Allgemeine Sicherheitsempfehlungen für Android

Zusammenfassung

Das Betriebssystem Android wird vom Rechenzentrum nicht unterstützt. Folgende grundsätzlichen Sicherheitseinstellungen, die von Gerät zu Gerät und Version unterschiedliche sein können, sind zu beachten.

Diese Anleitung richtet sich besonders an folgende Zielgruppen:

- **Studierende**
- **Zweit- und Gasthörende**
- **Lehrende**
- **Mitarbeitende**
- **Einrichtungen und Gremien (z.B. Fachschaftsräte)**
- **Arbeitsbereiche / Gruppen (z.B. Projekte)**
- **Sekretariate**
- **Gäste der Friedrich-Schiller-Universität**

Auf dieser Seite findet man Informationen zu folgenden Themen:

Exchange Account

Die Einrichtung des Exchange Kontos unter Android wird im folgendem Anleitungsartikel beschrieben.

Ortungsdienste

Unter Verwendung von GPS, Bluetooth, WLAN und Mobilfunk, ermitteln die Ortungsdienste den ungefähren Standort des Gerätes und sollten deaktiviert werden.

Passwortschutz

Das Gerät ist immer vor unberechtigten Zugriff durch mindestens eine 4-stellige PIN zu schützen. (Sperrbildschirm aktivieren)

- Zusätzlich wird empfohlen nach z.B. 10 fehlgeschlagenen Anmeldeversuchen alle Daten auf dem Gerät zu löschen
- Bildschirm-Timeout einstellen, z.B. 1 Minute
- Einstellungen für die Gerätesicherheit und die SIM-oder USIM-Karte; sorgfältig abwägen
- Steuerung eines verlorenen oder gestohlenen Geräts über das Internet zulassen

Diagnose- & Nutzungsdaten

Bei aktivierter Funktion werden täglich Diagnose- und Nutzungsdaten, zur Verbesserung von Produkten und Diensten, weiter gesendet, welche u.a. auch Ortsinformationen enthalten können. Diese Funktionen deaktivieren.

VPN

Außerhalb vom „eduroam“ sollte immer eine VPN Verbindung genutzt werden.

Anwendungen

Die Installation von Anwendungen unbekannter Quellen ist nicht empfehlenswert.

Updates

Das Gerät sollte wöchentlich auf Softwareaktualisierungen überprüft werden. Andernfalls können bekannt gewordene Sicherheitslücken ausgenutzt werden.

- automatische Aktualisierung überprüfen
- anzeigen lassen und aktiv nach Abwägungen der Notwendigkeit ausführen
- Updates des Betriebssystems und der Sicherheit Software immer ausführen
- Beachten der möglichen anfallenden Kosten

Datensicherung

Es wird empfohlen, ein Backup des Gerätes auf einem PC zu erstellen.
Die Unsicherheiten beim Speichern von Daten auf Servern, die nicht zur Rechtshoheit der Bundesrepublik Deutschland gehören, sind zu bedenken.

Sicheres Löschen

Bei Stilllegung und Nutzerwechsel, sowie Virenbefall sind alle Medien, Daten und Einstellungen unwiderruflich zu löschen.

Vorgehen bei Verlust

- Wird ein Gerät gestohlen oder verloren, muss es aus der Ferne deaktiviert werden, um unbefugten Zugang zu verhindern.
- Bei Verlust eines Gerätes ist umgehend das IT-Servicezentrum zu informieren
- Ein Diebstahl ist zusätzlich und unverzüglich bei der nächsten Polizeidienstelle, für Jena Telefon +49 3641 810, anzuzeigen und das Aktenzeichen zu notieren

Titel: "Sicherheitsempfehlungen Allgemein für Android"

Stand: 30.10.2020

FRIEDRICH-SCHILLER-
UNIVERSITÄT
JENA