Erläuterungen zur Meldepflicht von IT-Sicherheitsvorfällen

Im Kapitel 3.7 des IT-Sicherheitskonzepts des KIT, vgl. https://s.kit.edu/it-sicherheitskonzept, 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 (z. B. PCs, Laptops, Tablets, Smartphones, Datenträger wie USB-Sticks, Server, WLAN Router) oder IT-Dienste des KIT (z. B. Exchange, Sharepoint, Webseiten)
- der dort gespeicherten vertraulichen Informationen (z. B. Passwörter, Klausuren, Forschungsergebnisse, Erfindungen) inklusive personenbezogener Daten (z. B. Arbeitsverträge oder Auszüge daraus, Reisekostenabrechnungen und dort eingetragene Informationen wie Bankverbindungen, Studienverlaufsdaten, Noten).

Die Regelungen für die Meldepflicht wurden Anfang 2018 aus folgenden Gründen geändert:

- die zunehmende Anzahl von Angriffen auf die IT-Infrastruktur und die IT-Dienste des KIT sowie auf die dort gespeicherten vertraulichen Informationen,
- geänderte gesetzliche Vorschriften,
- die Tatsache, dass Angriffe heute nicht mehr alleine durch technische Sicherheitsmaßahmen wie Virenscanner und Firewalls erfolgreich abgewehrt werden können, sondern nur dann, wenn jede/jeder aufmerksam mithilft und Vorfälle im Kontext von IT-Sicherheit meldet,
- da so schneller auf Vorfälle reagiert werden kann und so das Risiko für das KIT und jede/jeden so gering wie möglich gehalten werden kann.

Folgende IT-Sicherheitsvorfälle müssen Sie melden, sobald Sie diese feststellen

Verlust von Geräten (z. B. PCs, Laptops, Smartphones) über die Sie auf Dienste oder Daten des KIT zugreifen[1]. Dabei ist es zweitrangig, ob die Geräte gestohlen wurden oder verloren gingen.

Verlust von Datenträgern (z. B. USB-Sticks, CDs) auf denen vertrauliche Informationen und insbesondere personenbezogene Daten gespeichert sind[1]. Dabei ist es zweitrangig, ob die Geräte gestohlen wurden oder verloren gingen.

[1] Eine Meldung ist besonders wichtig, wenn der mobile Datenträger bzw. die Informationen darauf nicht verschlüsselt waren. Ggf. ist der Verlust dann zusätzlich als sog. Datenpanne zu melden, vgl. https://www.dsb.kit.edu/359.php.

Entdecken von Geräten (z. B. WLAN-Routern, kleinen Boxen, PCs, Laptops) in den eigenen Räumen, die plötzlich da sind, aber nicht angekündigt wurden. Schauen Sie sich dazu um, welche Geräte in ihren Räumen vorhanden sind. Klären Sie mit Ihrem lokalen IT-Beauftragten, ob diese alle ihre Berechtigung haben.

Erpressung oder Nötigung, sich nicht regelkonform zu verhalten, insbesondere wenn jemand Unbekanntes hierdurch unbedingt Zugriff auf Ihre Geräte oder Ihre Räume haben möchte. Kriminelle, denen es nicht gelingt, sich technisch in die IT-Infrastruktur bzw. die IT-Dienste des KIT zu hacken, versuchen so an die entsprechenden Informationen oder IT-Infrastrukturen zu gelangen.

Identitätsdiebstahl, nachdem Sie versehentlich, z. B. auf einer Phishing-Webseite oder am Telefon, ein Passwort preisgegeben haben und Kriminelle dieses Passwort (genauso oder in ähnlicher Form) nutzen können, um Zugriff auf Ihr KIT-Benutzerkonto oder andere am KIT genutzten Benutzerkonten zu erhalten, und so Ihre Identität für dieses Benutzerkonto übernehmen kann.

Schadsoftware auf Geräten, über die Sie auf die Infrastruktur, die Dienste und/oder vertrauliche Informationen des KIT zugreifen, nachdem Sie z. B. versehentlich in betrügerischen Nachrichten auf Links geklickt, Anhänge geöffnet, Dateien von nicht vertrauenswürdigen Quellen heruntergeladen oder Datenträger von nicht vertrauenswürdigen Quellen genutzt haben. Schadsoftware kann auch auf Geräten von Gästen, während oder unmittelbar nach einem Besuch am KIT auftreten.

Wenn Sie einen der oben genannten IT-Sicherheitsvorfälle festgestellt haben, melden Sie sich direkt bei Ihrem lokalen IT-Beauftragten und/oder schicken Sie eine E-Mail an das KIT-CERT (cert@kit.edu). Gemeinsam mit Ihnen wird dann die Situation analysiert und besprochen, was getan werden kann, um die Wahrscheinlichkeit eines Schadenseintritts und die Schwere eines Schadens für das KIT und Sie so gering wie möglich zu halten. Bitte haben Sie keine Angst, IT-Sicherheitsvorfälle zu melden.

Falls Sie den **Versuch eines Angriffs** feststellen (z. B. einen Diebstahls- oder Erpressungsversuch oder den Erhalt einer betrügerischen Nachricht), können Sie dieses ebenfalls Ihrem lokalen IT-Beauftragten melden, auch wenn kein Schaden entstanden ist. Dies hilft, die allgemeine Bedrohungslage für das KIT besser einstufen und entsprechende Maßnahmen einleiten zu können. **Um betrügerische E-Mails zu melden**, richten Sie sich den Ordner Spam_KIT ein und verschieben sie diese dorthin, vgl. https://s.kit.edu/it-sicherheit.meldeverfahren.

Wenn Sie **unsicher** sind, ob das von Ihnen Beobachtete ein IT-Sicherheitsvorfall ist oder Ihnen einfach etwas ungewöhnlich vorkommt, kontaktieren Sie vorsichtshalber Ihren lokalen IT-Beauftragten oder schicken Sie eine E-Mail an beratung-itsec@scc.kit.edu. Gemeinsam mit Ihnen wird das Beobachtete dann bewertet.