RFC 2350

1. About This Document

This document about the adoption of RFC2350 –expectation of a Computer Security Incident Response – that Black Cert do his job of the best practice

1.1 Date of Last Update

This is version 1.11, published 4th of July, 2016.

1.2 Distribution List for Notifications

Notifications of updates are submitted to our mailing list .

Subscription requests for this list should be sent to ; the body of the message should consist of the word "subscribe" or asking for join and give name, institution and telephone number.

1.3 Locations where this Document May Be Found

The current version of this CERT description document is available from the Black Cert WWW site, its URL is http://www.blackcert.hu

The English version is available at http://www.blackcert.hu/en

1.4 Authenticating this Document

Both the Hungarian and English versions of this document have been signed with the ID-CERT's PGP key.

2. Contact Information

2.1 Name of the Team

Black Cert

Black Computer Emergency Response Team

2.2 Address

7. Salétrom Street, Budapest

Hungary 1085

2.3 Time Zone

Budapest (GMT+ 0100)

2.4 Telephone Number

+36 1 785 9901

+36 1 951 2991

2.5 Facsimile Number

None available.

2.6 Other Telecommunication

None available.

2.7 Electronic Mail Address

This is a mail alias that relays mail to the human(s) on duty for the Black CERT.

alarm@blackcert.hu

This is email for reporting incident in Phishing/Spoofing.

alarm@blackcert.hu

This is email for reporting incident in network.

alarm@blackcert.hu

This is email for reporting incident in IPR (Intellectual Property Rights).

alarm@blackcert.hu

This email for reporting Spam .

alarm@blackcert.hu

2.8 Public Keys and Other Encryption Information

Black CERT

Fingerprint : 7180 3F59 566F 3DD9 ED56 4B9D 20B9 982E 191C C812

Website: http://www.blackcert.hu

Email: alarm@blackcert.hu

This key still has relatively few signatures; efforts are underway to increase the number of links to this key in the PGP “web of trust”. In the meantime, since most fellow CERTs at CERT.org have at least one staff member who knows the Black CERT HelpDesk, it has signed the BLACK CERT key, and will be happy to confirm its fingerprint and that of its own key to those people who know BLACK CERT, by telephone or in person.

2.9 Team Members

Gergo Gyebnar, BLACK CERT founder and coordinator chief

Tibor Luter, BLACK CERT Manager

Donat Kovacs, BLACK CERT Incident Response Officer – HelpDesk

Backup coordinators and other team members, along with their areas of expertise and contact information, are listed in the BLACK CERT web pages, at http://www.blacekcert.hu

2.10 Other Information

General information about the BLACK CERT, as well as links to various recommended security resources, can be found at http://www.blackcert.hu

2.11 Points of Customer Contact

The preferred method for contacting the BLACK CERT is via e-mail at ; e-mail sent to this address will "biff" the responsible human, or be automatically forwarded to the appropriate backup person, immediately. If you require urgent assistance, put "urgent" in your subject line.

If it is not possible (or not advisable for security reasons) to use e-mail, the BLACK CERT can be reached by telephone during regular office hours. Telephone messages are checked less often than e-mail.

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

3. About BLACK CERT

3.1 Mission Statement

1. To coordinate the incidents handling involving community locally and internationally.

2. It is built from community and the results will be given back to the community.

3. To increase the internet security awareness in Hungary by provide services for his client

4. To have research in internet security which is needed by the Hungarian internet community.

3.2 Constituency

BLACK CERT constituent is general and not-opened (for public).

3.3 Sponsoring Organization / Affiliation

BLACK CERT is periodically sponsored by its constituent.

BLACK CERT is affiliated with various CSIRT around the world which based on a required basis.

3.4 Authority

BLACK CERT does not have the operational authority of the constituency both in Indonesia and abroad, but only to inform the various complaints of network incidents, and relies entirely on the cooperation with the parties involved in an incident related networks.

BLACK CERT expects to work closely with the sys-admin and user from various organizations including ISPs, NAP, Telecommunication Operator, Corporate (Banking, Private and Public), Government and the University, and as far as possible, avoid authoritarian relationships.

4.Policies

4.1 Types of Incidents and Level of Support

BLACK CERT is currently dealing with a number of incidents which have occurred in various organizations.

BLACK CERT provides incident response services based on reports constituents.

4.2 Co-operation, Interaction and Disclosure of Information

All information received will be treated as CONFIDENTIAL by ID-CERT, regardless of priority.

When reporting these types of incidents are sensitive, please state clearly (example: the use of the label "SENSITIVE" in the email title) and if possible use an encryption method for sending email.

4.3 Communication and Authentication

For secure communication, the following is BLACK CERT PGP key:

Bits = 2048 Keys;

Keys ID = 2048R/82711AC7

Fingerprint= 73F3 7A69 8B1F C0FF 25F8 391C 37A9 E70E 8271 1AC7

-----BEGIN PGP PUBLIC KEY BLOCK-----

Version: GnuPG v2

mQENBFebPh8BCAD2FrKjAA6tqRVtVbIx0NYy2Xz2amcEbDQiRZ2mjqAwqQl4ejNB

MDOg0Hr7NHCArbOltXG0A9hXkshyvn5aQDk0czrz2B0bXokvESRnSuIeQhbT0so7

OYlW5BWEsRw46IxvD0wvaOD1VGDzTlvVdyIrbvERnKtfBoqIzHraNlgk7QpGNxKN

SlmCQ4ZGUi37odCRp29hTGZ61ojj4o2tns4rmUN0/4YOkWxbWscTmEF7IL8+kuku

H/hwjBqocDUdHeJIDcjNOrL+kKgPt6zJilSEYiRpSLD5ms+5+hM5i0Adt7/ASVzm

Q/TuaLMRQxmTZc3CV+gXg9+Yg7JBsCRu1AMDABEBAAG0V0JsYWNrQ2VsbCAtIERl

ZmVuY2UgU3lzdGVtcyAoRGVmZW5jZSBTeXN0ZW1zIC0gSW5jaWRlbnQgUmVwb3J0

aW5nKSA8YWxhcm1AYmxhY2tjZXJ0Lmh1PokBOQQTAQgAIwUCV5s+HwIbAwcLCQgH

AwIBBhUIAgkKCwQWAgMBAh4BAheAAAoJEDep5w6CcRrHOkAIAO6vQ5AkA/4vcsZO

FJg6dWrQnkUpMD1qRI9d8MgPhWLmdQFq5JMzy66XZ6ha6UwlKv1HLz1dM92B6Tnk

b4+XxKrJc5sPyBrnN65PfAjqSlsBOAqA2gNr1tOTeyA+HmXg6pzmlY9HCV79jgeb

Uioa05NFZXbxDx4ZXWNGAL8tzhw4g3U6RhahC/BuAjQuKFfZ+M2qyXZ+7ZiQX4jo

0gt/x/uwPwTp+rw9HzsFyumuCOHaKDF3xLHYK1yuhvglQORl2AJybuJt5tyTax7n

tLgJV9wN1L8G2KfTy8f89j5/RQkL6vjNZ6u3xu63PK354Pufqoym6e/YxpF5x4MV

ngOF34y5AQ0EV5s+HwEIANBmukOGAoLfj61uK6xjJeSc95XBxJaiXVcFiUL+iR8q

c7nHcnHD7M9qEKE1Yik6vbbxncepUhiwyg55EduvQfiVy3P4/ZR6qbZHzjMlvy9I

+tZuVC9Z5f8IFAu5lKBqnK63fRkfce6n5KxZEnitdKibblt3aM0A8ZcHH7Y5W+01

c8fRxqLJaquPej/2PuqIBVxAEHWMhDaSiAHg3ddRz3g1msY5zv9gwnbHc1CCkAxA

O+6xJ8twbxjRUokC9vWq9ahwj0QtdPGQ+i49+RsiwwRjcmBt2q+2VCzU34qY3cTV

JFr9B0iiKj++IuXOAon42Mlz0j7VwPCNOd+Tnceh51MAEQEAAYkBHwQYAQgACQUC

V5s+HwIbDAAKCRA3qecOgnEaxwZVB/0e7wxde5tYcr8lvx/JnT2G/z68D9Xs3QSt

8Jw5iGB2KF0AfHzoeOIHT6PTxgwew39b2899ZE1hghlv9QFl7S97YpMKu7Yj+822

VUs11QIOaIkCMSJLxOSJkL8owunjtAauWRiNHGGBcyARjVfQ+nJHSikEGps50ypO

whb4bUFmTFJbZcYcmEqnKuL20QxWaVHOsd+yPATUGAu7nyIm1wqnCHw4wTcBvrCp

xqCyHfUfXVnxUGHEkozvubUG9yt+QDhW4lQcSoa+VPuPqxS/Fj4ZMc0IlEM9042d

srRRh7uB9Je6CLiQpM77LPtXsDtzbDCIhthQJMJmf6HMASiKrJQj

=hdlL

-----END PGP PUBLIC KEY BLOCK-----

5.Services

5.1 Incident Response

BLACK CERT will help sys-admins to handle the technical aspects and the organization – under contractual relationship – of the incident. Notably, BLACK CERT will provide assistance or advice on the management aspects of the following incidents:

5.1.1 Incident Triage

Investigate whether an incident actually occurred.

Determining the extent of the incident.

5.1.2 Incident Coordination

Determine the initial cause of the incident (the use of sensitivity/weaknesses).

Facilitate contact with others who may be involved.

Facilitating contacts with other CSIRT Security team and/or the appropriate official Law/Act accordingly, if necessary.

Make reports to other CSIRTs.

Compiling notices/announcements to the user/users, if necessary.

5.1.3 Incident Resolution

Eliminate weaknesses, carried out by the reported party.

Securing the system from the effects of the incident, carried out by the reported party.

Evaluate whether certain actions possible to obtain results that are comparable to the costs and risks, particularly actions directed at a claim or disciplinary action: gathering evidence, observation of one incident that is happening, setting a trap for the intruders, etc.

Conducted by law enforcement or other related parties in compliance with the applicable legislation.

In addition, BLACK CERT will collect statistics concerning incidents occurring in or involving community-ID-CERT, and will notify the community as necessary to help protect against known attacks.

To use BLACK CERT incident response service, please send an e-mail as mentioned in the section above 2.11

Please note that the amount of assistance available varies according to the parameters described in section 4.1

5.2 Proactive Activities

BLACK CERT coordinates and take care of the following services to the extent possible that depending on the source:

Information/Data Services

Security contact list of organization, administrative and technical. This list is available to the public, through a common channel available such as www and/or Domain Name Service or by contacting BLACK CERT through the contact listed in section 2.11.

Mailing list to inform security contacts for new information/data relating to their computing environment.

This list is only available for sys-admins and BLACK CERT Constituents.

Storage is provided by the vendor and patches related to security for various operating systems. This storage is available to the general public in any license restrictions allow it, and is provided through public channels such as www and/or ftp.

Equipment storage and security documentation to be used by the sysadmin. If possible, ready-to-install version of the precompiled will be provided. The storage will be provided to the general public via the www or ftp as above.

"Clipping" service for a variety of existing sources, such as mailing lists and newsgroups. Results clipping also available in a limited mailing list on the website, depending on the sensitivity and importance.

Reactive services

Members of the BLACK CERT will get service in accordance with what is reporting. BLACK CERT have the tools that are monitoring and focus on complaints from the community and constituents.

Details on the above services can be viewed on BLACK CERT website, as in section 2.10 above, with instructions for joining the mailing list, download the information/data, or participate in certain services such as central logging and file integrity checking service.

Incident Reporting Forms

Other alternative, the report can be sent to by attaching at least:

- Log file

- Timestampt

- Name of the complaining

- Telephone number to call