

CSIRT Description for TP CERT

Table of Contents

1. Document Information 2

- 1.1. Date of Last Update 2
- 1.2. Distribution List for Notifications 2
- 1.3. Locations where this Document May Be Found 2
- 1.4. Authentication this Document 2

2. Contact Information 2

- 2.1. Name of the Team 2
- 2.2. Address 2
- 2.3. Time Zone 2
- 2.4. Telephone Number 2
- 2.5. Facsimile Number 2
- 2.6. Other Telecommunication 2
- 2.7. Electronic Mail Address 2
- 2.8. Public Keys and Encryption Information 2
- 2.9. Team Members 2
- 2.11. Points of Customer Contact 3

3. Charter 3

- 3.1. Mission Statement 3
- 3.2. Constituency 3
- 3.3. Sponsorship and/or Affiliation 3
- 3.4. Authority 3

4. Policies 3

- 4.1. Types of Incidents and Level of Support 3
- 4.2. Co-operation, Interaction and Disclosure of Information 4
- 4.3. Communication and Authentication 5

5. Services 5

- 5.1. Incident Response 5
 - 5.1.1. Incident Triage 6
 - 5.1.2. Incident Coordination 6
 - 5.1.3. Incident Resolution 6
- 5.2. Proactive Activities 6

6. Incident Reporting Forms 6

7. Disclaimers 6

1. Document Information

1.1. Date of Last Update

This is version 1.02, published 2008/01/16.

1.2. Distribution List for Notifications

None available at this moment.

1.3. Locations where this Document May Be Found

The current version of this CSIRT description document is available from the TP CERT WWW site; its URL is <http://www.tp.pl/cert/>

Please make sure you are using the latest version.

1.4. Authentication this Document

The text versions of this document have been signed with the TP CERT's PGP key. The signatures are also on our Web site, under: <http://www.tp.pl/cert/>

2. Contact Information

2.1. Name of the Team

"TP CERT": Telekomunikacja Polska Computer Emergency Response Team

2.2. Address

TP CERT
TELEKOMUNIKACJA POLSKA
Ul. Dzielna 52
01-029 Warszawa
Poland

2.3. Time Zone

GMT +0100 - Central European Time (CET)

GMT +0200 - Daylight Saving Time (from last Sunday in March to last Sunday in October)

2.4. Telephone Number

+48 22 887 17 88, working hours only (ask for the TP CERT)

2.5. Facsimile Number

+48 22 824 14 52 (this is *not* a secure fax)

2.6. Other Telecommunication

None available at this moment.

2.7. Electronic Mail Address

<cert@telekomunikacja.pl> This is a mail alias that relays mail to TP CERT team members on duty handling all incoming mails.

2.8. Public Keys and Encryption Information

The TP CERT has a PGP key for encryption and signing, whose KeyID is 0xCB779BD0 and whose fingerprint is AFA2 E965 6949 1BCB ED09 E17A DBFC 5A3B CB77 9BD0.

The key and its signatures can be found at the usual large public keyservers and also Public PGP key is available from the Web site at: <http://www.tp.pl/cert/>

2.9. Team Members

Piotr Smialek is the TP CERT coordinator.

Backup coordinator is Artur Barankiewicz.

General information about the TP CERT, as well as links to various recommended security resources and services, can be found at <http://www.tp.pl/cert/>

2.11. Points of Customer Contact

The preferred method for contacting the TP CERT is via e-mail at <cert@telekomunikacja.pl>; e-mail sent to this address will be handled by the responsible human.

If it is not possible (or not advisable for security reasons) to use e-mail, the TP CERT can be reached by telephone and fax during regular office hours (please, check Section 2.4 and 2.5).

TP CERT's hours of operation are generally restricted to regular business hours (09:00-17:00 Monday to Friday except holidays).

If possible, when submitting your report, use the form mentioned in Section 6.

3. Charter

3.1. Mission Statement

The main purposes of the TP CERT are:

- to assist users of TP network in implementing proactive measures to reduce the risks of computer security incidents, in particular:
 - providing a consultancy and education services for users,
- to assist users of TP network in responding to such incidents when they occur, in particular:
 - providing a single point of trusted contact for users to deal with computer security incidents and problems,
 - a complex coordination of all responses to an incident (handling incidents) with special emphasis on exchanging information between various interested parties,

3.2. Constituency

The TP CERT's constituency is all users and organizations of the TP (contains all those systems connected to TP network: AS 5617, 29535).

3.3. Sponsorship and/or Affiliation

The TP CERT is sponsored by the Telekomunikacja Polska (Polish Telecom) which is part of.

3.4. Authority

The TP CERT operates under the auspices of, and with authority delegated by, the management of Telekomunikacja Polska.

The TP CERT expects to work cooperatively with system administrators and users (customers) at TP network, and, insofar as possible, to avoid authoritarian relationships. However, should circumstances warrant it, the TP CERT has the authority to take the measures it deems appropriate to properly handle a computer security related incident.

4. Policies

4.1. Types of Incidents and Level of Support

The TP CERT is authorized to address all types of computer security incidents which occur, or threaten to occur, at TP's constituency (see section 3.2). TP CERT handles all types of security incidents, that occurred or threaten to its constituency (may act upon request of one of its constituents, or may act if a constituent is, or threatens to be, involved in a computer security incident - see section 3.1).

The level of support given by TP CERT 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 TP CERT's

resources at the time. Resources will be assigned according to the following priorities, listed in decreasing order:

- root or system-level attacks on any Management Information System, or any part of TP backbone network infrastructure or attacks on any large public service machine;
- compromise of restricted confidential service accounts or software installations, compromise of confidential data or integrity, also used for system administration;
- denial of services attacks or any other attempts of limiting availability of service or information (especially massive distributed attacks) on any of the above 3 items;
- any of the above malicious actions at other sites, originating from the constituency of TP CERT;
- large-scale attacks of any kind, e.g. "social engineering" attacks, password cracking attacks;
- threats, harassment, and other criminal offenses involving individual user accounts;
- compromise of individual user accounts on multi-user of desktop systems;
- forgery and misrepresentation, and other security-related violations of local rules and regulations, e.g. e-mail forgery, spam e-mail;

Types of incidents other than those mentioned above will be prioritized according to their apparent severity and extent.

TP CERT will basically accept any incident report that involves an incident with one of the constituents either as a victim or as a suspect. However, TP CERT encourages the engagement of qualified security staff at the involved organization in an early stage. Whenever feasible, TP CERT will contact the relevant Site Security Contact of the organization allegedly involved, even if the end user has chosen not to do so.

While the TP CERT understands that there exists great variation in the level of system administrator expertise at TP, and while the TP CERT will endeavor to present information and assistance at a level appropriate to each person, the TP CERT cannot train system administrators on the fly, and it cannot perform system maintenance on their behalf. In most cases, the TP CERT will provide pointers to the information needed to implement appropriate measures.

The TP CERT is committed to keeping the TP system administration community informed of potential vulnerabilities, and where possible, will inform this community of such vulnerabilities before they are actively exploited.

4.2. Co-operation, Interaction and Disclosure of Information

While there are legal and ethical restrictions on the flow of information from TP CERT, many of which are also outlined in the TP (Polish Telecom), and all of which will be respected, the TP CERT acknowledges its indebtedness to, and declares its intention to contribute to, 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 neighboring sites where necessary, the TP CERT will otherwise share information freely when this will assist others in resolving or preventing security incidents.

In the paragraphs below, "affected parties" refers to the legitimate owners, operators, and users of the relevant computing facilities. It does not refer to unauthorized users, including otherwise authorized users making unauthorized use of a facility; such intruders may have no expectation of confidentiality from the TP CERT. They may or may not have legal rights to confidentiality; such rights will of course be respected where they exist.

Information being considered for release will be classified as follows:

- Private user information is information about particular users, or in some cases, particular applications, which must be considered confidential for legal, contractual, and/or ethical reasons.

Private user information will be not be released in identifiable form outside the TP CERT.

- Intruder information is similar to private user information, but concerns intruders.

While intruder information, and in particular identifying information, will not be released to the public (unless it becomes a matter of public record, for example because criminal charges have been laid), it will be exchanged freely with system administrators and CSIRTs tracking an incident.

- Private site information is technical information about particular systems or sites.

It will not be released without the permission of the site in question, except (for some special cases) as provided for below.

- Vulnerability information is technical information about vulnerabilities or attacks, including fixes and workarounds.

Vulnerability information will be released freely, though every effort will be made to inform the relevant vendor before the general public is informed.

- Statistical information is embarrassing information with the identifying information stripped off.

Statistical information will be released at the discretion of the TP IT&N Department Security. Statistical information will be released only after adequate preprocessing in the form of official periodical reports.

- Contact information explains how to reach system administrators and CSIRTs.

Contact information will be released freely, except where the contact person or entity has requested that this not be the case, or where TP CERT has reason to believe that the dissemination of this information would not be appreciated.

4.3. Communication and Authentication

In view of the types of information that the TP CERT will likely be dealing with, 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-sensitivity data. If it is necessary to send highly sensitive data by e-mail, PGP will be used. Network file transfers will be considered to be similar to e-mail for these purposes: sensitive data should be encrypted for transmission.

Where it is necessary to establish trust, for example before relying on information given to the TP CERT, or before disclosing confidential information, the identity and bona fide of the other party will be ascertained to a reasonable degree of trust. Within TP, and with known neighbor sites, referrals from known trusted people will suffice to identify someone. Otherwise, appropriate methods will be used, such as a search of FIRST members, the use of WHOIS and other Internet registration information, etc, 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 (PGP in particular is supported).

For PGP keys of TP CERT see also section 2.8.

5. Services

5.1. Incident Response

TP CERT will assist system administrators in handling the technical and organizational aspects of incidents. In particular, it will provide assistance or advice with respect to the following aspects of incident management:

5.1.1. Incident Triage

The main goals of incident triage are:

- investigating whether indeed an security incident occurred,
- determining the extent and severity of the incident (including a potential impact on the constituency), etc.

5.1.2. Incident Coordination

The goal follow is to provide a complex coordination incidents with particular emphasis on exchanging information between various involved parties. These include but are not limited to:

- determining the initial cause of the incident (exploited vulnerability),
- facilitating contact with other sites which may be involved,
- facilitating contact with appropriate security teams and/or law enforcement officials if necessary,
- making reports to other CSIRTs, if applicable
- composing announcements to users (members of the constituency), if applicable.

5.1.3. Incident Resolution

The incident resolution only is performed in very limited range, mainly due to limited resources. In fact limited to special cases. The actual range of activities in such cases collecting the evidence of the incident, or other disciplinary actions, are contemplated.

In addition, TP CERT will collect statistics concerning incidents which occur within or involve the TP community, and will notify the community as necessary to assist it in protecting against known attacks.

To make use of TP CERT's incident response services, please fill in the incident report form available at <http://www.tp.pl/cert/> or send e-mail as per section 2.11 above.

Please remember that the amount of assistance available will vary according to the parameters described in section 4.1.

5.2. Proactive Activities

The TP CERT coordinates and maintains the following services to the extent possible depending on its resources:

- Information services
 - the official website of TP CERT is main security point of view and channel for unrestricted distributing information by TP CERT, as well as the most important pointers to information from other sites that might be important or interesting, protecting your computer etc.
- Archiving services
 - recording of security incidents handled will be kept. While the records remain confidential, periodic statistical reports will be made available to the TP constituency;

6. Incident Reporting Forms

If possible, use the following form when reporting a security incident: <http://www.tp.pl/cert/>

There are overall guidelines and incident reporting samples available, containing all information that should be included in an incident report, Web site at: <http://www.tp.pl/cert/>

7. Disclaimers

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