BEUTH HOCHSCHULE
FÜR TECHNIK
BERLIN

University of Applied Sciences

Empfehlungen zum dienstlichen Umgang mit Mobilgeräten

Laptop, Smartphone, Tablet & Co.

Hochschulrechenzentrum

Mai 2020



> Inhalt

1 Einleitung 2
2 Geltungsbereich 3
2.1 Dienstliche Mobilgeräte 3
2.2 Private Mobilgeräte 3
3 Datenkategorien und ihre Eignung zur mobilen Nutzung 4
4 Richtlinie für Laptops 5
4.1 Absicherung des Gerätes gegen unbefugten Zugriff 5
4.2 Umgang mit Betriebssystem und Software 5
4.3 Nutzung von Cloud-Diensten 5
4.4 Verlust des Gerätes 5
4.5 Ausmusterung von nicht ausreichend abzusichernden Geräten 5
5 Richtlinie für Smartphones, Tablets etc. 6
5.1 Absicherung des Gerätes gegen unbefugten Zugriff 6
5.2 Umgang mit Betriebssystem und Apps 6
5.3 Abruf von E-Mails, Kalender, Adressbuch 6
5.4 Nutzung von Cloud-Diensten 6
5.5 Verlust des Gerätes 7
5.6 Ausmusterung von nicht ausreichend abzusichernden Geräten 7
6 Weiterführende Dokumente 8
> Impressum 9

1 Einleitung

Dieser Leitfaden beinhaltet grundsätzliche Empfehlungen für alle Mitglieder und Angehörige der Beuth Hochschule für Technik Berlin, die zu dienstlichen Zwecken mobile Endgeräte (u.a. Laptops, Smartphones, Tablet-PCs) einsetzen. Dieser Leitfaden soll der Sensibilisierung dienen.

Mobilgeräte werden immer kleiner, leistungsfähiger und sind bei vielen Mitarbeitern nicht mehr aus dem Alltag wegzudenken. Die Benutzung solcher Geräte hat sich in den letzten Jahren vervielfacht und dieser Trend wird sich weiter fortsetzen.

Auf Laptops kommen dafür herkömmliche Desktop-Betriebssysteme (v.a. Windows und OS X) zum Einsatz und es lassen sich die dort üblichen Sicherheitsregelungen umsetzen. Auf Smartphones und Tablets laufen dagegen spezielle, an das Gerät angepasste Betriebssysteme (v.a. Android, iOS und Windows Phone), deren Bedienung sich von Desktop-Betriebssystemen unterscheidet. Heutige Smartphones werden hauptsächlich für den Consumer-Bereich entwickelt und sind auf einfache Benutzung ausgelegt, daher unterstützen sie teilweise nur rudimentäre Sicherheitsfeatures.

Darüber hinaus birgt die Nutzung von Mobilgeräten erhöhte Sicherheitsrisiken:

- 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

Die Sicherheitsrisiken auf dienstlichen und privaten mobilen Endgeräten liegen in der Verantwortung des Nutzers. Der Nutzer eines mobilen Endgerätes ist ungeachtet der vom HRZ bereitgestellten Sicherheitsfeature verantwortlich für:

- Schutz vor Diebstahl der mobilen Endgeräte
- Die Vertraulichkeit der Daten auf mobilen Endgeräten
- Die Sicherung der Daten von mobilen Endgeräten
- Schutz vor Schadsoftware und deren Übertragung in die Infrastruktur der Beuth Hochschule
- Lizenzrechtlichen Ansprüchen bei eigener Installation von Software

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

2 Geltungsbereich

Die Empfehlungen dieses Dokuments richten sich an alle Mitglieder und Angehörige der Beuth Hochschule, die Mobilgeräte zu dienstlichen Zwecken nutzen. Sie gelten auch für dienstlich genutzte Privatgeräte, sofern diese eingesetzt werden.

Alle Nutzer eines Mobilgerätes sind für die Absicherung ihres Gerätes und der darauf befindlichen Daten in der Regel selbst verantwortlich! Durch den Nutzer muss sichergestellt werden, dass eine qualifizierte Person die Verantwortung für die sachgerechte Betreuung übernimmt. Dies kann grundsätzlich auch der Nutzer selbst sein, alternativ kann die Administration durch einen ausgewiesenen IT-Administrator der ihn DV-technisch betreuenden Einrichtung.

2.1 Dienstliche Mobilgeräte

Für dienstliche Mobilgeräte wird die Umsetzung der in diesem Leitfaden aufgeführten Empfehlungen dringend angeraten. Die 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 (vgl. 5.1) 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 (vgl. 5.1) automatisch aktiviert.

Es wird darauf hingewiesen, dass die dienstliche Nutzung von Privatgeräten, neben den Gefahren für die Informationssicherheit der Beuth Hochschule, auch ein Risiko für die Daten des Nutzers darstellt, da unter anderem die fehlerfreie Funktion der Geräte und des Verwaltungssystems (Microsoft Exchange etc.) nicht garantiert werden kann. Im Falle eines Defektes oder Anwenderfehlers kann es zum Verlust der auf dem Gerät gespeicherten Daten kommen. Von der dienstlichen Nutzung privater Geräte wird daher abgeraten. Die Beuth Hochschule schließt diesbezüglich sämtliche Haftungsansprüche aus.

3 Datenkategorien und ihre Eignung zur mobilen Nutzung

Im Allgemeinen sollten stets so wenige Daten wie möglich auf Mobilgeräten gespeichert werden. Zusätzlich sind bestimmte Daten für die Speicherung zur mobilen Nutzung von vorneherein ungeeignet. Für die Entscheidung, welche Daten auf Mobilgeräten gespeichert werden können, bildet ihr Schutzbedarf die grundlegende Richtschnur. Dazu wurde an der Beuth Hochschule eine Schutzbedarfsanalyse entwickelt, die hierzu herangezogen werden sollte. Die Schutzbedarfsanalyse weist lediglich auf einen typischen Schutzbedarf hin, der tatsächliche Bedarf ist jedoch vom Inhalt der Daten abhängig und kann vom Empfohlenen abweichen.

Daten lassen sich in die folgenden Kategorien einteilen:

Kategorie	**Hinweis auf typischen Schutzbedarf**
Daten, die aus öffentlich zugänglichen Quellen stammen	Keiner
Dienstliche (nicht wissenschaftliche) Daten (z.B. aus den Bereichen Verwaltung und Lehre)	Normal bis sehr hoch
Wissenschaftliche Daten (z.B. Untersuchungsergebnisse, Messreihen)	Normal bis sehr hoch
Personalaktendaten, Personalvertretungsdaten	Sehr hoch
Private Daten (z.B. Kontaktdaten von Freunden)	Normal bis sehr hoch

In jedem Fall sind die folgenden Aspekte zu beachten:

- Für personenbezogene Daten (sowohl mit dienstlichem als auch privatem Bezug) gelten die Bestimmungen des Datenschutzes
- Auch Daten ohne Personenbezug können einen sehr hohen Schutzbedarf haben (zum Beispiel auf Grund von Geheimhaltungsvereinbarungen).

Der Schutzbedarf der Daten wird grundsätzlich hinsichtlich der drei Schutzziele Verfügbarkeit, Integrität und Vertraulichkeit differenziert bestimmt. Entsprechend differenziert müssen Vorkehrungen zur Sicherheit der Daten getroffen werden. Aus dem Schutzbedarf der Daten folgt zwingend die Eignung oder Nicht-Eignung zur Speicherung auf dem Mobilgerät:

Schutzbedarf	**Eignung für die Ablage**
Daten mit keinem bis normalen Schutzbedarf	Ja
Daten mit hohem Schutzbedarf	Nur verschlüsselt
Daten mit sehr hohem Schutzbedarf	nein

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 eines sicheren Kennwortes (mind. 12 Zeichen; Groß- /Kleinschreibung; Zahlen; Sonderzeichen)
- Automatische Sperrung des Gerätes bei Inaktivität
- Die Festplatte des Gerätes sollte verschlüsselt sein, falls Daten mit hohem Schutzbedarf darauf (vgl. 3) gespeichert werden.
- 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 sollte bei der Installation und Verwendung von Betriebssystem und zusätzlicher Software folgende Punkte beachten:

Regelmäßiges Aktualisieren des Betriebssystems und aller installierten Programme
Installation des vom HRZ empfohlenen Virenschutzes und einer Personal Firewall.
Installation von Software (falls gestattet) nur aus vertrauenswürdigen Quellen (z.B. Hersteller-Webseite)
Überprüfung der Nutzungsbedingungen einer Software. Software, die nur für den Privatgebrauch kostenfrei zur Verfügung steht, muss für kommerzielle Nutzung, Forschung und dienstliche Zwecke gegebenenfalls ordnungsgemäß lizenziert werden.
Deinstallation von Software, die nicht (mehr) benötigt wird

4.3 Nutzung von Cloud-Diensten

Cloud-Dienste sollten ausschließlich mit Verschlüsselung aller Daten verwendet werden.

4.4 Verlust des Gerätes

Bei Verlust eines dienstlichen Mobilgerätes sollte umgehend die DV-technisch betreuende Einrichtung informiert werden, die das Gerät administriert (meist HRZ oder IT-Administrator des Fachbereiches). Ferner sollte der Nutzer unmittelbar seine Passwörter von verwendeten Kennungen der Beuth Hochschule ändern, um eine unberechtigte Nutzung seines Zuganges auszuschließen.

4.5 Ausmusterung von nicht ausreichend abzusichernden Geräten

Mobilgeräte, die weder durch die DV-technisch betreuende Einrichtung noch durch den Nutzer hinreichend abgesichert werden können, sollten nicht mehr zu dienstlichen Zwecken genutzt werden und fachgerecht ausgemustert werden (sichere Löschung der darauf vorhandenen Daten, Entsorgung über zuständige HRZ oder Fachbereich).

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 (vgl. 3) 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 sollte bei der Installation und Verwendung von Betriebssystem und Apps folgende Punkte beachten:

- Regelmäßiges Aktualisieren des Betriebssystems und aller installierten Apps Installation des vom HRZ empfohlenen Virenschutzes sofern möglich
- Installation von Apps nur aus den offiziellen App-Stores (z.B. Google Play für Android bzw. App Store für iOS)
- Überprüfung der Nutzungsbedingungen einer App. Apps, die nur für den Privatgebrauch kostenfrei zur Verfügung stehen, müssen für kommerzielle Nutzung, Forschung und dienstliche Zwecke gegebenenfalls ordnungsgemäß lizensiert werden.
- Überprüfung der Berechtigungen einer App bei Installation. Apps, die unnötigen Zugriff auf (dienstliche) E-Mails, Adressbuch oder Kalender erfordern, sollten vermieden werden (z.B. WhatsApp).
- Löschung von Apps, die nicht (mehr) benötigt werden.
- Verzicht auf Jailbreak (iOS) oder Rooting (Android)

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 durch das HRZ betriebenen Microsoft Exchange Server verwendet werden. Der Abruf der dienstlichen E-Mails über IMAP / POP3 sollte vermieden werden. Die Nutzung von Exchange ActiveSync bietet die folgenden Möglichkeiten:

- Überblick für den Nutzer, welche Mobilgeräte mit seinem Exchange Zugang verbunden sind
- Fernlöschen einen Geräts bei Verlust durch den Nutzer
- Zentrale Anwendung der vom HRZ empfohlenen Sicherheitseinstellungen
- Konfigurierbare Sicherheitseinstellungen für verschieden Nutzergruppen

5.4 Nutzung von Cloud-Diensten

Cloud-Dienste sollten ausschließlich mit Verschlüsselung aller Daten verwendet werden.

5.5 Verlust des Gerätes

Bei Verlust eines dienstlichen Mobilgerätes sollte umgehend die DV-technisch betreuende Einrichtung informiert werden, die das Gerät administriert (meist HRZ oder Fachbereich). Ferner sollte der Nutzer unmittelbar seine Passwörter von verwendeten Kennungen der Beuth Hochschule ändern, um eine unberechtigte Nutzung auszuschließen.

Der Nutzer 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 Benutzer oder mit seiner Zustimmung erfolgen.

5.6 Ausmusterung von nicht ausreichend abzusichernden Geräten

Mobilgeräte, die weder durch eine DV-technisch betreuende Einrichtung noch durch den Nutzer hinreichend abgesichert werden können, sollten nicht mehr zu dienstlichen Zwecken oder mit dienstlichen Daten genutzt werden und fachgerecht ausgemustert werden (sichere Löschung der darauf vorhandenen Daten, Entsorgung über HRZ oder Fachbereich). Privatgeräte sind in ausschließlich privater Nutzung zu belassen.

6 Weiterführende Dokumente

[1] „Bring Your Own Device (BYOD) - Rechtliche Probleme und Handlungsempfehlungen“
https://www.dfn.de/fileadmin/3Beratung/Recht/handlungsempfehlungen/Bring_Your_Own_Device.pdf

[2] „DFN Infobrief Recht“,

Kapitel „Die rechtlichen Herausforderungen von „Bring Your Own Device“ – Lifestyle contra Sicherheit“

https://www.dfn.de/fileadmin/3Beratung/Recht/1infobriefearchiv/2015/Infobrief_Recht_04-2015.pdf

Impressum

Beuth Hochschule für Technik Berlin

Hochschulrechenzentrum