IT-Sicherheitsbeauftragter
Ansprechpartner: Andreas Lorenz
Telefon: 0721 608-24500
E-Mail: andreas.lorenz@kit.edu
Stand: April 2018

Richtlinie zum Umgang mit mobilen Geräten des KIT

Gültig ab: 19.04.2018
Version 2

Um das Risiko eines Datenabflusses bei mobilen Geräten wie Smartphones, Tablets oder Notebooks zu verringern, sind nachfolgende Regeln zu beachten. Häufig tritt Datenabfluss durch Diebstahl eines Geräts auf. Neben dem unmittelbaren Verlust des Geräts kommt erschwerend hinzu, dass die Daten, die sich auf dem Gerät befunden haben, durch den Täter eingesehen und missbräuchlich genutzt werden können.

Schutz vor Datendiebstahl

- **Identifizierung des Nutzers:** Identifizierungsmaßnahmen wie Einschaltkennwort oder PIN sind zu verwenden. Eine automatische passwortgeschützte Sperrung bei Inaktivität, etwa Bildschirmschoner oder Tastensperre, ist ebenfalls zu aktivieren, falls technisch möglich. Der eingestellte Zeitraum der Inaktivität bis zur Sperrung sollte nicht mehr als 30 Minuten (Notebook) bzw. 1 Minute (Smartphone) betragen.

- **Datenverschlüsselung:** Wenn Daten auf Geräten transportiert werden, sollten diese verschlüsselt werden. Dies gilt sowohl nur für aktive Geräte als auch für mobile Datenträger, etwa USB-Sticks oder mobile Festplatten. Manche Geräte erlauben die Verwendung eines Festplattenkennworts – es wird empfohlen, von dieser Möglichkeit Gebrauch zu machen. Wenn der Speicher des Gerätes über Speicherkarten – etwa mittels einer SD-Karte – erweitert wird, sollte auch der Inhalt dieser Karten nach Möglichkeit verschlüsselt werden.

Schutz vor Gerätemanipulation

- **Installation und Aktualisierung von Software:** Bei der Installation von Software etwa aus den einschlägigen App-Stores der Smartphonehersteller oder aus dem Internet allgemein ist besondere Vorsicht geboten. Gerade bei Smartphones ist das genaue Verhalten eines Softwarepakets in der Regel nicht ohne weiteres für den Anwender überprüfbar.
  Nicht benötigte Software sollte daher im Zweifel besser nicht installiert werden. Gerade kleine Spiele und dergleichen werden in zunehmendem Maße dazu verwendet, Schadsoftware zu verbreiten, und sollten unbedingt gemieden werden.
  Das Installieren von nicht zu dienstlichen Zwecken benötigter Software ist nicht zulässig, sofern schützenswerte Daten auf dem Gerät gespeichert sind.
  Sicherheitsrelevante Aktualisierungen von mobilen Geräten sind zeitnah durchzuführen, sofern auf elektronischem Wege Daten mit ihnen ausgetauscht werden.
  Ist es nicht möglich oder sprechen gewichtige Gründe dagegen, sicherheitsrelevante Aktualisierungen zeitnah einzuspielen, so ist anderweitig mit geeigneten Mitteln dafür Sorge zu

Karlsruher Institut für Technologie

tragen, dass die Verwundbarkeiten der mobilen Geräte, die durch diese Aktualisierungen behoben werden, nicht ausgenutzt werden können.
Es wird empfohlen, sich vom Hersteller über sicherheitsrelevante Aktualisierungen informieren zu lassen und, sofern vorhanden und möglich, Automatismen zur Aktualisierung zu verwenden.

- **Physische Kontrolle:** Die unbeaufsichtigte Weitergabe des Geräts an Dritte ist – auch vorübergehend – nicht zulässig, sofern schützenswerte Daten darauf gespeichert sind.
  Eine unbeaufsichtigte Weitergabe des Geräts an Dritte ist auch darüber hinaus zu vermeiden.
  Lassen Sie das Gerät nicht unbeaufsichtigt.
  Melden Sie sowohl Ihrem zuständigen IT-Verantwortlichen als auch der geräteausgebenden Stelle, falls ein Gerät verloren gegangen ist. Dies gilt auch, falls das Gerät wieder aufgefunden wird, sich aber in der Zwischenzeit im Zugriff von Unbefugten befunden hat. Nur mit dieser Meldung kann in der Situation entsprechend reagiert werden, etwa durch Sperrung der SIM-Karte oder Neuinitialisierung des Geräts.
  Es sollten allgemeine Vorkehrungsmaßnahmen gegen Diebstahl getroffen werden; beispielsweise sollte ein Mobilgerät nicht sichtbar in Fahrzeugen gelagert werden, auch wenn diese verschlossen sind.
  Mobile Geräte sind nach Möglichkeit physisch zu sichern, etwa mit Hilfe eines Kensington-Schlosses.

Schutz vor Angriffen auf die Kommunikation

Sämtliche Funk- (etwa WLAN, Bluetooth), Infrarot- und andere Kommunikationsschnittstellen sollten deaktiviert werden, während sie nicht benutzt werden.
Wo möglich, soll eine Datenübertragung über verschlüsselte Kanäle erfolgen, um ein Ausspähen von Daten zu erschweren.

Außerbetriebnahme des Gerätes

Vor Außerbetriebnahme eines Gerätes sind die auf dem Gerät gespeicherten Daten bei Bedarf entsprechend zu sichern und in jedem Fall unwiederbringlich zu löschen. Die Konfiguration des Gerätes ist zurückzusetzen, so dass mit dem Gerät nicht mehr auf geschützte Unternehmensressourcen – etwa VPN-Zugang – zugegriffen werden kann.

Datensparsamkeit

Auf mobilen Geräten sollten nur die Daten gespeichert werden, die unbedingt benötigt werden. Gegebenenfalls können Daten über die bekannten Remotezugänge des KIT nachgeladen werden. Es wird insbesondere darauf hingewiesen, dass die Speicherung von Passwörtern im Klartext nicht zulässig ist. Zudem sollten die für die Benutzerauthentifikation und die Verschlüsselung verwendeten Passwörter in jedem Fall die derzeit gültigen Anforderungen hinsichtlich Passwortlänge und Komplexität erfüllen.

Auslandseinsatz

Bei Dienstreisen ins außereuropäische Ausland sind ergänzend zu dieser Richtlinie auch die „Empfehlungen zu Dienstreisen ins außereuropäische Ausland“ zu beachten:
http://www.dsb.kit.edu/downloads/19-10-2011Merkblatt_Dienstreiseempfehlung_deutsch_KIT(1).pdf