-----BEGIN PGP SIGNED MESSAGE-----

Hash: SHA256

Opis CSIRT dla Trecom.

==========

1. Informacje o dokumencie

Dokument zawiera opis zespołu reagowania na incydenty Trecom według RFC 2350. Dokument nakreśla podstawowe informacje na temat zespołu CSIRT takich jak sposób kontaktu, opis odpowiedzialności oraz oferowane usługi.

1.1 Data ostatniej aktualizacji

Wersja dokumentu 1.00, opublikowana 30.09.2020.

1.2 Rozpowszechnianie powiadomień o zmianach w dokumencie

Powiadomienia o aktualizacjach są publikowane przez stronę www trecom.pl.

1.3 Miejsce, gdzie można znaleźć dokument

Aktualna wersja dokumentu opisującego CSIRT jest dostępna na stronie internetowej:

https://www.trecom.pl/RFC2350-pl.txt

1.4 Poświadczenie dokumentu

Dokument w wersji Polskiej i Angielskiej został podpisany przy użyciu klucza GPG, poświadczenie dokumentu

może być zweryfikowane poprzez klucz GPG wystawiony na cert@trecom.pl, a opublikowany pod adresem internetowym:

https://www.trecom.pl/CSIRT-PGPcert.asc

2. Informacje kontaktowe

2.1 Nazwa zespołu

Trecom CSIRT

2.2 Adres

„Trecom Spółka Akcyjna" Sp. k.

ul. Czyżewska 10

02-908 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 22 488 72 00

2.5 Numer faksu

Niedostępny.

2.6 Pozostała telekomunikacja

Niedostępna.

2.7 Adres poczty elektronicznej

cert@trecom.pl

2.8 Klucze publiczne i inne informacje o szyfrowaniu

Klucz GPG używany przez Zespół Trecom CSIRT:

User ID: CSIRT grupy Trecom.pl <cert@trecom.pl>

Key ID: 0xC66B8EF4 Key type: RSA

Key size: 4096 Expires: 20.10.2032

Fingerprint: F075 D598 3020 B272 2DCC 14E3 D798 F256 C66B 8EF4

Ten klucz może być uzyskany z usług katalogowych lub bezpośrednio ze strony internetowej:

https://www.trecom.pl/CSIRT-PGPcert.asc

2.9 Inne informacje

Ogólne informacje o Trecom CSIRT można znaleźć na:

https://soc.trecom.pl/

2.10 Punkty kontaktu z klientem

Preferowaną metodą kontaktu z zespołem Trecom CSIRT jest e-mail.
Komunikacja z naszym zespołem powinna byc zabezpieczona z użyciem
kluczy kryptograficznych w celu zapewnienia poufności i integralności wiadomości.

Godziny pracy zespołu Trecom CSIRT są ograniczone do regularnych godzin pracy
(9:00-17:00 od poniedziałku do piątku z wyłączeniem świąt).

3. Statut

3.1 Misja

Misją działania zespołu Trecom CSIRT jest pomoc klientów i parterów biznesowych w
zapobieganiu, identyfikowaniu i minimalizowaniu zagrożeń bezpieczeństwa
teleinformatycznego oraz wsparcie w zakresie zarzadzania tymi zagrożeniami.

3.2 Obszar działania

Zespół Trecom CSIRT wspiera w ramach obowiązków podmioty prywatne, publiczne
oraz rządowe, z którymi mamy podpisane umowy na świadczenie usług zarządzania incydentami.

Stale dostosowujemy nasz obszar działania podążając za potrzebami naszych klientów.
W szczególności obszar działania obejmuje conajmniej ASN, IP oraz domeny naszych klientów.

3.3 Sponsorowanie i przynależność

Zespół Trecom CSIRT jest prywatnym, samofinansowanym podmiotem.

3.4 Upełnomocnienie

Zespół Trecom CSIRT obsługuje i koordynuje incydenty w imieniu swoich klientów, z którymi związany jest umową.

4. Polityki

4.1 Typy incydentów i poziom wsparcia

Domyślnym priorytetem wszystkich incydentów jest priorytet średni, wyjątkiem są ustalenia umowne, które nadają im inny priorytet. Incydenty obsługiwane dobrowolnie, w interesie publicznym mają zatem priorytet średni bez względu na priorytet przesłony w zgłoszeniu. O podniesieniu priorytety decydują każdorazowo dyżurny operator na podstawie analizy przy przyjęciu zgłoszenie do obsługi.

4.2 Współpraca, interakcja i ujawnienie informacji

Zespół Trecom CSIRT każdy zgłoszony incydent traktuje jak informacje poufną. Informacje, które zostaną rozpoznane przy triażu jako wrażliwe lub potencjalnie szkodliwe, są przetwarzane w wydzielonym jednorazowym środowisku (tzw. sandbox). Zalecamy, przy zgłaszaniu incydentu i szyfrowanie poufnych informacji przy użyciu udostępnionego klucza publicznego lub kontakt z zespołem Trecom CSIRT w celu doboru bezpiecznego kanału komunikacyjnego.

Zespół Trecom CSIRT wykorzystuje Information Sharing Traffic Light Protocol (ISTLP, https://www.trusted-introducer.org/ISTLPv11.pdf). Przesłane Informacje oznaczone ISTLP będą przetwarzane zgodnie z ustalonymi procedurami.

W szczególnych przypadkach informacje przekazywane do zespołu Trecom CSIRT mogą być przesyłane do zaufanych podmiotów (takich jak dostawca usług internetowych jak i zespołów współpracujących CSIRT)
w zakresie niezbędnej wiedzy i wyłącznie w celu obsługi incydentów.
Zespół Trecom CSIRT nie zgłasza incydentów do organów ścigania, jeżeli nie wymaga tego Polskie prawo lub klienta którego mogłoby zgłoszenie dotyczyć.

4.3 Komunikacja i uwierzytelnianie

Zespół Trecom CSIRT wykorzystuje szyfrowania GPG w celu zapewnienia poufności i integralności komunikacji. Prosimy o przesyłanie wrażliwych informacje wyłącznie przez zaszyfrowaną wiadomość.

Wiadomości dotyczące incydentów przesyłane przez zespół Trecom CSIRT są podpisane kluczem GPG (patrz punkt 2.8) oraz sa szyfrowane w przypadku gdy zawierają wrażliwe informacje.

5. Usługi

5.1 Reagowanie na incydenty

Zespół Trecom CSIRT świadczy usługi wsparcia w obsłudze incydentów związanych z bezpieczeństwem teleinformatycznym zarówno w aspekcie technicznym jak i organizacyjnym. Zdolności zespołu Trecom CSIRT obejmują cały proces reagowania na incydenty w tym:

- przygotowanie
- wykrycie i analiza

- ograniczenia, likwidacja i odtwarzanie
- wyciąganie wniosków, analiza zebranych dowodów i rekomendacje.

5.2 Działania aktywne

Zespół Trecom CSIRT dokłada wszelkich starań, aby zwiększyć odporności na incydenty bezpieczeństwa oraz ograniczyć ich wpływ u klientów, z którymi ma podpisane stosowne umowy.

5. Formularze zgłaszania incydentów

Formularz zgłoszenia incydentów zlokalizowany pod adresem https://www.trecom.pl/Incident_form.html
.

6. Zastrzeżenia

Podczas przygotowywania wszelkich informacji, powiadomień i alertów zostaną podjęte wszelkie środki ostrożności. Trecom CSIRT nie ponosi odpowiedzialności za błędy lub pominięcia ani za szkody wynikające z wykorzystania informacji zawartych w tym dokumencie.

-----BEGIN PGP SIGNATURE-----

iQIzBAEBCAAdFiEE8HXVmDAgsnItzBTj15jyVsZrjvQFAl+QHaUACgkQ15jyVsZr
jvTRSA/+NacoEvcCSKAgsVHnVZUJg/vt1tkG0xMsndlsBDS5G16JqG4Nl8egOUcC
RTNiY+1tNCnVVkPwEPufVxF0HD0XfP4sNoxD37r2dh0lKL8SKAS6YBR9QeNkMcyP
EesmYcWJS0V2zTtvd2Ib3eNk5/t1fJmiN+WwkLyQ4dxih8aSLA6Pkpfoi2JBQG28

UGS8NalgF4cehFsEUMis3ShxdF9GFKAGOokOLzXiv676NjmSRuU0uikNNUDsenLV

Ny3sdH8BnkDcuS0AX3iUIO3xxVwxmgnKCRSfPLwLB6SXmL+6hfBpr408rcMLcoEw

sQLVUgwTHQvR6GPKIlXsvrnwPEdKWfRMxxROZXlT+2pj4ExcelGq5qwv+L3xuIfK

+oV+P1zfGXIop1WrxzXG5lKDdt72hmhzSVU6jeIPv7SXaVoxHpR/A88aJItZNZdt

rB8mjldp7Az8pL8jeHgQl+JL+ciBwNVMeblm/9xymvMCknQICnEFxQuXYRI20dI6

pE7JK/N94th8aXHwka6ZghybJf7NYurYks0LiNBjdvamSeWi1MlLZAjYsDiQojzn

7C3HT4sXfg2sqkTm1gavmbLrT1VE/cR1s7ndaFabRAQpWX7piDcY/IG9GOTdBcHD

QiP464JvkkDrfjaGeIXWpb3xLMGpruwtijbWM8dWFIZDIgjLTdk=

=OpCt

-----END PGP SIGNATURE-----