KIT-CERT Organisational Framework

Contents

1 Information about this document

This document contains the organisational framework of KIT-CERT.

1.1 Version History

The current version is d7b4651. It was published on 2023-12-12.

Date	Description
2023-12-12	Update name of SCC[10]
2023-07-28	Initial publication of this document

2 Mandate

Mandate is documented in "IT-Sicherheitskonzept für das KIT"[8] and in "IT-Sicherheitsleitlinie"[9]. It is determined by the highest governing body of the KIT, the KIT Präsidium. The KIT-CERT is mandated as central coordination center for information security incidents and is the dedicated contact point for law enforcement agencies.

3 Constituency

3.1 Clients

The KIT-CERT constituency is the Karlsruhe Institute of Technology community (Mitglieder und Angehörige des KIT) and guests and partners (Gäste und Partner), as defined in the context of the following policies:

- Gemeinsame Satzung des Karlsruher Instituts für Technologie (KIT)[5]
- Gesetz über die Hochschulen in Baden-Württemberg (Landeshochschulgesetz - LHG), §9 Abs. 1 Satz 1 und Satz 2[7]
- Gesetz über das Karlsruher Institut für Technologie (KIT-Gesetz - KITG)[6]
- Ordnung für die digitale Informationsverarbeitung und Kommunikation (IuK) am Karlsruher Institut für Technologie (KIT)[12]
- IT-Sicherheit am KIT: Leitlinie des Karlsruher Instituts für Technologie[9]

In particular, the constituency includes these groups of people:

- KIT students
- KIT employees
- KIT professors
- KIT guests and partners

3.2 Networks

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
- 157.180.228.0/22
- 157.180.232.0/22
- 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.

3.3 Domains

KIT-CERT will operate on every domain registered by KIT, foremost on the domain *kit.edu*.

3.4 Autonomous Systems

KIT-CERT is assigned to the autonomous system AS34878.

4 Authority

KIT-CERT is an organizational part of the Scientific Computing Center (SCC), but is the designated coordination center for all computer security incidents at KIT.

KIT-CERT strives to work cooperatively with system administrators and users throughout KIT, and to avoid authoritarian relationships whenever possible.

However, should circumstances warrant it, the KIT-CERT will appeal to the KIT CISO to exert their authority, directly or indirectly, as necessary.

In order to protect the infrastructure of KIT, KIT-CERT can – both temporarily and permanently – remove systems from the central infrastructure as well as disable user access as mandated by the I&C regulations.

5 Responsibility

Our mission and responsibility is to prevent damage caused by information security incidents at KIT. We are responsible for the security incident management at KIT, including prevention, analysis and recovery of security incidents and coordination of resulting crisis.

We consult for secure operation of IT systems and are the central contact point for abuse of IT systems and services at KIT. We act as contact points for responsible disclosure and coordinate inquiries by law enforcement agencies.

6 Service Description

Note: This description is based on the FIRST CSIRT Services Framework, Version 2.1[3]

6.1 Service Area: Information Security Event Management

6.1.1 Monitoring & Detection

References: FCSF 5.1, FCSF 8.1

We operate a cluster to systematically collect, parse, store and analyze logs and metadata of KITnet connections. We offer interfaces for selected services and constituents. We also collect information from external sources.

6.1.2 Detection of successful Phishing and misbehaving accounts

References: FCSF 5.1

We analyze and assess automatically if a user misbehaves or lost their credentials to the mail services of KIT. We take appropriate action to secure the reputation of KIT in that case.

6.1.3 Mailfiltering and Malware Detection

References: FCSF 5.1

We filter and detect mails with malicious content using established spam filter and malware detection engines on central mail servers.

6.2 Service Area: Information Security Incident Management

6.2.1 Information Security Incident Report Acceptance

References: FCSF 6.1

We accept reports of security incidents via mail at cert@kit.edu.

6.2.2 Information Security Incident Analysis

References: FCSF 6.2

We analyze and assess reported or detected security incidents.

6.2.3 Artifact and Forensic Evidence Analysis

References: FCSF 6.3

Based on the severity or certainty of information provided, we run further investigation and / or do forensic analysis of information security incidents.

6.2.4 Information Security Incident Coordination

References: FCSF 6.5

We coordinate incident resolution in close collaboration with system administrators and responsible parties.

6.2.5 Crisis Management Support

References: FCSF 6.6

We support responsible parties to properly manage ongoing crisis.

6.3 Service Area: Vulnerability Management

6.3.1 Vulnerability Discovery

References: FCSF 7.1

KIT-CERT does not engage in vulnerability research. We use several sources to be informed about vulnerabilities in KITnet. If we discover vulnerabilities in the investigation of an incident, we handle them as well.

6.3.2 Vulnerability Report Intake

References: FCSF 7.2

We accept reports of vulnerabilities via mail at cert@kit.edu. KIT-CERT appreciates responsible disclosures. Note that we cannot provide monetary or material compensation. However, we do provide letters of acknowledgement.

6.3.3 Vulnerability Analysis

References: FCSF 7.3

We analyze and assess reports of vulnerabilities.

6.3.4 Vulnerability Coordination

References: FCSF 7.4

In case we find a vulnerability in a system or service during incident response, we coordinate with responsible parties.

6.3.5 Vulnerability Disclosure

References: FCSF 7.5

If we have information about a specific vulnerability in our IT, we will inform the responsible persons. KIT-CERT tries to evaluate the information it has. For more information, see our policy at: https://cert.kit.edu/p/vulnerability_disclosure_policy

6.3.6 Vulnerability Response

References: FCSF 7.6

Based on the severity of vulnerabilities, we take appropriate action, e.g. scanning the KITnet to find vulnerable services and contacting the responsible parties for a vulnerable service. If we do not have a way to search for vulnerable services, we inform the KIT community to take action if they are affected.

6.4 Service Area: Situational Awareness

6.4.1 Analysis and Synthesis

References: FCSF 8.2

We process our collected data and process them to create a realistic picture of the current security risks.

6.4.2 Communication

References: FCSF 8.3

We inform our constituents about high-level threats and their impacts on the KIT-CERTS business.

KIT-CERT informs the management of KIT about current threats and risks of security incidents.

We are committed to participation in the CSIRT community. KIT-CERT strives to share its information to the CSIRT community and building a strong bond of trust with other CSIRTs in our networks.

6.5 Service Area: Knowledge Transfer

6.5.1 Training and Education for ITB

References: FCSF 9.2

We provide the required IT security training for IT appointees (IT-Beauftragte). The training includes topics on secure system administration, network planning, handling of security incidents and the information security management system of KIT.

6.5.2 Talks & Presentations

References: FCSF 9.2

We give talks and presentations about our work on an irregular basis in varying contexts.

6.5.3 Technical and Policy Advisory

References: FCSF 9.4

Together with the responsible persons, we develop technical guidelines and policies for KITs information security management system.

7 Service Level Description

For the services sec. 6.2.1 ('Information Security Incident Report Acceptance') and sec. 6.3.2 ('Vulnerability Report Intake') we provide an initial reaction within 1 business day. All other services are provided on a best-effort basis.

Note that in accordance with [11] 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.

8 Incident Classification

We use the following criteria as guidance for prioritization of incoming incidents, loosely ordered by priority:

- Physical Safety of human beings
- Impact on KIT as a whole
- Impact on individual constituents
- Reputational Damage

9 Integration in Existing CSIRT Systems

We are members of:

- EDUCV, a working group of CERTs in the german higher education sector
- CERT-Verbund, a network of CERTs in germany
- Trusted Introducer, a european network of CSIRTs and CERTs
- FIRST, a global network of CSIRTs and CERTs

We strive to attend meetings and workshops of these communities.

10 Code of Conduct

KIT-CERT complies with the Trusted Introducer Code of Conduct[1].

11 Processes

11.1 Escalation to Governance Level

We strive to work directly with system administrators. However, if the potential damage exceeds a certain threshold or KIT-CERT does not receive an answer, we will escalate to the corresponding person in charge. If the circumstances require it, we will escalate to the presidium of KIT directly or via the CISO.

11.2 Audit and Feedback Process

KIT's CISO will review KIT-CERT quarterly.

Topics are:

- Changes in framework conditions
  - organizational changes
  - changes in legislation
  - technical developments (including new types of threats / defense mechanisms)
- Discuss necessary/planned/completed changes in service provision
- Review of the aspects to be considered according to SIM3 (OHTP)

11.3 Emergency Reachability Process

In case of a emergency, please call us, or write a mail with a subject starting with 'URGENT:'. Outside business hours in case of an emergency please call the KIT Alarmzentrale.

11.4 Best Practice Internet Presence

Our official web presence is cert.kit.edu, canonical mail is: cert@kit.edu. We provide a security.txt[4]. Mailboxes described in RFC2142[2] are either redirected to cert@kit.edu or the recipients know how to contact us.

11.5 Secure Information Handling Process

We accept PGP and SMIME encrypted mail, public keys are listed on our website. We will adhere to the Traffic Light Protocol. Unless otherwise noted, information send to us will be handled as TLP:AMBER+STRICT. If possible we will anonymize or pseudomize information we share.

11.6 Outreach Process

We maintain our presence in the web at cert.kit.edu and meet regularly with the "IT-Beauftragten", the contact person for the decentral organized IT.

11.7 Peer-to-Peer Process

As described in sec. 9 we take part in the EDUCV, share our insights with our peers on a best effort service.

References

[1] *CCoP - CSIRT Code of Practice*. URL: https://www.trusted-introducer.org/TI-CCoP.pdf.

[2] D. Crocker. *RFC 2142 - MAILBOX NAMES FOR COMMON SERVICES, ROLES AND FUNCTIONS*. URL: https://www.rfc-editor.org/rfc/rfc2142.

[3] FIRST. *FIRST CSIRT Services Framework, Version 2.1*. URL: https://www.first.org/standards/frameworks/csirts/csirt_services_framework_v2.1.

[4] E. Foudil and Y.Shafranovich. *RFC 9116 - A File Format to Aid in Security Vulnerability Disclosure*. URL: https://www.rfc-editor.org/rfc/rfc9116.

[5] *Gemeinsame Satzung des Karlsruher Instituts für Technologie (KIT)*. URL: https://www.sle.kit.edu/downloads/AmtlicheBekanntmachungen/2011_AB_022.pdf.

[6] *Gesetz über das Karlsruher Institut für Technologie (KIT-Gesetz - KITG)*. URL: https://www.landesrecht-bw.de/jportal/?quelle=jlink&query=KITG+BW&psml=bsbawueprod.psml&max=true&aiz=true.

[7] *Gesetz über die Hochschulen in Baden-Württemberg (Landeshochschulgesetz - LHG)]*. URL: https://www.landesrecht-bw.de/jportal/portal/t/h1c/page/bsbawueprod.psml/action/portlets.jw.MainAction?p1=0&eventSubmit_doNavigate=searchInSubtreeTOC&showdoccase=1&doc.hl=0&doc.id=jlr-HSchulGBWrahmen&doc.part=R&toc.poskey=#focuspoint).

[8] *IT-Sicherheitskonzept des KIT*. URL: https://www.cert.kit.edu/p/itsec-konzept.

[9] *IT-Sicherheitsleitlinie des KIT*. URL: https://www.cert.kit.edu/p/itsec-leitlinie.

[10] Public Relations Office of Karlsruhe Institute of Technology. *KIT Renames Information Technology Center*. URL: https://www.kit.edu/kit/english/pi_2023_092_kit-renames-information-technology-center.php.

[11] *Memorandum of Understanding zur Rolle der IT-Beauftragten (ITB) der Organisationseinheiten (OE) im KIT*. URL: https://www.scc.kit.edu/misc/itbv-dokumente/20110325_Benennung_ITB_MoU.pdf.

[12] *Ordnung für die digitale Informationsverarbeitung und Kommunikation (IuK) am Karlsruher Institut für Technologie (KIT)*. URL: https://www.cert.kit.edu/p/iuk-ordnung.