Fachhochschule Kaiserslautern
University of Applied Sciences

Betriebswirtschaft
Zweibrücken

Handout

Thema:

IT-Security bei mobile devices

Studierende

Baumann, Ron	861272
Schmitt, Max	859021

Korrektor:

Prof. Dipl.-Ing. Klaus Knopper

Abgabedatum:

22.11.2013

Inhaltsverzeichnis

Abbildungsverzeichnis

1. Einleitung

Mobile Endgeräte erfreuen sich großer Beliebtheit und finden Ihre Anwendung sowohl im privaten wie auch im geschäftlichen Einsatz. In diesem Zusammenhang ist der Begriff ubiquitous computing zu nennen, dem Wunsch nach ständig aktuellen verfügbaren Informationen.[1]

Die Universität Lübeck definiert ubiquitous computing in der folgenden Art und Weise:

„Unter dem Begriff "Ubiquitous Computing" wird die Allgegenwärtigkeit von kleinsten, miteinander drahtlos vernetzten Computern verstanden, die unsichtbar in beliebige Alltagsgegenstände eingebaut werden oder an diese angeheftet werden können.“[2]

Diese Allgegenwärtigkeit bietet jedoch auch eine Vielzahl von Schwachstellen, sodass sich die Frage nach dem Schutz von vertraulichen, persönlichen und geschäftlichen Daten stellt. Dabei stellt die Heterogenität der Geräteklassen (Tablet, Smartphone) auf der einen Seite und die unterschiedlichen Betriebssysteme (iOS, Android) auf der anderen Seite ein Erschwernis dar, welches ganzheitlich bei der Konzeptionierung Beachtung finden sollte.[3]

[1] Vgl. https://www.bsi.bund.de/DE/Publikationen/Broschueren/mobile/index_htm.html.
[2] http://www.iti.uni-luebeck.de/index.php?id=uc.
[3] Vgl. https://www.bsi.bund.de/DE/Publikationen/Broschueren/mobile/index_htm.html.

Mobile Endgeräte –Abgrenzung

Um ein Verständnis zum Begriff der mobilen Endgeräte zu erhalten, wird im Folgenden der Begriff verdeutlicht. Mobile Endgeräte besitzen nach der Definition des Bundesamtes für Sicherheit in der Informationstechnik (BSI) spezielle Betriebssysteme sowie ein verbrauchsreduzierendes Energiemanagement. Zudem verfügen diese über mehrere Kommunikationsschnittstellen wie beispielsweise GSM, Bluetooth oder WLAN. Unter Betrachtung dieser Schnittstellen könnten auch Notebooks inkludiert werden, was im Rahmen dieser Ausarbeitung nicht eindeutig geklärt wird.[4]

Als letzte Eigenschaft mobiler Endgeräte wird die virtuelle Speicherverwaltung aufgeführt, die den jeweiligen Anwendungen einen adressierten Speicher zuweist, sobald diese aktiv genutzt werden.[5]

[4] Vgl. https://www.bsi.bund.de/DE/Publikationen/Broschueren/mobile/index_htm.html.
[5] Vgl. ebenda.

2. Aspekte der Sicherheit

Unter dem Kapitel Aspekte der Sicherheit werden drei verschiedene Betrachtungen subsumiert. Zum Ersten wird ein spezifischer Gerätetyp mit seinen Komponenten betrachtet. Darauf aufbauend folgt die Betrachtung des gesamten Kommunikationsweges sowie die abschließende Fokussierung auf die unterschiedlichen Geräteklassen.

1.1 Gerätetyp

Innerhalb eines spezifischen Gerätetyps kann ein mobiles Endgerät in folgende Kriterien unterteilt werden:

a) Hardware: CPU, RAM.
b) Software: Betriebssystem, Kommunikations- und Anwendungssoftware.
c) Schnittstellen: Funk (LTE, UMTS, WLAN, Bluetooth, NFC). Kabelgebunden (USB).
d) Speichermedien: SD- / MMC-Karte, OTA.[6]

[6] Vgl. https://www.bsi.bund.de/DE/Publikationen/Broschueren/mobile/index_htm.html.

1.2 Kommunikationsweg

Entlang eines Kommunikationsweges bestehen unterschiedliche sicherheitsrelevante Aspekte, welche nachstehend stichwortartig aufgelistet werden:

a) Verbindung zu einem WLAN-Router.
b) Kommunikation mit einem anderen mobilen Endgerät über Bluetooth.
c) Sprachkommunikation mit einem anderen mobilen Endgerät.
d) Besuch einer Website.
e) Besuch eines App-Stores.
f) Öffnung einer VPN-Verbindung.[7]

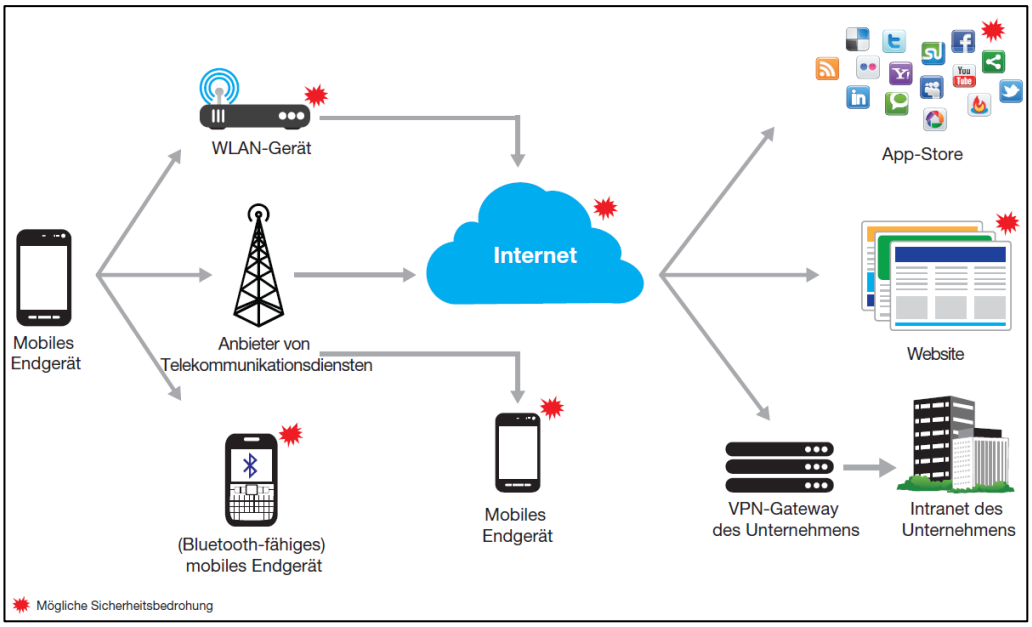

Abbildung 1: Aspekte der Sicherheit - Kommunikationswege[8]

[7] Vgl. http://public.dhe.ibm.com/common/ssi/ecm/de/sew03027dede/SEW03027DEDE.PDF.

[8] http://public.dhe.ibm.com/common/ssi/ecm/de/sew03027dede/SEW03027DEDE.PDF.

1.3 Geräteklassen

Nach der Definition eines einzelnen Gerätetyps sowie der Betrachtung des gesamten Kommunikationsweges erfolgt in einer kurzen Fassung die abschließende Aufführung der Geräteklassen, welche an dieser Stelle nicht weiter thematisiert werden.

a) Handy.
b) PDA / Communicator.
c) Spielekonsolen.
d) Smartphones.
e) Notebooks.
f) Tablets.

2 Sicherheitsverfahren und Gefahren

In dem folgenden Kapitel werden die aktuellen Sicherheitsverfahren, die potenziellen Gefahren sowie abschließend einige Beispiele aktueller Bedrohungen und ergriffener Sicherungsmaßnahmen dargestellt.

2.1 Aktuelle Sicherheitsverfahren

Im Bereich der aktuellen Sicherheitsverfahren werden vier Hauptpunkte adressiert, wobei diese Auflistung keinen Anspruch auf Vollständigkeit erhebt:

a) Authentisierung (Benutzername und Passwort, ggf. biometrische Verfahren).
b) Sandbox-Verfahren: Kontrolle und Unterbindung von bestimmten Zugriffen (Herstellen einer Internetverbindung).
c) Zugriffsabfrage: Bestätigung des Zugriffs auf Kontakte, Kalender und Ortungsfunktionen.
d) Verschlüsselung des Dateisystems.[9]

[9] Vgl. https://www.bsi.bund.de/DE/Publikationen/Broschueren/mobile/index_htm.html.

2.2 Potenzielle Gefahren

Die potenziellen Gefahren werden zuerst stichwortartig illustriert und im Folgenden auszugsweise verdeutlicht:

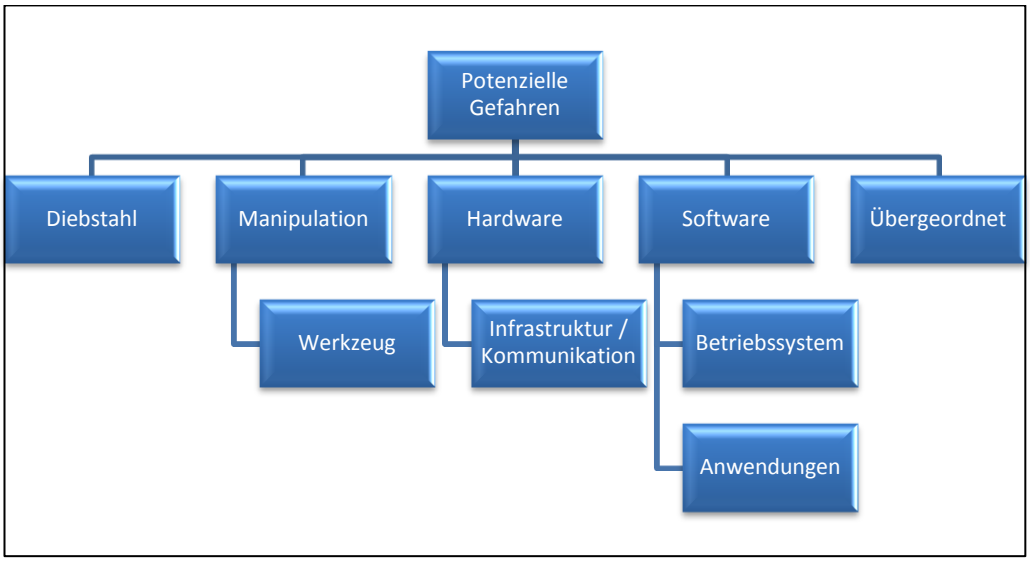

Abbildung 2: Potenzielle Gefahren[10]

a) Manipulation: Ein Dieb könnte das mobile Endgerät stehlen, Schadcode einbauen und dem Besitzer ohne Kenntnis über die Modifikation zurückgeben. Dadurch könnte das Smartphone beispielsweise Nachrichten versenden, ohne dass der Besitzer dieses bemerkt.
b) Im Bereich der Hardware respektive der Infrastruktur wäre an dieser Stelle die sog. Man-in-the-middle Attacke aufzuführen.
c) Unter der Kategorie Software →Betriebssysteme könnte das Sicherheitsleck des kopierten Fingerabdrucks zum Entsperren des neuen iPhones 5s verstanden werden.[11]

[10] Eigene Erstellung.
[11] Vgl. https://www.bsi.bund.de/DE/Publikationen/Broschueren/mobile/index_htm.html.

d) Bei den Anwendungen in der Kategorie Software wäre an Programmierfehler zu denken, die ausgenutzt werden, um Schadcode in das mobile Endgerät zu übertragen.

e) Die Kategorie „Übergeordnet“ betrachtet die allgemeine Sichtweise auf Viren, Trojaner und sonstige Malware, aber auch die Aufzeichnung von Bewegungsprofilen sowie den Zugriff auf Unternehmensressourcen.[12]

2.3 Aktuell vs. Potenziell

Die im Folgenden aufgeführte Darstellung zeigt in Kurzfassung, welche aktuellen Beispiele im Rahmen der Sicherheitsmaßnahmen bzw. der Gefahren existieren. Da diese jedoch ohne eine weitere Erläuterung wenig aussagekräftig ist, folgt dieser Darstellungsform eine kurze Erläuterung:

		
Master- Key		✘
Lockout / Norton	✓ ?	
Geschenke		✘
SNS-over-IP	✓ ?	
trust | me	✓	

Abbildung 3: Sicherheitsmaßnahmen / Gefahren - Beispiele[13]

[12] Vgl. https://www.bsi.bund.de/DE/Publikationen/Broschueren/mobile/index_htm.html.
[13] Eigene Erstellung.

a) Master-Key: *„Durch diese Sicherheitslücke können installierte Apps ohne Zustimmung der Anwender verändert werden: Cyberkriminelle können legitime Apps "aktualisieren" und darin bösartigen Code einfügen, ohne Original-Signaturschlüssel der Entwickler.“*[14]

b) Lookout / Norton: Diese mobilen Sicherheitstools bieten eine Geräteortung, Prüfung der Aktualität der Apps, Back-up von Kontakten.
Fraglich ist nur, ob diese Applikationen wirklich einen Mehrwert schaffen, da diese Funktionalität am Beispiel eines iPhones bereits seitens des Herstellers angeboten wird.[15]

c) Geschenke: Eine Sicherheitsfirma führte einen Test durch, indem CDs an Passanten verteilt wurden. Diese CDs waren modifiziert, und zwar in der Form, dass diese einen bestimmten Server kontaktierten. So konnte festgestellt werden, dass Mitarbeiter vieler großer Banken die CD an Ihrem Arbeitsplatz eingelegt hatten.[16]

d) SNS over IP (=sichere netzübergreifende Sprachkommunikation): *„SNS over IP soll eine sichere VoIP-Sprachkommunikation über öffentliche Netze etwa auf Basis von WLAN oder UMTS ermöglichen und nutzt dafür den bereits für SNS im Mobilfunk eingesetzten Krypto-Chip. Das BSI hebt hervor, dass sich SNS over IP als abhörsicherer Ersatz von DECT-Schnurlostelefonen für die gebäudeinterne Telefonie eignet.“*[17]

e) trust me (trusted mobile equipment): Betrieb mehrerer virtualisierter Smartphones auf einem Gerät.[18]

---

[14] http://www.securitymanager.de/news/details-ungebremster_anstieg_bei_mobilen_bedrohungen.html.
[15] Vgl. https://www.lookout.com/de/mobile-threat-network.
[16] Vgl. http://www.drivelock.de/portals/0/files/public/whitepaper/Threats_from_Mobile_Devices_(DE).pdf.
[17] http://www.heise.de/ix/meldung/BSI-spezifiziert-verschluesselte-Internet-Telefonie-1465676.html.
[18] Vgl. http://www.aisec.fraunhofer.de/de/medien-und-presse/pressemitteilungen/2013/trust-me.html

3. Sicherheitskonzept

Aufgrund der Recherche wird im Folgenden das eigens erstellte Sicherheitskonzept bzw. dessen Prozess der Entstehung dokumentiert, welches an dieser Stelle nicht weiter ausgeführt wird, um dem Umfang dieser wissenschaftlichen Arbeit gerecht zu werden.

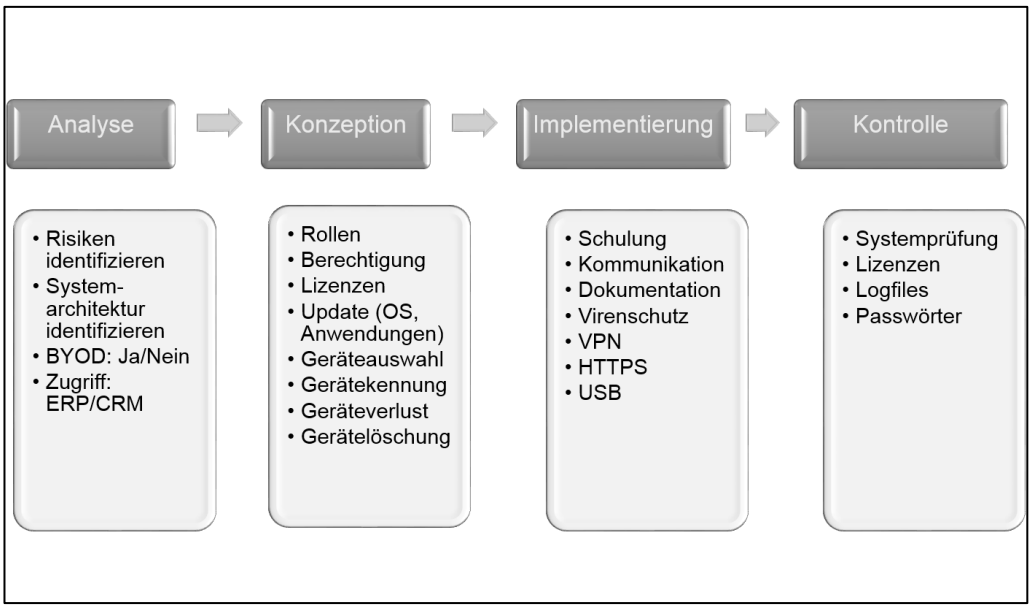

Abbildung 4: Sicherheitskonzept[19] [20]

[19] Eigene Erstellung.
[20] https://www.bsi.bund.de/DE/Publikationen/Broschueren/mobile/index_htm.html.

4. Chancen durch Förderung von BYOD aus Unternehmenssicht [21]

- Gesteigerte Flexibilität und Mobilität
- Mitarbeiter können ihre Aufgaben besser ausführen (Zufriedenheit steigt)
- Produktivitätssteigerung
- Kostenreduktion

➔ BYOD bietet großes Potenzial für Unternehmen

4.1 Risiken durch Förderung von BYOD aus Unternehmenssicht [22]

- Datenverlust
- Datenschutz
- Angriff auf Unternehmensprozesse
- Total Costs of Ownership

➔ Private Mobilgeräte stellen großes Sicherheitsrisiko für Unternehmen dar

[21] Vgl. http://public.dhe.ibm.com/common/ssi/ecm/de/sew03027dede/SEW03027DEDE.PDF

[22] Vgl. http://www.iais.fraunhofer.de/fileadmin/user_upload/Abteilungen/ART/pdfs/IAIS_ART_BYOD_Poster_BringYourOwnDevice_v1.0.3.pdf

4.2 IMSI Catcher [23]

- Man in the Middle Angriff
- Simuliert eine reguläre Funkzelle aus dem GSM Netz
- Handy sucht sich immer stärkste Zelle in der Nähe
- Einseitige Authentifikation bei GSM (Handy muss Zelle durch IMSI + IMEI beweisen, dass es echt ist, nicht andersrum)
- z.B. Abgehende Gespräche abhören

4.3 Wie kann man sich schützen?

- App-Berechtigungen beachten und individuell verwalten
- End-To-End Verschlüsselung
    - Silent Circle (iOS + Android; kostenpflichtig)
        - Silent Phone
        - Silent Text
        - www.silentcircle.com
    - Whisper Systems (Android; kostenlos; aufgekauft durch Twitter, Open Source)
        - RedPhone
        - SecureText
        - www.whispersystems.org
- CyanogenMod
    - Custom Firmware für Android
    - Verschlüsselte SMS
    - Ohne “Gapps” (Google Apps und Framework)
    - www.cyanogenmod.org

[23] Vgl. http://www.datenschutz.hessen.de/dapoju01.htm

5. Mobile Device Management [24] [25]

- Verwalten von privaten und geschäftlichen Mobilgeräten
    - Geräteinformationen abrufen
    - Geräte lokalisieren
    - „Unsichere“ Geräte ausschließen (z. B. Erkennung von Jailbreak und Root)
    - Sperren von Kamera, App Stores oder bestimmten Apps
    - Geräte konfigurieren (z. B. WLAN-Zugang und Apps einrichten)
    - Bestimmte Daten, Apps oder das komplette Gerät remote löschen

➔ MDM erlaubt Verwalten von geschäftlichen und privaten Mobilgeräten und gewährleistet somit die Umsetzung des erarbeiteten Sicherheitskonzepts aber:

- Einschränkungen der privaten Mobilgeräte der Mitarbeiter
- Keine 100 % Sicherheit

[24] Vgl. http://www.apptec360.com/mobile_device_management.html.
[25] Vgl. https://www.citrix.de/products/xenmobile/overview.html.

6. Weitere Links

Netstat für iPhone, iPod touch und iPad im App Store von iTunes http://tinyurl.com/ohkyz6e

Sitzen die NSA-Späher am Pariser Platz? http://tinyurl.com/qhvo9pw

The body-worn “IMSI catcher” for all your covert phone snooping needs http://tinyurl.com/lczwmfx

Literaturverzeichnis

Bedrohungen durch mobile Geräte - Wie Sie Ihre vertraulichen Daten schützen. [Online] [Zitat vom: 20. 11 2013.] http://www.drivelock.de/portals/0/files/public/whitepaper/Threats_from_Mobile_Devices_(DE).pdf.

Eckert, C. trust | me – Sichere mobile Endgeräte für mehr Sicherheit in Firmennetzen. *Fraunhofer AISEC.* [Online] [Zitat vom: 20. 11 2013.] http://www.aisec.fraunhofer.de/de/medien-und-presse/pressemitteilungen/2013/trust-me.html.

Gärtner, M. 4. IT-Grundschutz-Tag 2013. *Bundesamt für Sicherheit in der Informationstechnik.* [Online] [Zitat vom: 20. 11 2013.] https://www.bsi.bund.de/SharedDocs/Termine/DE/2013/4_IT_Grundschutztag_2013.html.

—. Mobile Endgeräte und mobile Applikationen: Sicherheitsgefährdungen und Schutzmaßnahmen. *Bundesamt für sicherheit in der Informationstechnik.* [Online] [Zitat vom: 20. 11 2013.] https://www.bsi.bund.de/DE/Publikationen/Broschueren/mobile/index_htm.html.

Heise, C. BSI spezifiziert verschlüsselte Internet-Telefonie. *heise online.* [Online] [Zitat vom: 20. 11 2013.] http://www.heise.de/ix/meldung/BSI-spezifiziert-verschluesselte-Internet-Telefonie-1465676.html.

Kao,, I.-L. Sicherheit mobiler Endgeräteim Geschäftsumfeld. [Online] [Zitat vom: 20. 11 2013.] http://public.dhe.ibm.com/common/ssi/ecm/de/sew03027dede/SEW03027DEDE.PDF.

Lookout. NAHTLOSE SICHERHEIT FÜR SMARTPHONES UND TABLETS. *Lookout.* [Online] [Zitat vom: 20. 11 2013.] https://www.lookout.com/de/mobile-threat-network.

Maehle, E. Ubiquitous Computing. *Universität zu Lübeck.* [Online] [Zitat vom: 20. 11 2013.] http://www.iti.uni-luebeck.de/index.php?id=uc.

Zschau, O. Ungebremster Anstieg bei mobilen Bedrohungen. *securitymanager.de.* [Online] [Zitat vom: 20. 11 2013.] http://www.securitymanager.de/news/details-ungebremster_anstieg_bei_mobilen_bedrohungen.html.