10-10-2014

DANCERT RFC2350 Description

Date:	10-10-2014
Dissemination Level:	Public
Owner:	DANCERT
Authors:	DANTE

Document Revision History

Version	Date	Description of change	Person
1.0	10-10-14	First version issued	Jan Kohlrausch

Table of Contents

1 DOCUMENT INFORMATION

1.1 DATE OF LAST UPDATE

2014-11-06

1.2 DISTRIBUTION LIST FOR NOTIFICATIONS

Not Applicable

1.3 LOCATIONS WHERE THIS DOCUMENT MAY BE FOUND

http://www.dante.net/dancert/dante_rfc2350.pdf

2 CONTACT INFORMATION

2.1 NAME OF THE TEAM

Official name:

DANCERT

Short name:

DANCERT

2.2 ADDRESS

DANCERT
City House
126-130 Hills Road
Cambridge
CB2 1PQ, UK

2.3 TIME ZONE

Time zone is UTC

2.4 TELEPHONE NUMBER

Main number:

+44 1223 866 140

Emergency number:

+44 1480 484694

2.5 Facsimile Number

Fax number:

+44 1480 484680

2.6 Other Telecommunication

Not applicable

2.7 Electronic Mail Address

Please send incident reports which relate to the GÉANT or DANTE network to cert@oc.geant.net. Alternative address: dancert@dante.net

2.8 Public Keys and Encryption Information

```
User ID:      DANCERT SECURITY TEAM <cert@oc.geant.net>
Key ID:       0x2636B332       Key type:      RSA
Key size:     2048             Expires:       never
Fingerprint:  19C1 7A82 AEB3 11FE 6960  8559 3963 F3EB 2636 B332
```

2.9 Team Members

2.10 Other Information

Other information is available at the Trusted Introducer directory at http://trusted-introducer.org/directory/teams/dancert.html

2.11 Points of Customer Contact

The preferred method for contacting is via e-mail:

- For security incidents to cert@oc.geant.net
- For Network, server, service issues dnoc@dante.net
- For application related issues to systems@dante.net

3 CHARTER

3.1 MISSION STATEMENT

DANCERT is the Computer Emergency Response Team (CERT) of DANTE serving users of services delivered by DANTE. The main constituents are National Research and Education Networks (NRENs) in the GEANT project. It deals with computer and network security incidents related to DDOS, Bots, Spamming and infrastructure vulnerabilities that involve services operated by DANTE - for example the GEANT network.

3.2 CONSTITUENCY

The primary constituency are NRENs and associated CERTs participating in the GÈANT project and/or connected to the GÉANT network.

3.3 SPONSORSHIP AND/OR AFFILIATION

DANTE (Delivery of Advanced Network Technology to Europe) was established in 1993 to coordinate pan-European research and education (R&E) networking on behalf of Europe's National Research and Education Networks (NRENs).

GÉANT, the flagship project, serves some 50 million users across Europe, reaches over 100 countries worldwide and is the most advanced international network of its type. Like many of our projects it is co-funded by the European Commission along with European NRENs.

3.4 AUTHORITY

The DANCERT operates under the auspices of, and with authority delegated by, the Delivery of Advanced Network Technology to Europe (DANTE).

DANCERTs assists NRENs and associated CSIRTs to analyse, resolve, and to mitigate network based attacks. As such, it provides services to detect anomalies and attacks on the backbone and to apply network filter to mitigate distributed denial of service attacks.

4 POLICIES

4.1 TYPES OF INCIDENTS AND LEVEL OF SUPPORT

DANCERT is authorized to address all types of computer security incidents which occur, or threaten to occur, on the DANTE or GÉANT network. These include, for example, distributed denial of service attacks, network scans, and compromised machines.

The level of support given by DANCERT 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 the DANCERT's resources at the time. Resources will be assigned according to the following priorities, listed in decreasing order:

- Incident affecting the confidentiality and integrity of data or systems in the DANTE or GÉANT network.
- Incidents that seriously affect the operation and availability of the GÈANT network
- Incidents that affect the NREN networks (e.g. distributed denial of service attacks)
- All other attacks that affect the NREN networks

DANCERT assists the NRENs to mitigate or to resolve from these incidents which includes, for example, to block malicious traffic. Furthermore, the NRENs are informed about security incident that have been detected on the GÈANT network and are related to their network.

Note that no direct support will be given to end users; they are expected to contact their system administrator, network administrator, or department head for assistance. The DANCERT will support the latter people.

4.2 CO-OPERATION, INTERACTION AND DISCLOSURE OF INFORMATION

DANCERT strives to closely collaborate with the NREN and CSIRT community to protect the infrastructure and data of the GÉANT project.

If not agreed otherwise, supplied information are kept confidential. Only data that is required to resolve from the specific incident are disclosed to concerned parties (need to know). DANCERT provide means to support encryption and integrity of data that is submitted to or disclosed by DANCERT.

For data classification, DANCERT supports the Information Sharing Traffic Light Protocol that comes in with the tags WHITE, GREEN, AMBER or RED. The data will be handled appropriately. A description can be found at

http://www.terena.org/activities/tf-csirt/publications/ISTLP-v1.1.pdf

4.3 Communication and Authentication

DANCERT supports PGP for encrypted mails whereas the usage of PGP in all cases where sensitive information is involved is highly recommended. The details of the current PGP key can be found in Sec. 2.8.

Requests for information or security controls such as firewall filters are restricted to authorised NREN or associated CSIRT members. For authentication issues, DANTE maintains information about authorised representatives or use other means (e.g. telephone call back) to authenticate a person.

5 Services

5.1 Incident Response

DANCERT will assist system administrators and NREN CSIRTs in handling the technical and organizational aspects of security incidents on the GÈANT and DANTE network. In particular, it will provide assistance or advice with respect to the following aspects of incident management:

5.2 Incident Triage

- Assessment of the severity of the incident. If required the incident will be escalated to the General Management.
- Hand off to the appropriate team (e.g. GÉANT NOC)

5.3 Incident Coordination

- Determining the cause and extend of the incident and involved sites (e.g. DDoS)
- Dissemination of incident reports to NRENs

5.4 Incident Resolution

- Providing advice to affected sites
- Removing the vulnerability
- Securing the system from the effects of the incident
- Application of network filters, if applicable

5.5 Proactive Activities

- Network monitoring to detect attacks as early as possible
- Sharing information with the CSIRT community and constituency

6 INCIDENT REPORTING FORMS

There are no reporting forms available.

7 DISCLAIMERS

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