Informationsblatt
zum
Umgang mit mobilen Geräten

Arbeitsgruppe IT-Sicherheit
der TU Clausthal

2016-11-22

Bei der Benutzung von mobilen Geräten (Laptops, Tabletts bzw. Smartphones) können über die normalen Risiken hinaus weitere Gefahren auftreten. Generell gilt die IT-Sicherheitsrichtlinie der TU Clausthal. Darauf aufbauend gelten die besonderen Regeln für mobile Geräte. Jeder Nutzer verpflichtet sich, diese Regeln gewissenhaft einzuhalten.

Zu A.4: Räumlicher Zugangsschutz

Mobile Geräte können problemlos aus dem Büro an andere Wirkungsstätten mitgenommen werden. Teilweise sind die Geräte so klein, dass sie in der Westentasche mitgenommen werden können. Aufgrund der geringen Größe hat der Benutzer besonders darauf zu achten, dass das Gerät nicht aus Versehen verloren wird oder von Dritten unbemerkt entwendet werden kann. Sofern das Gerät nicht genutzt wird, empfiehlt es sich, das Gerät z. B. in einer verschlossenen Aktentasche zu transportieren.
Mobile Geräte können sehr leicht beschädigt werden, wodurch auch die Datenspeicher beeinträchtigt werden können. Um Datenverluste zu vermeiden, empfiehlt es sich, mobile Geräte mit einer Schutzhülle zu versehen.

Zu A.5: Sicherung mobiler Geräte

Mobile Geräte bieten eine Vielzahl von möglichen Schutzmechanismen an. Angefangen über die Eingabe eines PIN-Codes bis hin zu Kennwörtern oder Finger-Scannern sind etliche Möglichkeiten denkbar. Mobile Geräte unterliegen der besonderen Gefahr, dass des Diebstahls, daher sind alle Möglichkeiten auszuschöpfen, dass im Falle eines Verlustes, niemand an die schützenswerten Daten gelangen kann.
Bei etlichen Applikationen gibt es weitere Schutzmöglichkeiten. Wo immer diese vorhanden sind, sollten sie genutzt werden. Es empfiehlt sich, getrennte Kennwörter für das Gerät und die Applikation zu nutzen.

Zu A.6: Kontrollierter Software-Einsatz

Auf den mobilen Geräten dürfen nur die freigegebenen Applikationen zum Einsatz kommen. Die Freigaben erteilt der jeweilige IT-Beauftragte in Abstimmung mit dem Rechenzentrum. Damit soll verhindert werden, dass durch die Installation von weiterer Software heimlich „Hintertüren“ eingebaut werden, durch die schützenswerte Daten ausgespäht werden könnten.

Zu A.11: Gebrauch von Kennwörtern

Kennworte dienen dazu, fremden Personen den Zugang zu mobilen Geräten zu verweigern. Die genannten Regeln sind sinnvolle Vorgaben, mit denen sichergestellt werden kann, dass das jeweilige Kennwort nicht durch erraten oder ausprobieren von Dritten geknackt werden kann. Wenn Sie sich sicher sind, ihr Kennwort korrekt eingegeben zu haben, der Zugang zum Gerät aber verweigert wird, dann könnte es einem Angreifer gelungen sein, in Ihr Gerät einzudringen und z. B. Ihr Kennwort zu verändern. Wenn Sie auch nur den Verdacht haben, dass jemand unbefugt in Ihr Mobilgerät eingedrungen sein könnte, sollten sie das zuständigen IT-Personal informieren. Auf keinen Fall sollten sie weiter versuchen, Ihr Kennwort einzugeben (z. B. weil es abgehört werden könnte ...).

Zu A.16: Datensicherung

Wie bereits erläutert, ist es gerade bei mobilen Geräte wahrscheinlicher, das ein Datenverlust auftritt (z. B. durch Diebstahl, Zerstörung des Gerätes, ...). Daher ist es bei diesen Geräten um so wichtiger, eine zuverlässige und regelmäßige Datensicherung auf einem weiteren Gerät durchzuführen. Idealerweise wird die Sicherung automatisch durchgeführt. Oftmals werden von den Geräte”=Herstellern sogenannte Cloud”=Dienste angeboten. Schützenswerte Daten dürfen unter keinen Umständen in den Cloudspeichern des Geräteherstellers oder anderer Fremdhersteller gespeichert werden, da für die Sicherheit der Daten nicht garantiert werden kann. Stattdessen sind die vom Rechenzentrum angebotenen Sicherungsmethoden zu verwenden (z. B. der OwnCloud-Service des RZ).

Zu A.18: Physisches Löschen von Datenträgern

Wenn das mobile Gerät nicht weiter genutzt werden soll (Z. B. Verkauf, Ende der Nutzungsperiode, ...), muss vor der Weitergabe des Gerätes sichergestellt sein, dass alle schützenswerten Daten gelöscht wurden. Welche Methoden das im Einzelnen sind, ist von Gerät zu Gerät unterschiedlich, daher kann hier keine Aufzählung vorgenommen werden. Idealerweise sollten Sie die Löschung gemeinsam mit dem IT-Personal durchführen. Damit kann sichergestellt werden, dass das IT-Personal nicht von den Schutzmechanismen des Gerätes an der Löschung gehindert wird.

Erklärung

(Zum Verbleib beim Benutzer des Gerätes)

Hiermit erkläre ich, dass ich die Regelungen der IT-Sicherheitsrichtlinie sowie die oben abgedruckten Erläuterungen zur Anwendung der Richtlinie auf mobile Geräte zur Kenntnis genommen habe. Ich versichere, die Richtlinie ordnungsgemäß zu beachten und bei der Benutzung des mir zur Verfügung gestellten mobilen Gerätes die notwendige besondere Sorgfalt walten zu lassen.

Name, Vorname: _____

Institut: _____

Typ des mob. Gerätes: _____

Serien-Nr.: _____

Inventar-Nr.: _____

Datum: _____ Unterschrift: _____

Erklärung

(Zum Verbleib im Rechenzentrum)

Hiermit erkläre ich, dass ich die Regelungen der IT-Sicherheitsrichtlinie sowie die oben abgedruckten Erläuterungen zur Anwendung der Richtlinie auf mobile Geräte zur Kenntnis genommen habe. Ich versichere, die Richtlinie ordnungsgemäß zu beachten und bei der Benutzung des mir zur Verfügung gestellten mobilen Gerätes die notwendige besondere Sorgfalt walten zu lassen.

Name, Vorname: _____

Institut: _____

Typ des mob. Gerätes: _____

Serien-Nr.: _____

Inventar-Nr.: _____

Datum: _____ Unterschrift: _____