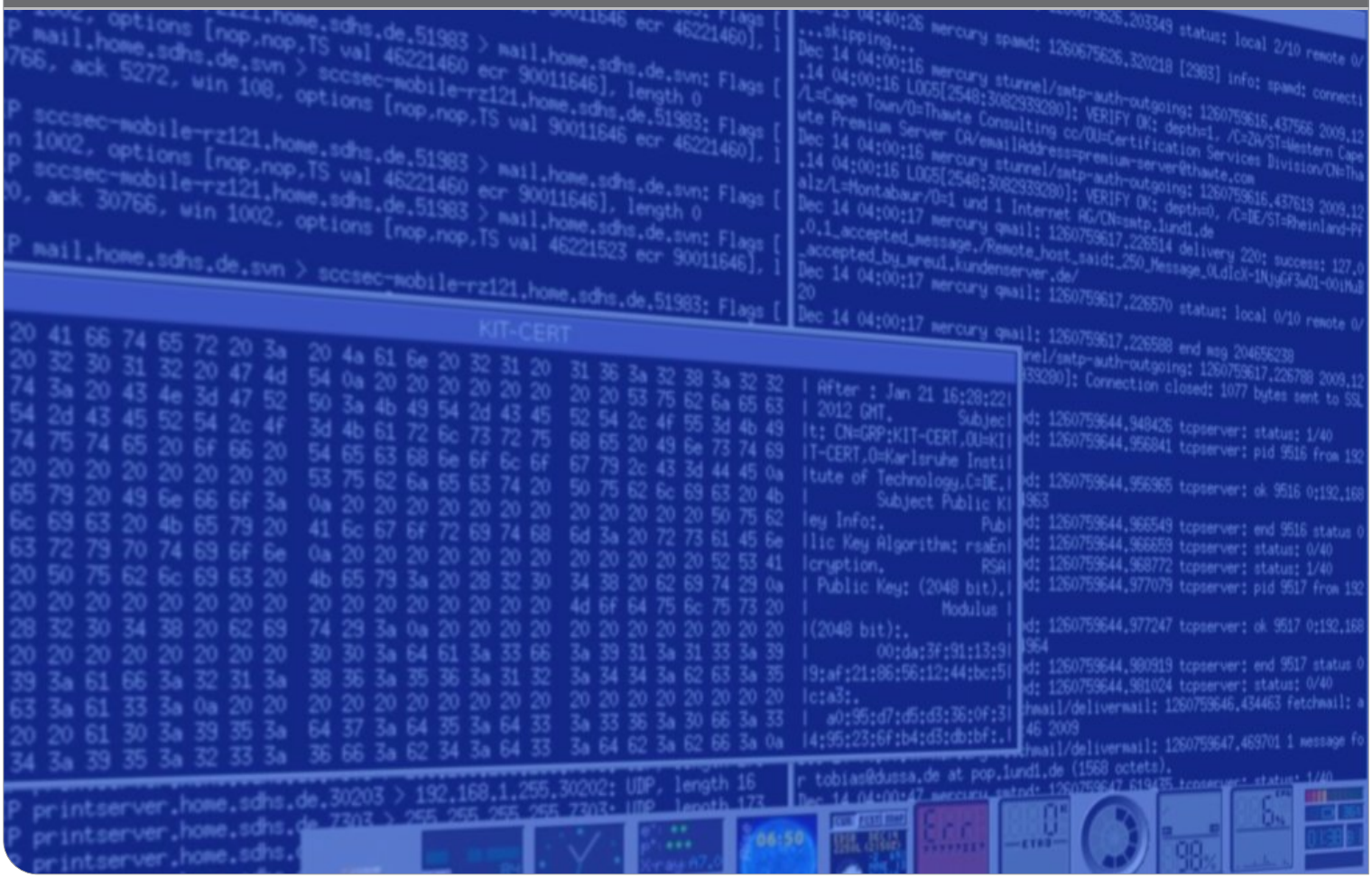
Karlsruhe Institute of Technology

CERT Description

as per RFC 2350

Tobias Dussa

COMPUTER EMERGENCY RESPONSE TEAM



KIT CERT

Contact

Karlsruhe Institute of Technology (KIT)
Computer Emergency Response Team (CERT)

Tobias Dussa
Manager

Campus South
Zirkel 2
76131 Karlsruhe
Germany

Telephone: +49 721 608-42479
Fax: +49 721 608-9-42479
E-Mail: tobias.dussa@kit.edu

www.cert.kit.edu

Published by

Karlsruhe Institute of Technology (KIT)
Computer Emergency Response Team (CERT)
Zirkel 2 | 76131 Karlsruhe | Germany

Telephone: +49 721 608-45678
Fax: +49 721 608-9-45678
E-Mail: cert@kit.edu

Revised on 2018-03-23 (Revision 9/564f439)

www.kit.edu

Contents

Revision History

Version	Effective as of	Author(s)	Change(s)
1	2012-11-07	Dussa, Tobias	Initial revision.
2	2013-03-06	Dussa, Tobias	Network list updates; URL updates; spelling corrections; minor additions.
3	2013-10-17	Dussa, Tobias	Updated team member information; unified IPv6 address notation; spelling corrections.
4	2017-02-14	Dussa, Tobias	Updated team member information; updated policy references; minor corrections; minor layout changes; fixed notation inconsistency.
5	2018-01-26	Dussa, Tobias	Updated team member information.
6	2018-03-23	Dussa, Tobias	Updated network information.

1 About this Document

1.1 Date of Last Update

This is version 6, published on 2018-03-23 (revision 9/564f439).

1.2 Distribution List for Notifications

Notifications of updates are submitted to our mailing list cert-info@lists.kit.edu.

Subscription requests for this list should be sent to the Sympa listserver at cert-info-request@lists.kit.edu; the subject of the message should consist of the word `subscribe`. Send the word `help` instead if you don't know how to use a Sympa list server. Additional help to this list is available at `https://www.lists.kit.edu/sympa/help`. Archives of this list are available at `https://www.lists.kit.edu/sympa/info/cert-info`. Logging on with your subscribed mail address is required to view the archives.

This mailing list is moderated.

1.3 Locations Where this Document May Be Found

The current version of this CERT description document is available from the KIT-CERT website; its URL is `https://www.cert.kit.edu/p/rfc2350`.

Please make sure you have the latest version.

1.4 Authenticating this Document

This document has been signed with the KIT-CERT PGP key. The key's fingerprint can be found on the KIT-CERT web site and in the SCC-News (the printed newsletter of the Steinbuch Centre for Computing). The public key can be downloaded from the usual key servers, for example the MIT public key server (`http://pgpkeys.mit.edu`). See section 2.9 for more information.

2 Contact Information

2.1 Name of the Team

KIT-CERT: Karlsruhe Institute of Technology Computer Emergency Response Team.

2.2 Address

KIT-CERT
Karlsruhe Institute of Technology
Steinbuch Centre for Computing

76128 Karlsruhe
Germany

2.3 Date of Establishment

KIT-CERT was established March, 14th 2008.

2.4 Timezone

Europe/Berlin (UTC+01, and UTC+02 on DST).

2.5 Telephone Number

+49 (721) 608-45678 (ask for KIT-CERT).

2.6 Facsimile Number

+49 (721) 608-9-45678 (be advised that this is *not* a secure fax).

2.7 Other Telecommunications

Not available.

2.8 Electronic Mail Address

KIT-CERT can be reached via cert@kit.edu. This is a mail alias that relays mail to the KIT-CERT staff on duty.

2.9 Public Keys and Other Encryption Information

The KIT-CERT PGP key has the KeyID `0x291D553CD742DE72` and the following fingerprint: `69AF DA25 704D FD54 3BA1  C408 291D 553C D742 DE72`.

The public key is as follows:

```
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: GnuPG v1.4.6 (GNU/Linux)

mQGiBEfq1YkRBACz0Ew1CZE80Fz9vCIGoupQKnUvLzjVYl6gN2eno4Qne2NME0sQ
sVIUKojZUF774pI+HIKB5TATh77GoXfOD0LeniUwbJ9/PgV3++41L33tQYy07AUF
1gvIK2Elwn1NF493e4gZCiEwBZf5Dyi9tYhfrtNo6IgKR6Wkaz6HjzVAZwCg9jQg
0+Vy1yQWFcBLUXb4K60LT1ED/3iIg40658cN6W+nzuM5Cxfe4xT8Ig2Ug3IJ6Y1F
nfdNC4FDf5w5RnClDpk2gaUYhjJFLV2odfWNJizlzsFq43r4gAlpvMbuaY9U60kr
TqILTkwMpOQ2PAzZZekbZHJbmaoCLDmKzP4sn6b3QE5HBP+BXh4FxfgaESjCg1IM
KM/gA/9n51Spe62Upnf3Dsalk5ynFad0WXCMKUJQy/xXbk1ke9dSngxU8LA0E+kM
I0W6W7Lo1b1eX0PT5mY+cAJf4q6hENNQTOh0NBg3hnHiIBm6mQqH/G1sC9v1gLWC
r5+S4gwl0C4LTPB77pRIoEFSSAPqO7BFema5j9ySudtbVwbni7QXS0lULUNFUlQg
PGNlcnRAa2l0LmVkdT6IYAQTEQIAIAUCR+rViQIbAwYLCQgHAwIEFQIIAwQWAgMB
Ah4BAheAAAoJECkdVTzXQt5yQlQAni9WSeicIF3pvtnz/0ux4Yqrw5ZJAJ9aKvje
0rqcd/gRSQrN69dLLZpRqLkCDQRH6tWMEAgAtZzpGMpYay0ORq6k0RlKBeofQGpH
VogKJwI9Va3LkfhPrb6UPYmSZM7iQFWOZ4SbqRvQ4oflfdwKqn94e3SQBmemWs6r
hGbxGbrmC4gsRHaAKam+XiKn+GsW93Y3Y0Zy++k0/UPadHtrVDrYd0iy3dzlMP/s
sdvkFLs+fck4/e9wo2RZ0lC+pt7ihiPem3Yh1euqT10y8CdBhRJeaZLZuAj5/rHp
tgeuiNpgnIBK908YjZ0Iis3oxVCL3ZyOfOjvxujag73pO95Tm7mMNE83qgVyJ2xN
uu/FObPDIgGOBcMYCoJ4CdTpJFOVkTgf6uzjDBIgBtqHVxXP0K/4PM+wLwADBQf9
GciKe/5W9KngdY3/Rh38++cv1sWPHvGDE0TVx8HjJXU2KGIYugPH98KYcbqAYM/g
TSDPQjx6vx6lDdIiHTSzE6vGj0Pjy0tjiLdKmYKHR8EabeRap9QTwpn7BxOGcnL7
Z57jKksxFmx+UAISBG5Gx1+KF5OIqPlzwFTKivtUFXCS9+xGQJnjefL5Wk8tj46G
hoc86vkgaWFkvlClKqVtdXipIjUDzGYV+iKsniBSO6L0FHoa0Vr265rcrte4YOR6
Jl8Yc9UHQwsB5Yb3+VjQVAs7HEwXcxTyZE7FnWQWrqie7UZzmEbxY+ZZ+u7pPaKV
ADbLoWlWuqeAueyMOmR9JYhJBBgRAgAJBQJH6tWMAhsMAAoJECkdVTzXQt5yLu8A
n04d1ETvPDdNwKn/LHT7A8sZiDptAKDUd3U3Qfcdj+sD9S0lnBWT5GyVQA==
=GMy5
-----END PGP PUBLIC KEY BLOCK-----
```

The key and its signatures can be found on the usual public key servers. Additionally, the key can be found at http://www.cert.kit.edu.

KIT-CERT seeks to gain as many signatures from other teams or individuals for the KIT-CERT public key in an effort to further the PGP "web of trust."

2.10 Team Members

Tobias Dussa from the IT Security and Service Management department is the KIT-CERT coordinator. Backup coordinators and other team members and contact information, are listed in the KIT-CERT web pages at http://www.cert.kit.edu.

List of team members:

- Dussa, Tobias (Team Coordinator)
- Lang, Matthias

- Lorenz, Andreas
- Reese, Heiko (Backup Team Coordinator)
- Stadie, Ulrich
- Tuellmann, Thorsten

Management, liaison and supervision are provided by Tobias Dussa, head of IT Security, Steinbuch Centre for Computing, Karlsruhe Institute of Technology.

2.11 Other Information

General information about the KIT-CERT as well as links to various recommended security resources can be found at `http://www.cert.kit.edu`.

2.12 Points of Customer Contact

The preferred method for contacting the KIT-CERT is via e-mail through cert@kit.edu; e-mail sent to this address will be delivered to the on-duty staff. If urgent assistance is required, include the keyword `[URGENT]` in your subject line.

If it is not possible or not advisable for security reasons to contact the KIT-CERT via e-mail, contact may be made by telephone during regular office hours. Voicemail is checked less frequently than e-mail.

The KIT-CERT hours of operation are generally restricted to regular business hours (09:00–17:00 local time, Monday through Friday, except on holidays).

3 Charter

3.1 Mission Statement

The goals of the KIT-CERT are

1. to assist the Karlsruhe Institute of Technology community in responding to computer-security-related incidents when they occur, and
2. to assist members of the KIT community in implementing proactive measures to reduce the risk of such incidents to occur.

3.2 Constituency

The KIT-CERT constituency is the Karlsruhe Institute of Technology community, as defined in the context of the following policies:

- »Ordnung für die digitale Informationsverarbeitung und Kommunikation (IuK) am Karlsruher Institut für Technologie (KIT) [IuK-Ordnung]« ("IT Processing and Communication Regime") of the Karlsruhe Institute of Technology, published on 2013-10-15, and found at https://www.cert.kit.edu/p/iuk-ordnung.
- »IT-Sicherheit am KIT: Leitlinie des Karlsruher Instituts für Technologie« ("IT Security Guideline") of the Karlsruhe Institute of Technology, effective as of 2009-10-01, and found at https://www.cert.kit.edu/p/itsec-leitlinie.

These two sets of policies will be referred to as KIT Policy in their entirety. However, notwithstanding any statements made by the above-mentioned policies, KIT-CERT services will be provided for on-site systems only.

3.3 Sponsorship and/or Affiliation

KIT-CERT maintains affiliations with various University and Industrial CSIRTs throughout Germany on an as-needed basis.

KIT-CERT cooperates closely with DFN-CERT, OSCG/WLCG (CERN), and EGI-CSIRT in terms of incident handling.

KIT-CERT ist also member of the German CERT-Verbund, is accredited at TI (Trusted Introducer) and is a full member at FIRST (Forum of Incident Response and Security Teams).

3.4 Authority

KIT-CERT operates under the auspices of, and with authority delegated by, the Steinbuch Centre of Computing at the Karlsruhe Institute of Technology. For further information on the mandate and authority of the Steinbuch Centre of Computing, please refer to the SCC Policies and the founding contract of the SCC.

KIT-CERT strives to work cooperatively with system administrators and users throughout the Karlsruhe Institute of Technology, and to avoid authoritarian relationships whenever possible. However, should circumstances warrant it, the KIT-CERT will appeal to the KIT CIO to exert its authority, directly or indirectly, as necessary.

All members of the KIT-CERT are members of the IT Security Council of the KIT, and have all of the privileges and responsibilities assigned to system Administrators by the SCC Policies, or are members of the university management.

Members of the Karlsruhe Institute of Technology community who wish to appeal the actions of the KIT-CERT should contact the head of Department IT Security and Service Management. If this recourse is not satisfactory, the matter may be referred to the Directorate of the Steinbuch Centre for Computing, in the case of perceived problems with existing policy, or to the Karlsruhe Institute of Technology CIO (in that order, in the case of perceived errors in the application of existing policy).

3.5 Operated Network Numbers

KIT-CERT will operate on the following public IPv4 networks:

- 129.13.0.0/16
- 141.3.0.0/16
- 141.52.0.0/16
- 141.70.44.0/23
- 141.70.81.0/24
- 192.108.45.0/24
- 192.108.46.0/24
- 192.108.47.0/24
- 192.108.68.0/24
- 193.174.1.192/29
- 193.196.32.0/20

KIT-CERT will operate on the following IPv6 networks:

- 2001:638:304::/48
- 2001:7c0:409::/48
- 2a00:1398::/29

KIT-CERT will also operate on various private networks operated by the KIT. Furthermore, the KIT-CERT is assigned to the autonomous system AS34878.

4 Policies

4.1 Classification of incoming Information

All incoming information will be classified as confidential or higher. This strict classification scheme prevents the inadventant disclosure of information that is classified through other (external) classification schemes that may not correspond to those of KIT-CERT.

4.2 Record retention

The records containing information about security incients are retained with no scheduled date for deletion. This applies to records stored either electronically or as hardcopy.

Electronic information is stored in a central database. This database is only accessible over authenticated and secured connections. Encrypted backups of this database are made on a daily basis and stored within the backup systems provided by SCC.

If hardcopies of incident documentation are produced, they are stored in lockers accessible to KIT-CERT personnel only.

Classified incident reports may be compiled and printed for KIT executive management. Sanitized and unclassified reports may be compiled and published for educational purposes.

4.3 Record deletion

Media such as hard disk drives, floppies or flash drives are deleted in accordance with the guidelines provided by Bundeamt für Sicherheit der Informationstechnik (BSI), Germany's Federal Office for Information Security.

The deletion of optical media is performed by a special shredding maschine. For the deletion of hardcopies paper shredding machines are used.

All deletion actions are recorded in a logfile and are performed by KIT-CERT personnel only.

4.4 Types of Incidents and Levels of Support

KIT-CERT is authorized to address all types of computer security incidents which occur, or threaten to occur, at the Karlsruhe Institute of Technology.

The level of support offered by the KIT-CERT varies with the type and severity of the incident or issue, the type of constituent, the size of the user community affected, and the KIT-CERT resources available at the time; though in all cases some response will be made. Resources will be assigned according to the following priorities, listed in decreasing order:

1. Threats to the physical safety of human beings.

2. Root or system-level attacks on any central IT-management system or any part of the backbone network infrastructure.

3. Root or system-level attacks on any large public-service machine, either multi-user or dedicated-purpose.
4. Compromise of restricted confidential service accounts or software installations.
5. Denial of service attacks on any of the above-mentioned systems.
6. Any of the above at other sites, originating from Karlsruhe Institute of Technology.
7. Large-scale attacks of any kind, e. g. sniffing attacks, "social engineering" attacks or password-cracking attacks.
8. Threats, harassment, or other criminal offenses involving individual user accounts.
9. Compromise of individual user accounts on multi-user systems.
10. Compromise of desktop systems.
11. Forgery, misrepresentation, or other security-related violations of local rules and regulations, e. g. netnews or e-mail forgery or unauthorized use of IRC bots.
12. Denial-of-service attacks on individual user accounts, e. g. mail bombing.

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

Note that no direct support will be given to end users; they are expected to contact their respective system administrators, network administrators, or department heads for assistance. KIT-CERT will provide support to the latter group of persons.

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

KIT-CERT is committed to keeping the Karlsruhe Institute of Technology system-administration community informed of potential vulnerabilities, and, whenever possible, will inform this community of such vulnerabilities before they are actively exploited.

4.5 Cooperation, Interaction and Disclosure of Information

While there are legal and ethical restrictions on the flow of information from the KIT-CERT, many of which are also outlined in the SCC Policy, and all of which will be respected, the KIT-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 whenever necessary, the KIT-CERT will otherwise share information freely when this will support 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 KIT-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 being released in identifiable form outside the KIT-CERT, except as provided for below. If the identity of the user is disguised, then the information can be released freely, for example to show a sample `.cshrc` file as modified by an intruder or to demonstrate a particular social engineering attack.

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 brought forward, 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 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.

Embarrassing information includes the statement that an incident has occurred, and information about its extent or severity. Embarrassing information may concern a site or a particular user or group of users. Embarrassing information will not be released without the permission of the site or users in question, except as provided for below.

Statistical information is embarrassing information with the identifying information stripped off. Statistical information will be released at the discretion of the Steinbuch Centre for Computing.

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 be not the case, or where KIT-CERT has reason to believe that the dissemination of this information would not be appreciated.

Potential recipients of information from the KIT-CERT will be classified as follows:

Because of the nature of their responsibilities and consequent expectations of confidentiality, **members of the Karlsruhe Institute of Technology management** are entitled to receive whatever information is necessary to facilitate the handling of computer security incidents which occur in their jurisdictions.

Members of the board of directors of the Karlsruhe Institute of Technology, members of directorate of the Steinbuch Centre for Computing, members of legal department, members of the IT-Security Council, and the Chief Information Officer are entitled to receive whatever information they request concerning a computer security incident or related matter which has been referred to them for resolution. The same is true for the KIT Security Department, when its assistance in an investigation has been enlisted, or when the investigation has been instigated at its request.

System administrators at the Karlsruhe Institute of Technology will be given confidential information as far as is necessary in order for them to assist with an investigation, or in order to enable them to secure their own systems.

Users at the Karlsruhe Institute of Technology are entitled to information which pertains to the security of their own computer accounts, even if this means revealing "intruder information," or

"embarrassing information" about another user. Users at the Karlsruhe Institute of Technology are entitled to be notified if their account is believed to have been compromised.

The Karlsruhe Institute of Technology community in general will receive no restricted information, except where the affected parties have given permission for the information to be disseminated. Statistical information may be made available to the general KIT community. There is no obligation on the part of the KIT-CERT to report incidents to the community, though it may choose to do so; in particular, it is likely that the KIT-CERT will inform all affected parties of the ways in which they were affected, or will encourage the affected site to do so.

The public at large will receive no restricted information. In fact, no particular effort will be made to communicate with the public at large, though the KIT-CERT recognizes that, for all intents and purposes, information made available to the Karlsruhe Institute of Technology community is in effect made available to the community at large, and will tailor the information accordingly.

The computer-security community will be treated the same way the general public is treated. While members of KIT-CERT may participate in discussions within the computer-security community, such as newsgroups, mailing lists (including full-disclosure lists such as `bugtraq`), and conferences, they will treat such forums as though they were the public at large. While technical issues (including vulnerabilities) may be discussed at any level of detail, any examples taken from KIT-CERT experience will be disguised to avoid identification of the affected parties.

The press will also be considered as part of the general public. KIT-CERT will not interact directly with the press concerning computer security incidents, except to point them toward information already released to the general public. If necessary, information will be provided to the Karlsruhe Institute of Technology public-relations department, and to the customer-relations group of the Steinbuch Centre for Computing. All incident-related queries will be referred to either one or both of these two bodies. The above does not affect the ability of members of KIT-CERT to grant interviews on general computer security topics; in fact, they are encouraged to do to, as a public service to the community.

Other sites and CSIRTs , when they are partners in the investigation of a computer security incident, will in some cases be entrusted with confidential information. This will happen only if the foreign site's bona fide can be verified, and the information transmitted will be limited those parts that are likely to be helpful in resolving the incident. Sharing of such information is most likely to happen in the case of sites well known to KIT-CERT; for example, several other German universities have informal but well-established working relationships with Karlsruhe Institute of Technology in such matters.

For the purposes of resolving a security incident, otherwise semi-private but relatively harmless user information such as the provenance of connections to user accounts will not be considered highly sensitive, and can be transmitted to a foreign site without excessive precautions. "Intruder information" will be transmitted freely to other system administrators and CSIRTs. "Embarrassing information" can be transmitted when there is reasonable assurance that it will remain confidential, and when it is necessary to resolve an incident.

Vendors will be considered as foreign CSIRTs for most intents and purposes. KIT-CERT wishes to encourage vendors of all kinds of networking and computer equipment, software, and services to improve the security of their products. In aid of this, a vulnerability discovered in such a product will be reported to its vendor, along with all technical details needed to identify and fix the problem. Identifying details will not be given to the vendor without the permission of the affected parties.

Law enforcement officers will receive due cooperation from the KIT-CERT, including any information they require to pursue an investigation, in accordance with the SCC Policy and all relevant laws.

4.6 Communication and Authentication

In view of the types of information that the KIT-CERT will likely be dealing with, telephones will be considered sufficiently secure to be used, even if they do not provide encryption of the voice stream. Unencrypted e-mail will not be considered particularly secure, but sufficient for the transmission of low-sensitivity data. If it is necessary to send highly-sensitive data by e-mail, PGP/GPG/SMIME will be used as appropriate. Network file transfers will be considered to be similar to e-mail for these purposes: sensitive data will be encrypted for transmission.

Where it is necessary to establish trust, for example before relying on information given to the KIT-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 the Karlsruhe Institute of Technology, 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, 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/GPG/SMIME).

5 Services

5.1 Incident Response

KIT-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

- Investigating whether indeed an incident occurred.
- Determining the extent of the incident.

5.1.2 Incident Coordination

- Determining the initial cause of the incident, i. e., identifying the vulnerability exploited by the attacker.
- Facilitating contact with other sites which may be involved.
- Facilitating contact with Karlsruhe Institute of Technology Security and/or appropriate law enforcement officials, if necessary.
- Making reports to other CSIRTs.
- Composing announcements to users, if applicable.

5.1.3 Incident Resolution

- Removing the vulnerability, if possible.
- Securing the system from the effects of the incident.
- Evaluating whether certain actions are likely to reap results in proportion to their cost and risk, in particular those actions aimed at an eventual prosecution or disciplinary action: collection of evidence after the fact, observation of an incident in progress, setting traps for intruders, and so on.
- Collecting evidence where criminal prosecution, or university disciplinary action, is contemplated.

In addition, the KIT-CERT will collect statistics concerning incidents which occur within or involve the Karlsruhe Institute of Technology community, and will notify the community as necessary to assist in protecting against known attacks.

To make use of KIT-CERT incident response services, please send an e-mail as per section 2.12 above. Please remember that the amount of assistance available will vary according to the parameters described in section 4.4.

5.2 Proactive Activities

KIT-CERT coordinates and maintains the following services to the extent possible, depending on its resources:

5.2.1 Information Services

- Mailing lists to inform security contacts of new information relevant to their computing environments. These lists will be available only to Karlsruhe Institute of Technology system administrators.
- Repository of vendor-provided and other security-related patches for various operating systems. This repository will be available to the general public wherever license restrictions allow it, and will be provided via commonly-available channels such as the World Wide Web and/or FTP.
- Repository of security tools and documentation for use by system administrators. Where possible, precompiled ready-to-install versions will be supplied. These will be supplied to the general public via WWW or FTP as above.

5.2.2 Training Services

- Members of the KIT-CERT will offer periodic seminars on computer-security-related topics; these seminars will be open to Karlsruhe Institute of Technology system administrators.

5.2.3 Auditing Services

- Security level assignments. Machines and subnets of those networks defined in section 3.5 at the Karlsruhe Institute of Technology will be audited and assigned a security level. This security level information will be available to the Karlsruhe Institute of Technology community to facilitate the setting of appropriate access privileges. However, details of the security analyses will be confidential and available only to the parties concerned.
- Operation of central network-traffic monitoring and analysis for the purpose of intrusion detection.
- Operation of intrusion-prevention systems at chosen points of the network.
- Records of security incidents handled will be kept. While the records will remain confidential, periodic statistical reports will be made available to the Karlsruhe Institute of Technology community.

Detailed descriptions of the above services, along with instructions for joining mailing lists, downloading information, or participating in certain services are available on the KIT-CERT web site, as per section 2.11 above.

6 Incident Reporting Forms

Incidents can be reported via any communication channel to KIT-CERT and are not required to meet any particular form.

7 Disclaimers

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