

Richtlinie zum Umgang mit mobilen Geräten des KIT

Motivation

Der Umgang mit mobilen Geräten wie PDAs, Smartphones oder Notebooks ist heutzutage für jedermann Alltag. Um das Risiko eines (ungewollten) Datenverlustes zu verringern, sind nachfolgende Regeln zu beachten. Häufig tritt Datenverlust 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.

Diese Richtlinie orientiert sich an den Empfehlungen des BSI „Mobile Endgeräte und mobile Applikationen: Sicherheitsgefährdungen und Schutzmaßnahmen“. Nachfolgende Maßnahmen entsprechen der Gliederung des Dokuments des BSI, reflektieren jedoch auch die zum Zeitpunkt der Ausgabe bestehenden technischen Möglichkeiten der Absicherung innerhalb des KIT. Diese Richtlinie wird in regelmäßigen Abständen auf Aktualität geprüft und bei Änderung in einer neuen Version veröffentlicht.

Ergänzend zu dieser Richtlinie sind auch die Empfehlungen zu Dienstreisen ins außereuropäische Ausland zu beachten.

Gültigkeitsbereich

Der Gültigkeitsbereich der Richtlinie wird durch die zum Zeitpunkt der Veröffentlichung gültigen Nutzungsordnungen und Betriebsvereinbarungen des KIT geregelt.

Maßnahmen zum Schutz vor Datendiebstahl

- **Identifizierung des Nutzers:** Aktivieren von Identifizierungsmaßnahmen für den Nutzer (zum Beispiel Einschaltkennwort oder PIN). Eine automatische passwortgeschützte Sperrung bei Inaktivität (z. B. Bildschirmschoner, Tastensperre) ist ebenfalls zu aktivieren, falls technisch möglich. Der Zeitraum der Inaktivität bis zur Sperrung sollte nicht mehr als 30 Minuten betragen.
- **Datenverschlüsselung:** Wenn Daten auf Geräten transportiert werden, sollten diese verschlüsselt werden. Dies gilt sowohl nur für aktiv genutzte Geräte, als auch für mobile Datenträger (USB-Sticks, mobile Festplatten etc.). Manche Geräte erlauben die Verwendung eines Festplattenkennworts – es wird empfohlen, von dieser Möglichkeit Gebrauch zu machen. Wenn der Speicher des Gerätes über Speicherkarten (zum Beispiel SD-Karte) erweitert wird, ist auch der Inhalt dieser Karten nach Möglichkeit zu verschlüsseln.
- **Physische Sicherung:** Mobile Geräte sind nach Möglichkeit physisch zu sichern (zum Beispiel mit einem Kensingtonschloss), um einen Gelegenheitsdiebstahl zu vermeiden.

Maßnahmen zum Schutz vor Gerätemanipulation

- **Weitergabe:** Die Weitergabe des Geräts an Dritte oder Fremde ist - (auch vorübergehend) nicht zulässig.
- **Verlustmeldung:** Melden Sie sowohl Ihrem zuständigen IT-Verantwortlichen als auch der geräteausgebenden Stelle, falls ein Gerät verloren gegangen ist. Dies gilt auch, falls sich Geräte nach kurzer Zeit wieder auffinden. Nur mit dieser Meldung kann in der Situation entsprechend reagiert werden (zum Beispiel durch Sperrung der SIM-Karte oder Neu-Initialisierung des Geräts).
- Lassen Sie das Gerät nie unbeaufsichtigt.

Maßnahmen zum Schutz vor Angriffen auf die Kommunikation

- **Schnittstellen deaktivieren:** Sämtliche Funk- (WLAN, Bluetooth etc.), Infrarot- und andere Kommunikationsschnittstellen sind zu deaktivieren, sofern diese nicht benutzt werden.

- **Kommunikationssicherheit:** Wo möglich, muss eine Datenübertragung über verschlüsselte Kanäle erfolgen, um ein Ausspähen von Daten zu erschweren.

Maßnahmen bei Außerbetriebnahme des Gerätes

- **Datenlöschung:** 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 (zum Beispiel VPN-Zugang) zugegriffen werden kann.

Allgemeine Empfehlungen

- **Datensparsamkeit:** Wenn Daten unbedingt auf mobilen Geräten benötigt werden, sollte die Auswahl der Daten auf das Nötigste beschränkt 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.
- Allgemeine Vorkehrungsmaßnahmen gegen Diebstahl sollten getroffen werden (Auch in verschlossenen Fahrzeugen dürfen Geräte nicht sichtbar gelagert werden).

Version

Diese IT-Sicherheitsrichtlinie wurde in der Version 1.0 von ASDUR am 24.03.2010 empfohlen.

Veröffentlichung

Sie tritt zum 24.03.2010 in Kraft und wird auf den Internetseiten des CIO als Sicherheitsrichtlinie für das KIT veröffentlicht. Der IT-Sicherheitsbeauftragte kommuniziert deren Veröffentlichung im Auftrag des CIO in den entsprechenden Gremien.

Weiterführende Informationen

- Weiterführende Informationen zum Umgang mit mobilen Geräten erhalten Sie auf den Internetseiten des BSI unter folgendem URL:
https://www.bsi.bund.de/cln_156/ContentBSI/Publikationen/Broschueren/mobile/index_htm.html
- Hinweise zur sicheren Datenlöschung erhalten Sie auf den Webseiten der ZENDAS unter folgenden URL: <http://www.zendas.de/themen/vernichtung/speichermedien.html>