Universitätsklinikum Würzburg

Servicezentrum Medizin-Informatik
Leitung: Dipl.-Inform. H. Greger

Datenschutzhinweis

Eine an sich bequeme Funktion des Android-Betriebssystems kann unter Umständen Passwörter und sonstige Zugangsdaten in falsche Hände liefern. Lesen Sie, wie Sie diese Möglichkeit deaktivieren.

Hintergrund ist, dass Sie sich im WLAN „eduroam“ mittels ihrer Klinikums-Zugangsdaten (Windows-Benutzername und –Passwort) authentifizieren. Dieser Zugang bietet für Sie auch Zugriff auf weitere Dienste des SMI (SAP, E-Mail, etc.).

Eigentlich hört sich das ganz komfortabel an, jedoch hat die Sache einen entscheidenden Haken: **Bei den meisten Smartphones und Tablets mit dem Android-Betriebssystem ist eine Funktion zur Sicherung der Zugangsdaten und Passwörter standardmäßig aktiviert.**

Diese Daten werden bisher noch im **KLARTEXT** auf den Servern von Google gespeichert, was bei der Diskussion um Datenweitergabe an Geheimdienste eine besondere Note erhält. Hierdurch kann Dritten Zugriff auf sensible Daten Ihres Klinik-Benutzerzugangs gewährt werden, ohne dass Sie davon Kenntnis erlangen.

Bitte passen Sie die Einstellungen Ihres Androiden entsprechend an.

Wo Sie diese Einstellung auf Ihrem Android-Smartphone finden, wird nachfolgend beschrieben:

- **Android 2.x:** Unter "Einstellungen" den Punkt "Datenschutz" auswählen und den Unterpunkt "Meine Daten sichern" deaktivieren.
- **Ab Android 4.x:** Unter "Einstellungen" den Punkt "Sichern und Zurücksetzen" auswählen und den Unterpunkt "Meine Daten sichern" deaktivieren.

TIPP: Legen Sie stattdessen ein Backup auf Ihrem privaten Rechner an. Sinnvollerweise sollten Sie nach der Deaktivierung der Funktion „Meine Daten sichern“ zusätzlich alle auf Ihrem Android-Smartphone gespeicherten Passwörter ändern.

SMI SERVICEZENTRUM MEDIZIN-INFORMATIK