CYNET CSIRT

RFC2350

VERSION 1.1 – 2021.05.06

TLP: WHITE

Table of Contents

1. Purpose of a document

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

1.1 Date of last revision

This is version 1.1, published in May 2021. 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 csirt@cynet.ac.cy.

1.3 Position where the document can be found

The current version of this document described by the CYNET-CSIRT is always available on the https://csirt.cynet.ac.cy website under the About Us section. Please check that you are reading the latest version.

1.4 Document authentication

This document has been signed with the CYNET-CSIRT PGP key. The PGP fingerprint is available on the https://csirt.cynet.ac.cy link.

2. Point of contact information

2.1 Group name

CYNET-CSIRT.

2.2 Address

CYNET-CSIRT.

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 693091, +357 22 693084.

2.5 Hotline number (Local)

1490

2.6 Fax Number

+357 22 895494

2.7 Other Communications

In case the classical landline or hotline communication is not feasible, please contact us on the following numbers: +357 97 681189.

2.8 Electronic Management

csirt@cynet.ac.cy is the primary email address for contacting the CYNET-CSIRT reporting.csirt@cynet.ac.cy is the email address that can be used for incident reporting. Incidents can also be reported via our website at https://csirt.cynet.ac.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

The CYNET-CSIRT has a PGP key, with Fingerprint:

2B6A 3A25 8739 1D7D 1FAD 12B5 3287 24DE 4C11 2B9B

The public key and its signatures can be found on the usual large public key servers as well as on the CYNET-CSIRT public website. At the link site https://csirt.cynet.ac.cy.

2.10 Team members

Information about the team can be available upon request.

2.11 Other Information

General information about the CYNET-CSIRT can be found on the website at the link https://csirt.cynet.ac.cy.

2.12 Point of Contacts

The suggested method for contacting the CYNET-CSIRT is via csirt@cynet.ac.cy. All incidents can be reported on reporting.csirt@cynet.ac.cy.

CYNET-CSIRT 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 CYNET-CSIRT provides services and operates at 7:30 am to 15:30 pm weekdays. 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

CYNET-CSIRT provides incident response and security services to all Academic Institutions, Research Institutes and educational networks that are members of the Cyprus Research & Academic Network (CYNET).

It also provides early warning, alerts, announcements and dissemination of information to its constituency and relevant parties regarding risks and incidents. This is accomplished by acting as an intermediary between affected parties and offering, when required, technical advice leading to the resolution of the incident. The affected parties may be internal or external entities to CYNET. CYNET-CSIRT aims to educate its members about the effects of cyber threats and cyber-crime, and train them to provide early warnings, alerts, announcements and efficient use of the respective tools.

3.2 Establishment

The CYNET-CSIRT was established in 2017 according to the Commissioner of Electronic Communications and Postal Regulation decision Action No. 358/2010. The effective start date where the team went into operation is Thursday 1st of September 2018.

Responsibilities of the CYNET-CSIRT:

1. The response to the information security incidents in cooperation with the universities and research institutes of Cyprus, as well as similar organisations;
2. Awareness raising in the field of information security;
3. Cooperation with European CSIRT teams;

3.3 Constituency

CYNET-CSIRT's constituency is the CYNET community, comprising Academic Private Institutes and similar organisations, Research Institutes and similar organisations and Public and Private Schools.

CYNET-CSIRT may provide CSIRT support to other public or private organizations upon signing a binding legal agreement.

Το «Κυπριακό Ερευνητικό και Ακαδημαϊκό Δίκτυο» θα παρέχει πληροφόρηση/ενημέρωση σε όλους τους χρήστες μηχανογραφικής υποδομής των πανεπιστημιακών ιδρυμάτων καθώς και όλους τους Κυπριακούς πολίτες που θα τυγχάνουν εξυπηρέτησης από τη Υπηρεσία καθώς και υποστήριξη πρώτου βαθμού-τηλεφωνική υποστήριξη σε όλους τους Κύπριους πολίτες που θα τυγχάνουν εξυπηρέτησης από την Υπηρεσία και οι οποίοι αντιμετωπίζουν απώλεια υπηρεσίας λόγω καταστροφικού συμβάντος.

Η ενημέρωση δεν θα περιορίζεται μόνο στην αποστολή ενημερωτικών/white papers και στη παροχή της δυνατότητας λήψης από την ιστοσελίδα αναβαθμίσεων για διάφορα λογισμικά. Η ενημέρωση είναι δυνατόν να παρέχεται και σε συνεργασία με τους παροχείς υπηρεσιών ηλεκτρονικών επικοινωνιών π.χ. παροχείς ,υπηρεσιών διαδικτύου (ISPs)

Ν.112(Ι)/2004, Αρ. 3850, 30.4.2004 Παρ Ι παράγραφος 6

The "Cyprus Research and Academic Network" shall provide information/briefing to the entirety of the computer infrastructure users of the university institutions, as well as information/briefing in addition to first class support - telephone support - to all Cypriot citizens who receive services by the Service and who will be faced with service loss, due to a catastrophic event.

The information shall not only be limited to the distribution of informative emails but shall also include the publication of various technical documents/white papers on the Cyprus Research and Academic Network website, and the availability of the provision of upgrades regarding various software, through the website. The information may also be provided in collaboration with electronic communications service providers, for example, internet service providers. (ISPs)

N.112(I)/2004, Αρ. 3850, 30.4.2004 Παρ Ι παράγραφος 6 - Obligations of the Cyprus Research and Academic Network

3.4 Affiliation

CYNET-CSIRT is the Incident Response Team of the Cyprus Academic and Research Network (CYNET). CYNET-CSIRT cooperates with other European CSIRT teams, inter alia, the National CSIRT-CY team and the Digital Security Authority of Cyprus.

3.5 Authority

CYNET-CSIRT coordinates incidents on behalf of its constituency. CYNET-CSIRT is authorized to take operational actions regarding vulnerabilities and mitigation of incidents. Such actions may include but are not limited to blocking access to the CYNET network.

4. Policies

4.1 Types of Incidents and Level of Support

CYNET-CSIRT is authorized to address all types of computer security incidents which occur, or threaten to occur, at CYNET and its members (as defined in 3.2).

CYNET-CSIRT is committed to informing its constituency and to issue alerts and warnings. Furthermore, it analyses the logs from incidents, vulnerabilities and artefacts and performs incident response. The team actively maintains and tests a list of updated security software tools that are used to assist in various activities such as system audits, vulnerability analysis, antivirus and malware handling tasks. These tools are available to all interested parties and to the best of the team's knowledge do not contain software that may exploit known or unknown system vulnerabilities. In addition, it collects various documents related to security issues, such as technical "how to" guides and documentation on system security related techniques, such as system installations, evidence handling, etc.

CYNET-CSIRT will respond to request for assistance by other CSIRTs external to CYNET. CYNET-CSIRT will usually respond within the same work day to request for incident response.

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

4.2 Co-operation, Interaction and Disclosure of Information

The CYNET-CSIRT highly regards the importance of operational cooperation and information sharing between Computer Security Incident 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 CYNET-CSIRT operates in accordance with the GDPR and supports the Traffic Light Protocol (TLP).

CYNET-CSIRT aims to (and is working towards) participate in the TF-CSIRT (Task Force - Computer Security Incident Response Team) program of TERENA and attend its meetings. It also aims to participate in the Trusted Introducer that has been established to facilitate the communication between European CSIRTs.

CYNET-CSIRT wishes to acknowledge the spirit of cooperation that created the Internet. Therefore, while appropriate measures will be taken to protect the identity of members of our constituency and members of neighbouring sites, CYNET-CSIRT will otherwise share information freely in order to assist with the resolution and/or prevention of security incidents. CYNET-CSIRT may release information to any third party or to governing authorities whenever there is a legal obligation to do so.

Vulnerability information will be released freely, though every effort will be made to inform and work with the relevant vendor before the general public is informed. Statistical information will be released at the discretion of CYNET-CSIRT. Other sites and CSIRT's, when they are partners in the investigation of a computer security incident, can be trusted with confidential information. This will happen only if the other site's credentials can be verified and the information transmitted will be limited to that which is likely to be helpful in resolving the incident. Law enforcement officers will receive legally required cooperation from CYNET-CSIRT.

4.3 Communication and Authentication

For normal communication not containing sensitive information CYNET-CSIRT might use conventional methods like unencrypted e-mail or fax.

For Secure communication, the preferred method of communication is by digitally signed email by using either PGP (to be established) or other well-known cryptographical means.

Note digital signatures with self-signed certificates will not be considered secure. Telephone communication 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 non-sensitive data. Where it is necessary to establish trust, for example before relying on information given to CYNET-CSIRT, or before disclosing confidential information, the identity and trust level of the other party will be ascertained to a reasonable degree. Within the constituency, and referrals from known trusted people will suffice to identify someone. Otherwise, appropriate methods will be used, such as a search of FIRST or TI members, the use of WHOIS and other Internet registration information, along with telephone call-back or e-mail mail-back to ensure that the 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. Note that self-signed digital certificates are not considered adequate for establishing the identity of the communicating party.

5. Services

5.1 Reactive Services

5.1.1 Alerts and Warnings

This service involves disseminating information that describes an intruder attack, security vulnerability, intrusion alert, computer virus or hoax and providing any short-term recommended course of action for dealing with the resulting problem. The alert, warning or advisory is sent as a reaction to the current problem to notify constituents of the activity and to provide guidance for protecting their systems or recovering any systems that were affected.

5.1.2 Incident Response

CYNET-CSIRT will inform and assist IT-security teams and NOCs in handling and responding to incidents. In particular, it will provide assistance or advice with respect to the following aspects of incident management:

5.1.2.1 Incident Triage

- ✓ Investigating the validity of the incident.
- ✓ Determining the operational impact of the incident.
- ✓ Assigning a priority for incident response.

5.1.2.2 Incident Coordination

- ✓ Document the incident.
- ✓ Coordinate contact with other sites which may be involved.
- ✓ Coordinate contact CYNET Management.
- ✓ Provide information reports to other CSIRTs.
- ✓ Provide announcements to users, if applicable.

5.1.2.3 Incident Resolution

- ✓ Technical assistance and analysis of compromised systems.
- ✓ Collecting statistics and evidence about incidents that could be used for protecting against future attacks.

5.2 Proactive Services

The proactive services of CYNET-CSIRT include:

- ✓ security announcements (including, but not limited to intrusion alerts, vulnerability warnings, and security advisories)
- ✓ real-time data analysis
- ✓ vulnerability analysis (including website vulnerability assessment)
- ✓ malware classification
- ✓ threat intelligence sharing

5.3 Security Quality Management Services

Besides the technical side of its work, CYNET-CSIRT will perform coordinated actions for:

- ✓ Awareness Building and
- ✓ Education and Training

6. Incident report forms

The incident report form is available on the website https://csirt.cynet.ac.cy. Incidents or related information can be reported via email on reporting.csirt@cynet.ac.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 CYNET-CSIRT assumes no responsibility for errors or omissions, or for damages resulting from the use of the information contained within.