Opis CSIRT NSZW CERT (wersja polska)

==========

1. Informacje o dokumencie

Ten dokument zawiera opis zespołu NSZW CERT zgodnie z RFC 2350.

Dostarcza podstawowych informacji o NSZW CERT, sposobach

kontaktu, opisuje obowiązki zespołu i oferowane usługi.

1.1 Data ostatniej aktualizacji

Wersja dokumentu 1.0, opublikowana 2020/05/22.

1.2 Lista dystrybucyjna powiadomień o zmianach w dokumencie

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

1.3 Miejsce, w którym można znaleźć dokument

Aktualna wersja tego dokumentu może być znaleziona na:

http://www.nszw.pl/soc

1.4 Wiarygodność dokumentu

Niniejszy dokument został podpisany przy użyciu klucza PGP NSZW CERT. Więcej szczegółów w rozdziale 2.8.

2. Informacje kontaktowe

2.1 Nazwa zespołu

"NSZW CERT": Zespół ds. Reagowania na incydenty Cyberbezpieczeństwa - nazywany dalej jako NSZW SOC

2.2 Adres

NSZW SOC

ul. Fieldorfa 2, 54-049 Wrocław, Polska

2.3 Strefa czasowa

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

2.4 Numer telefonu

+48 71 306 4002

2.5 Telefaks Numer

+48 71 7359 300

2.6 Inne możliwości komunikacji

Niedostępne

2.7 Elektroniczny adres e-mail

it@nszw.pl

2.8 Klucze publiczne i inne informacje o szyfrowaniu

NSZW CERT korzysta z klucza PGP:

Fingerprint: 06DE 9DC6 573C A263 198A 798B EA32 55A5 D4B0 CB61

Klucz publiczny można znaleźć na naszej stronie internetowej:

http://www.nszw.pl/soc

2.9 Członkowie zespołu

Zespół SOC NSZW składa się z ekspertów w dziedzinie zagadnień Cyberbezpieczeństwa.

2.10 Inne informacje

Więcej informacji na temat SOC NSZW można znaleźć na:

http://www.nszw.pl/soc

2.11 Punkty kontaktu z klientem

NSZW SOC preferuje kontakt mailowy. W sprawach ogólnych:

Kontakt jest możliwy w godzinach pracy: 08:00-16:00 czasu lokalnego od poniedziałku do piątku z wyjątkiem dni ustawowo wolnych od pracy w Polsce.

Zgłoszenia incydentów, sytuacje awaryjne:

Kontakt telefoniczny z SOC NSZW oraz / lub wiadomość e-mail zawierająca szczegóły podane telefonicznie.

Telefon SOC NSZW jest dostępny przez cały czas.

3. Statut

3.1 Misja

Celem zespołu SOC NSZW jest podejmowanie działań minimalizujących prawdopodobieństwo wystąpienia incydentów Cyberbezpieczeństwa, oraz aktywności minimalizujących skutek ich wystąpienia.

Wsparcie dla działań krajowych w zakresie bezpieczeństwa cybernetycznego.

3.2 Zakres działania

SOC NSZW zapewnia wsparcie w zakresie obsługi zdarzeń bezpieczeństwa dla swoich klientów

3.3 Finansowanie i przynależność

SOC NSZW jest wewnętrzną jednostką NSZW Sp. z o.o.

Jest finansowany przez NSZW Sp. z o.o.

3.4. Umocowanie

SOC NSZW działa pod auspicjami i upoważnieniem kierownictwa NSZW Sp. z o.o. i jest związany jego wewnętrznymi regulacjami.

SOC NSZW obsługuje i koordynuje incydenty w imieniu NSZW Sp. z o.o. oraz jej klientów.

4. Zasady obsługi incydentów (polityki)

4.1 Rodzaje incydentów i poziom wsparcia

SOC NSZW jest dedykowany do obsługi wszystkich rodzajów incydentów związanych z bezpieczeństwem komputerowym, które występują lub mogą wystąpić w środowisku teleinformatycznym w zakresie świadczonych usług.

Klasyfikacja incydentów i sposób ich obsługi są określone w Polityce zarządzania incydentami dla NSZW Sp. z o.o.

Sposób obsługi incydentów przez NSZW SOC zależy od rodzaju i wagi incydentu lub zdarzenia, elementów, na które oddziałuje incydent, ilości użytkowników, których dotyczy incydent oraz dostępności zasobów NSZW w tym czasie. Dla zdarzeń określa się priorytety stosownie do ich dotkliwości i rozmiaru.

4.2 Współpraca, interakcja i ujawnianie informacji

SOC NSZW 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 informacje związane z obsługiwanymi incydentami są traktowane jako poufne. Informacje wrażliwe (takie jak dane osobowe, konfiguracje systemu, znane luki, etc.) są szyfrowane, jeśli muszą być przesyłane w niezabezpieczonym środowisku.

Informacje przesyłane do NSZW SOC mogą być przekazywane zgodnie z potrzebą stronom zaufanym (takim jak dostawcy usług internetowych, inne zespoły CERT) wyłącznie w celu obsługi incydentów.

4.3 Komunikacja i uwierzytelnianie

NSZW SOC 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 Reakcja na incydenty

NSZW SOC świadczy usługi dla NSZW Sp. z .o. i jej klientów dotyczące obsługi incydentów związanych z bezpieczeństwem informacji w zakresie technicznym i organizacyjnym.

Usługi NSZW SOC obejmują pełny cykl reagowania na incydenty:

- obsługę
- zarządzanie
- rozwiązywanie
- łagodzenie.

5.1.1 Ocena incydentów

Usługa obejmuje:

- Nadawanie priorytetu stosownie do rodzaju i wagi incydentu.
- Przeprowadzenie badania, czy zdarzenie miało rzeczywiście miejsce.

- Określenie zakresu incydentu.

5.1.2 Koordynacja incydentów

- Określenie początkowej przyczyny zdarzenia (wykorzystanie podatności)
- Ułatwianie kontaktu z innymi stronami które mogą być zaangażowane
- Kontakt z CSIRT NASK i/lub w razie potrzeby z odpowiednimi organami ścigania
- Tworzenie raportów dla innych CSIRT
- Redagowanie ogłoszeń dla użytkowników, jeśli dotyczy.

5.1.3 Rozwiązywanie incydentów

Obejmuje:

- Powiadamianie zespołu i koordynację odpowiednich działań,
- Śledzenie postępów prac zaangażowanego zespołu,
- Obsługę żądań raportowania,
- Przedstawianie raportów.

5.2 Działania proaktywne

NSZW SOC prowadzi działania mające na celu zwiększenie odporności środowiska informatycznego na zdarzenia związane z bezpieczeństwem i ograniczające potencjalny wpływ tych zdarzeń.

6. Formularze zgłaszania incydentów

Wspomniana powyżej Polityka zarządzania incydentami dla NSZW Sp. z o.o. definiuje zestaw informacji niezbędnych do zgłaszania incydentów, ale w razie potrzeby użytkownik może wysłać e-mail z odpowiednimi informacjami.

W nagłym wypadku lub sytuacji kryzysowej prosimy o przekazanie do NSZW SOC co najmniej następujących informacji:

Dane kontaktowe i informacje organizacyjne: imię i nazwisko oraz nazwa organizacji i adres, adres e-mail, numer telefonu, adresy IP, nazwę domenową FQDN oraz wszelkie inne istotne elementy techniczne i obserwacje; Wyniki skanowania (jeśli istnieją) i / lub wyciąg z rejestru log systemu, pokazujący problem.

7. Zastrzeżenia

Podczas przygotowywania informacji, powiadomień i alertów zostaną podjęte wszelkie środki ostrożności.

NSZW SOC nie ponosi odpowiedzialności za błędy, pominięcia ani za szkody wynikające z wykorzystania informacji zawartych w tym dokumencie.

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

mQGNBF7LaGcBDACkVss+KRxSHDJuY49YNj1a03cQPWVkT6CQLkgJQLWBFx06mUcj
JK0w92CY69SbibRTUB5+CLvhipvdJElAT5h/jwTXV7Kwoqu7v1UmVTk+54aPGbfb
PIUj+q9UBCOrVEC/o3ZnOfdoYukY5e0Z82FkmDCCudzmQfKxFdaQOIrCr+epwyaQ
L4g8jkSBn1LQ6RJjfjiWmcyWSELq1cjUI1qb8jqmLyojBHw+uUktgq6baj6c4lpf
pEnjVh9b97zQ1HrCrRM+JJdq4Z7u1rFr+Q7/4VGKchYRVAKXvY9hD0Vswc+5Ht54
VIlcmoVJv2BvmerKOG+prZfvC9nliYiwpdSVI3ZKB0dxuLrZfdXXzTsVIO+qtIuj
ahnwz40Pvw4JiOXA4IVrtjzbO/ZB6M0Nq1gHuImzGQDm+wjHUIrdPevZSZ87alDW
Vewt5NHcn0PKVs0PmHtO8oW0XGl+Fu8BVY2otL5aQ7WxpoFMfDmPpBnMlrl/+QZW
MmZ10ziyIa+uUZ0AEQEAAbQcTnN6dyBTcC4geiBvLm8uIDxpdEBuc3p3LnBsPokB
1AQTAQgAPhYhBAbencZXPKJjGYp5i+oyVaXUsMthBQJey2hnAhsDBQkILw45BQsJ
CAcCBhUKCQgLAgQWAgMBAh4BAheAAAoJEOoyVaXUsMthUtML/AoRUkFPczf7hBpm
QlLTDp1zph+L4ixGPtcVWYB5dTHBIzDb58uDDwQhdhmqmjXEabxngjZKMiejd18T
+qaOegDdkt404c9zxGJidHUcSveWKO061k8etrO1C7spHh92RRwTfUCUaDGgzaGQ
b0GP2uMNXkHjYu9sUPly+OgMqypZoK4nYnpLFn5E1+FHYJjFJbTiUV4jA9NQNTid
b5/yFSLY6AgQvfnzjdHhfjh2dp0MwJmg4MbahPlz4l+D81ng12F7unaTlb9BHkQd
GOCIve0Wbj/9VozVxbM4uhew9c8XvLn3oU1jVjB8eWE3UqyWscKOvH0ju3M35smV
/ZF4CnN6buj5YTTLBNlA5jCVxu6UiARDECVZkutNTWDr71H6HOepPUEgylGu0KkW
y6aaUaI6Qym0UZddus7vGopFKt5fvw2hM50wZv7N1tNnlptt0iOZHyHNzSfDAinp
Le19Ek8To0v2N1S43tZvcZ0+P+yCcPVUMj43ZGRDh37H4ni1krkBjQRey2hnAQwA
vYWtv2GvRodrg0JFUU7c4iqKauhpb66kz07WdykVEV4Uu9jRDJjcqsVW51OsTpuE
vaP4l5q9Fy1Iw6A4p2kpxR/Yb9HFohiANWDO9s6FOWquGTBAb1nOzOF9XHVF94VX
ImDvJtpAsec7pm0s95Wlp62tpm4z/t3mCKXNoAbBE3AFXpQTUOnlRVTt9Mjq7CGh
tiE4FQDei1/rU19BSymxjlWIv+sqXiQGbhj017q/NzJINdTKPsQuwoxHPnn5R6GV
mnxFixFDvA85IlchAwKMqJqhTi+PBEisqpw+pdwIujfzlKEl6v+RLoBRAlKifZy0
wLPGRmd2AHgyawYu6t9zqBHDeuM3xoBH5LCaCZVcM5tkG0DQCIfdHZOZjJfOGXBo
+PtRwCo3ZWRAGlqNpoGB/NxNSdh4oh400IB3el9ZjqdtmZSfPWxtlM6eghsetg1y
Kya7lB0bGeXM5SnfqxNGOahDBhRMSzx6yf53myRDEvPVzTbU0wnZ+4I40CHDWo5f
ABEBAAGJAbwEGAEIACYWIQQG3p3GVzyiYxmKeYvqMlWl1LDLYQUCXstoZwIbDAUJ
CC8OOQAKCRDqMlWl1LDLYYq5C/9/sGIEfmlxU79rcAX3jj8BhjeVzLTcC0lvB0x7

idOTHR92HUZ7m4XyAA3UDHZwPuyx746GqAWinhjSKh9HG96V6+AQx07d5a2qCkNw
1QqR7mFGznYsaFzPDds3RD9nBxC1sOxFyen/LLhDFNwHeJSMN1cZ6nk50oxDlt/g
Gr49oZTD6tN+ZF5Vo0IToGxhci9r5mB0A1W23x4hAlAoKNjjJw8VWlsGtiRhGzFO
KNxtSp+ximhcb1nfotGiquhEXm3DZL1IE8Ou/OYgW19tiWnVZYRqaJvrb4qeXteS
mcbmwvt/1Qz5+FC+Ao/u4AoHcMWY6CpjUdY9FbQXhPhqKDsjhdvTsqH7Od3tBYVe
bvSs1MU+vwgwgulCKqgGokHcVBEAa8KQqNWE0oJVH4apyOfmilWHdnd06j3+6WUY
sYr/c0/iiICH4HQBy1fR0v5aD+dQAYPc2P8z3yYFzhEICHK5g0QpEZuxK+Jhnr3w
A7efYOve1NHn4j45XBpGOLhAIM4=
=7MpT
-----END PGP PUBLIC KEY BLOCK-----