Erläuterungen zur Meldepflicht von IT-Sicherheitsvorfällen

Im Kapitel 3.7 des IT-Sicherheitskonzepts ist die Meldepflicht für IT-Sicherheitsvorfälle geregelt. Dieses Dokument hat zum Ziel, die dortigen Regelungen zu erläutern. Bitte lesen Sie diese Erläuterungen aufmerksam durch.

Das KIT bittet alle um Mithilfe bei der Steigerung des Sicherheitsniveaus

- der IT-Infrastruktur des KIT (hierzu zählen z. B. alle PCs, Laptops, Tablets, Smartphones, Server, WLAN Router) und
- der am KIT gespeicherten Daten (z. B. Klausuren, Noten) und insbesondere personenbezogener Daten (z. B. Arbeitsverträge, Reisekostenabrechnungen und dort eingetragene Informationen wie Bankverbindungen).

Die Regeln für die Meldung von IT-Sicherheitsvorfällen wurden Anfang 2018 geändert. Hintergründe hierfür sind

- die zunehmende Anzahl von Angriffen auf die IT-Infrastruktur des KIT und die dort gespeicherten Daten,
- geänderte gesetzliche Vorschriften und
- die Tatsache, dass Angriffe nicht mehr alleine durch technische Sicherheitsmaßnahmen wie z. B. Virenscanner und Firewalls erfolgreich abgewehrt werden können, sondern nur dann, wenn jeder mithilft, z. B. indem Vorfälle erkannt und gemeldet werden.

Folgende Vorfälle sind zeitnah zu melden

Verlust von Geräten (z. B. PCs, Laptops, Smartphones), die entweder Eigentum des KIT sind oder private Geräte, über die Sie auf Dienste oder Daten des KIT zugreifen (z. B. private Laptops, über die Sie KIT-E-Mails abrufen). Melden Sie bitte auch, wenn Sie den Versuch eines Diebstahls beobachtet haben, auch wenn kein Schaden entstanden ist. Letzteres ist wichtig, um die Bedrohungslage besser einstufen und entsprechende Maßnahmen einleiten zu können.

Verlust von Datenträgern (z. B. USB-Sticks, CDs), auf denen wichtige oder personenbezogene Daten gespeichert sind (z. B. Passwörter, Klausuren, Bewerbungen, Noten, Gehaltsabrechnungen). Melden Sie bitte auch hier, wenn Sie den Versuch eines Diebstahls beobachtet haben, dieser aber verhindert wurde. Auch dies ist zur Beurteilung der Bedrohungslage wichtig.

Täuschung durch betrügerische Nachricht, wenn Sie eine betrügerische Nachricht (z. B. eine Phishing-E-Mail) nicht direkt als solche erkannt haben, sondern z. B. auf den Link geklickt oder den Anhang geöffnet haben. Informationen darüber, wie Sie betrügerische Nachrichten zukünftig erkennen können, finden Sie im Faltblatt „Betrügerische Nachrichten“.

Entdecken von Schadsoftware auf Geräten, die entweder Eigentum des KIT sind oder private Geräte, über die Sie auf Dienste oder Daten des KIT zugreifen. Ein Hinweis für Schadsoftware auf diesen Geräten ist, dass diese sich plötzlich anders verhalten (z. B. sehr langsam werden). Wenn Gäste - vor Ort, während oder unmittelbar nach dem Besuch am KIT - über Schadsoftware auf ihrem Gerät berichten, melden Sie dies bitte.

Entdecken von Geräten (z. B. WLAN-Routern, kleine Boxen, anderen PCs/Laptops) in den eigenen Räumen, die plötzlich da sind, aber nicht angekündigt wurden. Schauen Sie sich bei Gelegenheit einmal um, welche Geräte jetzt da sind. Ggf. klären Sie mit den lokalen IT-Beauftragten ab, ob die Geräte, die Sie vorfinden, alle ihre Berechtigung haben. Wenn zukünftig weitere dazukommen, melden Sie diese bitte.

Erpressung oder Nötigung, sich nicht regelkonform zu verhalten (z. B. wenn jemand Unbekanntes unbedingt Zugriff auf Ihre Geräte oder Ihre Räume haben möchte). Kriminelle, denen es nicht gelingt, sich technisch in die IT-Systeme des KIT zu hacken, versuchen es ggf. über Angehörige und/oder Mitarbeiter des KIT. Unabhängig davon, wie Sie selbst auf die Erpressung bzw. Nötigung reagiert haben und ob Kriminelle erfolgreich waren oder nicht, melden Sie bitte die Vorfälle.

Wenn Sie einen der oben genannten IT-Sicherheitsvorfälle entdeckt haben, melden Sie sich bitte umgehend bei Ihrem **lokalen IT-Beauftragten** oder schicken Sie eine E-Mail an **cert@kit.edu**. Gemeinsam mit Ihnen wird dann die Situation analysiert und besprochen, was getan werden kann, um das Risiko so gering wie möglich zu halten, dass Kriminelle dem KIT schaden können (z. B. mit den erhaltenen sensiblen Daten).

Wenn Sie unsicher sind, ob das von Ihnen Beobachtete ein IT-Sicherheitsvorfall ist oder Ihnen einfach etwas komisch vorkommt, kontaktieren Sie zur Sicherheit Ihren lokalen IT-Beauftragten oder schicken Sie eine E-Mail an beratung-itsec@scc.kit.edu. Gemeinsam mit Ihnen wird dann entschieden, ob es sich hierbei um einen IT-Sicherheitsvorfall handelt.

Das Melden von IT-Sicherheitsvorfällen ist für uns alle neu. Bitte haben Sie keine Angst.

Vielen Dank für Ihre Aufmerksamkeit. Wenn Sie noch Fragen oder Anregungen haben, melden Sie sich bitte bei beratung-itsec@scc.kit.edu.