DKCERT

DKCERT RFC 2350

The following profile of DKCERT has been prepared in adherence to RFC 2350, Expectations for Computer Security Incident Response.

1. **Document Information**
   - **1.1.** Date of Last Update
     Version 1.23, published February 20, 2023.
   - **1.2.** Distribution List for Notifications
     Changes to this document are not distributed by a mailing list. Please address questions or remarks by e-mail to: cert (at) cert.dk
   - **1.3.** Locations where this document may be found
     The current version of this profile is always available at:
     https://www.cert.dk/About_DKCERT/RFC2350

2. **Contact Information**
   - **2.1. Name of the Team**
     DKCERT
   - **2.2. Address**
     Produktionstorvet, Building 426
     DK-2800 Kgs. Lyngby
     Denmark
   - **2.3. Time Zone**
     CET, Central European Time (UTC+1, between last Sunday in October and last Sunday in March)
     CEST (also CET DST), Central European Summer Time (UTC+2, between last Sunday in March and last Sunday in October)
   - **2.4. Telephone Number**
     +45 3588 8255 (Monday through Friday from 9 a.m. to 4 p.m.)
   - **2.5. Other Telecommunication**
     X (Twitter): @dkcert. LinkedIn: https://www.linkedin.com/company/dkcert/
   - **2.6. Electronic Mail Address**
     cert (at) cert.dk
   - **2.7. Public Keys and Encryption Information**
     DKCERT uses PGP for digital signatures and to receive encrypted information. The keys are available on public PGP/GPG key servers and at *https://www.cert.dk*
     Address: *cert (at) cert.dk*
     Key-ID: 79D294CE
     Fingerprint: B14C 2840 133D E7E9 21B1 27CB 903C 41BD 79D2 94CE
   - **2.8. Team Members**
     A full list of DKCERT team members is not publicly available. Team members will

normally identify themselves to the reporting party in an official communication regarding an incident, but are not obligated to do so.

2.9. Other Information

General information about DKCERT is available at https://www.cert.dk

2.10. Points of Customer Contact

The main point of contact is the DKCERT mail addresses:

cert (at) cert.dk : General contact e-mail address.
abuse (at) cert.dk : E-mail address dedicated to incidents.

You may also call DKCERT at +45 3588 8255 to report an incident. Our regular hours (local time in respect to public holidays in Denmark) are Monday through Friday from 9 a.m. to 4 p.m. Outside normal working hours we refer to the e-mail addresses.

2.11. Service Level Objectives

All inquiries will be answered within 2 hours of receipt during business hours which are 8 a.m. to 4 p.m. from Monday to Friday.

Inquiries received before and after business hours will be answerd next businees day + 2 hours (NBD+2).

3. Charter

3.1. Mission Statement

The mission of DKCERT is to create an increased focus on information security within the area of research and education by building and creating current, relevant and useful knowledge. This knowledge enables DKCERT to publish warnings and other information about potential risks and emerging security incidents to its constituency.

3.2. Constituency

The constituency of DKCERT is forskningsnettet, the Danish National Research and Education Network, with all connecting institutions.

3.3. Sponsorship and/or Affiliation

DKCERT is a service provided by DeiC, Danish e-Infrastructure Consortium, an organization under Danish Agency for Higher Education and Science. DKCERT currently resides under the Technical University of Denmark (DTU).

3.4. Authority

DKCERT handles incident response, coordinates action, performs internal and external scans of the institutions' infrastructure and warns our constituency about cyber security events. We have no legal authority to demand that incidents are addressed, unless in violation of the acceptable use policy for Forskningsnettet.

4. Policies

4.1. Types of Incidents and Level of Support

DKCERT handles various types of security incidents. The level of support depends on the type of the incident and the severity as determined solely by the DKCERT staff.

4.2. Co-operation, Interaction and Disclosure of Information

All incoming information is handled confidentially by DKCERT, regardless of its priority.

Information that is sensitive or classified is only communicated and stored in a secure environment, if necessary using encryption. DKCERT will use the information obtained to help solve security incidents. Information will only be distributed to other teams and team members according to relevant legislation and on a need-to-know basis, preferably as anonymized data. DKCERT uses the Traffic Light Protocol (TLP v2.0) for classifying information as well as the NATO/EU classification scheme if needed.

4.3. Communication and Authentication

E-mail is the preferred method of communication. When the content is sensitive or requires authentication, the DKCERT PGP key is used for signing e-mail messages. All sensitive or confidential communication to DKCERT should be encrypted using the team's PGP key.

5. Services

5.1. Incident response

Incident response is provided as stated in “2.11 Points of Customer Contact”. DKCERT will investigate incidents and coordinate responses from relevant stakeholders. This may include involvement of experts, tools and other capabilities to act, analyze and communicate with stakeholders and media.

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.
Facilitating contact with other sites that may be involved.
Communicate with stakeholders and media.

5.1.3. Incident Resolution

Providing advice to the reporting constituent that may help remove the vulnerabilities that caused the incident and help secure the systems from the effects of the incidents.
Evaluate and give advice to stakeholders as to which actions are most suitable to provide desired results regarding the incident resolution.
Provide assistance in evidence collection and data interpretation when needed.
Evaluate the frequency, the amount and the severity of the incident for public warning.

5.2. Proactive Activities

DKCERT provides information to its constituency such as news stories, articles, reports, advisories, fact sheets, and white papers in order to prevent or correct ICT related security incidents or to prepare for such incidents and reduce the impact.

5.3. DPO Service

The DKCERT DPO service helps research and education institutions comply with the General Data Protection Regulation. The service provides DPO services to those universities and educational institutions who do not wish to hire their own DPO, or who need advice regarding the latest practices and interpretations of the regulation as seen by educational and research institutions in the EU.

5.4. Vulnerability scanning

DKCERT scans the networks of its constituency on a regular basis in order to discover vulnerable systems.

6. Incident Reporting Forms

DKCERT prefers to receive a detailed description of an incident via e-mail.

7. Disclaimers

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

[EOF]