TLP:CLEAR

1. About this document

This document contains a description of O2 Czech Republic CERT according to RFC 2350. It provides basic information about the O2 Czech Republic CERT, the ways it can be contacted, describes its responsibilities and the services offered.

1.1 Date of Last Update

This is version 2 from 23. 8 2023.

1.2 Distribution List for Notifications

There is no distribution list for notifications. Any specific questions or remarks please address to the O2 Czech Republic CERT mail address cert@o2.cz.

1.3 Locations where this Document May Be Found

The current version of this document is available to download on https://www.o2.cz/soukromi/cert.

2. Contact Information

2.1 Name of the Team

O2 Czech Republic CERT (O2.cz CERT)

2.2 Address

(O2.cz CERT)
O2 Czech Republic a.s.
Za Brumlovkou 266/2
Prague 4
140 22
Czech Republic

2.3 Time Zone

Time-zone (relative to GMT): GMT01/GMT02(DST)

2.4 Telephone Number

+420 602 341 564

2.5 Facsimile Number

Not available

2.6 Other Telecommunication

Not available

2.7 Electronic Mail Address

For incident reports, please use the address abuse@o2.cz.
For general questions please use the address cert@o2.cz.

2.8 Public Keys and Encryption Information

For encrypted communication with O2.cz CERT, you may use the following key:
UID: O2.cz CERT (O2.cz CERT) cert@o2.cz
Fpr: 98CC E6AF CCF7 D513 CEA5 1926 615B A4B5 CFEA CC7C
Public key is downloadable from https://www.o2.cz/soukromi/cert

2.9 Team Members

The team leader of O2.cz CERT and the Security Director is Radek Sichtanc. A full list of O2.cz CERT members is not publicly available.

2.10 Other information

General information about O2.cz CERT can be found at https://www.o2.cz/soukromi/cert.

2.11 Points of Customer Contact

The preferred method for contacting O2.cz CERT is via e-mail. Incident reports and related issues should be sent to abuse@o2.cz. For general questions send an e-mail to cert@o2.cz.
If it is not possible (or not advisable for security reasons) to use e-mail, O2.cz CERT can be reached by telephone at +420 602 341 564.
O2.cz CERT's hours of operation are generally restricted to regular business hours (09:00-17:00 Monday to Friday, except holidays).

3. Charter

3.1 Mission Statement

The purpose of O2.cz CERT is to contribute to the security of the company's ICT infrastructure by building and maintaining the capacity to identify, react to, and resolve computer and information security issues. Our goal is to assist users of O2 Czech Republic network in implementing proactive measures to reduce the risks of computer security incidents, and to assist them in responding to such incidents when they occur.

3.2 Constituency

The target group of O2.cz CERT is all companies and users of O2 Czech Republic (includes all systems connected to the O2 Czech Republic network: AS5610, AS20884). Please note, however, that due to the nature of the services provided to users of the O2 Czech Republic network, different types of target groups are provided with different levels of support (details can be found in chapters 4.1 and 5.1)

3.3 Sponsorship and/or Affiliation

O2.cz CERT is part of O2 Czech Republic a.s.

3.4 Authority

O2.cz CERT operates under the auspices of, and with authority delegated by, the management of O2 Czech Republic. O2.cz CERT has the mandate to manage and support the handling of cyber security incidents.

4. Policies

4.1 Types of Incidents and Level of Support

O2.cz CERT is authorized to address all types of computer security incidents which occur, or threaten to occur, in our constituency.

The level of support given by O2.cz CERT will vary depending on the type and severity of the incident or issue, the type of constituent, the size of the user community affected and O2.cz CERT's resources at the time, though in all cases some response will be made. Special attention will be given to issues affecting critical information infrastructure.
O2.cz CERT will generally accept any incident report that involves an incident with one of the constituents either as a victim or as a suspect. However, only in cases when report concerns internal O2 Czech Republic infrastructure, O2.cz CERT is able to handle the incidents. For individual and B2B customers, incident response is limited to critical situation. Note that no direct support will be given to end users; they are expected to contact their system administrator, network administrator or security managers. O2.cz CERT will support the latter people.

O2.cz CERT is committed to keeping its constituency informed of potential vulnerabilities, and where possible, will inform this community of such vulnerabilities before they are actively exploited.

4.2 Co-operation, Interaction and Disclosure of Information

O2.cz CERT follows internal Data Handling Policy and declares full support for the Information Sharing Traffic Light Protocol. Information sent in and labelled according to ISTLP will be handled appropriately.

O2.cz CERT may share information submitted on a need-to-know basis with trusted parties (other CERT/CSIRT teams, other ISPs) for the sole purpose of incident handling. O2.cz CERT operates within the bounds of the Czech legislation.

4.3 Communication and Authentication

Unencrypted e-mail is used for normal communication not containing sensitive information. For secure communication, PGP-Encrypted e-mail is used.

5. Services

5.1 Incident Response

O2.cz CERT handles all technical and organizational aspects of incident response. In particular, it provides the following services:

5.1.1. Incident triage

The main goals of incident triage are:
- investigating whether indeed a security incident occurred,
- determining the extent and severity of the incident (including a potential impact on the constituency).

5.1.2. Incident Coordination

The goal follow is to provide a complex coordination between various involved parties. This includes but is not limited to:
- identification of the root cause of the incident
- contact the involved parties to investigate the incident and take the appropriate steps,
- facilitate contact to other parties which can help resolve the incident,
- making reports to other CERTs or CSIRTs, if applicable and
- communicate with stakeholders and media.

Due to limited resources, this service is primarily served for internal O2 Czech Republic infrastructure and B2B customers. In very rare critical situations, incident coordination is provided to individual customers.

5.1.3. Incident resolution

The incident resolution only is performed in limited range for internal O2 Czech Republic infrastructure only. This includes but is not limited to:
- removing the vulnerability,
- securing the system from the effects of the incident,
- collecting evidence and data interpretation,
- etc.

5.2 Proactive Activities

O2.cz CERT is involved in activities focusing on
- raising security awareness in its constituency,
- public announcements concerning serious security threats,
- observation of current trends in technology and security,
- distribute relevant knowledge to its constituency.

6. Incident reporting forms

There are no specific forms available for incident reporting purposes. Use the following basic rules for reporting incidents using e-mail:

- A report must contain your contact and organizational information - first name and last name of the reporter, organization name (if applicable), e-mail and telephone number
- A report must contain IP address and type of incident, approximate time when the incident started, when the incident was detected, and logs relevant to the problem (where applicable)

- A report about spam (or a malicious e-mail attachment) must contain a copy of the full e-mail header from the e-mail which is considered to be spam (or which contains the attachment in question).
- A report about phishing or pharming must contain the URL and IP address of the web page along with its source code, if possible.

7. Disclaimers

While every precaution will be taken in the preparation of information, notifications and alerts, O2.cz CERT assumes no responsibility for errors or omissions, or for damages resulting from the use of the information contained within.