RFC2350

Έκδοση 1.2 -2018.02.14

TLP1: WHITE

[1] TLP Sources may use TLP: WHITE when information carries minimal or no foreseeable risk of misuse, in accordance with applicable rules and procedures for public release.

Contents

---

1. Purpose of a document

The document describes the operation of the National CSIRT-CY according to RFC2350.

1.1 Date of last revision

This is version 1.2, published in February 2018. This version is in effect until it is overwritten by a recent version.

1.2 Distribution list

Changes to this document will not be shared through email or any other mechanism. Please send any questions or comments to info@csirt.cy

1.3 Position where the document can be found

The current version of this document described by the National CSIRT-CY is always available on the http://www.csirt.cy website under the About Us section. Please check that you are using the latest version.

1.4 Document authentication

This document has been signed with the National CSIRT-CY PGP key. The PGP fingerprint is available on the http://www.csirt.cy link.

2. Point of contact information

2.1 Group name

National CSIRT-CY.

2.2 Address

National CSIRT-CY.
8, Ilioupoleos, 1101, Nicosia, Cyprus.

2.3 Zone Time

• EET, Eastern European Time (UTC/GMT + 2 hours).

2.4 Telephone number

+357 22 693094, +357 22 693095.

2.5 Hotline number (Local)

1490.

2.6 Fax Number

+357 22 693096.

2.8 Public Keys and other Encryption information

The National CSIRT-CY has a PGP key, with Fingerprint:
3B8CE53084F38F7C245B269CFA7FF237B641952D

The public key and its signatures can be found on the usual large public key servers as well as on the National CSIRT-CY public website. At the link site http://www.csirt.cy

2.9 Team members

Group members are available on request.

2.10 Other Information

General information about the National CSIRT-CY can be found on the website at the link http://www.csirt.cy

2.11 Points of contact

The suggested method for contacting the National CSIRT-CY is via info@csirt.cy. All incidents can be reported on reporting@csirt.cy

National CSIRT-CY encourages the use of secure email (for example, with PGP encryption) when exchanging sensitive information.

Alternatively, the telephone number referred to in § 2.4 may be used.

The National CSIRT-CY provides services and operates 24 hours a day, 7 days a week.

3. Charter

3.1 Mission Statement

National CSIRT-CY envisions the increase of the security posture of The Republic of Cyprus by enhancing cyber protection of its National Critical Information Infrastructures (CII), banks and ISPs. National CSIRT-CY shall coordinate and assist CII owners/administrators, banks and ISPs to ensure the existence of (at least) a minimum level of security, by implementing proactive and reactive security services to reduce the risks of network information and cyber security incidents, as well as respond to such incidents as and when they occur. National CSIRT-CY shall also undertake awareness actions in order to educate the local population and National stakeholders about the adverse effects of cyber threats and cybercrime. In an earnest effort to enhance the security posture of the nation the National CSIRT-CY shall provide timely advisories to all its constituents and make necessary efforts to introduce advance security services such as security testing, vulnerability scanning and active network monitoring.

3.2 Establishment and responsibilities

The National CSIRT-CY was established in 2016 by the government decision Action No. 81/477. The main responsibilities and services provided to the Critical Information Infrastructures (CII), Banks and ISPs from the National CSIRT-CY are:

Reactive: These services are triggered by an event or on request.

a. Incident Handling (Incl. Analysis, Response on site, Response support, Response Coordination)
b. Vulnerability Handling (Incl. Analysis, Response, Response Coordination)
c. Artifact Handling (Incl. Analysis, Response, Response Coordination)

Proactive: These services provide assistance and information to help prepare, protect and secure constituent systems.

a. Alerts and Warnings
b. Announcements
c. Technology Watch
d. Security Audits and Assessments
e. Configuration and Maintenance of Security Tools, Applications and Infrastructures
f. Development of Security Tools
g. Intrusion detection Services
h. Security Related Information Dissemination

i. Security Quality Management Services: These services augment existing and well-established services that are independent of incident handling.
j. Artifact Handling (Incl., Artifact analysis, Artifact response, Artifact response coordination)
k. Forensic analysis
l. Risk Analysis
m. Business Continuity and Disaster Recovery Planning
n. Security Consulting
o. Awareness Building
p. Education/Training

4. Policies

4.1 Incident Handling and level of support

The level of support offered by the National CSIRT-CY depends on the type of constituent, the severity and the impact of the incident.

4.2 Cooperation, Interaction and Disclosure of Information

The National CSIRT-CY highly regards the importance of operational cooperation and information sharing between Computer Emergency Response Teams, and also with other organizations which may contribute towards or make use of their services. All sensitive data and information (personal data, system/service configuration, vulnerabilities with their locations) are transmitted encrypted. The National CSIRT-CY operates in accordance with the GDPR.

4.3 Communication and Authentication

The suggested method for contacting the National CSIRT-CY is via info@csirt.cy. All incidents can be reported on reporting@csirt.cy. National CSIRT-CY encourages its counterparts to use secure email (for example, PGP) when exchanging sensitive information.

Alternatively, the telephone number referred to in § 2.4 may be used.

The National CSIRT-CY provides services and operates 24 hours a day, 7 days a week.

5. Services

5.1 Incident Response

The National CSIRT-CY will help system administrators to handle the technical and organizational issues occurred from incidents. In particular, it provides help or advice on the following:

5.1.1 Incident Triage

a. Investigating whether indeed an incident occurred.
b. Assessing and prioritizing the incident.
c. Conducting investigation.

5.1.2 Incident Coordination

a. Determining the involved organizations.
b. Contact the involved organizations to investigate the incident and take the appropriate steps.
c. Facilitate contact to other parties which can help resolve the incident.
d. Contacting or facilitating contacting appropriate law enforcement officials, if necessary.

5.1.3 Incident Resolution

a. Technical assistance and analysis of compromised systems.
b. Support in restoring affected systems and services to their previous status.
c. Collecting statistics and evidence about incidents, that could be used for protecting against future attacks.

5.2 Proactive Activities

Preventing and Reactive services

a. Issuing of threats/attacks and proposed preventive measures.
b. Information and awareness of security tools and events.
c. Creation of security documents that help minimize vulnerabilities.

d. Security alerts.
e. Vulnerability assessments.
f. Malware analysis.

6. Incident report forms

The incident report form is available on the website www.csirt.cy

7. Disclaimer

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