Explanations Regarding the Obligation to Report IT Security Incidents

Section 3.7 of the IT Security Concept of KIT (https://s.kit.edu/it-security-concept) covers the obligation to report IT security incidents. The corresponding provisions will now be explained in more detail below. Read these explanations carefully.

KIT requests your help in enhancing the security level of:

- The IT infrastructure of KIT (including e.g. all PCs, laptops, tablets, smartphones, servers, WLAN routers) or IT services of KIT (e.g. Exchange, Sharepoint, Website management)
- The confidential information stored at KIT (e.g. passwords, exams, research results, inventions) and in particular personal data (e.g. employment contracts, travel expense accounting and information needed for this purpose such as bank accounts, course of studies, exams results).

In early 2018, the rules for reporting IT security incidents were changed.
The reasons are:

- The increasing number of attacks on KIT's IT infrastructure , IT services and the data stored there,
- Changed legal regulations, and
- The fact that attacks can no longer be fended off successfully by technical security measures alone, e.g. virus scanners and firewalls, but only when everyone attentively helps, e.g. by detecting and reporting incidents.
- As this allows a quicker response to inicidents and thus the risk for KIT or everyone can be kept as low as possible.

Report the following incidents promptly:

Loss of devices (e.g. PCs, laptops, smartphones) via which you access services or data of KIT. It is of secondary importance whether the devices were stolen or lost.

Loss of data carriers (e.g. USB sticks, CDs) on which confidential or personal data are stored[1]. It is of secondary importance whether the devices were stolen or lost.

[1] A message is particularly important if the mobile date medium or the information on it was not encrypted. If necessary, the loss must also be reported as a so-called data breach – click: https://www.dsb.kit.edu/359.php

Discovery of devices (e.g. WLAN routers, small boxes, other PCs/laptops) in your rooms, which are suddenly found there, but have never been announced. Just have a look around to find out which devices exist at your workplace. If applicable, ask your local IT appointee of the business unit whether the devices existing in your room are all needed.

Blackmail or coercion to not behave in agreement with the rules, especially if an unknown person wishes to have access to your devices or your rooms. Criminals, who fail to hack into KIT's IT infrastructure or IT services, may try to gain access via relatives and/or employees of KIT.

Identity theft after you have accidentally shared a password on a phishing website or over the phone, so that criminals can use it in the same or in another form to gain access to your KIT user account or other accounts used at KIT and are able to assume your identity for this account.

Malicious software on devices via you access IT infrastructure or IT services of KIT, and/or confidential information after you inadvertently click on links in fraudulent messages, open attachments, download files from untrusted sources or use disks from untrusted sources. Malicious software may also appear on guests' devices during or immediately after a visit to KIT.

If you have experienced any of the above IT security incidents, please contact your IT appointee of the business unit directly and/or send an e-mail to KIT-CERT (cert@kit.edu). Together with you, the situation is analyzed and discussed what can be done to minimize the probability of a damage and the severity of a damage to KIT and you. Please do not be afraid to report IT security incidents.

If you detect **an attempted attack** (e.g. an attempt at theft or blackmail, or the incoming of a fraudulent message), please also report this to your IT appointee of the business unit, even if no damage has occurred. This helps to better assess the general threat situation at KIT and to take appropriate measures. **To report fraudulent e-mails**, please set up the Spam_KIT folder and move them there, click: https://s.kit.edu/it-security.reporting-procedure

If you are unsure whether an incident you have observed is an IT security incident or simply seems a little bit unusual, please contact your IT appointee of the business unit as a precaution or send an e-mail to beratung-itsec@scc.kit.edu. Together with you the observed incident will be evaluated.