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

Hash: SHA256

CSIRT Description for Trecom

==========

1. About this document

This document contains a description of the Trecom Computer Security Incident Response Team according to RFC 2350. It provides basic information about the CSIRT in terms of how to contact the team, describes its responsibilities and the offered services.

1.1 Date of Last Update

This is version 1.00, published on 30.09.2020.

1.2 Distribution List for Notifications

Notifications of updates are submitted by the Trecom website

1.3 Locations where this Document May Be Found

The current version of the CSIRT description is available on the Trecom website:

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

1.4 Authenticating this Document

Document in English and Polish has been signed with GPG key and its authenticity can be verified with cert@trecom.pl GPGkey as published on trecom website: https://www.trecom.pl/CSIRT-PGPcert.asc

2. Contact Information

2.1 Name of the Team

Trecom CSIRT

2.2 Address

„Trecom Spółka Akcyjna" Sp. k.
ul. Czyżewska 10
02-908 Warszawa
Polska

2.3 Time Zone

Central European Time (CET) - UTC+1
Central European Summer Time (CEST) - UTC+2 according to EU regulations
(from the last Sunday of March to the last Sunday of October)

2.4 Telephone Number

+48 22 488 72 00

2.5 Facsimile Number

Not available

2.6 Other Telecommunication

Not available

2.7 Electronic Mail Address

cert@trecom.pl

2.8 Public Keys and Other Encryption Information

Trecom CSIRT uses the GPG key:

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

This key can be received from directory servers or directly from our website:

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

2.9 Other Information

General information about Trecom CSIRT can be found at

https://soc.trecom.pl/

2.10 Points of Customer Contact

The preferred contact medium for Trecom CSIRT is encrypted e-mail.
Please use our cryptographic keys above to ensure the integrity
and confidentiality of the message

Normal business operational hours of CSIRT Trecom hours are
generally restricted to regular business hours:
09:00-17:00 Monday to Friday except for polish holidays.

3. Charter

3.1 Mission Statement

The mission of Trecom CSIRT is to support Customer's and business partners in
protecting its assets and in avoiding, identifying, and mitigating the cyber threats.

3.2 Constituency

Trecom CSIRT is the Response team for the private, governmental, and non-governmental entities
who signed an agreement to use our incident management services.

We continuously update our constituency according to the ASN, IP
and domain data provided to us by our Customers.

3.3 Sponsorship and/or Affiliation

Trecom CSIRT is a private, self-funding entity.

3.4 Authority

Trecom CSIRT coordinates incidents on behalf of its Customers
and adhere to the contractual terms.

4. Policies

4.1 Types of Incidents and Level of Support

All incidents are registered by default in middle priority (średni)
unless there are other contractual agreements. All Incidents handled
regardless of the label attached to incident notification by submitter
are therefore treated as a middle priority. Incident Handler during triage
based on information in incident form can increase the priority.

4.2 Co-operation, Interaction, and Disclosure of Information

Trecom CSIRT declares that all information related to incidents handled is considered Confidential.
All Information evident to be harmful is handled only in a secure environment (sandbox).
When reporting an incident with sensitive information please use encryption or contact
Trecom CSIRT to arrange different channels of secure communication.

Trecom CSIRT fully supports for the Information Sharing Traffic Light Protocol
(https://www.trusted-introducer.org/ISTLPv11.pdf).
All pieces of information sent to our team are labeled according to ISTLP will be handled

appropriately.

Incidents submitted to Trecom CSIRT in some cases can be distributed to our trusted parties (such as ISPs, other CERT teams) during the incident handling process.

Trecom CSIRT does not report incidents by default to the Law Enforcement Agencies unless required by the polish law or its client's national law.

4.3 Communication and Authentication

Trecom CSIRT uses GPG encryption to enforce the confidentiality and integrity of communication. We expect all sensitive information will be sent in are encrypted.

By default messages send by Trecom CSIRT staff are signed with a GPG key. If messages contain sensitive information we are encrypting emails.

5. Services

5.1 Incident Response

Trecom CSIRT will assist its clients in handling the technical and organizational aspects of security incidents. Trecom CSIRT capabilities cover the full cycle of incident response

- Preparation
- Detection and Analysis
- Containment, Eradication, and Recovery
- Lessons learned, Collected evidence analysis and Recommendation

5.2 Proactive Activities

Trecom CSIRT makes efforts to enhance constituents immunity to security incidents and to limit the impact of incidents that occur in the environment of our clients.

6. Incident Reporting Forms

Trecom CSIRT has created a local form designated for reporting incidents to the team. The Form can be found on our website: https://www.trecom.pl/Incident_form.html

7. Disclaimers

While every precaution will be taken in the preparation of information, notifications, and alerts, Trecom CSIRT assumes no responsibility for errors or omissions, or damages resulting from the use of the information contained within.

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

iQIzBAEBCAAdFiEE8HXVmDAgsnItzBTj15jyVsZrjvQFAl+QHlgACgkQ15jyVsZr
jvSTcQ//WhukyzMwCEellSt9BvLw+HZtKmFKZdkIhn7iRegaAM1z2Aukt5YCEngu
Bcw6uIegN7aC6i5fapGQI9Zaez7ghM2nK5bt3hRc/JHCGUzTa4BNqbje10hoCtxV
2caeaBhWw7vgcU0YhCuEqjEQp7GL653NLXgdRDwDdob5L1eR/ran8d1P4GRXOxr4
GpWbRMwIW9m5+Tv8cYv3dbChnXc+mVptUdHHgPW8tULm5W4Ku0XL9dBewiqj754b
DlFjcA+AwcopI1dc7jaiqjpvXGOtEuniK8IIFIHlcGca+QOmKvmKlzoVINsxUHfa
hhCWK2bqru0yLiazQIvQLFGpbk4zDI2H1VaXzUw2HKzVkqmQzc48YQ5rngq/Yv/+
JDU7OBoMqcCxWqJEKoUCm558Ayfvddv/RvkyAsni1PafxV+u0GUrVL+4hTRf7SCT
1m9Xsa9M12TKBiwyG0lciE1Dzz4c+16dlf23q3WSGH5nc31n4hgb6//mmrsbCT6L
Pr1yM99OyToIv8ujhDH1gV4cAb/UTXG/oktu6BkbGST5+7X9igZpoQiGQfCONPjO
gA4spZClFZelXPZs2qXNBcTLLuYs5xL0/oXNuwN975qNh0RwQeL02g1QbX0iBRq0
QekTWMtyaO/60pceTxicc37f/EnaXJwPdB2CPIOSg/HMoWO/098=

=a1aC

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