów z sektora prywatnego oraz publicznego, z którymi Netia S.A ma zawartą umowę z w zakresie wsparcia w reagowaniu na incydenty bezpieczeństwa komputerowego.

3.3 Sponsorowanie i przynależność

Netia SOC funkcjonuje w ramach Netia S.A.

3.4 Umocowanie

Netia SOC działa pod auspicjami i upoważnieniem kierownictwa Netia S.A..

Ponadto Netia SOC działa na podstawie umów z klientami biznesowymi Netia S.A. i na warunkach wynikających z tych umów.

4 Polityki

4.1 Typy incydentów i poziom wsparcia

Domyślnym priorytetem dla wszystkich zgłoszonych incydentów jest priorytet normalny. Inna klasyfikacja może mieć zastosowanie na podstawie zapisów umów. O ewentualnej zmianie priorytetu decyduje zespół Netia SOC.

4.2 Współpraca, interakcja i ujawnienie informacji

Wszystkie informacje dotyczące obsługi incydentów traktowane są jako poufne. Zalecamy, aby przy zgłaszaniu incydentów i podawaniu informacji poufnych, korzystać z szyfrowania PGP lub ewentualnie ustalić z Netia SOC innego bezpieczny kanał komunikacyjny.

Netia SOC deklaruje pełne wsparcie dla Information Sharing Traffic Light Protocol (FIRST TLP v1.0, https://www.trusted-introducer.org/ISTLP.pdf). Informacje wysłane i oznaczone zgodnie z ISTLP będą przetwarzane w odpowiedni sposób.

Informacje przekazane Netia SOC mogą być przekazane do zainteresowanych stron, takich jak inne zespoły CSIRT / CERT, właściciele lub administratorzy dotkniętych incydentem zasobów, na zasadzie „niezbędnej wiedzy”, wyłączenie w celu obsługi incydentów (w zakresie niezbędnym do identyfikacji i ograniczenia zagrożenia).

Netia SOC samodzielnie nie zgłasza incydentów do organów ścigania, o ile nie wynika to z przepisów prawa. Jednakże w przypadku postępowań prowadzonych przez uprawnione organy, możemy przekazać informacje na ich wniosek.

4.3 Komunikacja i uwierzytelnianie

Netia SOC zabezpiecza wrażliwe informacje zgodnie z odpowiednimi przepisami prawa i wewnętrznymi zasadami.

W szczególności respektujemy oznaczenia poufności zdefiniowane przez autorów informacji przekazanych do Netia SOC.

W przypadku informacji o niskiej wrażliwości możliwy jest kontakt z Netia SOC przy użyciu nieszyfrowanej wiadomości e-mail lub drogą telefoniczną, ale dla zapewnienia poufności i integralności komunikacji, rekomendujemy stosowanie PGP/GPG (patrz punkt 2.8). Wszystkie wrażliwe informacje, które są przesyłane, powinny być szyfrowane.

W celu weryfikacji autentyczności otrzymanej informacji lub jej źródła czy uwierzytelnienia osoby nawiązującej kontakt, możliwe jest użycie ogólnodostępnych źródeł informacji jak np. baza WHOIS, serwisy społecznościowe, rejestry. W uzasadnionych przypadkach może być stosowane potwierdzenie telefoniczne bądź spotkanie.

5 Usługi

Netia oferuje swoim Klientom m.in. usługi Security Operations Center (SOC) w modelu as-a-service obejmujące usługi reagowania na incydenty. Ponadto świadczymy szereg usług profesjonalnych z obszaru cyberbezpieczeństwa. Szczegółowe informacje można znaleźć na stronie: https://www.netia.pl/pl/csirt/rfc

5.1 Reagowanie na incydenty

- analiza zdarzeń w systemach SIEM
- analiza i kwalifikacja podejrzeń incydentów
- obsługa incydentów
- obsługa podatności
- analiza IoC (Indication of Compromise)

5.2 Działania proaktywne

- wsparcie w tworzeniu strategii rozwoju bezpieczeństwa
- wdrażanie rozwiązań bezpieczeństwa
- utrzymywanie i rozwój rozwiązań bezpieczeństwa
- ostrzeżenia o nowych podatnościach i zagrożeniach
- testy podatności
- budowanie świadomości bezpieczeństwa

6 Formularze do zgłaszania incydentów

Incydenty powinny być zgłaszane e-mail na adres csirt@netia.pl, najlepiej zaszyfrowane naszym publicznym kluczem PGP.

Kontaktując się z Netia SOC, prosimy o przekazanie poniższych informacji:

1. Dane kontaktowe i informacje organizacyjne — imię i nazwisko osoby, nazwa i adres organizacji, adres e-mail, numer telefonu,
2. Rodzaj i krótkie podsumowanie incydentu/zdarzenia,
3. Źródło zdarzenia/incydentu - w jakim systemie zostało zaobserwowane, publiczne adresy IP źródłowe i docelowe itp.,
4. Dotknięte podmioty lub systemy,
5. Szacowany wpływ - np. utrata dostępności usług),
6. Dodatkowe informacje i obserwacje, które doprowadziły do wykrycia incydentu — wyniki skanowania (jeśli występują), wyciąg z dziennika przedstawiający problem itp.

W przypadku przekazania podejrzanego e-maila, prosimy o upewnienie się, że wszystkie nagłówki, treść i załączniki są zawarte.

7 Zastrzeżenia

Pomimo, że podczas przygotowywania informacji, powiadomień i ostrzeżeń dokładamy wszelkiej staranności, Netia SOC nie ponosi odpowiedzialności za błędy lub pominięcia, ani za szkody powstałe w wyniku wykorzystania zawartych informacji w nich zawartych.