RFC2350

Version 2.0

Last Updated 30/04/19

TLP: White

1. Purpose of this document

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

1.1 Date of last revision

The version of this document is 1.1, published in April 2019. This version is in effect until a more recent version overwrites it.

1.2 Distribution list for alerts

Changes to this document will not be shared through an email list or any other mechanism.

1.3 Position where the document can be found

The latest and current version of the RFC2350 of the National CSIRT-CY is always available from the http://www.csirt.cy link. Please check that you are reading 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. Contact Information

2.1 Team name

National CSIRT-CY

2.2 Address

8, Ilioupoleos, 1101, Nicosia, Cyprus

2.3 Zone Time

a. EET, Eastern European Time (UTC + 2h between last Sunday of October and last Sunday in March).

b. EUST, Eastern European Summer Time (UTC + 3, between last Sunday in March and last Sunday in October).

2.4 Telephone number

+357 22 693094, +357 22 693095

2.5 Hotline number (Local)

1490

2.6 Fax Number

+357 22 693096

2.7 Other Communications

Not available

2.8 Electronic Management

info@csirt.cy is the primary email address for contacting the National CSIRT-CY report@csirt.cy is the email address that can be used for incident reporting. Incidents can also, be reported via our website at www.csirt.cy

All emails are processed using our incident logging system, and ticket numbers are issued and assigned to all communication. It is recommended to use the assigned ticket number for all communications regarding the same incident.

2.9 Public Keys and other Encryption information

National CSIRT-CY PGP fingerprint 3B8CE53084F38F7C245B269CFA7FF237B641952D

The key and its signatures can be found on the usual large public key servers.

2.10 Team members

Information about the team can be available upon request.

2.11 Other Information

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

2.12 Customer Contact Points

The suggested method of contacting the National CSIRT-CY is via email to info@csirt.cy. Any incident related emails can be emailed to reporting@csirt.cy. The National CSIRT-CY encourages our constituents to use PGP encryption when sending any sensitive information to the National CSIRT-CY. Emails send to cert@, abuse@, webmaster@ and security@ will also be handled via our ticketing system as usual — any other email addresses are not monitored.

In addition, and when instructed, constituents can forward malicious files to the two email addresses (reporting@csirt-lab.cy and info@csirt-lab.cy) that operate on a completely isolated network for further analysis.

Regular office hours are workdays 7:30 – 19:00.

Reporting an incident is possible by telephone 24/7 by calling at the hotline 1490. The analyst on duty will involve all the necessary specialists as needed.

3 Charter

3.1 Mission Statement

The 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.

CSIRT-CY shall coordinate and assist CII owners/administrators 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.

CSIRT-CY shall also undertake awareness actions 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, CSIRT-CY shall provide timely advisories to all its constituents and make necessary efforts to introduce advanced security services such as security testing, vulnerability scanning and active network monitoring.

The National CSIRT-CY is responsible for processing the data and notifying the competent authorities.

3.2 Establishment

The National CSIRT was established in 2016.

Responsibilities of the National CSIRT-CY

1. The response to the information security incidents in Cyprus in cooperation with the owners and administrators/providers of national critical information infrastructures, electronic communications operators, ISPs;
2. Awareness raising in the field of information security;
3. Cooperation with European and international CSIRT teams;
4. Representing the Republic of Cyprus in the area of Cybersecurity as part of the, soon to be established, NIS Authority.

Constituency

CSIRT-CY approved constituency

1. Cyprus Internet Users (General public and businesses, including SMEs).
2. Cybersecurity community in Cyprus, e.g. Cybersecurity professional and other related professional bodies, chapters.
3. Electronic Communications Network and Service Providers in Cyprus, including ISPs.
4. Law Enforcement Agencies (LEAs).
5. Critical Information Infrastructures (private and government, including critical Electronic Communications Network and Service Providers in Cyprus, including ISPs).
6. Digital Service Providers (DSPs).
7. Academic CSIRT and Government CSIRT.

3.3 Affiliation

The National CSIRT-CY works for the Digital Security Authority.

1. The National CSIRT-CY is a member and actively takes part in the following
    a. CSIRTs Network.
    b. Full member of First since the 23rd of April 2018.
    c. Accredited member of Trusted Introducer since the 21st of June 2018.

2. In addition, the National CSIRT-CY cooperates with other competent Authorities in the following situations:

    a. For matters of National importance at the Government level.
    b. For security issues related to the Critical infrastructure of the Government.
    c. For data protection issues - to the Data Protection Authority.
    d. For suspected criminal activity - at the Cyprus Police Cyber Crime Unit.

3.4 Authority

The Council of Ministers of the Republic of Cyprus with the Action No. 81/477 approved the establishment of the National CSIRT-CY on the 22/10/16.

4 Policies

4.1 Incident types and level of support

The National CSIRT-CY is authorised to address all incidents related or may relate to the critical infrastructure of the Republic of Cyprus.

All incidents are prioritised according to the type, importance and severity of each case. Incidents directly affecting essential service providers and the primary constituency of the National CSIRT-CY are treated with high priority.

The level of support given by the National CSIRT-CY will be based case by case and will depend on the type of the constituent, the type and severity of the incident, the services affected, the size of the user community affected and available sources at the time. In all cases, initial contact will be made with the requestor. An indicative reaction time can be seen on the table below.

Incident Classification	Maximum reaction time to report on incident
Abusive Content	24h
Malicious Code	1h
Information Gathering	24h
Intrusion Attempts	24h
Intrusions	1h
Availability	1h
Information Content Security	2h
Fraud	4h
Vulnerable	24h
Other	2h

4.2 Collaboration, Handling and Disclosure of Information

The National CSIRT-CY maintains cooperation with all the Cypriot competent authorities, Law Enforcement Agencies (LEAs) and all the ISPs. The National CSIRT-CY will share information on a need to know basis directly with the authority/agency requesting relevant information. Where necessary the information will be anonymised excluding information not helping towards the resolution of the issue.

The National CSIRT-CY understands and supports the Traffic Light Protocol (TLP).

4.3 Communication and Authentication

Depending on the information transmitted the National CSIRT-CY telephones will be considered sufficiently secure to be used even unencrypted. Unencrypted e-mail will not be considered particularly secure, but will be sufficient for the transmission of low-sensitive data. If it is necessary to send highly sensitive data by e-mail, PGP will be used. Where it is necessary to establish trust, and before disclosing confidential information, the identity of the other party will be ascertained to a reasonable degree of trust. Within constituency referrals from known, trusted people will suffice to identify someone. Otherwise, appropriate methods will be used, such as a search of FIRST members or Trusted Introducer database and with telephone call-back or e-mail mail-back to ensure that the other party is not an impostor. Incoming e-mail whose data must be trusted will be checked with the originator personally, or by means of digital signatures.

5 Services

The services offered by the National CSIRT-CY can be grouped into three categories.

1. Reactive Services – during an incident.
2. Proactive Services – measures in securing networks against possible threats.
3. Awareness Raising Services – distribution and delivery of educational information to raise the security maturity level and the security knowledge of an organisation.

Reactive Services

5.1 Incident Response

The National CSIRT-CY operates 24/07 via an on-call system and can help in incident handling and response. The National CSIRT will help the system administrators to manage the technical and organisational issues of an incident by providing help and advice on the following issues of incident management.

5.1.1 Incident Triage

a. Analyse if an incident is real.
b. Determination of its extent.
c. Initial incident classification.

5.1.2 Incident co-ordination

Coordination of the incident includes:

a. Determination of the root cause of the incident.
b. Facilitate contact with appropriate law enforcement agencies, if necessary.
c. Create reports for other CSIRTs, if required.
d. Coordinate response to distributed attack incidents.
e. Create announcements to users and relevant stakeholders.
f. Inform the CSIRTs Network, Forum members and TI Accredited and Certified teams

5.1.3 Incident analysis

a. Collection on site (or remotely), preservation, documentation and analysis of the data collected.

5.1.4 Incident Resolution

a. The National CSIRT-CY will provide
    1. Assistance in removing the vulnerability and issue.
    2. Assistance in securing the system from further complications caused by the incident.
    3. Aid in the restoration of the constituent's services.

5.2 Proactive Services

a. Vulnerability Scans (remotely and on site)
b. Alerts and warnings
c. Technology Watch
d. Security Audits/Assessments
e. Configuration and Maintenance of Security
f. Development of security tools
g. Intrusion Detection services

5.3 Awareness Raising Services

a. Presentations and Lectures on Information Security related topics in Governmental institutions.
b. Presentations and Lectures on Information Security related topics in Schools and Universities.
c. Active participation in TF-CSIRT, CSIRTs Network, Cyber Drills and relevant IT Security Conference in Cyprus and the Region.
d. The organisation of Annual Information Security Conferences.
e. The Organisation of Security specialised meetings and discussion within the constituency.
f. Maintain and regularly posts about security-related alerts on http://www.csirt.cy/alerts available to the general public.
g. Maintain and regularly posts about security-related news on http://www.csirt.cy/securitynews open to the general public.
h. Dissemination of validated security relevant information to the general public and organisations that will be interested in the information.

6 Incident report forms

The Incident reporting form is available on www.csirt.cy if needed. Incidents or related information can be reported via email on info@csirt.cy, reporting@csirt.cy or via the phone on 1490 on a 24/7 basis.

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 damages resulting from the use of the information contained within.