1 RFC 2350

1.1 1. Document Information

This document contains a description of CZ.NIC-CSIRT according to RFC 2350. It provides basic information about the CSIRT team, the ways it can be contacted, describes its responsibilities and the services offered.

1.1. Date of Last Update

This is version 1.1. as of 2015/02/20.

1.2. Distribution List for Notifications

There is no distribution list for notifications.

1.3. Locations where this Document May Be Found

The current version of this document can always be found at http://www.nic.cz/csirt.

1.2 2. Contact Information

1.2.1 2.1. Name of the Team

CZ.NIC-CSIRT

1.2.2 2.2. Address

CZ.NIC, z.s.p.o., CSIRT Team
Milesovska 5
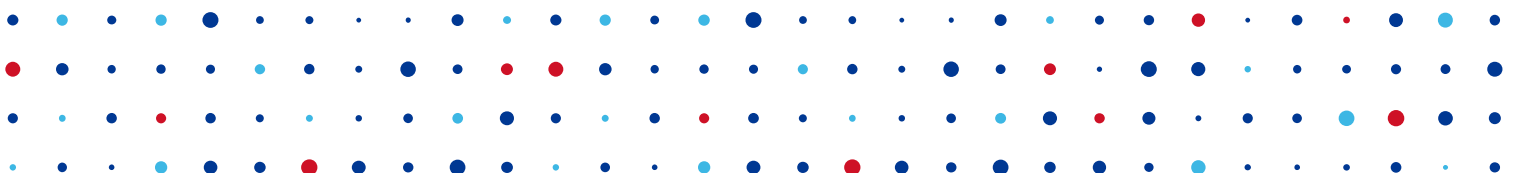130 00 Prague 3
Czech Republic

1.2.3 2.3. Time Zone

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

1.2.4 2.4 Telephone Number

+420 222 745 111

1.2.5 2.5 Facsimile Number

+420 222 745 112

1.2.6 2.6 Other Telecommunication

None.

1.2.7 2.7 Electronic Mail Address

Please send incident reports to csirt@nic.cz

1.2.8 2.8 Public Keys and Encryption Information

Every team member use his own PGP key. Fingerprints can be found in chapter 2.9.

1.2.9 2.9 Team Members

The CZ.NIC-CSIRT team members are Martin Peterka, Ondrej Sury, Zuzana Duracinska, Pavel Basta, Edvard Rejthar and Michal Prokop

Basic information about team members :
Martin Peterka
email : martin.peterka@nic.cz
PGP key : A4BE 75CD B803 E20E 2B75 A7E6 E592 7502 DCEA 5E22

Ondřej Surý
email: ondrej.sury@nic.cz
PGP key: BF7C 46FD 71E3 ACBA A1A5 1D5F 6189 1931 7A1F DB7C

Pavel Bašta
email: pavel.basta@nic.cz
PGP key: 433C A7C2 5AB8 0293 3581 7691 A964 C99A E040 4418

Michal Prokop
email: michal.prokop@nic.cz
PGP key: 437D EE6B 90BC FA94 274B C113 4AE0 CC78 D66E BB7F

Zuzana Duračinská
email: zuzana.duracinska@nic.cz
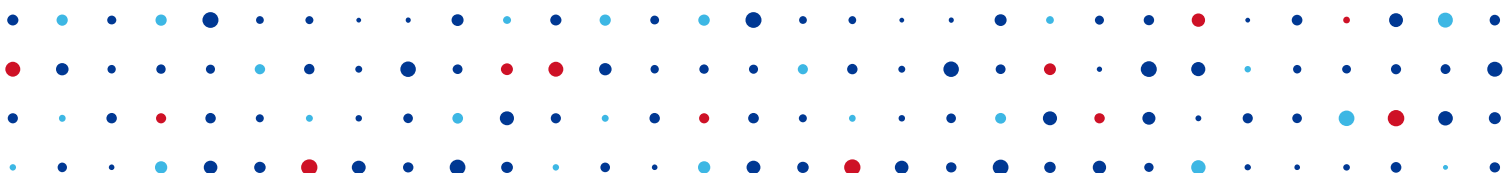PGP key: 9B1B 3668 F2F0 E132 A8CD 5F6F 064B 0DF5 F417 80DF

Edvard Rejthar
email: edvard.rejthar@nic.cz
PGP key: 43B5 C63A E512 2B55 E241 11F6 BA3D 915E F50B CBD8

1.2.10 2.10 Other Information

For our application MDM which use email address malware@nic.cz
is PGP key fingerprint:
8DBE 52F4 BF24 3C5B 05D6 2ED0 016E 1403 267B 03EC

1.2.11 2.11 Points of Customer Contact

The preferred method to contact CZNIC-CSIRT team is to send an e-mail to the address
csirt@nic.cz. This will create a ticket in our tracking system and alert the human on duty. In urgent
cases you can use phone number +420 222 745 111.
Days/Hours of Operation: 09:00 to 17:00 Monday to Friday

1.3 3. Charter

1.3.1 3.1 Mission Statement

CZ.NIC-CSIRT solve incidents within .CZ domain registry system and incidents in .CZ domain
names if they are used in a fashion that endangers the national or international computer security.

1.3.2 3.2 Constituency

The constituency are CZ.NIC association and another CERTs and end users.

1.3.3 3.3 Sponsorship and/or Affiliation

CZ.NIC-CSIRT is part of CZ.NIC z.s.p.o., the .CZ domain name registry

1.3.4 3.4 Authority

CZ.NIC-CSIRT is department of CZ.NIC association and operates with authority delegated by
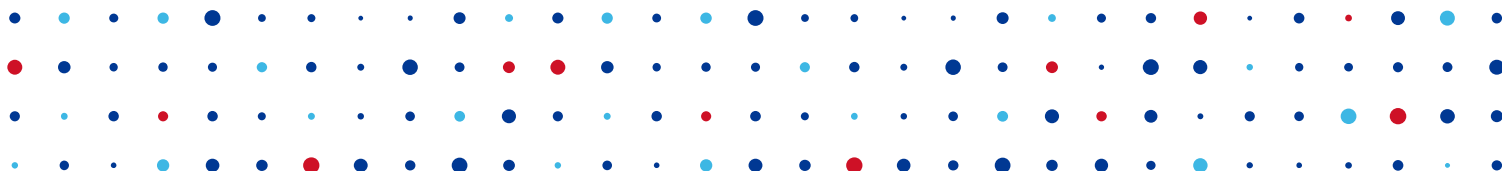association.
As described in 3.1., team is responsible for solving incidents within .cz registry and for preparing
expertises in concrete cases of incidents in .CZ domain names. For more information see chapter
4.1.

1.4 4. Policies

1.4.1 4.1 Types of Incidents and Level of Support

CZ.NIC-CSIRT team is responsible for incident handling within AS25192 and incident relating to
nameservers for .cz and 0.2.4.e164.arpa.

The CZ.NIC association is entitled to invalidate the delegation of the Domain Name at its own
discretion if the same is used in a fashion that endangers the national or international computer
security, particularly if through the Domain Name or through the services which are made available
by the same a harmful content (especially viruses, malware) is distributed or if the content of a
different service is masqueraded (especially phishing), or if the hardware that is made available
through the Domain Name becomes a control centre of interlinked hardware network distributing
the harmful content (especially botnet).

The CZ.NIC association is entitled to invalidate the delegation of the Domain Name for a period of up to 1 month, even repeatedly; however the association is not obliged to actively seek the Domain Names which would fit the definitions mentioned hereinabove.

Decisions concerning the examination of conditions for invalidation of the delegation and the procedure of invalidation are determined by CZ.NIC-CSIRT.

The procedure taken under this provision cannot be used to enforce the protection of the third parties' property rights against spam distribution if the conditions given in the first sentence of this provision are not fulfilled.

1.4.2 4.2 Co-operation, Interaction and Disclosure of Information

CZ.NIC-CSIRT is ready to cooperate with other organizations and teams.
We operate under the restrictions imposed by Czech law. It involves especially Civil code and Data Protection law.

1.4.3 4.3 Communication and Authentication

For normal communication not containing sensitive information we use unencrypted e-mail.
For secure communication PGP-Encrypted e-mail will be used.

1.5 5. Services

1.5.1 5.1 Incident Response

CZ.NIC-CSIRT will handle the technical and organizational aspects of incidents. In particular, it will provide assistance or advice with respect to the following aspects of incident management:

1.5.1.1 5.1.1. Incident Triage

- Determining whether an incident is authentic
- Assessing and prioritizing the incident

1.5.1.2 5.1.2. Incident Coordination

- Determine the involved organizations
- Contact the involved organizations to investigate the incident and take the appropriate steps
- Facilitate contact to other parties which can help resolve the incident.

1.5.1.3 5.1.3. Incident Resolution

- Removing the vulnerability
- Securing the system from the effects of the incident
- Collecting evidence where criminal prosecution is contemplated
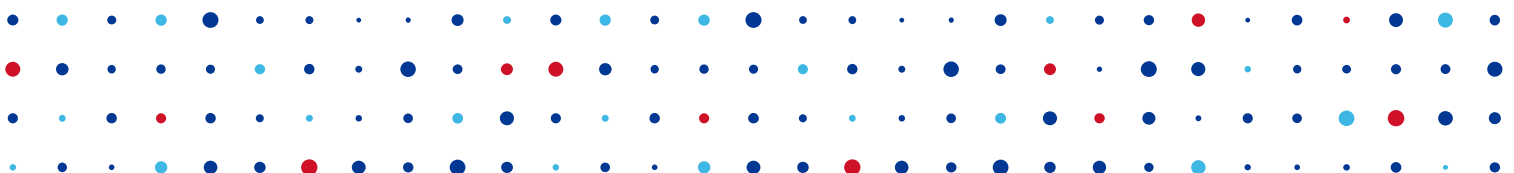
CZ.NIC-CSIRT will also collect statistics about incidents within its constituency.

1.5.2 5.2 Proactive Activities

- CZ.NIC-CSIRT do not pursue proactive activities.

1.6 6. Incident Reporting Forms

There are no local forms available yet. Please use our basic rules for creating incident report:
- A report must contain your contact and organizational information - name and organization name, e-mail, telephone number
- A report must contain IP address and and case type
- A report about scanning must contain a cut from a log showing the problem
- A report about spam or virus must contain a copy of the full mailheader from the e-mail which is considered to be a spam or virus
- A report about phishing or pharming must contain URL, and source of the web page if possible

1.7 7. Disclaimers

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