Handlungsempfehlung der Goethe-Universität Frankfurt zur Nutzung von mobilen Geräten

Diese Handlungsempfehlung gilt für alle Angehörigen der Goethe-Universität Frankfurt. Sie regelt die sichere Nutzung von mobilen Geräten. Ordnungen und Satzungen der Goethe-Universität, insbesondere die IT-Sicherheitsordnung, IT-Sicherheitsrichtlinie und die IuK-Nutzungsordnung[1], werden durch diese Handlungsempfehlung nicht berührt.

Mittlerweile entsprechen die mobilen, internetfähigen Geräte kleinen Computern, mit denen gearbeitet und kommuniziert wird und auf denen vertrauliche Daten gespeichert werden. Dadurch gelten für sie mindestens die gleichen Sicherheitsanforderungen wie für stationäre Computer.

Die Sicherheit spielt im Grunde sogar eine noch größere Rolle, denn die Möglichkeit, die Geräte immer und überall dabei zu haben und sie ständig mit dem Internet zu verbinden, birgt zusätzliches Gefahrenpotenzial. Die dienstliche Nutzung von privaten Geräten ist nicht nur praktisch, sondern stellt zusätzliche Anforderungen an die sichere Verwendung der Geräte.

Das Sicherheits-Management-Team (SMT) der Goethe-Universität empfiehlt folgende Maßnahmen für die Informationssicherheit mobiler Geräte:

1) Achten Sie **beim Kauf** von mobilen Geräten auf Aktualität des Betriebssystems sowie **Verfügbarkeit von Updates**.

2) Sorgen Sie für einen **Basisschutz** und führen Sie regelmäßig Sicherheitsupdates durch.

   - Halten Sie das Betriebssystem und sämtliche installierte Software und Apps mit **Sicherheitsupdates** immer auf dem neuesten Stand. Viele Angriffe zielen auf bekannte Schwachstellen, die erst durch Updates der Hersteller geschlossen werden. Aktivieren Sie daher die **automatische Update-Funktion**, damit Sicherheitsupdates direkt nach dem Erscheinen eingespielt werden.

3) Installieren Sie Apps nur **aus vertrauenswürdigen Quellen** und prüfen Sie die Zugriffsberechtigungen.

   - Informieren Sie sich vor Installation einer App, wenn Ihnen der Anbieter nicht bekannt ist. Eine kurze Suche im Internet reicht meistens aus, um sich zu informieren. Entfernen Sie **veraltete Anwendungen** oder solche, die Sie nicht mehr nutzen. Denn jede zusätzliche App ist eine mögliche Sicherheitslücke.

[1] Allgemeine Nutzungsordnung für die Informationsverarbeitungs- und Kommunikationsinfrastruktur der Goethe-Universität Frankfurt

- Viele Apps räumen sich ohne erkennbaren Grund umfassende Rechte ein. Ein Zugriff auf beispielsweise Standortdaten, Adressbuch oder den Telefonstatus ist nicht bei jeder App notwendig. Prüfen Sie daher kritisch, ob die **Zugriffsrechte** zum Erfüllen der Funktionalität wirklich notwendig sind.

4) Nutzen Sie **Sperrcodes und Passwörter**.

   - Der Zugriff auf mobile Geräte und deren Anwendungen muss durch Schutzvorkehrungen wie Passwort, PIN usw. abgesichert werden.

5) Aktivieren Sie Schnittstellen nur bei Bedarf und sichern Sie diese.

   - Deaktivieren Sie Drahtlosschnittstellen, wie **Bluetooth oder NFC**, wenn Sie diese nicht benötigen. So ist Ihr Gerät weniger anfällig für Cyber-Angriffe.

6) Schließen Sie Ihr mobiles Gerät nur an **vertrauenswürdige Rechner** an.

7) Nutzen Sie öffentliche Hotspots mit erhöhter Vorsicht.

   - Öffentliche WLAN- Hotspots sollten nicht bedenkenlos genutzt werden, da diese nicht immer eine sichere, verschlüsselte Verbindung zur Verfügung stellen. Gerade beim Umgang mit sensiblen Daten (z. B. Online-Banking, Shopping etc.) ist eine **verschlüsselte Verbindung** unerlässlich.

   - Nutzen Sie am besten eine **VPN-Verbindung**. Das Hochschulrechenzentrum (HRZ) bietet eine kostenlose VPN-Lösung für alle Universitätsangehörigen. Weitere Informationen finden Sie unter: https://www.rz.uni-frankfurt.de/vpn

8) Lassen Sie Ihr Gerät nicht aus den Augen.

   - Um das Gerät vor unbefugtem Zugriff und Manipulation zu schützen, sollten Sie Ihr Smartphone **niemals unbeobachtet lassen oder verleihen**. Verlorene oder gestohlene dienstliche Geräte müssen dem zuständigen IT-Support gemeldet werden.

9) Surfen Sie mit gesundem Menschenverstand.

   - Bewahren Sie sich eine gesunde Skepsis, welcher Empfehlung beispielsweise für eine App Sie folgen wollen, was Sie von wo installieren beziehungsweise worauf Sie alles klicken. Nicht alles hält letztlich, was es verspricht, und leere Versprechungen werden gerne genutzt, um Schadsoftware auf dem Gerät zu installieren.

10) Schützen Sie Ihre Daten.

   - Nutzen Sie die Funktionen zur **Datenverschlüsselung**, wenn vorhanden, oder verschlüsseln Sie sensible Daten selbst mit einer Verschlüsselungssoftware.

- Erstellen Sie regelmäßig **Sicherungskopien**.

11) Prüfen Sie unbekannte Rufnummern vor Rückruf.

- Aktuelle Informationen zu missbräuchlich genutzten Rufnummern finden Sie auf der Webseite der Bundesnetzagentur. Lassen Sie bei Bedarf unerwünschte Rufnummern zu Mehrwertdiensten von Ihrem Netzbetreiber sperren.

  https://www.bundesnetzagentur.de/Rufnummernmissbrauch

12) Löschen Sie alle Speicher, bevor Sie das Gerät verkaufen oder entsorgen.

- Wenn Sie nicht möchten, dass Ihre gespeicherten Daten beim Verkauf oder bei der Entsorgung Ihres Gerätes in falsche Hände geraten, dann sollten alle Datenspeicher (**interner Speicher und SD-Karten**) sicher gelöscht werden. Die SIM-Karte und ggf. die SD-Karten sollten Sie entfernen und – falls Sie diese nicht weiterverwenden wollen – vernichten.

13) Bei Fragen können Sie sich an Ihren zuständigen IT-Support bzw. an Ihre/n IT-Sicherheitsbeauftragte/n wenden.

Informationsquellen

- Bundesamt für Sicherheit in der Informationstechnik (BSI)
  https://www.bsi-fuer-buerger.de

- DFN Computer Emergency Response Team (DFN-CERT)
  https://www.dfn-cert.de

- IT-Sicherheitsmanagement-Team (SMT) der Goethe-Universität
  https://www.uni-frankfurt.de/smt

- Goethe-Universität Computer Emergency Response Team (GU-CERT)
  https://www.rz.uni-frankfurt.de/gu-cert

- Hochschulrechenzentrum (HRZ) der Goethe-Universität
  https://www.uni-frankfurt.de/hrz/it-sicherheit