Technische Universität Berlin

# Umgang mit mobilen IT Geräten

# Inhaltsverzeichnis

# 1. Einleitung/Präambel

Dieser Leitfaden zum Umgang mit mobilen Geräten in der TU Berlin enthält grundsätzliche Empfehlungen für alle Mitglieder der TU Berlin, die zu dienstlichen Zwecken mobile Endgeräte (u.a. Laptops, Smartphones, Tablet-PCs) einsetzen. Dieser Leitfaden dient der Sensibilisierung für IT-Sicherheit und Risiken, die beim Einsatz von mobilen Geräten eintreten können.
Grundsätzlich sind dabei zwei Geräteklassen zu unterscheiden
a) Laptops, auf denen herkömmliche Desktop-Betriebssysteme (Windows, Linux und OS X) zum Einsatz kommen und sich damit die üblichen Sicherheitsregelungen umsetzen lassen und
b) Smartphones und Tablets auf denen spezielle, an das Gerät angepasste Betriebssysteme (Android, iOS und Windows Phone) eingesetzt werden, deren Bedienung sich von Desktop-Betriebssystemen unterscheidet.
Speziell im Bereich der Smartphones und Tablets liegt der Entwicklungsschwerpunkt der Hersteller häufig auf dem Consumer-Bereich, wodurch nur einige wenige, technisch begrenzte Sicherheits- und Enterprisemanagementfeatures bereitgestellt werden können.
Gegenüber fest installierten IT Geräten bringt die Nutzung von mobilen Geräten ebenfalls ein erhöhtes Risiko in verschiedenen Bereichen mit sich. Dies betrifft vor allem:

- Verlust oder Diebstahl des Gerätes und dadurch unter Umständen Zugriff auf vertrauliche Daten durch Unbefugte
- Manipulation des Gerätes durch bösartige Software/Apps
- Unbeabsichtigter, automatischer Datenabfluss an externe Cloud-Dienste

Dieser Leitfaden soll zur Sensibilisierung gegenüber potentiellen Risiken beitragen und entsprechende Handlungsempfehlungen geben.

# 2. Geltungsbereich

Die Empfehlungen dieses Dokuments richten sich an alle Mitglieder der TU Berlin, die Mobilgeräte zu dienstlichen Zwecken nutzen. Sie gelten auch für dienstlich genutzte Privatgeräte, sofern diese eingesetzt werden.
Alle Nutzerinnen und Nutzer eines Mobilgerätes sind für die Absicherung ihres Gerätes und der darauf befindlichen Daten in der Regel selbst verantwortlich. Durch den Nutzer/die Nutzerin muss sichergestellt werden, dass eine qualifizierte Person die Verantwortung für die sachgerechte Betreuung übernimmt. Dies kann grundsätzlich auch der Nutzer/die Nutzerin selbst sein, alternativ kann die Administration durch einen ausgewiesenen IT-Administrator der eigenen Einrichtung erfolgen.

## 2.1. Dienstliche Mobilgeräte

Die hier beschriebenen Empfehlungen sollen das Risiko des ungewollten Abflusses von Daten an Dritte verringern. Die wichtigste Regel lautet, so wenig dienstliche Daten wie möglich auf dem Gerät zu speichern (Prinzip der Datensparsamkeit). Vom Speichern von privaten Daten auf dienstlichen Geräten wird abgeraten. Bei Nutzung des zentralen Microsoft Exchange Systems werden durch den ActiveSync Client auf den meisten Mobilgeräten einige der empfohlenen Sicherheitseinstellungen und Anforderungen automatisch aktiviert.

## 2.2. Private Mobilgeräte

Auch für dienstlich genutzte Privatgeräte werden die in diesem Leitfaden beschriebenen Empfehlungen dringend angeraten. Es gelten zusätzlich alle allgemeinen Regelungen zu Datenschutz und Datensicherheit. Bei Nutzung des zentralen Microsoft Exchange Systems werden durch den ActiveSync Client auf den meisten Mobilgeräten einige der empfohlenen Sicherheitseinstellungen und Anforderungen automatisch aktiviert. Von der dienstlichen Nutzung privater Geräte wird abgeraten.

# 3. Speicherung von Daten

Dem Grundsatz der Datensparsamkeit folgend sollten auch auf mobilen Geräten so wenig wie möglich Daten gespeichert werden. Welche Daten auf mobilen Geräten gespeichert werden dürfen kann anhand der Risikobewertung und der damit verbundenen Klassifizierung der Daten festgelegt werden. Dabei sind personenbezogene oder personenbeziehbare Daten immer der höchsten Schutzklasse zuzuordnen. Gleiches gilt für vertrauliche oder kritische Geschäftsdaten. Die Speicherung solcher Daten darf auf keinen Fall auf mobilen Geräten erfolgen. Daten mit der Klassifikation „hoher Schutzbedarf“ dürfen nur verschlüsselt gespeichert werden, für alle anderen Daten ist eine unverschlüsselte Speicherung zulässig. Die Klassifizierung erfolgt durch den Eigentümer der Daten in Zusammenarbeit mit der Behördlichen Datenschutzbeauftragten.

# 4. Empfehlungen für Laptops

Die folgenden Empfehlungen gelten für Laptops, Tablet-PCs etc., die mit herkömmlichen Betriebssystemen wie z.B. Windows, OS X oder Linux betrieben werden.

## 4.1. Absicherung des Gerätes gegen unbefugten Zugriff

Jeder Nutzer sollte folgende Sicherheits-Regelungen befolgen:

- Sperrung des Gerätes mithilfe einer PIN bzw. eines Kennwortes
- Automatische Sperrung des Gerätes bei Inaktivität
- Die Festplatte des Gerätes sollte verschlüsselt sein, falls Daten mit hohem Schutzbedarf darauf gespeichert werden.
- Das Gerät sollte stets sicher verwahrt werden und es sollte keine Weitergabe des entsperrten Gerätes an Dritte erfolgen.
- Bei der Verwendung von öffentlichen, ungesicherten Netzen (z.B. WLAN-Hotspots) sollte eine sichere verschlüsselte Verbindung genutzt werden (z.B. VPN).
- Die Nutzung und der Anschluss von Datenträgern und Geräten aus unbekannter Herkunft sollte vermieden werden.

## 4.2. Umgang mit Betriebssystem und Software

Jeder Nutzer/jede Nutzerin sollte bei der Installation und Verwendung von Betriebssystem und zusätzlicher Software folgende Punkte beachten:

- Regelmäßiges Aktualisieren des Betriebssystems und aller installierten Programme
- Installation einer aktuellen Virenschutzsoftware mit regelmäßigen Updates und einer Personal Firewall (zum Beispiel SOPHOS AV)
- Installation von Software nur aus vertrauenswürdigen Quellen (z.B. Hersteller-Webseite)
- Es ist ausschließlich Software zu installieren für die die benötigten Lizenzen vorhanden sind.
- Deinstallation von Software, die nicht (mehr) benötigt wird

## 4.3. Verlust des Gerätes

Bei Verlust eines dienstlichen Mobilgerätes ist umgehend der zuständige IT-Administrator zu informieren. Ferner müssen unmittelbar alle Passwörter die auf dem verlorenen Gerät verwendet wurden geändert werden, um eine unberechtigte Nutzung der Zugänge auszuschließen. Sollten auf dem Geräte sensible Daten gespeichert gewesen sein, ist weiterhin eine Meldung an cert@tu-berlin.de zu senden.

## 4.4. Ausmusterung von nicht ausreichend abzusichernden Geräten

Mobile Geräte, die nicht mehr hinreichend abgesichert werden können, sollten nicht mehr zu dienstlichen Zwecken genutzt und fachgerecht ausgemustert werden.

# 5. Empfehlungen für Smartphones, Tablets etc.

Die folgenden Empfehlungen gelten für Smartphones, Tablets etc., die mit mobilen Betriebssystemen wie z.B. Android, iOS oder Windows Phone betrieben werden.

## 5.1. Absicherung des Gerätes gegen unbefugten Zugriff

Grundsätzlich sollten folgende Sicherheits-Regelungen beachtet werden:

- Sperrung des Gerätes mithilfe einer PIN bzw. eines Kennwortes
- Automatische Sperrung des Gerätes bei Inaktivität
- Der Festspeicher des Gerätes sollte verschlüsselt sein, falls Daten mit hohem Schutzbedarf darauf gespeichert werden; wenn zusätzlich zum Festspeicher Speicherkarten dauerhaft in dem Gerät eingesetzt werden, sollten diese ebenfalls verschlüsselt werden.
- Das Gerät sollte stets sicher verwahrt werden und es sollte keine Weitergabe des entsperrten Gerätes an Dritte erfolgen.
- Nicht benötigte Schnittstellen sollten bei Nichtnutzung deaktiviert werden (z.B. Bluetooth, WLAN, Entwicklermodus).
- Das Gerät sollte nicht über den USB-Anschluss an unbekannten Quellen angeschlossen werden; auch nicht um den Akku des Gerätes zu laden (z.B. öffentliche Ladestationen an Flughäfen).

- Bei der Verwendung von öffentlichen, ungesicherten Netzen (z.B. WLAN-Hotspots) sollte eine sichere verschlüsselte Verbindung genutzt werden (z.B. VPN).

## 5.2. Umgang mit Betriebssystem und Apps

Jeder Nutzer/jede Nutzerin sollte bei der Installation und Verwendung von Betriebssystem und Apps folgende Punkte beachten:

- Regelmäßiges Aktualisieren des Betriebssystems und aller installierten Apps
- Installation eines aktuellen Virenschutzprogramms sofern möglich
- Installation von Apps nur aus den offiziellen App-Stores (z.B. Google Play für Android bzw. App Store für iOS)
- Es dürfen ausschließlich ordnungsgemäß lizensierte Apps installiert werden.
- Überprüfung der Berechtigungen einer App bei Installation. Apps, die unnötigen Zugriff auf (dienstliche) E-Mails, Adressbuch oder Kalender erfordern, sollten vermieden werden.
- Löschung von Apps, die nicht (mehr) benötigt werden
- Jailbreak (iOS) oder Rooting (Android) von dienstlichen Geräten ist nicht gestattet

## 5.3. Abruf von E-Mails, Kalender, Adressbuch

Um dienstliche E-Mails, Kalender und Adressbuch zu synchronisieren, sollte ausschließlich der Exchange ActiveSync Client mit dem von tubIT betrieben Microsoft Exchange Server verwendet werden. Der Abruf der dienstlichen E-Mails über IMAP sollte vermieden werden. Die Nutzung von Exchange ActiveSync bietet die folgenden Möglichkeiten:
Überblick für den Nutzer/die Nutzerin, welche Mobilgeräte mit seinem Exchange Zugang verbunden sind

- Fernlöschen eines Gerätes bei Verlust durch den Nutzer /die Nutzerin
- Zentrale Anwendung der empfohlenen Sicherheitseinstellungen

## 5.4. Nutzung von Cloud-Diensten

Es sollten die zentral durch tubIT bereitgestellten Cloud-Dienste genutzt werden.

## 5.5. Verlust des Gerätes

Bei Verlust eines dienstlichen Mobilgerätes ist umgehend die Dienststelle und der zuständige IT-Betreuer zu informieren. Ferner müssen unmittelbar alle Passwörter die auf dem verlorenen Gerät verwendet wurden geändert werden, um eine unberechtigte Nutzung der Zugänge auszuschließen.
Der Nutzer/die Nutzerin kann bei Bedarf über Exchange ActiveSync selbständig sein Gerät aus der Ferne auf Werkseinstellungen zurücksetzen und damit sensible Daten auf dem Gerät löschen. Daten auf einer Speicherkarte werden u.U. nicht bei jedem Gerät gelöscht. Die Fernlöschung wird erst ausgeführt, wenn sich das Gerät mit dem Exchange-Server verbindet. Das Gerät muss dafür über eine Netzanbindung und ausreichend Batteriekapazität verfügen.
Eine Fernlöschung darf nur durch den Nutzer/die Nutzerin oder mit seiner/ihrer Zustimmung erfolgen.
Sollten auf dem Geräte sensible Daten gespeichert gewesen sein, ist weiterhin eine Meldung an cert@tu-berlin.de zu senden.

## 5.6. Ausmusterung von nicht ausreichend abzusichernden Geräten

Mobile Geräte, die nicht mehr hinreichend abgesichert werden können, sollten nicht mehr zu dienstlichen Zwecken genutzt werden und fachgerecht ausgemustert werden. Privatgeräte sind in ausschließlich privater Nutzung zu belassen.

# 6. Inkrafttreten

Diese Leitlinie wurde von der CIO der TU Berlin beschlossen und tritt mit Beschluss in Kraft.