Smartphone und Co

Was sind "mobile Geräte"?

Mobile Geräte gehören mehr und mehr zum alltäglichen Leben. Hierzu zählt man Mobiltelefone (u.a. Smartphones), Notebooks (Laptops, Tablets), aber auch Chipkarten und USB-Sticks.

Mobile Geräte werden sowohl im Privatbereich als auch bei der täglichen Arbeit eingesetzt. So ist es möglich, dass sich auf ein und demselben Gerät neben den privaten Daten und Anwendungen des Benutzers oder der Benutzerin auch sensible Daten befinden.

Im Folgenden werden alle Geräte, die Daten speichern können und beweglich sind, als mobile Geräte bezeichnet.

+ **Besondere Gefahren**

Besondere Gefahren

Kleine Geräte können leicht gestohlen werden oder verloren gehen!

Mobile Geräte und Speichermedien unterliegen jedoch besonderen Gefahren, denn sie können leichter vergessen, verloren oder gestohlen werden.

+ **Moderne Kommunikationstechnologien**

Moderne Kommunikationstechnologien

Achtung: Jeder hört mit!
Mobile Geräte mit Benutzeroberflächen wie Smartphones bieten nicht nur Möglichkeiten zum Telefonieren, zur Adressverwaltung oder auch zum Betrachten und Bearbeiten von Dokumenten. Sie können auch zum Surfen im Internet oder zum Austausch von Kurznachrichten und Fotos verwendet werden.

Das alles geschieht kabellos mittels "Wireless"- (Drahtlos-) Technologien wie Bluetooth oder WLAN und natürlich den Telefon- und Datennetzen UMTS und LTE. Problematisch ist dabei, dass oft schwer festzustellen ist, wer bei einer drahtlosen Datenübertragung mithört und ob dieser Zugang gerade ausspioniert wird. Gerade unverschlüsselte WLANs erlauben leicht Angriffe auf die über sie übermittelten Daten.

Bei vielen Anwendungen auf Smartphones ("Apps") verlangen diese bei der Installation weitgehende Rechte, die nicht immer benötigt werden.

+ **WLAN - Wireless Local Area Network**

WLAN - Wireless Local Area Network

Bei Wireless LAN (WLAN) handelt es sich um eine Funknetzwerktechnik, die – wenn einmal aufgebaut – wie ein normaler, aber kabelloser Netzwerkzugang funktioniert. WLANs stehen aber auch in Cafés, Hotels oder anderen öffentlichen Bereichen bereit.

So verhalten Sie sich richtig:

- Wenn eine eigene drahtgebundene Netzwerkverbindung möglich ist, ist diese der WLAN-Technik vorzuziehen.
- Wenn WLAN eingesetzt wird, muss grundsätzlich der höchstmögliche Sicherheitsstandard zur Verschlüsselung des Zugangs gewählt werden (derzeit WPA2 zukünftigt WPA3).
- Jeder ungewöhnliche Vorgang auf Ihrem Endgerät in Verbindung mit Funknetzen könnte ein Angriff sein; im Zweifel deaktivieren Sie die WLAN-Verbindung und informieren Sie Ihre Ansprechperson.
- Sollten Sie keine Kenntnis über die Funktion und das Einstellen dieser Mechanismen haben, so informieren Sie sich bitte bei Ihrer Ansprechperson.
- Besuchen Sie wenn möglich nur Internetseiten, die per https aufrufbar sind.

+ Notebooks

Notebooks

So verhalten Sie sich richtig

Richtig

- Das Notebook mindestens einmal pro Woche mit dem Hochschulnetz verbinden, um Software-Updates und Konfigurationsänderungen zu ermöglichen
- Dem Virenschutzprogramm bei Nutzung täglich die Aktualisierung ermöglichen.
- Bei Fehlermeldungen des Virenscanners oder der Verschlüsselungssoftware sofort die Ansprechperson benachrichtigen
- Regelmäßig alle Daten sichern und Sicher aufbewahren
- Wenn möglich die Daten im Endgerät verschlüsseln

Falsch

- Notebook und Login-Informationen an Dritte weitergeben
- Die Konfiguration des Notebooks selbständig verändern
- Unberechtigte Personen das Gerät bedienen lassen

+ Mobiltelefone und Smartphones

Mobiltelefone und Smartphones

So verhalten Sie sich richtig
Heute haben viele Handys umfangreiche, computerähnliche Funktionen. Entsprechend ist auch hier Vorsicht geboten, vor allem beim Speichern von Informationen auf dem Smartphone:

- Beim Einschalten sollte standardmäßig die PIN-Abfrage erfolgen

- Alle drahtlosen, nicht für die aktuelle Nutzung benötigten Kommunikationsmöglichkeiten des Geräts sollten aus Sicherheitsgründen deaktiviert sein (Bluetooth, WLAN)

+ Apps und "Bring your own device"

Apps und "Bring your own device"

Viele Apps wollen mehr Rechte haben, als es für ihre Nutzung erforderlich ist. Verweigern Sie den Apps diese Rechte oder verzichten Sie ganz auf sie.

Folgende Punkte sollten Sie stets beherzigen

- Installieren Sie nur solche Apps, die sie benötigen und löschen sie die anderen
- Schränken Sie die Zugriffsberechtigungen für Ihre Kontakte, Standortangaben etc. bei Apps möglichst ein
- Löschen Sie nicht mehr benötigte WLAN-Netzwerke
- Installieren Sie alle verfügbaren Updates für das Gerät und Apps

+ Mobile Datenträger

Mobile Datenträger

Schnell und flexibel!
Trotz Vernetzung, E-Mail und Internet kann es notwendig sein, Daten zwischen zwei nicht verbundenen Rechnern auszutauschen. Zu diesem Zweck werden üblicherweise mobile Datenträger wie CDs/DVDs oder USB-Sticks verwendet (auch MP3-Player, Smartcards und Chipkarten können hierfür benutzt werden).

Dabei ist doppelte Vorsicht geboten:

- Zum einen können auf diese Weise vertrauliche Informationen an Unbefugte geraten
- Zum anderen können durch die Verwendung mobiler Datenträger leicht Viren und andere schädliche Programme auf das Gerät gelangen.

+ Schutz mobiler Datenträger

Schutz mobiler Datenträger

So verhalten Sie sich richtig

- Auf mobilen Datenträgern sollten, wenn möglich, keine geheimen oder vertraulichen Daten gespeichert werden
- Ist die Speicherung vertraulicher Daten notwendig, so sind diese zu verschlüsseln
- Darüber hinaus sollten alle mobilen Datenträger vor der Verwendung mit einem aktuellen Virenscanner auf Viren untersucht werden

- Mobile Datenträger müssen an einem sicheren Ort aufbewahrt werden

---

+ Zusammenfassung

Zusammenfassung

Mobile Geräte und Datenspeicher stellen aufgrund ihrer Größe und Beweglichkeit ein besonderes Sicherheitsrisiko dar.

Folgende Regeln wurden wie folgend sinngemäß zusammengefasst sind:

- Passwortschutz bzw. PIN-Abfrage aktivieren
- Mobile Datenträger immer zuerst auf Viren untersuchen
- Mobile Geräte sicher aufbewahren
- Für regelmäßige Software-Updates und Konfigurationsüberprüfungen sorgen
- Nicht benötigte drahtlose Kommunikationsmöglichkeiten möglichst deaktivieren

---