SOC365 CSIRT profile

1. DOCUMENT INFORMATION

This document contains a description of Security Operation Center 365 CSIRT according to RFC 2350. It provides basic information about the SOC365 CSIRT, the ways it can be contacted and describes the services offered.

1.1 Date of Last Update

This is version 1.0 of 01. 12. 2022.

1.2. Distribution List for Notifications

N/A.

1.3 Locations where this Document may be found

The current version of this document is avalaible on https://www.soc365.cz/files/RFC2350_SOC365_CSIRT_EN.pdf

2. CONTACT INFORMATION

2.1 Name of the Team

Security Operation Center 365 CSIRT.

2.2 Address

Ripska 11c
627 00, Brno
Czech Republic

2.3 Time Zone

CET/CEST.

2.4 Telephone Number

+420 515 919 570.

2.5 Facsmile Number

+420 543 211 754.

2.6 Other Telecommunication

N/A.

2.7 Electronic Mail Address

Please use csirt@soc365.cz for communication.

2.8 Public Keys and Encryption Information

Please use csirt@soc365.cz for secure communication.

PGP key:

Type: RSA/4096   Expires: 2028-02-28

Fpr: 461A 982F 168F 3BE0 01C2 4B0C CDD1 D13F EAE2 DCE1

UID: CSIRT SOC365 <csirt@soc365.cz>

2.9 Team Members

Information is not provided about the SOC365 CSIRT team members on the website. Please use our e-mail address to contact us.

Team members will identify themselves to the reporting party with their full name in an official communication regarding an incident.

2.10 Other Information

General information can be found at www.soc365.cz.

2.11 Points of Customer Contact

The preferred method for contacting SOC365 CSIRT is via e-mail.

In case it is not possible (or not advisable for security reasons) to use e-mail, emergency telephone number can be use if needed.

3. Charter

3.1 Mission statement

Our goal is to proactivelly counter cybersecurity threats, react to incidents, coordinate actions to solve them and effectively prevent them.

3.2 Constituency

Our contituency are public or private sector institutions and critical information infrastructure of the Czech republic and Slovakia.

4. Policies

4.1 Types of Incidents and Level of Support

Pre-set baseline priority for all incident is normal priority. Team members of CSIRT SOC365 will perform a deeper analysis of the given phenomenon, on the basis of which he will categorize the detection and, if necessary, activate the incident response process according to the established parameters.

4.2 Co-operation, Interaction and Disclosure of Information

Any incoming information is handled safely without regards to content or impact.

Sensitive information is handled according to our clasification scheme and cryptography is used if applicable.

4.3 Communication and Authentication

PGP/GnuPG is used for all sensitive communication or information transfer or team members are instructed to use any legal means of authentication (e.g. calling third subject to identify).

5. Services

5.1 Incident Response

Processing is according to internal directive. Process includes categorization, ticketing and notifications.

5.1.1. Triage

- Assessment of credibility
- Classification of priority, according to the Decree. 82/2018 Coll., decree on cyber security
- Assignment to an analyst or solver

5.1.2. Coordination and Resolution

- Contacting all concerned parties related to the incident
- Taking appropriate measures
- Informing other CSIRT Teams if necessary

5.2 Proactive Activities

We regulary analyze public and provided information about cyber security trends and news. If any relevant information is found, deeper investigation takes place and if confirmed we distribute recommendation and warnings.

6. Incident reporting Forms

No special reporting form is used.

7. Disclaimers

None.