DIVSI
Deutsches Institut
für Vertrauen und
Sicherheit im Internet

DIVSI Studie
Wissenswertes über den Umgang mit Smartphones

DIVSI Studie
Wissenswertes über den Umgang mit Smartphones

Fraunhofer AISEC

DIVSI
Deutsches Institut für Vertrauen und Sicherheit im Internet

Hamburg, Oktober 2014

IMPRESSUM

Deutsches Institut für
Vertrauen und Sicherheit
im Internet (DIVSI)
Mittelweg 110 B
20149 Hamburg
www.divsi.de

Fraunhofer AISEC
Fraunhofer-Institut für Angewandte
und Integrierte Sicherheit
Parkring 4
85748 Garching bei München
www.aisec.fraunhofer.de

ISSN 2196-6729

Inhaltsverzeichnis

Vorwort

Claudia Eckert
Leiterin des
Fraunhofer-Instituts
AISEC

Liebe Leserinnen und Leser,
Always-in, also nahezu ununterbrochen über das Internet verbunden zu sein, ist für viele Menschen heute eine Selbstverständlichkeit. Möglich wird dies durch die allgegenwärtigen Smartphones, wie Apple iPhones, Android-basierte mobile Geräte, BlackBerrys oder auch Windows Phones, die aus dem privaten und beruflichen Alltag nicht mehr wegzudenken sind. Smartphones ermöglichen uns, jederzeit, beispielsweise über soziale Netze, Kontakt zu Freunden, Partnern oder auch Geschäftskunden zu halten, uns wichtig erscheinende Augenblicke in Bild und Ton festzuhalten und sofort mit anderen zu teilen, mobil einzukaufen und natürlich auch klassisch Mails und SMS zu versenden. Mittels Smartphones lassen sich Geräte zum Beispiel der Heimumgebung von Ferne kontrollieren, Türen öffnen und schließen oder auch Vitalfunktionen kontinuierlich überwachen. Die fast unüberschaubare Vielfalt an Apps, die häufig kostenlos oder gegen geringe Gebühr auf die Geräte geladen werden können, bringt uns den Planetenhimmel greifbar nah, weist uns in Form von Navigationshilfen den Weg oder hilft uns mit diversen Multimedia-Angeboten Wartezeiten, zu verkürzen.

Die globale Währung in dieser Smartphone-Ökonomie sind die Daten, die wir über uns, unsere Vorlieben, Kontakte, Aufenthaltsorte etc. preisgeben. Doch welche dieser Daten geben wir eigentlich bewusst und freiwillig preis, bzw. welche Daten werden ohne unser Wissen im Hintergrund automatisch erhoben und verarbeitet? Welche Möglichkeiten habe ich eigentlich, um einzuschreiten, wenn ich nicht möchte, dass bestimmte Daten vom Smartphone erfasst oder gar außerhalb meines Smartphones gespeichert und zugänglich gemacht werden?

Solche Fragen waren der Ausgangspunkt für die Untersuchungen, deren Ergebnisse in der vorliegenden, von Fraunhofer AISEC im Auftrag des Deutschen Instituts für Vertrauen und Sicherheit im Internet (DIVSI) durchgeführten Studie zusammengefasst sind. Um selbstbestimmt und souverän über die Preisgabe von sensiblen Daten bestimmen zu können, ist es notwendig, zu verstehen, welche Daten wann erhoben werden, was mit diesen Daten geschieht und welche Wahlmöglichkeiten bestehen, diese Datenerhebung und Weitergabe zu kontrollieren, bei Bedarf zu unterbinden oder auch nur gezielt einzuschränken. Auch ist es wichtig, zu verstehen, welche möglicherweise unerwünschten Auswirkungen eine bewusste Deaktivierung von Diensten haben kann, aber natürlich auch, was es bedeutet bzw. welche Konsequenzen es haben kann, einer App bestimmte Zugriffsrechte zu gewähren.

Das Ziel der vorliegenden Studie war es, auf diese Fragen eine Antwort zu finden und damit Nutzerinnen und Nutzern von Smartphones für diese Thematik zu sensibilisieren und Hilfestellungen mit dem Umgang der Daten auf den Smartphones zu geben. Die Studie versteht sich als einen Beitrag zur Erhöhung der digitalen Souveränität der Bürger; sie zielt nicht darauf ab, Verbote oder Gebote zu postulieren.

Wir wünschen den Lesern eine anregende und interessante Lektüre.

Prof. Dr. Claudia Eckert — München, im Oktober 2014

1. Einleitung

In der heutigen Zeit stehen der maximalen Mobilität in Privat- und Berufsleben die Bedenken über die Sicherheit der auf dem mobilen Gerät verarbeiteten und gespeicherten Daten gegenüber. Während die Benutzung eines Smartphones ganz gleich mit welchem Betriebssystem aufgrund der intuitiven Benutzeroberfläche kinderleicht ist, fehlt der großen Mehrheit der Smartphone-Nutzer das Verständnis über die komplexen Abläufe im Hintergrund. Welche Daten (E-Mails, Fotos, Nutzungsdaten etc.) verarbeitet und gespeichert werden und welche Kontrollmöglichkeiten ein Nutzer darüber besitzt, ist vielen Nutzern kaum bewusst.

Die vorliegende Studie verfolgt das vordringliche Ziel, ein Bewusstsein dafür zu schaffen, welchen Einfluss über die Weitergabe und Verarbeitung von Daten der durchschnittliche Nutzer von Smartphones besitzt. Untersucht wurde, ob, und wenn ja, welche technisch einfach umzusetzenden Möglichkeiten dem Nutzer innerhalb der Standardeinstellungen der jeweiligen Betriebssysteme zur Verfügung stehen. Die Basis zur Beantwortung der Fragen bildeten deshalb frei verfügbare technische Dokumentationen, die die jeweiligen Hersteller ihren Nutzern zur Verfügung stellen, sowie Geräte der verschiedenen Hersteller, um die Angaben zu validieren. Zudem wurden stichprobenhaft technische Untersuchungen an den Geräten durchgeführt. Die Studie hat explizit nicht das Ziel, die gegebenen Möglichkeiten der Betriebssysteme zu umgehen und durch Einsatz von Know-how, das einem durchschnittlichen Nutzer nicht zur Verfügung steht, zu verändern.

Vielmehr geht es in der Studie darum, anhand der verfügbaren Dokumentationen der Hersteller aufzuzeigen, in welcher Weise die Daten der Nutzer verarbeitet und gespeichert werden. Auch hier war das vordringliche Ziel, ein Bewusstsein dafür zu schaffen, welche Daten von den Systemen gespeichert und verarbeitet werden. Um nachvollziehbare und vergleichbare Ergebnisse zu ermitteln, basieren die durchgeführten technischen Untersuchungen auf einer festgelegten (und von Nutzern nachvollziehbaren) Minimaleinstellung von aktivierten Diensten für jedes der untersuchten Smartphone-Betriebssysteme. Anhand praktischer Tests werden die möglichen Konsequenzen bereits dieser minimalen Konfigurationen erläutert. Eine vollständige und umfassende Sicherheitsanalyse in Bezug auf die tatsächlichen Informations- und Datenflüsse auf den technischen Geräten bietet die Studie nicht.

Abschließend gibt die Studie einige Hinweise zum Umgang mit den Smartphones der vier untersuchten Betriebssysteme, sodass Nutzern ohne tiefes technisches Verständnis zumindest eine grobe Orientierung für einen bewussten Umgang mit den Daten gegeben wird. Dem Nutzer steht es natürlich frei, die Freiheitsgrade für die Aktivierung und Übermittlung von Daten selber zu wählen. Die Studie soll lediglich einen Beitrag zur bewussteren Entscheidungsfindung leisten.

Untersucht werden die vier in Deutschland verbreitetsten mobilen Betriebssysteme [16] in ihrer zum Zeitpunkt der Untersuchung (März 2014) aktuellen Version:

ANDROID Googles Betriebssystem Android, seit 2008 erhältlich, wird auf einer Vielzahl von Geräten unterschiedlicher Hersteller eingesetzt. Betrachtet wurde Android in der Version 4.4 in einer unmodifizierten[1] Version.

BLACKBERRY OS Das Betriebssystem moderner BlackBerry-Smartphones und -Tablets – das erste BlackBerry-Smartphone erschien 1999 – ist BlackBerry OS in der Version 10, welches hier betrachtet

[1] Android ist ein quelloffenes Betriebssystem und darf daher durch Dritte erweitert werden, z.B. durch Gerätehersteller. Eine unmodifizierte Version enthält keine Zusatzerweiterungen Dritter.

wurde. BlackBerry OS 10 wurde 2013 vorgestellt. Es lässt sich mit dem Betriebssystem älterer Geräte (BlackBerry OS 6 oder 7) nicht vergleichen.

iOS Das mobile Betriebssystem iOS von Apple wird seit 2007 im iPhone und mittlerweile im iPad und im iPod Touch eingesetzt. iOS wurde in der Version iOS 7 untersucht.

WINDOWS PHONE Seit Oktober 2010 gibt es Windows Phone von Microsoft. Verschiedene Hersteller rüsten ihre Geräte mit diesem Betriebssystem aus. Die betrachtete Version ist Windows Phone 8.

Die Studie gliedert sich wie folgt: Kapitel 2 stellt vorab einige zentrale Erkenntnisse der Studie vor, auf die im weiteren Verlauf näher eingegangen wird. In Kapitel 3 werden die vier mobilen Betriebssysteme genauer vorgestellt. Kapitel 4 untersucht, welche privaten Daten auf einem Smartphone existieren und in der Studie genauer betrachtet werden. Anschließend beschreibt Kapitel 5 die Basisdienste, die bereits beim ersten Einschalten eines Smartphones eingerichtet werden, und analysiert bereits bei diesem Vorgang anfallende Datenflüsse. Dabei wird auf die dem Nutzer verfügbaren Einstellungsmöglichkeiten eingegangen sowie auf die Nutzungsbedingungen der Betriebssysteme. Kapitel 6 betrachtet die Grundfunktionen eines Smartphones in Bezug auf deren Umgang mit privaten Daten und deren Kopplung mit Cloud-Diensten. Kapitel 7 geht auf Drittanbieter-Apps und die damit verbundenen Problematiken ein. Kapitel 8 fasst Hinweise für Smartphone-Nutzer nach unterschiedlichen Betriebssystemen zusammen. Abschluss der Studie bildet Kapitel 9 mit einem Ausblick.

2. Zentrale Erkenntnisse

- Die Studie zeigt, welche privaten Daten mit potenziell sensiblen Inhalten auf einem Smartphone anfallen.
- Ohne Kundenkonto beim Hersteller lassen sich einige Funktionen des Smartphones nur eingeschränkt nutzen. Auch der Zugang zu neuen Apps erfordert i.d.R. die Einrichtung eines Kundenkontos.
- Alle Hersteller behalten sich vor, dass bei Spracheingaben zur Steuerung Daten an externe Server zur Verarbeitung geschickt werden. Dies schließt alle in diesen Spracheingaben gegebenenfalls vorhandenen sensiblen Informationen ein.
- Bei eingeschalteten Ortungsdiensten können Smartphones für unterschiedliche Zwecke regelmäßig Standortdaten an die Hersteller senden.
- In einer praktischen Untersuchung wurde gezeigt, dass schon bei der Einrichtung des Telefons, noch bevor der Nutzer selbst eine App gestartet hat, Netzwerkverbindungen aufgebaut und Daten versendet werden.
- Die Erhebung von Nutzungs- und Diagnosedaten erfolgt laut Hersteller in anonymisierter Form. Bis auf Android bieten alle Betriebssysteme eine Option zur Deaktivierung der Erhebung.
- Die Datenschutzbestimmungen der Hersteller sind sehr ähnlich, erlauben aber einen gewissen Interpretationsspielraum. Stimmt der Nutzer den Datenschutzbestimmungen zu, dürfen die Hersteller i.d.R. die erhobenen Daten zur Bereitstellung und Verbesserung ihrer Dienste nutzen und diese an Partner weitergeben.
- Viele private Daten auf Smartphones können mit Cloud-Diensten der Hersteller synchronisiert werden. Die Angebote unterscheiden sich von Hersteller zu Hersteller im Umfang und auch in der Entscheidungsfreiheit, die einem Nutzer zugestanden wird. Registriert ein Nutzer ein Microsoft-Konto auf seinem Windows Phone, werden auf dem Gerät gespeicherte Kontakte und Kalenderdaten mit dem Microsoft-Dienst automatisch synchronisiert. Dies kann nicht deaktiviert werden.
- Mit Nutzung von Drittanbieter-Apps und deren Zugriff auf private Daten gelten die Datenschutzbestimmungen des jeweiligen Anbieters. Ein Nutzer ist selbst dafür verantwortlich, ob er sich auf diese einlässt oder nicht. Der Betriebssystemhersteller ist an dieser Stelle nicht mehr verantwortlich.
- Ein plattformübergreifender Vergleich des Spiels *Angry Birds* als kostenfreie App mit einer kostenpflichtigen Version hat gezeigt, dass die kostenfreie Version deutlich mehr Daten überträgt als die kostenpflichtige Version des Spiels. Dies lässt sich allerdings nicht einfach auf andere Apps übertragen.
- Souveränität und Schutz vor ungewünschtem Datenabruf bieten die Betriebssysteme in unterschiedlichen Ausprägungen.
  - Welche Daten durch das Betriebssystem vor dem Zugriff von Apps für den Nutzer erkennbar geschützt werden, unterscheidet sich je nach Betriebssystem.
  - Oft muss der Nutzer sich schon bei der Installation einer App entscheiden, auf welche Daten die App zugreifen darf. Während er bei Android und Windows Phone eine Liste benötigter Rechte komplett bestätigen oder auf die Installation der App verzichten muss, kann er bei BlackBerry selektiv Rechte vergeben.
  - Für den Nutzer ist es leichter, Zugriffsrechte zu vergeben, wenn er Informationen darüber erhält, warum der Zugriff benötigt wird, und ihn in den Kontext seiner eigenen Interaktion mit einer App setzen kann. iOS regelt die Rechtevergabe auf diese Weise und nicht bei der Installation einer App.

- Wenn Berechtigungen in Gruppen zusammengefasst werden und der Nutzer der Gruppe zustimmen muss, kann dies problematisch sein. Bei Android können sich bei App-Updates die Berechtigungen innerhalb einer bereits bestätigten Gruppe ändern, ohne dass der Nutzer erneut zustimmen muss. Das bedeutet z.B., dass Apps, die auf die Anrufstatistik zugreifen dürfen, nach einem Update unter Umständen Anrufe ohne Nutzerinteraktion führen können.
- Nutzer können Apps bei BlackBerry OS und iOS nachträglich die Zugriffsrechte entziehen (oder erteilen). Bei einem unmodifizierten Android und Windows Phone ist dies nicht möglich.
- Bei keinem Betriebssystem kann der Nutzer nachvollziehen, wann Zugriffe auf private Daten erfolgt sind. Eine Ausnahme stellen Standortdaten auf Android und iOS dar. Hier ist erkennbar, welche Anwendungen zuletzt auf Standortdaten zugegriffen haben.

3. Betrachtete mobile Betriebssysteme

Der Begriff *Betriebssystem* umfasst im Rahmen dieser Studie alle Softwarekomponenten eines mobilen Endgerätes, die einerseits die Geräte-Hardware steuern und andererseits Ausführungsumgebungen für Anwendungen auf den mobilen Endgeräten bereitstellen.[2]

Der Zusammenhang eines Betriebssystems mit der Geräte-Hardware kann je nach Hersteller unterschiedlich ausgeprägt sein. So obliegt es diesem z.B., seine Software zu lizenzieren, sodass Smartphone-Hersteller diese auf ihren Geräten einsetzen können. Während Apple und BlackBerry dies nur für ihre eigenen Smartphones erlauben, wird Android und Windows Phone von vielen Smartphone-Herstellern auf deren Geräten angeboten. Daneben sind einige Unterschiede der Ökosysteme für Nutzer leicht ersichtlich, wie z.B. die unterschiedlichen App-Markets der Hersteller. Ein Android-Nutzer kann Apps nicht im Apple App Store kaufen und umgekehrt.

Einer Studie des Kantar Worldpanels [16] zufolge teilt sich der Marktanteil von mobilen Betriebssystemen in Deutschland im Wesentlichen in die vier hier betrachteten auf (Stand März 2014): Android stellt mit 77 % das verbreitetste mobile Betriebssystem dar, gefolgt von Apples iOS (15,3 %), Windows Phone (6,6 %) und BlackBerry OS (0,5 %). Neben diesen gibt es noch weitere Betriebssysteme (z.B. Firefox OS[3] oder Sailfish OS[4]), deren gemeinsamer Anteil sich aber nur auf 0,6 % beläuft.

In den nachfolgenden Abschnitten werden die untersuchten Betriebssysteme kurz vorgestellt. Die Darstellungen informieren über die Eigenschaften der einzelnen Systeme und das Ökosystem, in das die Systeme eingebettet sind. Verkürzt dargestellt werden unter *Ökosystem* hier alle Interaktionen des Betriebssystems mit externen Komponenten zusammengefasst, die während des Betriebs des Systems regelmäßig vorkommen. Im Falle mobiler Betriebssysteme sind als Teile von deren Ökosystem insbesondere die Geräte relevant, die Möglichkeiten zur Entwicklung von Apps durch *App-Frameworks* sowie die Anbindung an Verteilungspunkte bzw. Bezugspunkte von Apps, die App-Markets, haben.

Android

➜ **BETRIEBSSYSTEM & GERÄTE** Das Betriebssystem Android in der Version 4.4 ist ein quelloffenes[5], Linux-basiertes System, das von der Open Handset Alliance weiterentwickelt wird. Die Steuerung dieser Initiative unterliegt hauptsächlich Google. Android kommt auf verschiedenen Geräten (u.a. Smartphones, Tablet-PCs und Netbooks) unterschiedlicher Hersteller zum Einsatz.

Aus der Quelloffenheit Androids ergibt sich bei Aktualisierungen des Betriebssystems eine Herausforderung für die Gerätehersteller. Grund hierfür ist, dass die unterschiedlichen Endgeräte, die Android als Betriebssystem nutzen, in der Hardware voneinander abweichen. Daher kann ein Gerätehersteller ein Update von Android nicht direkt einsetzen, sondern muss gerätespezifische Anpassungen vornehmen. Dies bedeutet auch, dass sicherheitsrelevante Aktualisierungen des Betriebssystems nur zeitlich verzögert vom jeweiligen Gerätehersteller integriert werden können.

---

[2] Nicht betrachtet werden Hardware- sowie Softwarekomponenten, die für den Betrieb von Baseband-Prozessoren benötigt werden. Diese Prozessoren implementieren die Signalerzeugung sowie -verarbeitung, die zur Kommunikation in Mobilfunknetzen zum Einsatz kommt.

[3] http://www.mozilla.org/de/firefox/os/ (Letzter Zugriff 29.07.2014)

[4] https://sailfishos.org (Letzter Zugriff 29.07.2014)

[5] Quelloffene bzw. Open-Source-Software bezeichnet Software, deren Quell-Code prinzipiell von jedem gelesen werden kann. Dies ermöglicht es, die Funktionsweise einer Software nachzuvollziehen und gegebenenfalls zu modifizieren.

Der Betriebssystemkern basiert auf Linux, welcher die Hardware-Unterstützung, geräteunabhängige Programmierschnittstellen sowie Benutzerschnittstellen bereitstellt. Seit seinem ersten offiziellen Release im Jahre 2008 hat sich Android rasant verbreitet und ist heute (Juli 2014) das am weitesten verbreitete Betriebssystem für mobile Endgeräte.

➜ **APP-FRAMEWORK** Apps für Android werden in Java entwickelt und jeweils in einer Instanz der Dalvik Virtual Machine (VM) ausgeführt. Dabei handelt es sich um eine für die Anforderungen mobiler Endgeräte modifizierte Java Virtual Machine. Apps werden voneinander isoliert, indem Android sowohl auf Prozess als auch auf Dateiebene jede App mit einer eigenen Unix User ID ausführt. Daher haben Android-Apps grundsätzlich nur Lese- und Schreibrechte in ihrem eigenen Verzeichnis. Weiterhin kann auch die Ausführung der Apps in ihrer eigenen VM als Isolierung von anderen Apps bewertet werden, allerdings stellt dies keinen expliziten Teil des Android-Sicherheitsmodells dar. Grund hierfür ist, dass Android Apps auch Bibliotheken einbinden können, die außerhalb der VM ausgeführt werden.

➜ **APP-MARKET** Android-Apps können vom Google Play Store, dem offiziellen App-Market von Google, bezogen werden. Außerdem lassen sich Android-Apps von Drittmärkten herunterladen und installieren.

BlackBerry OS

➜ **BETRIEBSSYSTEM & GERÄTE** Das Betriebssystem BlackBerry OS in Version 10 (BB OS) kommt ausschließlich auf mobilen Endgeräten des Herstellers BlackBerry (vormals Research In Motion (RIM)) zum Einsatz. Der Quellcode von BlackBerry OS ist *Closed Source*, d.h., der Quellcode steht nicht öffentlich zur Verfügung.

Eine Besonderheit von BB OS liegt darin, dass es Benutzern zwei unterschiedliche, voneinander getrennte Bereiche bereitstellt. Dadurch lassen sich private und berufliche Apps sowie damit verbundene Daten auf Ebene des Betriebssystems voneinander trennen.

➜ **APP-FRAMEWORK** Apps für BB OS können u.a. in den Programmiersprachen C++ sowie QT Modeling Language (QML) entwickelt werden.

➜ **APP-MARKET** Nutzer von BB OS können die Apps über den BlackBerry-eigenen App-Market, BlackBerry App-World, beziehen. Zusätzlich bietet BlackBerry OS ab Version 10.2.1 die Möglichkeit, Android-Programme direkt auszuführen. Dazu muss die Applikation (als .apk-Datei) auf das BlackBerry-Smartphone kopiert werden, dort kann sie anschließend direkt ausgeführt werden. Außerdem lassen sich Apps von Drittmärkten herunterladen und installieren.

iOS

➜ **BETRIEBSSYSTEM & GERÄTE** Das Betriebssystem iOS in der betrachteten Version iOS 7 ist das Betriebssystem der Firma Apple. Es kommt auf allen mobilen Endgeräten von Apple zum Einsatz (iPhone, iPad, iPod etc.). iOS basiert auf Mac OS X, dem Betriebssystem, welches auf Apple-Notebooks sowie Desktop-Rechnern eingesetzt wird. Der Quellcode von iOS ist *Closed Source*, d.h., der Quellcode steht nicht öffentlich zur Verfügung.

➜ **APP-FRAMEWORK** Apps für iOS werden in der Programmiersprache ObjectiveC entwickelt. Zur Entwicklung von Apps für iOS steht daher nur eine Auswahl öffentlicher Programmierschnittstellen (API) zur Verfügung. Konzeptionell ähnelt der Aufbau von iOS dem von Android. Auch hier werden unterschiedliche APIs genutzt, um grafische Oberflächen zu generieren, ortsabhängige Dienste bereitzustellen und Betriebssystemfunktionen zu nutzen.

Auch iOS isoliert Apps voneinander. Dabei wird der Zugriff einer App, die nicht Teil des Werkzustandes des Gerätes ist, beschränkt. Standardmäßig können Drittanbieter-Apps nicht außerhalb ihres Verzeichnisses lesend oder schreibend auf andere Ressourcen zugreifen.

App-Market-Apps für iOS können von privaten Nutzern ausschließlich über den Apple-eigenen App-Market Apple App Store installiert werden.

Windows Phone

➜ **BETRIEBSSYSTEM & GERÄTE** Windows Phone 8 (WP8) bezeichnet das aktuelle Betriebssystem für Smartphones der Firma Microsoft. Es kommt auf Smartphones unterschiedlicher Hersteller (darunter Nokia, Samsung, HTC sowie Huawei) zum Einsatz. Der Quellcode von Windows Phone ist *Closed Source*, d.h., der Quellcode steht nicht öffentlich zur Verfügung.

➜ **APP-FRAMEWORK** Zur Entwicklung von Apps für Windows Phone werden XAML, C# sowie C++ genutzt. Wie im Falle der anderen Betriebssysteme werden auch auf dem Windows Phone Apps isoliert voneinander ausgeführt. Ähnlich wie im Falle von Android, iOS und BB OS beschränkt WP8 den Zugriff auf Ressourcen außerhalb einer App.

➜ **APP-MARKET** Private Nutzer können Apps für Windows Phone nur über den Windows Phone Store, den von Microsoft vorgesehenen Vertriebsweg im Windows-Phone-Ökosystem, installieren.

4. Private Daten auf Smartphones

Smartphones sind kleine, leistungsfähige Computer, die ihre Nutzer überall begleiten können und die viele der Erreichbarkeit wegen nie ausschalten. Im Zuge ihrer umfassenden Möglichkeiten fallen auf ihnen viele verschiedene und zum Teil auch private Daten an.

Private Daten bezeichnen Daten eines Nutzers, die sensible Informationen beinhalten. Die Herausforderung für einen Nutzer besteht also zuallererst darin, zu bewerten, welche Informationen sensibel sind und welche nicht. Diese Fragestellung muss letztlich jeder selbst beantworten – sofern nicht von Seiten des Gesetzgebers bereits vorgegriffen wurde. Denn private Daten können zudem personenbezogene Daten sein, also Daten, über die eine Person eindeutig identifizierbar ist.[6] Personenbezogene Daten genießen einen besonderen Schutz: Will ein Betriebssystemhersteller diese Daten erheben und weiterverarbeiten, bedarf dies der ausdrücklichen Zustimmung des Nutzers.

Aber private Daten müssen nicht personenbeziehbar sein. So kann ein Nutzer die auf seinem Smartphone gespeicherte Kollektion an Podcasts oder Musik als private Daten erachten, personenbeziehbar sind solche Daten in der Regel nicht.[7]

Auch sind private Daten oft nicht einfach zu erkennen: Während auf einem Gerät gespeicherte Fotoaufnahmen oder Dokumente von einem Nutzer leicht in private und nicht private Daten unterschieden werden können, gibt es auch Daten, die sich nur schwer von einem Nutzer beobachten lassen, geschweige denn sich als private Daten bewerten lassen. Ein Beispiel ist die Aufzeichnung von Positionsdaten, die eine App ausführt, um z.B. abhängig vom Standort eines Nutzers Werbung einzublenden.

Die Lage wird komplexer, wenn man sich vergegenwärtigt, dass es sich bei den privaten Daten auf einem Smartphone nicht nur um die privaten Daten des Gerätebesitzers handelt. So werden Smartphones z.B. oft als Adressbuch oder Fotoapparat genutzt, also in Konstellationen, in denen der eigentliche Zweck der Anwendung darin liegt, auch Informationen über andere Menschen zu speichern:

- Im Adressbuch eines Smartphones speichert der Anwender Adressdaten, Telefonnummern und E-Mail-Adressen von Menschen, mit denen er in Kontakt steht. Dies kann nicht nur die oben genannten Daten betreffen, sondern auch weiter gehende Informationen wie den Beziehungsstatus zu dieser Person, etwa ob diese Person mit dem Besitzer des Telefons verwandt ist.
- Wenn ein Anwender sein Smartphone als Kamera verwendet, speichert er gleichzeitig auch Informationen über die fotografierten Menschen. Diese betreffen zunächst direkt die Tätigkeit, bei der die Abgebildeten fotografiert wurden, aber auch den Ort, insbesondere, wenn der Kamera erlaubt wurde, für Fotos den Standort zum Zeitpunkt der Aufnahme zu erfassen und abzuspeichern. Implizit lassen sich aus Fotos natürlich noch mehr Informationen herausziehen, wie Kleidungsstil, Geschlecht oder ungefähres Alter der abgebildeten Personen. Durch die Fortschritte im Bereich der Gesichtserkennung ist es auch möglich, die Personen auf Fotos zu erkennen, sofern eine ausreichend große Datenbasis zur Identifikation vorhanden ist.

---

[6] Personenbezogene Daten werden in § 3 Abs. 1 Bundesdatenschutzgesetz (BDSG) definiert als „Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (Betroffener)".

[7] Nicht behandelt wird hier der Fall sogenannter Quasi-Identifikatoren, also Daten, die isoliert keinen Personenbezug aufweisen, aber in Kombination mit anderen Daten identifikatorische Wirkung für eine einzelne Person entfalten.

Die Daten, die auf mobilen Endgeräten gespeichert sind, sind sehr umfangreich. Will ein Nutzer bewerten, ob bestimmte Daten für ihn sensibel sind, muss er zuerst in Erfahrung bringen, welche sich im Laufe der Nutzungszeit auf dem Gerät ansammeln.

In den folgenden Abschnitten werden Kategorien von Daten vorgestellt, deren Ausprägungen bei allen vier Betriebssystemen – Android, BlackBerry, iOS sowie Windows Phone – vorkommen können. Die Auflistung ist umfangreich und soll zur Sensibilisierung der Nutzer beitragen, erhebt aber keinen Anspruch auf Vollständigkeit.

4.1 Konfigurationsdaten

Hier werden Daten für die technischen Einstellungen des Smartphones erfasst. Diese hängen von den Präferenzen und Nutzungsgewohnheiten eines Nutzers ab und können daher als privat erachtet werden.

➜ **BENUTZERKONTEN & PASSWÖRTER** Damit Benutzer ihre Passwörter z.B. für ihr E-Mail-Konto nicht jedes Mal einzugeben brauchen, wenn sie einen Dienst nutzen möchten, müssen die Passwörter auf dem Smartphone gespeichert werden. Dies umfasst Passwörter für Web-Dienste wie Twitter oder Facebook, aber auch Passwörter für geschützte Netze, z.B. WLANs. Auch PINs für die Anbindung von Bluetooth-Geräten oder den Sperrbildschirm fallen hierunter.

➜ **FINGERABDRUCK** Hierbei handelt es sich um biometrische Informationen des Benutzers, die zur Authentizierung (etwa zur Entsperrung des Sperrbildschirms) des Benutzers gegenüber dem Endgerät verwendet werden.

➜ **ZERTIFIKATE** Einige Dienste bieten Benutzern als Alternative zu Passwörtern die Nutzung von Zertifikaten an. Um diese Alternative anwenden zu können, müssen die genutzten Zertifikate auf dem Smartphone gespeichert werden

➜ **INSTALLIERTE APPS** Die auf einem Endgerät installierten Apps können Informationen über die Vorlieben und das Nutzungsverhalten des Nutzers preisgeben, z.B. wenn eine Vielzahl von Spielen oder eine Dating-App installiert ist.

➜ **REGION- UND SPRACHEINSTELLUNG** Die konfigurierte Sprache sowie Angaben zur Region (u.a. im Rahmen der Festlegung der Zeitzone) lassen sich als profilbildende Informationen über den Gerätebenutzer verwenden.

4.2 Gerätedaten

Diese Daten spezifizieren das Gerät eines Nutzers sowie das mobile Funknetz, das er verwendet. Auch durch diese Informationen lässt sich das Profil eines Benutzers präzisieren.

➜ **BETRIEBSSYSTEMVERSION** Für die mobilen Betriebssysteme werden regelmäßig Updates und Upgrades vom Hersteller angeboten. Die entsprechende Versionsnummer kennzeichnet den aktuellen Stand.

➜ **GERÄTETYP** Die Informationen beschreiben den Typ des Endgerätes.

➜ **NETZBETREIBER** Diese Informationen beschreiben den verwendeten Netzbetreiber eines mobilen Endgerätes, wie z.B. Vodafone, Telekom oder O_2.

➜ **GERÄTE IDS** Smartphones verfügen über eine Vielzahl von Eigenschaften, über die ein einzelnes Gerät identifiziert werden kann, z.B. die IMEI, eine 15-stellige Seriennummer. Erhält eine App Zugriff auf eine solche ID, kann diese zur Profilbildung genutzt werden.

4.3 Kommunikationsdaten

Dies sind Informationen, die zur Nutzung von Kommunikationskanälen des mobilen Endgeräts benötigt werden (z.B. Rufnummern) oder die Eigenschaften eines Kommunikationskanals beschreiben, etwa in Form von Einschränkungen (z.B. Sperrliste).

➜ **ANRUFLISTE & ANRUFSTATISTIK** Mobile Endgeräte speichern Informationen zu gewählten, eingegangenen sowie entgangenen Anrufen. Dazu zählen die Rufnummern selbst, ihre Zuordnung zu gespeicherten Kontaktdaten (soweit möglich) sowie Anzahl, Zeitstempel und Dauer der Anrufe. Diese Daten können dazu dienen, ein detailliertes Bild über das Kommunikationsverhalten eines Nutzers zu liefern.

➜ **EIGENE RUFNUMMER** Die eigene Rufnummer dient oft als Identifizierungsmerkmal[8] gegenüber Anruf- oder SMS-Empfängern. Gerade bei Textnachrichten (SMS) ist dies von Bedeutung: Gelingt es einem Angreifer, die Absendenummer einer SMS zu fälschen, wird der Empfänger dieser SMS die darin enthaltenen Informationen dem vermeintlichen Absender zurechnen.[9]

➜ **SPERRLISTE** Mobile Endgeräte erlauben es Nutzern, Listen mit Kontakten zu pflegen, für die bestimmte oder alle Kommunikationskanäle zu ihrem Gerät gesperrt sind. Dies kann z.B. dazu eingesetzt werden, um unerwünschten Nachrichten vorzubeugen. Es ist daher wichtig, dass diese Listen nicht ohne Wissen oder gar gegen den Willen der Nutzer verändert werden.

4.4 Transferdaten

In diese Kategorie fallen Daten, die das Smartphone über vorgesehene Kommunikationskanäle verlassen. Hierzu zählen sowohl Daten, die ein Nutzer bewusst verschickt (etwa SMS oder E-Mails), als auch Daten, die von Anwendungen automatisiert verschickt werden. Ein solcher Versand ist dem Benutzer nicht unbedingt bewusst.

---

[8] Rufnummern sind eindeutige Nummern, die ein Mobilfunkanbieter (z.B. Deutsche Telekom oder Vodafone) Kunden bereitstellt. Aktive Mobilfunkrufnummern sind in der Regel ab Werk an eine SIM-Karte gebunden.

[9] Das tschechische Kunstprojekt Moral Reform der Gruppe Ztohoven zeigt, wie gefälschte Absenderrufnummern dazu eingesetzt wurden, Mitglieder des tschechischen Parlaments zu beeinflussen. Für weitere Informationen siehe http://ztohoven.com/mr/index-en.html.

➜ **SMS/MMS** Versendete und empfangene SMS/MMS verbleiben auf dem Smartphone, bis der Benutzer sie löscht.

➜ **E-MAILS** Empfangene E-Mails werden auf dem Smartphone so lange gespeichert, bis die eingestellte Löschregel erreicht ist. Auf Smartphones werden wegen des begrenzten Speichers üblicherweise Löschregeln benutzt, damit z.B. nur ein Teil der E-Mails auf dem Smartphone vorgehalten wird.

➜ **TEXTNACHRICHTEN** Versendete und empfangene Textnachrichten verbleiben auf dem Smartphone, bis der Nutzer sie löscht.

➜ **SPRACHEINGABE** Spracheingabe bei Smartphones bzw. Sprachsteuerung ermöglicht die Steuerung von Apps auf dem Smartphone über Sprache wie auch das Diktieren von Texten. Zur Erkennung der Spracheingabe wird diese i.d.R. vom Smartphone an einen Server geschickt, der sie verarbeitet und das Ergebnis zurückmeldet. Die Verarbeitung von Spracheingaben ist rechenintensiv und auf einem externen Server daher wesentlich schneller als auf einem Smartphone. Spracheingaben lassen Rückschlüsse auf die Benutzung des Smartphones zu und eignen sich daher auch zur Profilbildung.

➜ **ANONYME NUTZUNGSDATEN** Zur Fehlerdiagnose, Verbesserung und Weiterentwicklung von Anwendungen und Diensten eines mobilen Endgerätes sowie zur Analyse des Nutzerverhaltens sammeln Betriebssystemhersteller Nutzungsdaten. Oft sichern die Hersteller zu, dass sie Nutzungsdaten nur anonymisiert erheben. Für weitere Informationen zu Diagnose- und Nutzungsdaten siehe Unterkapitel 5.6.

4.5 Profildaten

Diese Kategorie fasst alle Informationen über einen Benutzer zusammen, die diesen individuell charakterisieren, d.h. zur Bildung eines Profils beitragen.

➜ **ALLGEMEINE INFORMATIONEN ÜBER DEN SMARTPHONE-BENUTZER** Daten wie Name, Alter, Geschlecht, Wohnort oder E-Mail-Adresse des Smartphone-Benutzers beinhalten Informationen, die ihn unmittelbar beschreiben.

➜ **KONTAKTE** Die gespeicherten Kontakte eröffnen Rückschlüsse über Umfeld und Persönlichkeit. So kann schon die bloße Anzahl (z.B. sehr wenige) und Art (z.B. eine Vielzahl an Arztpraxen) von Kontakten private Informationen über eine Person preisgeben. Neben der Standardanwendung eines Adressbuchs auf dem Endgerät können Kontakte auch in weiteren Apps des Geräts gespeichert sein (z.B. WhatsApp, Skype).

➜ **TERMINE** Termindaten eines Nutzers liefern u.a. detaillierte Informationen darüber, wann er sich an einem bestimmten Ort für welche Dauer mit anderen Personen verabredet. Wertet man verschiedene Termine aus, lassen sich leicht Rückschlüsse über Tätigkeiten, Gewohnheiten etc. ableiten.

➜ **AUFGABEN** Sie liefern ein aufschlussreiches Bild über Tätigkeiten. Auch hier können bereits auf Basis der Art und Häufigkeiten der Aktivitäten Aussagen über private Eigenschaften abgeleitet werden.

➜ **STANDORTDATEN** Smartphones können zur Positionsbestimmung eingesetzt werden und ermöglichen Apps den Zugriff auf Standortdaten des Geräts. Ständiger Zugriff auf solche Daten ermöglicht das Erstellen von eindeutigen Bewegungsprofilen.

➜ **BEWEGUNGSSENSOR** Smartphones besitzen meist einen Bewegungssensor, der Informationen über die Bewegung des Gerätes an Apps weitergeben kann, z.B. zur Steuerung von Spielfiguren in Spielen. Die Bewegungssensoren sind recht genau und können daher auch eingesetzt werden, um individuelle Bewegungsmuster zu erkennen, die sich zur Profilbildung eignen. [18, 11]

➜ **WECKZEITEN** Informationen zur Uhrzeit des Weckens ermöglichen Erkenntnisse über die Schlafgewohnheiten einer Person. Abweichungen der Weckzeiten an Arbeitstagen können etwa als Hinweis interpretiert werden, dass sich die Person im Urlaub befindet.

4.6 Mediendaten

Diese Kategorie umfasst alle Daten, die sowohl direkt mit dem in das Telefon eingebauten Mikrofon oder mit der Kamera aufgenommen werden, wie auch die Musik- und Filmsammlung.

➜ **AUDIO-AUFNAHMEN** Smartphones bieten die Möglichkeit, Audiosignale aufzuzeichnen und zu speichern. Unberechtigte Audio-Aufnahmen können zur unerwünschten Aufzeichnung privater Informationen des Nutzers führen. Ein Beispiel für erwünschte, aufgezeichnete Daten können Sprachmemos sein, also die Aufzeichnung von Sprachnotizen. Auch diese Daten können sensible Informationen enthalten, die ausschließlich für den privaten Gebrauch bestimmt sind.

➜ **MUSIK** Auf dem Smartphone gespeicherte Musikdateien ermöglichen Rückschlüsse über persönliche Präferenzen. Dies gilt insbesondere bei Musikstücken, die eine politische Aussage haben.

➜ **VIDEOS** Smartphones können Videos speichern oder mittels der integrierten Kamera aufnehmen. In jedem Fall lassen sich aus den so gewonnenen Sequenzen Rückschlüsse über den Nutzer ziehen.

➜ **FOTOS, BILDER & FOTOALBEN** Auf einem Smartphone gespeicherte Bilder und Fotos können Informationen über Aufenthaltsorte sowie Präferenzen des Nutzers geben. Da sie oft für Schnappschüsse benutzt werden, bilden diese Aufnahmen häufig andere Personen im Umfeld des Nutzers ab, was wiederum Rückschlüsse auf den privaten Umgang ermöglicht.

➜ **FOTO-METADATEN (Z.B. POSITIONSDATEN, UHRZEIT)** Mit dem Smartphone erstellte Fotos (und Videos) enthalten auch Informationen über das Foto selbst. Diese Daten dokumentieren etwa den Ort ihrer Aufnahme sowie den Zeitpunkt. Dies ermöglicht eine detaillierte Aussage darüber, wo und wann ein Bild erzeugt worden ist.

4.7 Internetdaten

Zu dieser Kategorie zählen alle Daten, die beim Surfen im Internet anfallen. Damit lässt sich die Zugriffshistorie auf Webseiten ebenso nachvollziehen wie genutzte Dienste oder digitale Identitäten.

➜ **IP-ADRESSE** Verfügt ein mobiles Endgerät über eine Verbindung zum Internet, so wird dem Gerät eine IP-Adresse zugewiesen. Oft eignet sich die IP-Adresse, um den Standort des Gerätes näherungsweise zu erkennen.

➜ **BROWSERVERLAUF/FAVORITEN/LESEZEICHEN** Häufig werden mobile Endgeräte genutzt, um auf Webseiten zuzugreifen. Information über das Surfverhalten eines Nutzers in Form von Browserverlauf sowie gespeicherten Favoriten und Lesezeichen beschreiben die Interessen und enthalten oft sensible Informationen (z.B. Besuch von Singlebörsen).

➜ **COOKIES** Cookies werden im Internet genutzt, um zurückkehrende Benutzer wiederzuerkennen, und werden dort u.a. von Werbenetzwerken zur Profilbildung genutzt. Dieser Mechanismus wird auch beim Surfen mit Smartphones eingesetzt.

➜ **WEB-CACHE** Dies sind Daten, die vom Webbrowser eines mobilen Endgerätes aus Optimierungsgründen zwischengespeichert werden. Die Optimierung besteht in der Vermeidung wiederholter Downloads von Inhalten, die erneut durch einen Nutzer ausgewählt werden (z.B. Betätigung des Zurück-Buttons des Browsers).

➜ **OFFLINE-INHALTE** Hierbei handelt es sich um Daten, die einem Nutzer bereitgestellt wurden, als dessen Endgerät mit dem Internet verbunden war. Er hat auch nach Beendigung der Verbindung, d.h. offline, darauf noch Zugriff.

➜ **WEB-FORMULARDATEN** Die Daten umfassen private, personenbezogene Informationen wie z.B. Name, Adresse, Telefonnummer, E-Mail-Adresse sowie Kreditkartendaten. Sie werden vom Webbrowser des mobilen Endgerätes gespeichert und können in definierten Formularfeldern wiederverwendet werden.

5. Basisdienste und Datenübermittlung

Ein Smartphone muss nach erstmaligem Einschalten zunächst durch den Nutzer eingerichtet werden. Das haben alle hier betrachteten Betriebssysteme gemein. Während des Einrichtungsvorgangs wird der Nutzer dazu aufgefordert, verschiedene *Basisdienste*, wie Ortungsdienste oder Sprachsteuerung, einzurichten. Welche Dienste bei der ersten Einrichtung konfiguriert werden sollen, unterscheidet sich von Betriebssystem zu Betriebssystem. In der Regel kann der Nutzer diese auch später noch konfigurieren. Die Einrichtung der Basisdienste erfordert vom Nutzer, verschiedene Entscheidungen über den Umgang mit den im Gerät gespeicherten Daten zu treffen. So kann er etwa erlauben, dass umfangreiche Diagnosedaten über das Telefon gesammelt und an den Hersteller übertragen werden oder dass der Standort des Gerätes ermittelt wird.

Auch erfordert die initiale Einrichtung der Smartphones vom Benutzer immer das Akzeptieren der Nutzungsbedingungen des jeweiligen Betriebssystems. Damit räumt der Anwender dem Hersteller verschiedene Rechte ein. In der Regel stimmt der Nutzer zu, dass seine Daten zur Erbringung der Dienste sowie deren Verbesserung genutzt werden dürfen. Wer diesen Nutzungsbedingungen nicht zustimmt, kann das Smartphone nicht verwenden.

Die Inhalte dieses Kapitels sind wie folgt strukturiert: Zunächst werden in Kapitel 5.1 Minimaleinstellungen vorgestellt, mit denen die Betriebssysteme initial eingerichtet werden können und deren Ziel es ist, möglichst wenige Daten zu generieren und zu senden. Anschließend wird untersucht, welche Daten die Betriebssysteme trotz dieser minimalen Einstellungen senden.

Die Kapitel 5.2 bis 5.6 beschreiben die Basisdienste der Betriebssysteme, die bereits nach erstmaligem Einrichten eines Endgerätes verfügbar sind. Im Fokus steht dabei, welche privaten Daten eines Nutzers die Dienste berühren können und welche Auswirkungen dies haben kann. Zur Verdeutlichung werden für jedes Betriebssystem die potenziell betroffenen privaten Daten vorangestellt, die in Kapitel 4 näher vorgestellt wurden.

Den Abschluss bilden die Nutzungs- und Datenschutzbestimmungen der Betriebssysteme, die in Kapitel 5.7 betrachtet werden. Dabei stehen der vorgebrachte Zweck der Datenerfassung, die Aufbewahrungsdauer erfasster Daten, Möglichkeiten der Herausgabe sowie die Weitergabe personenbezogener Daten an Dritte im Fokus der Betrachtung.

5.1 Smartphone einrichten

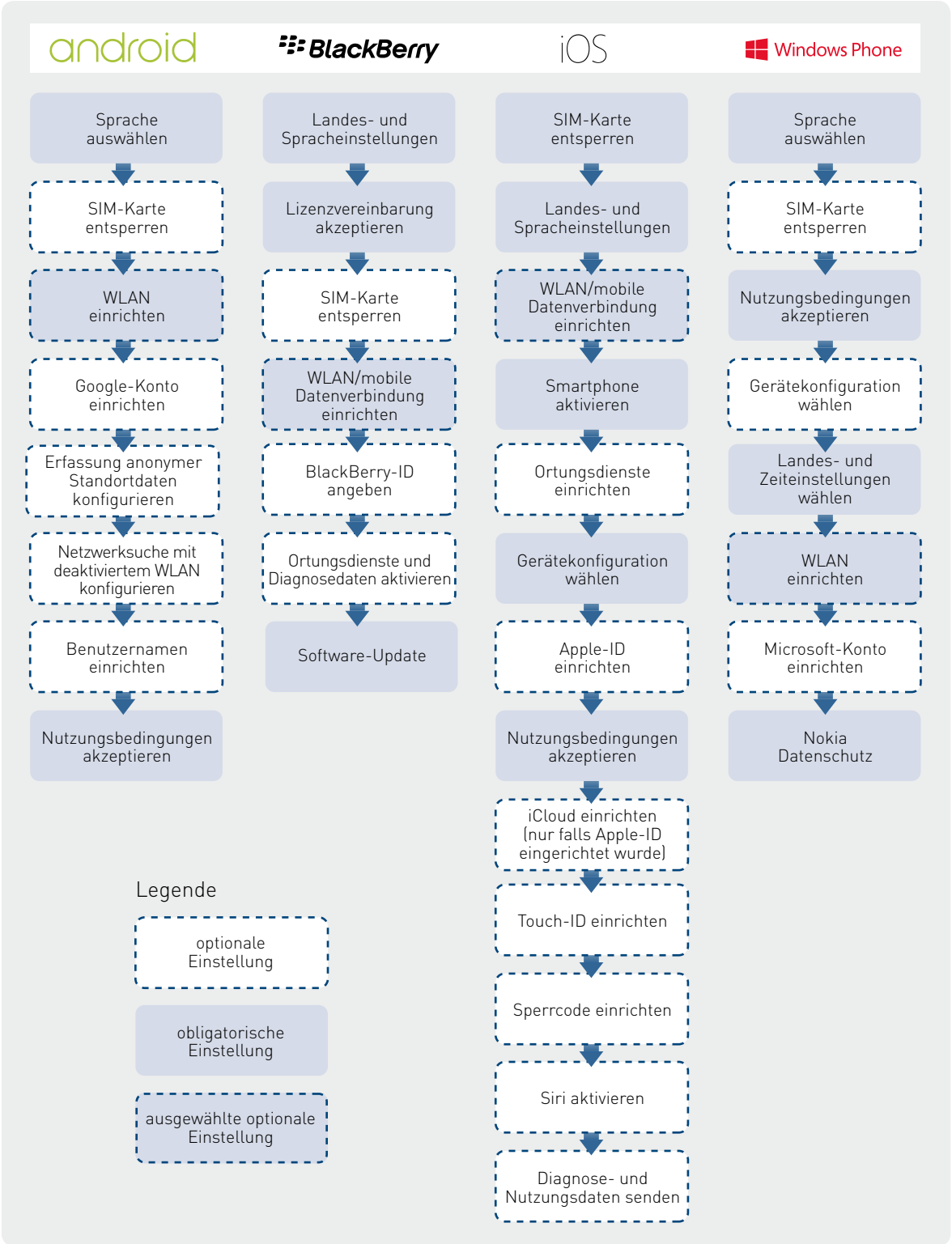
Nachfolgend werden die minimalen Einstellungen zur Einrichtung der vier Betriebssysteme aufgezeigt. Die *Minimaleinstellungen* eines Gerätes bezeichnen die Menge an Einstellungen, die zur Inbetriebnahme aktiviert werden müssen, damit die Grundfunktionen eines Smartphones (siehe Kapitel 6) überhaupt genutzt werden können. Dazu gehören die Möglichkeit zu telefonieren, d.h. das Endgerät in ein Mobilfunknetz einzubuchen, sowie eine Verbindung zum Internet.

Zunächst wird der Ablauf bei der Einrichtung eines Smartphones dargestellt. Dabei wird untersucht, ob der Nutzer eine Wahlmöglichkeit hat oder nicht. Folgende Geräte wurden in der Studie verwendet:

- **Android:** LG E960 Nexus 4 mit Android 4.4.3
- **BlackBerry OS:** BlackBerry Q5 mit BlackBerry OS 10.2.1.2977
- **iOS:** Apple iPhone 5s mit iOS 7.1.1
- **Windows Phone:** Nokia Lumia 920 mit Windows Phone 8.0

Anschließend wurde in praktischen Untersuchungen (siehe Unterkapitel 5.1.2) überprüft, welche Daten bei der Einrichtung eines Smartphones übertragen werden.

Abbildung 5.1: Schritte beim Einrichten eines Smartphones



5.1.1 Minimale Einstellungen

Abbildung 5.1 vergleicht den Ablauf bei der Einrichtung der verschiedenen mobilen Betriebssysteme. Zwar unterscheidet sich die Reihenfolge der einzelnen Schritte, der Nutzer wird aber in der Regel dazu aufgefordert, vergleichbare Basisdienste einzurichten. Hier gibt es aber auch Ausnahmen, insbesondere iOS lässt den Nutzer wesentlich mehr einrichten als die anderen Betriebssysteme.

Für die Minimaleinstellungen ist nun relevant, welche dieser Basisdienste Einfluss auf eine Datenübertragung haben und eingerichtet werden müssen. Das Ziel der Minimaleinstellungen ist es, möglichst wenige Dienste des Endgerätes zu aktivieren, um so die Übertragung von Daten – allen voran privater Daten des Nutzers – zu minimieren.

Einige Basisdienste, insbesondere die Einrichtung der Touch-ID und des Sperrcodes bei iOS, haben keinen Einfluss auf die Datenübertragung, fallen daher aus den Minimaleinstellungen heraus und werden in diesem Rahmen nicht aktiviert.

Eine Verbindung mit dem Internet ist Voraussetzung für die Nutzung einiger Grundfunktionen eines Smartphones. Dazu zählen u.a. der Empfang und Versand von E-Mails sowie das Surfen im Internet (siehe Kapitel 6). Sie kann entweder über WLAN oder über ein Mobilfunknetz etabliert werden. Letzteres setzt die Verwendung einer SIM-Karte voraus. Im Rahmen der durchgeführten praktischen Untersuchungen (siehe Unterkapitel 5.1.2) nutzten die Testgeräte als Zugangspunkt ein WLAN. Die Einrichtung eines WLAN wird daher in den Minimaleinstellungen gefordert.

Android

➜ **SPRACHAUSWAHL** Dieser Schritt ist obligatorisch. Ein Nutzer muss eine Sprache auswählen, um mit dem Endgerät interagieren zu können.

➜ **SIM-KARTE ENTSPERREN** In diesem Schritt wird der Nutzer aufgefordert, eine SIM-Karte in das Gerät einzusetzen. Dieser Schritt ist optional und kann bei der Einrichtung übersprungen werden. Allerdings ist ohne aktivierte SIM-Karte keine Nutzung der Telefonfunktion möglich.

➜ **WLAN EINRICHTEN** In diesem Schritt wird der Nutzer aufgefordert, ein verfügbares Drahtlosnetzwerk auszuwählen und das Gerät mit diesem zu verbinden. Grundsätzlich ist dieser Schritt optional. Für die im Rahmen der Untersuchung durchgeführten praktischen Tests wird eine Internetverbindung benötigt. Daher wird hier eine Verbindung über WLAN eingerichtet.

➜ **GOOGLE-KONTO EINRICHTEN** Hier kann ein Nutzer das Endgerät mit einem existierenden Google-Konto verknüpfen oder bei Bedarf hierfür ein neues Konto erstellen. Dieser Schritt ist optional und wird im Zuge der Minimaleinstellungen übersprungen. Für weitere Informationen zur Verknüpfung mit Google-Konten siehe Kapitel 5.2.

➜ **ERFASSUNG STANDORT KONFIGURIEREN** Der Nutzer kann entscheiden, ob er den Standortdienst von Google nutzen möchte, um so Apps auf dem Gerät Standortdaten mit hoher Genauigkeit bereitzustellen. Dieser Schritt ist optional und wird hier entsprechend minimaler Einstellungen des Gerätes deaktiviert. Weitere Informationen zur Erfassung von Standortdaten bei Android siehe Kapitel 5.4.

➜ **NETZWERKSUCHE** Diese Option bietet einem Nutzer an, auch bei ausgeschalteter WLAN-Funktion des Gerätes nach Drahtlosnetzen in der Umgebung des Nutzers zu suchen und diese Informationen

an Google zu übermitteln. Diese Einstellung ist optional. Mit Blick auf minimale Einstellungen wird dieser Dienst hier deaktiviert.

➜ **BENUTZERNAME EINRICHTEN** Hier wird der Nutzer zur Eingabe seines Namens aufgefordert. Diese Eingabe dient der Personalisierung des Gerätes und ist optional. Im Rahmen der Minimaleinstellungen wird auf diese Option verzichtet.

➜ **DATENSCHUTZVEREINBARUNG AKZEPTIEREN** Dieser Schritt muss durchgeführt werden. Der Nutzer wird dazu aufgefordert, die Datenschutz- sowie Nutzungsbestimmungen für Google-Dienste zu akzeptieren. Akzeptiert der Nutzer die Bedingungen nicht, kann das Gerät nicht verwendet werden. Für weitere Informationen zu Datenschutzbestimmungen für Android- bzw. Google-Dienste siehe Kapitel 5.7.

BlackBerry OS

➜ **SPRACHAUSWAHL** Dieser Schritt ist obligatorisch, ein Nutzer muss eine Sprache auswählen, um mit dem Endgerät interagieren zu können.

➜ **LIZENZVEREINBARUNG** An dieser Stelle wird der Nutzer zur Akzeptanz des BlackBerry Solution *License Agreement* aufgefordert. Dieser Schritt kann nicht übersprungen werden. Für weitere Informationen siehe Kapitel 5.7.

➜ **SIM-KARTE ENTSPERREN** Der Einsatz bzw. die Entsperrung einer SIM-Karte ist optional, bildet allerdings die notwendige Voraussetzung für die Verwendung der Telefonfunktion.

➜ **WLAN EINRICHTEN** An dieser Stelle wird der Nutzer zur Auswahl eines Drahtlosnetzes aufgefordert. Dieser Schritt kann nur unter der Voraussetzung übersprungen werden, dass eine Verbindung über das Mobilfunknetz hergestellt werden kann. Für die im Rahmen der Untersuchung durchgeführten praktischen Tests wird eine Internetverbindung über WLAN eingerichtet.

➜ **BLACKBERRY-ID** Hier kann der Nutzer eine gültige BlackBerry-ID angeben oder bei Bedarf eine neue erstellen. Dieser Schritt ist optional und wird hier entsprechend minimaler Einstellungen des Gerätes deaktiviert. Für weitere Informationen zu BlackBerry-IDs siehe Kapitel 5.2.

➜ **DIAGNOSE UND STANDORT** Dieser Schritt fordert den Nutzer zur Aktivierung von Diagnoseberichten und Standortdaten auf. Die Auswahl ist optional und wird im Rahmen der Minimaleinstellungen ausgelassen. Für weitere Informationen zu Diagnosediensten auf BlackBerry-Geräten siehe Kapitel 5.6.

➜ **SOFTWARE-UPDATE** In diesem Schritt wird nach einer Aktualisierung für BlackBerry OS gesucht. Dies umfasst neue Versionen des Betriebssystems selbst oder Sicherheits-Updates. Es wird an dieser Stelle nicht nach neuen Versionen für installierte Apps gesucht.

iOS

➜ SIM-KARTE ENTSPERREN Die Entsperrung der SIM-Karte ist obligatorisch für die Aktivierung des iPhones. Die SIM-Karte ist zudem erforderlich, um das Endgerät in ein Mobilfunknetz einzubuchen, d.h. die Telefoniefunktion des Gerätes nutzen können.

➜ LANDES- & SPRACHEINSTELLUNGEN Diese Schritte sind obligatorisch, ein Nutzer muss eine Sprache für die Interaktion mit dem Endgerät auswählen sowie ein Land, damit das iPhone landestypische Einstellungen nutzen kann, wie z.B. das Datumsformat.

➜ WLAN EINRICHTEN Hier wird der Nutzer aufgefordert, aus einer Liste verfügbarer Drahtlosnetze eines auszuwählen und sich mit diesem zu verbinden. Grundsätzlich ist dieser Schritt optional. Für die im Rahmen der Untersuchung durchgeführten praktischen Tests wird eine Internetverbindung benötigt. Daher wird hier eine Verbindung über WLAN eingerichtet.

➜ IPHONE AKTIVIEREN Dieser Schritt ist obligatorisch. Um das iPhone nutzen zu können, muss der Nutzer das Telefon aktivieren. Es ist möglich, das iPhone ohne mobile Netzwerkverbindung zu aktivieren, dann muss das iPhone mit einem Kabel an einen Computer angeschlossen werden und über iTunes[10] aktiviert werden.

➜ ORTUNGSDIENSTE An dieser Stelle kann der Nutzer die Ortungsdienste für das iPhone aktivieren oder deaktivieren. Mit Blick auf die Minimaleinstellungen des Gerätes werden die Ortungsdienste an dieser Stelle deaktiviert.

➜ GERÄTEKONFIGURATION WÄHLEN In diesem Schritt bietet iOS drei Auswahlmöglichkeiten an, um das iPhone zu konfigurieren. Das iPhone kann als neues iPhone konfiguriert werden oder als *iCloud-Backup* oder *iTunes-Backup*[11] wiederhergestellt werden.

➜ ACCOUNT EINRICHTEN Hier wird der Nutzer zur Verknüpfung einer Apple-ID mit seinem iPhone aufgefordert (bei Bedarf kann ein neues Konto erstellt werden). Dieser Schritt ist optional und wird im Zuge minimaler Einstellungen übersprungen. Für weitere Informationen zur Verknüpfung von iOS-Geräten mit einer Apple-ID siehe Kapitel 5.2.

➜ NUTZUNGSBEDINGUNGEN AKZEPTIEREN An dieser Stelle wird der Nutzer dazu aufgefordert, die Nutzungsbedingungen von Apple für iOS zu akzeptieren. Lehnt er dies ab, kann er das Gerät nicht verwenden.[12] Für weitere Informationen siehe Kapitel 5.7.

➜ iCLOUD EINRICHTEN Hat der Nutzer seine Apple-ID mit seinem iPhone verknüpft, kann er in diesem Schritt den Cloud-Dienst iCloud einrichten. Dieser Schritt ist optional und wird im Zuge minimaler Einstellungen des Gerätes übersprungen.

---

[10] iTunes ist ein Multimedia-Verwaltungsprogramm von Apple, das auch für die Synchronisierung von iOS-Geräten genutzt wird.

[11] Sowohl bei iCloud-Backup als auch bei iTunes-Backup handelt es sich um Dienste, die einen Gesamtzustand, d.h. Anwendungen und Daten eines iPhones zu einem bestimmten Zeitpunkt, abgespeichert haben (sogenannte Back-ups) und es ermöglichen, diesen Zustand auf einem iPhone wiederherzustellen.

[12] Bei eingelegter SIM-Karte können Notrufe getätigt werden.

➜ **TOUCH ID EINRICHTEN** An dieser Stelle kann der Nutzer die Touch-ID des iPhones einrichten.[13] Dies ermöglicht dem Nutzer das Entsperren des Telefons per Fingerabdruck. Dieser Schritt ist optional und wird im Rahmen minimaler Einstellungen übersprungen.

➜ **SPERRCODE EINRICHTEN** Hier wird der Nutzer aufgefordert, einen vierstelligen Sperrcode für das iPhone einzurichten. Dieser Schritt ist optional und wird im Rahmen minimaler Einstellungen übersprungen.[14]

➜ **SIRI AKTIVIEREN** An dieser Stelle kann der Nutzer Siri aktivieren, einen Dienst zur Spracheingabe und Sprachsteuerung auf dem iPhone. Dieser Schritt ist optional und wird mit Blick auf minimale Einstellungen deaktiviert.

➜ **DIAGNOSE** Dieser Schritt fordert den Nutzer zum Aktivieren der automatischen Sendefunktion von Diagnosedaten auf. Die Auswahl ist optional und wird entsprechend minimaler Einstellungen nicht aktiviert.

Windows Phone

➜ **SPRACHAUSWAHL** Dieser Schritt ist obligatorisch, ein Nutzer muss eine Sprache auswählen, um mit dem Endgerät interagieren zu können.

➜ **SIM-KARTE ENTSPERREN** Die Entsperrung der SIM-Karte ist optional, wird aber für die Verwendung der Telefonfunktion benötigt.

➜ **NUTZUNGSBEDINGUNGEN AKZEPTIEREN** An dieser Stelle wird der Nutzer dazu aufgefordert, die Datenschutz- sowie die Nutzungsbedingungen von Microsoft für Windows Phone zu akzeptieren. Wird dies verweigert, kann das Gerät nicht verwendet werden.[15]

➜ **GERÄTEKONFIGURATION WÄHLEN** In diesem Schritt bietet Windows Phone grundsätzlich zwei Optionen, *Empfohlen* und *Anpassen*, die beschreiben, wie das Gerät konfiguriert wird. Wählt ein Nutzer *Anpassen*, werden ihm fünf weitere Optionen präsentiert, die er jeweils deaktivieren kann (standardmäßig sind alle Optionen aktiv):

- Verwendung von Mobilfunk(daten)verbindungen auf dem Handy erlauben
- Berichte zur Verbesserung von Produkten und Diensten von Microsoft und Partnern senden
- Tastatureingabeinformationen senden, um Textvorschläge zu verbessern
- WLAN-Verbindungsdaten zur Erkennung von WLAN in der Umgebung sichern
- Windows-Phone-Updates automatisch herunterladen

Unter Berücksichtigung der Minimaleinstellungen des Gerätes (Erfordernis der Möglichkeit einer Internetverbindung) werden bis auf *Windows-Phone-Updates automatisch herunterladen* alle Optionen

---

[13] Die Touch-ID wurde von Apple mit dem Modell iPhone 5s eingeführt.

[14] Es handelt sich hier um eine Testkonfiguration, die Einrichtung eines Sperrcodes wird für den alltäglichen Gebrauch empfohlen (siehe Kapitel 8.3).

[15] Bei eingelegter SIM-Karte können Notrufe getätigt werden.

deaktiviert. Für weitere Informationen zu diesen Optionen siehe Kapitel 5.6. Wählt ein Nutzer die Option *Empfohlen*, werden automatisch alle unter Anpassen aufgeführten Optionen aktiviert.

➜ **LANDES- & ZEITEINSTELLUNGEN** An dieser Stelle wird der Nutzer aufgefordert, die Voreinstellungen zu Heimat, Zeitzone, Datum sowie die Uhrzeit zu bestätigen oder zu korrigieren. Zudem findet sich eine aktivierte Option *Meinen Standort an Microsoft senden, wenn mein Handy aktiviert ist*, welche im Zuge der Minimaleinstellungen deaktiviert wird.

➜ **WLAN EINRICHTEN** Hier wird der Nutzer aufgefordert, ein verfügbares Drahtlosnetzwerk auszuwählen und sich mit diesem zu verbinden. Grundsätzlich ist dieser Schritt optional. Für die im Rahmen der Untersuchung durchgeführten praktischen Tests wird eine Internetverbindung benötigt. Daher wird hier eine Verbindung über WLAN eingerichtet.

➜ **MICROSOFT-KONTO EINRICHTEN** Hier wird der Nutzer zur Verknüpfung eines Microsoft-Kontos mit dem Windows Phone aufgefordert (bei Bedarf kann ein neues Konto erstellt werden). Dieser Schritt ist optional und wird im Zuge minimaler Einstellungen übersprungen. Für weitere Informationen zur Verknüpfung von Windows-Phone-Geräten mit Microsoft-Konten siehe Kapitel 5.2.

➜ **NOKIA-DATENSCHUTZ** Dieser letzte Schritt ist spezifisch für das Testgerät und kann bei anderen Endgeräten anderer Hersteller (z.B. HTC) abweichen. Hier wird ein Nutzer aufgefordert, die Datenschutz- sowie Nutzungsbedingungen von Nokia zu akzeptieren. Dieser Schritt kann nicht übersprungen werden. Ferner wird dem Nutzer eine aktivierte Option *Am Verbesserungsprogramm von Nokia teilnehmen* präsentiert, welche im Rahmen der Minimaleinstellungen deaktiviert wird.

Implikationen der Minimaleinstellungen

Android

Verzichten Nutzer bei der Einrichtung eines Android-Gerätes auf die Verknüpfung mit einem *Google-Konto*, so können u.a. keine Apps über die auf dem Gerät installierte Google Play Market App installiert werden. Allerdings erlaubt Android auch eine Installation von Apps Dritter über alternative App-Markets. Dafür muss jedoch eine im Auslieferungszustand des Geräts aktivierte Sicherheitsfunktion abgeschaltet werden.

Weiterhin führt die *Deaktivierung von Standortinformationen* dazu, dass bestimmte Dienste, welche Standortinformationen benötigen (z.B. zur Erfassung von Positionsdaten von Fotos), nicht zur Verfügung stehen.

Im Zuge minimaler Einstellungen wurde die Option *Netzwerksuche nach verfügbaren Drahtlosnetzen* auch bei *deaktiviertem* WLAN abgewählt. Dies zieht keine direkten Einschränkungen der Gerätefunktionalität nach sich.

BlackBerry OS

Ohne BlackBerry-ID lässt sich ein BlackBerry-Gerät nur eingeschränkt nutzen, für die Installation weiterer Apps über die BlackBerry App-World wird eine BlackBerry-ID benötigt. Allerdings erlaubt BlackBerry OS auch eine Installation von Apps Dritter über alternative App-Markets. Dafür

muss jedoch eine im Auslieferungszustand des Geräts aktivierte Sicherheitsfunktion abgeschaltet werden.

Werden die Ortungsdienste deaktiviert, können Funktionen, die auf einer Standortbestimmung beruhen, nicht genutzt werden. Hierzu zählt sowohl die integrierte Karten-Anwendung, die auch Navigationsfunktionalität bietet, als auch die Nutzung der BlackBerry-Protect-Funktionalität, mit der ein verlorenes oder gestohlenes Telefon aufgespürt werden kann. BlackBerry Protect kann darüber hinaus nur verwendet werden, wenn eine BlackBerry-ID eingerichtet wurde.

Die Sendung von Diagnosedaten kann deaktiviert werden, ohne dass Einschränkungen in der Nutzung des Telefons zu erwarten sind.

iOS

Ohne Apple-ID lässt sich das Smartphone zwar generell nutzen, es können aber ausschließlich die vorinstallierten Apps verwendet werden. Das Installieren von weiteren Apps oder das Herunterladen von Musik oder Filmen aus dem iTunes-Store sind ohne Apple-ID nicht möglich.

Die Apple-eigenen Cloud-Dienste können nur in Verbindung mit einer Apple-ID genutzt werden. Diese beinhalten sowohl Back-up-Möglichkeiten als auch Dienste zum Auffinden und Sperren, falls das iPhone verloren wurde.

Die allgemeine Deaktivierung der Ortungsdienste schränkt die Verwendung des Smartphones als Navigationsgerät sehr stark ein, eine Turn-by-Turn-Navigation[16] ist beispielsweise nicht mehr möglich.

Wird Siri deaktiviert, wird damit die Sprachsteuerung des Smartphones sowie die Diktierfunktion abgeschaltet.

Die Deaktivierung der Übertragung von Diagnose- und Nutzungsdaten zieht keine direkten Einschränkungen der Nutzung des Smartphones nach sich.

Windows Phone

Die Beschreibungen der Optionen der Gerätekonfiguration *Berichte zur Verbesserung der Produkte und Dienste senden, Tastatureingabeinformationen senden, WLAN-Verbindungsdaten zur Erkennung von Drahtlosnetzen in der Umgebung sichern* geben keine Anhaltspunkte dafür, dass aus ihrer Deaktivierung Einschränkungen der Gerätefunktionalität resultieren.

Weiterhin ergeben sich keine Einschränkungen bei der Benutzung des Gerätes, wenn die Option *Meinen Standort an Microsoft senden, wenn mein Handy aktiviert ist* deaktiviert wird.

Aus dem Verzicht, das Gerät mit einem Microsoft-Konto zu verknüpfen, ergeben sich Einschränkungen hinsichtlich der Nutzung des Windows-Phone-Stores: Es können ohne Konto u.a. keine Apps des Stores über die auf dem Gerät installierte Windows Phone Market App installiert werden.

Letztlich führt der Verzicht eines Nutzers auf die *Teilnahme am Nokia-Verbesserungsprogramm* zu keinen direkten Einschränkungen der Funktionalität des Endgerätes.

[16] Turn-by-Turn-Navigation wird die Form der Navigation genannt, bei der einem Nutzer kontinuierlich durch Ansage oder Anzeige die Richtung gezeigt wird.

5.1.2 Minimale Einstellungen in der Praxis

Welche Verbindungen bauen die Geräte trotz der zuvor beschriebenen Minimaleinstellungen auf? Diese Frage wurde in praktischen Tests der vier Betriebssysteme geklärt. Die Untersuchungen betrachten also Verbindungen, welche das Gerät nach erstmaligem Einschalten trotz Minimaleinstellungen aufbaut. Die Verbindung zum Internet stellen die Smartphones dabei über WLAN her.

Der nachfolgende Abschnitt fasst die Ergebnisse der praktischen Tests zusammen und hebt wichtige Erkenntnisse hervor. Danach folgt pro Betriebssystem jeweils ein Abschnitt, in dem die Einzelergebnisse detailliert beschrieben werden.

Zusammenfassung der Ergebnisse

Für jedes der vier Betriebssysteme wurden in einem Zeitraum von 23 Stunden nach Einrichten die folgenden Eigenschaften der Verbindungen dokumentiert und untersucht:

- **Zieladresse:** Für jede Verbindung des Endgerätes wurde die Adresse der Gegenstelle untersucht. Diese liegt zunächst als IP-Adresse vor. Es wurde sodann versucht, dieser IP-Adresse einen sprechenden Hostnamen zuzuordnen.
- **Ausgetauschte Datenmenge:** Für jede Verbindung wurde die gesamte ausgetauschte Menge an Daten sowie die vom Gerät gesendeten Daten dokumentiert und untersucht.
- **Dauer der Verbindung:** Für jede Verbindung wurde die Dauer dokumentiert und untersucht.
- **Enthaltene Klartextinformationen:** Für jede Verbindung wurden die übertragenen Daten anhand der Datenpakete nachvollzogen und auf lesbare Informationen untersucht.
- **Verschlüsselung:** Für jede Verbindung wurde überprüft, ob eine Transportverschlüsselung, z.B. TLS[17], eingesetzt wurde.

Tabelle 5.1 fasst die Testergebnisse zusammen. Android und iOS weisen mit 10,89 MB und 68,19 MB ein sehr hohes Datenvolumen auf, was Betriebssystem-Updates geschuldet ist. Im Rahmen einer solchen Untersuchung von Netzwerkverkehr können immer Updates einzelner Apps oder des Betriebssystems auftreten.

Tabelle 5.1:
Zusammenfassung der Testergebnisse bei minimalen Einstellungen

	Android	BlackBerry OS	iOS	Windows Phone 8
Endpunkte	22	20	55	25
Verbindungen	97	296	202	69
Datenvolumen	10,89 MB	1,28 MB	68,19 MB	1,76 MB

[17] Transport Layer Security (TLS) ist ein kryptografisches Protokoll, das eingesetzt wird, um Kommunikationsverbindungen im Internet abzusichern, z.B. beim Aufruf von Online-Banking-Seiten.

Für die Bewertung, ob – und gegebenenfalls welche – private Daten das Telefon verlassen, ist das reine Datenvolumen nicht entscheidend. Daher wurden in dieser Studie alle Einzelverbindungen untersucht. Nachfolgend werden die wichtigsten Ergebnisse zusammengefasst.

➜ **KOMMUNIKATION MIT DEM HERSTELLER** Alle vier Betriebssysteme kommunizieren mit Endpunkten, die sich dem jeweiligen Hersteller des Betriebssystems zuordnen lassen.

➜ **VERSCHLÜSSELTE KOMMUNIKATION** Alle vier Betriebssysteme setzen für einen Teil aufgebauter Verbindungen TLS zur Verschlüsselung der Datenübertragung ein. Für diese Verbindungen lässt sich im Rahmen der durchgeführten Tests nicht feststellen, welche Daten von den Endgeräten übertragen wurden.

➜ **DURCHGEHENDE VERBINDUNGEN** Kurz nach Verbinden des Gerätes mit dem Internet wurden bei Android und iOS Verbindungen aufgebaut, die beinahe über den gesamten Testzeitraum aufrechterhalten wurden. Bei iOS handelte es sich dabei um den Basisdienst *Apple Push Notification Service (APNS)*. Dieser Dienst dient dem Empfang von Push-Nachrichten. Hinsichtlich Android bestand die andauernde Verbindung mit mtalk.google.com, ein Dienst, der u.a. zur Bereitstellung von Video- und Chat-Funktionen eingesetzt wird (z.B. Google+ Hangouts). Auch BlackBerry OS baut kurz nach dem Start eine Verbindung zu einem BlackBerry-Server auf, die über fast den gesamten Messzeitraum aktiv bleibt. Der Zweck dieser Verbindung blieb jedoch unklar.

➜ **WERBEDIENSTE** Einzig für Android ließ sich beobachten, dass mit einem Endpunkt zu Werbezwecken kommuniziert wurde. Der Endpunkt dieser Konversation lässt sich DoubleClick zuordnen, einem Unternehmen der Google-Gruppe.

➜ **UPDATE ZUR POSITIONSBESTIMMUNG** Android und BlackBerry OS bauen eine Verbindung zu xtra1.gpsonextra.net bzw. zu xtra3.gpsonextra.net auf. Dieser Host übermittelt Daten an die Endgeräte, die die Positionsbestimmung per GPS auf den Geräten verbessern. Verkürzt dargestellt handelt es sich um ein Update für den Basisdienst zur Positionsbestimmung.

➜ **CONTENT DELIVERY NETWORKS (CDN)** Alle vier Betriebssysteme bauen Verbindungen mit sogenannten Content Delivery Networks (CDN) auf. Ein Content Delivery Network (CDN) ist eine verteilte Architektur zur Auslieferung von Daten über das Internet. Verkürzt dargestellt werden etwa Videos in verschiedenen Rechenzentren vorgehalten und bei Anfragen eines Nutzers immer der günstigste Speicherort gewählt, z.B. auf Basis geografischer Nähe zwischen Nutzer und Video. So kann die Dienstgüte, z.B. für ruckelfreies Videostreaming, stark verbessert werden. CDNs eignen sich ferner zur Bereitstellung von Betriebssystem-Updates.

➜ **STANDORTBESTIMMUNG UND VERFÜGBARE WLANS** Eine Auffälligkeit ließ sich beim Windows Phone beobachten: Dieses baute Verbindungen mit einem Endpunkt auf, der Dienste zur Standortbestimmung anbietet. Welche Daten übertragen wurden, konnte allerdings aufgrund der eingesetzten Verschlüsselung nicht festgestellt werden. Der Hostname (inference.location.live.net) sowie bekannt gewordene Vorfälle[18] lassen vermuten, dass es sich um einen Dienst zur Standortbestimmung handelt.

[18] Für weitere Informationen siehe http://www.cnet.com/news/microsofts-webmap-exposes-phone-pc-locations/ (Letzter Zugriff 29.07.2014)

Laut Microsoft werden von diesem Dienst Zellinformationen sowie Informationen über Drahtlosnetze in Reichweite erfasst. Falls diese Daten tatsächlich erfasst und gesendet werden, steht dies im Widerspruch zu der im Test gewählten minimalen Einrichtung, bei der *WLAN-Verbindungsdaten zur Erkennung von WLAN in der Umgebung sichern* explizit deaktiviert wurde.

Einzelergebnisse der Betriebssysteme

Die nachfolgenden Abschnitte geben eine detaillierte Übersicht über die zentralen Ergebnisse der Untersuchung der einzelnen Betriebssysteme.

Android

Insgesamt kommunizierte das Gerät mit **22 Endpunkten (IP-Adressen)** und etablierte **97 Verbindungen**, wobei **10,89 Megabyte** Daten ausgetauscht wurden. Weitere Informationen über die Konversationen und Verbindungen beinhalten dies:

- Bei 13 der 97 Verbindungen wird der Transportkanal mit TLS verschlüsselt.
- 20 der 22 Endpunkte besitzen IP-Adressen, die auf Google registriert sind.
- 1 der 22 Endpunkte besitzt eine IP-Adresse, die auf Peer1hosting[19] registriert ist.
- 1 der 22 Endpunkte besitzt eine IP-Adresse, die auf Hetzner Online[20] registriert ist.
- Die längste Verbindung (bestehend aus mehreren Konversationen) besteht mit der URL mobile-gtalk.l.google.com (für weitere Informationen siehe unten), dauert fast 23 Stunden und beginnt innerhalb der ersten zehn Sekunden, nachdem das Gerät mit dem Internet verbunden ist.

Bei den untersuchten Verbindungen fällt auf:
Bereits wenige Sekunden nach der Herstellung der Verbindung des Gerätes wird eine Verbindung zu einem Server etabliert, dessen Hostname mobile-gtalk.l.google.com lautet und der die URL mtalk.google.com besitzt. Dieser Dienst gehörte vormals zum Google Talk Client, d.h. Voice & Chat-Dienst der seit 2013 durch Google+ Hangouts ersetzt wurde. Diese Verbindung wird etabliert, ohne dass eine Verknüpfung des Gerätes mit einem Google-Konto existiert

Unmittelbar nach Verbindung mit dem Internet wird Kontakt zu einem Server aufgebaut, dessen Host xtra3.gpsonextra.net lautet. Die Adresse gpsonextra.net ist registriert auf die Firma *Qualcomm*, den Hersteller des im Gerät verbauten Funkchips. Ziel dieser Konversation ist die Übermittlung von Daten an das Endgerät, um die Positionsbestimmung per GPS zu verbessern, dieser Datenaustausch wird nicht zur Positionsbestimmung des Gerätes genutzt.

Auch etabliert das Gerät unmittelbar nach Verbindungsaufbau mit dem Internet eine Verbindung mit einem Server, dessen Hostname www.googleadservices.com lautet und der unter der URL http://www. google.com/doubleclick/ zu erreichen ist. DoubleClick ist ein Unternehmen der Google-Gruppe, das Werbetechnologien bereitstellt.[21] Diese Verbindung besteht für mehr als elf Stunden. Der

[19] http://www.peer1hosting.co.uk/ (Letzter Zugriff 29.07.2014)

[20] http://www.hetzner.de/ (Letzter Zugriff 29.07.2014)

[21] Für weitere Informationen siehe http://www.google.com/doubleclick/ (Letzter Zugriff 29.07.2014).

Verbindungsaufbau enthält eine Anfrage, welche offenbar für die vorinstallierte YouTube-App eine bestimmte Metrik zu Werbezwecken anfordert (/pagead/conversion/).

BlackBerry OS

Insgesamt kommunizierte das Gerät mit **20 Endpunkten (IP-Adressen)** und etablierte **296 Verbindungen**, wobei **1,28 Megabyte** Daten ausgetauscht wurden.

- 10 der 296 Verbindungen wurden mit TLS verschlüsselt.
- 15 von 20 Endpunkten besitzen IP-Adressen, die auf BlackBerry registriert sind.
- 2 von 20 Endpunkten besitzen IP-Adressen, die auf Akamai (CDN-Anbieter) registriert sind.
- 1 von 20 Endpunkten besitzt eine IP-Adresse, die auf Google registriert ist.
- 2 von 20 Endpunkten besitzen IP-Adressen, die auf Qualcomm registriert sind.

Kurz nach dem Aufbau der Verbindung zum WLAN wird automatisch eine Verbindung zu BlackBerry (blackberry.com) aufgebaut, die über den gesamten Testzeitraum aktiv ist.

Unter den untersuchten Verbindungen sind folgende hervorzuheben:
Unmittelbar nachdem das Gerät mit dem Internet verbunden ist, wird ein Server über die Adresse xtra3.gpsonextra.net kontaktiert. gpsonextra.net ist registriert auf die Firma *Qualcomm* (Hersteller des eingebauten Funkchips). Ziel dieser Konversation ist die Übermittlung von Daten an das Endgerät, um die Positionsbestimmung per GPS zu verbessern.

Zwei unverschlüsselte Verbindungen werden zu time.blackberry.com aufgebaut. Über diese Verbindungen synchronisiert BlackBerry seine Uhrzeit.

Eine verschlüsselte Verbindung wird zu einem BlackBerry-ID-Server aufgebaut, obwohl bei der Durchführung des Tests keine BlackBerry-ID auf dem Telefon eingerichtet war

Zwei Verbindungen werden zu Servern mit Eyeball AnyFirewall Engines aufgebaut. Dabei handelt es sich laut der Produktwebseite[22][23] um Technologien zur Umgehung von NAT-Firewalls, wie sie in vielen Heimnetzwerken zu finden sind. Dies ermöglicht den Aufbau von Direktverbindungen zwischen zwei hinter solchen Firewalls befindlichen Geräten. Möglicherweise wird diese Funktionalität für den BlackBerry Messenger (BBM) benötigt, der sowohl VoIP als auch Videotelefonie zwischen verschiedenen Endgeräten ermöglicht.

iOS

Insgesamt kommunizierte das Gerät mit **55 Endpunkten (IP-Adressen)** und etablierte mit diesen Endpunkten **202 Verbindungen**, wobei **68,19 Megabyte** Daten ausgetauscht wurden. Weitere Informationen über die Konversationen:

- 39 der 55 Endpunkte besitzen IP-Adressen, die auf Apple registriert sind.
- 16 der 55 Endpunkte besitzen eine IP-Adresse, die auf Akamai registriert ist.
- 105 der 202 Verbindungen wurden mit TLS verschlüsselt.
- 97 der 202 Verbindungen waren unverschlüsselt.

[22] http://www.eyeball.com/products/stun-turn-ice-library/ (Letzter Zugriff 29.07.2014)

[23] http://www.eyeball.com/nat-traversal/ (Letzter Zugriff 29.07.2014)

Unter den untersuchten Verbindungen sind folgende hervorzuheben:
Über den gesamten Testzeitraum bestand eine Verbindung mit mu-courier.push-apple.com.akadns.net, dem APNS (Apple Push Notification Service), der für das Empfangen von Push-Nachrichten auf dem iPhone vorgesehen ist. Die Verbindung zum APNS lässt sich vom iPhone aus nicht deaktivieren, außer durch das Abstellen der Netzwerkverbindung.

Die Verbindung mit der wu.apple.com ist unverschlüsselt und lässt sich auf die vorinstallierte Aktien-App zurückverfolgen. Für die Aktien-App ist standardmäßig die Hintergrundaktualisierung aktiviert. Diese lässt sich aber in den Systemeinstellungen abstellen. Aus der Konversation kann man herauslesen, welche Daten abgefragt werden, d.h. welche Aktien den Nutzer interessieren.

Windows Phone

Insgesamt kommunizierte das Gerät mit **25 Endpunkten (IP-Adressen)** und etablierte **69 Verbindungen**, wobei **1,76 Megabyte** Daten ausgetauscht wurden. Weitere Informationen über die Konversationen und Verbindungen:

- Bei 31 der 69 Verbindungen wird der Transportkanal mit TLS verschlüsselt.
- 12 der 25 Endpunkte besitzen eine IP-Adresse, die auf Microsoft registriert ist.
- 6 der 25 Endpunkte besitzen eine IP-Adresse, die auf Akamai registriert ist.
- Die verbleibenden 7 IP-Adressen der insgesamt 25 Konversationen verteilen sich auf Deutsche Telekom, EdgeCast Networks (CDN, gehört zu Verizon), nebula (finnischer Internet-Anbieter), Verizon und Internet Assigned Numbers Authority (IANA)[24].
- Die längste Konversation besteht mit dem Host mscrl.microsoft.com unter der URL cs1.wpc.v0cdn.net (für weitere Informationen siehe unten), dauert etwa 14 Stunden und beginnt innerhalb der ersten 90 Sekunden, nachdem das Gerät mit dem Internet verbunden ist. Anhand des Hostnamens kann abgeleitet werden, dass es sich um einen Dienst handelt, der regelmäßig die sogenannte *Certificate Revocation List (CRL)* aktualisiert [10]. Die Liste enthält nicht mehr gültige Zertifikate sowie den Grund für die Ungültigkeit. Zertifikate werden u.a. zur Authentifizierung von Kommunikationspartnern, z.B. Webservern, genutzt.

Unter den untersuchten Verbindungen stechen hervor:
Etwa 13 Stunden nachdem das Gerät mit dem Internet verbunden wurde, wird eine verschlüsselte Verbindung zu dem Host inference.location.live.net unter der URL inference.location.glbdns2.microsoft.com aufgebaut. Aufgrund der Verschlüsselung können die übertragenen Daten nicht gelesen werden. Hostname sowie diverse Berichte[25] über die Aufzeichnung von Standortdaten deuten aber darauf hin, dass es sich hierbei um einen Dienst zur Standortbestimmung handelt. Laut Microsoft werden bei diesem Dienst Zellinformationen sowie Informationen über Drahtlosnetze in Reichweite erfasst. Falls diese Daten tatsächlich erfasst und gesendet werden, steht dies im Widerspruch zu der im Test gewählten minimalen Einrichtung, bei der *WLAN-Verbindungsdaten zur Erkennung von WLAN in der Umgebung sichern* explizit deaktiviert wurde (siehe Kapitel 5.1.1, Abschnitt Windows Phone).

---

[24] IANA ist ein US-amerikanisches Unternehmen, das unter anderem für die Zuordnung von IP-Adressen im Internet zuständig ist. Für weitere Informationen siehe https://www.iana.org/ (Letzter Zugriff 29.07.2014).

[25] Siehe z.B. http://www.cnet.com/news/microsofts-web-map-exposesphone-pc-locations/ (Letzter Zugriff 29.07.2014)

Weiterhin baut das Gerät – etwa eine Stunde nachdem es mit dem Internet verbunden wurde – eine Verbindung mit dem Host statsfe2.update.microsoft.com auf. Sodann übermittelt das Gerät u.a. folgende Informationen an den Host: eine (vermutlich) eindeutige ID für das Gerät, Zeitstempel des Berichtes, Gerätetyp, Betriebssystemversion sowie kompatible Prozessorarchitektur. Die Erfassung dieser Informationen ist konsistent mit den Angaben in den Nutzungsbedingungen zur Erhebung von sogenannten *Standardinformationen* über das Gerät (siehe Abschnitt Windows Phone in Kapitel 5.6).

Unmittelbar nachdem das Gerät mit dem Internet verbunden ist, wird zudem eine verschlüsselte Verbindung zu einem Server aufgebaut, dessen Hostname api.live.net lautet. Über diese Adresse können Webservices mit entsprechender Autorisierung alle Daten abrufen, die mit einem Microsoft-Konto verbunden sind. Der Aufruf der Programmierschnittstelle (API) findet zeitlich viel früher statt als die Aufforderung des Nutzers, während der Einrichtung seines Endgerätes dieses mit einem Microsoft-Konto zu verknüpfen.

5.2 Einrichten eines Kundenkontos

Kundenkonten dienen dazu, dem Nutzer Zugriff auf Dienste des Herstellers zu gewähren. Welche dies genau sind, ist dabei herstellerabhängig. In der Regel werden Dienste wie E-Mail-Konten oder Cloud-Synchronisierung angeboten. Auch für den Zugriff auf Management-Dienste wie etwa Remote Wipe wird ein Kundenkonto benötigt. Nicht zuletzt dient das Kundenkonto dazu, in den App-Markets einkaufen zu können wie in einem normalen Webshop.

Für die Nutzung vieler Dienste ist die Einrichtung eines Kundenkontos Voraussetzung. Sonst bleibt der Weg zu neuen Apps im Allgemeinen verschlossen. Der Nutzer hat bei allen Betriebssystemen die Wahl, ob er ein Kundenkonto eröffnen möchte oder nicht.

Android

POTENZIELL BETROFFENE DATEN: Gerätetyp, Netzbetreiber, Geräte-IDs, installierte Apps, E-Mail, Fotos, Foto-Metadaten, Termine, Aufgaben, Kontakte, allgemeine Informationen über den Smartphone-Benutzer, Browserverlauf

Für die Einrichtung eines Endgerätes, das mit Android betrieben wird, muss kein neues Google-Konto erstellt bzw. ein existierendes mit dem Gerät verknüpft werden. Ohne Konto können Nutzer nicht auf den Google Play Store zugreifen, um weitere Apps zu installieren. Die Nutzung eines Google-Kontos erfordert die Zustimmung zu

- den generellen Datenschutz- sowie Nutzungsbestimmungen von Google,
- den Datenschutz- sowie Nutzungsbestimmungen von Google Chrome sowie
- den Nutzungsbedingungen von Google Play.

Die Verknüpfung eines Gerätes mit einem Google-Konto führt zu einer Übertragung gerätespezifischer Daten zu Google. Diese Daten umfassen: Gerätetyp (z.B. LG E960 Nexus 4), Netzbetreiber (z.B. Vodafone), IMEI, letzte Aktivität sowie Registrierungsdatum. Diese Informationen können nach Anmeldung beim Google-Konto unter *Google Account* ➜ *Data Tools* ➜ *View Account Data* nachvollzogen werden.

Infolge einer Verknüpfung wird der Nutzer zudem gefragt, welche Daten mit dem Konto synchronisiert werden sollen. Hierzu zählen unter anderem die Personendetails, also allgemeine Informationen über den Nutzer des Endgerätes.

BlackBerry OS

POTENZIELL BETROFFENE DATEN: Geräte-IDs, Region und Spracheinstellungen, Betriebssystemversion, Gerätetyp, Netzbetreiber, allgemeine Informationen über den Benutzer, Standortdaten

Die Einrichtung einer BlackBerry-ID für die Nutzung eines BlackBerry-Geräts ist optional und erfordert die Zustimmung zu der BlackBerry-Datenschutzrichtlinie. Mit der Zustimmung räumt der Nutzer BlackBerry das Recht ein, auf persönliche Daten zuzugreifen. Diese Daten können Namen, Wohnanschrift, E-Mail-Adresse, Telefonnummer, BlackBerry-ID, Kontodaten und Einstellungen, Geräteidentifikationsmerkmale, die BlackBerry-PIN und Standortinformationen sein [8, Abschnitt 4].

Um eine BlackBerry-ID zu registrieren, muss der Anwender einen Nutzernamen wählen, seinen Vor- und Nachnamen angeben sowie eine Sicherheitsfrage inklusive dazugehöriger Antwort eingeben. Diese wird benutzt, um ein vergessenes Passwort neu zu setzen.

Für die Installation weiterer Apps aus der BlackBerry App-World wird ebenfalls die BlackBerry-ID benötigt. Um kostenpflichtige Apps herunterladen zu können, muss der Anwender Zahlungsinformationen in seinem BlackBerry-ID-Konto hinterlegen. Kostenlose Apps lassen sich ohne Eingabe von Zahlungsinformationen herunterladen und installieren.

Ebenso wird eine BlackBerry-ID für die Nutzung von BlackBerry Protect benötigt, das es Anwendern erlaubt, verlorene oder gestohlene Geräte aus der Entfernung zu orten oder zu löschen.

iOS

POTENZIELL BETROFFENE DATEN: Gerätetyp, Netzbetreiber, Geräte IDs, installierte Apps, E-Mail, Fotos, Foto-Metadaten, Termine, Aufgaben, Kontakte, allgemeine Informationen über den Benutzer

Für die Einrichtung eines Smartphones unter iOS ist es nicht zwingend notwendig, ein Konto bei Apple – eine sogenannte Apple-ID – einzurichten. Ohne können allerdings keine weiteren Apps installiert werden, und es ist nicht möglich, die Cloud-Dienste iCloud zu verwenden. Dies schließt auch Management-Dienste wie „Finde mein iPhone" ein, welche dem Nutzer bei Verlust des Smartphones helfen können, es wiederzufinden.

Zusätzlich zur Zustimmung zum iOS-Lizenzvertrag muss ein Nutzer bei der Einrichtung einer Apple-ID folgende Bestimmungen von Apple anerkennen:

- Nutzungsbedingungen für iCloud
- Datenschutzrichtlinie von Apple
- Nutzungsbedingungen für Game Center

Wird auf dem Smartphone die Apple-ID eingerichtet, kann die Synchronisation mit iCloud genutzt werden. Diese muss allerdings separat aktiviert werden, d.h., nach der allgemeinen Einrichtung der Apple-ID findet ohne weitere Nutzerinteraktion keine Übertragung von personenbezogenen Daten an Apple statt. Welche Daten an Apple übertragen werden, hängt davon ab, welche Synchronisationsoptionen der Nutzer bei der Aktivierung der iCloud einschaltet.

Windows Phone

POTENZIELL BETROFFENE DATEN: allgemeine Informationen über den Smartphone-Benutzer, Kontakte, Termine, SMS, installierte Apps, Benutzerkonten, Fotos, E-Mail

Bei der Einrichtung eines Windows-Phone-Gerätes ist es nicht notwendig, einen neuen Microsoft-Account zu erstellen oder einen existierenden mit dem Gerät zu verknüpfen. Will ein Nutzer zu einem späteren Zeitpunkt Apps aus dem Windows Phone Store über die Windows Phone Market App installieren, muss er zuvor das Telefon mit einem Microsoft-Account verbinden. Auch stehen Funktionen wie Xbox LIVE, Xbox Music und Backup sowie Online-Konto-Dienste wie *Mein Handy finden* nicht ohne Microsoft-Konto zur Verfügung. Zur Erstellung eines Microsoft-Kontos sind folgende Angaben notwendig: Geschlecht, Land/Region, Geburtsdaten und Postleitzahl.

Hat ein Nutzer ein Microsoft-Konto mit dem mobilen Endgerät verknüpft, werden alle diesem Konto bereits zugeordneten Kontakte auf das Gerät kopiert. Ähnlich verhält es sich mit Kontakten und Kalendereinträgen, die auf dem Endgerät gespeichert sind: Von diesen wird laut Microsoft *automatisch eine Sicherung erstellt*. D.h., Kontakte und Kalendereinträge werden auf einen Server von Microsoft hochgeladen und dort gespeichert.

Weiterhin wird der Nutzer während der Verknüpfung seines Gerätes mit einem Microsoft-Konto aufgefordert, vorhandene SMS-Nachrichten zu sichern, d.h. auf einen Microsoft-Server zu speichern, Fotos auf OneDrive (vormals SkyDrive) hochzuladen und zu speichern sowie die Handyeinstellungen zu sichern, d.h. Konfigurationsprofile des Gerätes (u.a. auf dem Gerät installierte Anwendungen, eingerichtete Konten, Favoriten im Browser, Anrufliste, weitere Einstellungen zu Anwendungen wie z.B. Fotos, SMS/MMS, Konto, Ortung, Internet Explorer, Sperrbildschirm, Spracherkennung usw.).

5.3 Sprachsteuerung aktivieren

Die Sprachsteuerung erlaubt die Bedienung des Smartphones über gesprochene Kommandos. Sie funktioniert ähnlich wie die Diktierfunktion. Während die Sprachsteuerung bereit ist, Befehle zu empfangen, wird über das Mikrofon des Smartphones alles aufgezeichnet, was der Nutzer sagt. Die Aufzeichnung wird dann an einen Server geschickt und dort mittels Spracherkennungsalgorithmen in Text umgewandelt. Spracherkennung ist rechenaufwendig und wird daher von den Herstellern auf externe Server ausgelagert. Der Text wird dann wieder zurück an das Smartphone geschickt, woraufhin es den Befehl ausführen kann.

Führt man sich vor Augen, dass bei jeder Nutzung der Sprachsteuerung die gesprochenen Befehle an externe Server geschickt werden, so wird klar, dass bei intensiver Nutzung dieser Funktionalität ein sehr genaues Nutzungsprofil des Smartphones erstellt werden kann.

Android

POTENZIELL BETROFFENE DATEN: Spracheingabe

Android bietet Nutzern die Funktion *Sprachsuche*, mit der Suchanfragen per Spracheingabe an das Gerät übergeben werden können. Die Spracheingaben werden an die Google-Server gesendet, um dort die Spracheingabe in Text umzuwandeln.

Google speichert für jede Suchanfrage die Sprache, das Land, die gesprochene Eingabe sowie den erkannten Text. Die Sprachsuche kann nur genutzt werden, wenn das Endgerät mit dem Internet verbunden ist.

Android bietet weiterhin die Möglichkeit, Sprachpakete (z.B. Deutsch) herunterzuladen. Auf diese Weise können Spracheingaben auch direkt auf dem Gerät ausgewertet (offline) und etwa für Diktierfunktionen genutzt werden.

BlackBerry OS

POTENZIELL BETROFFENE DATEN: Spracheingabe, installierte Apps, allgemeine Informationen über den Smartphone-Benutzer, Kontakte, Standortdaten, Musik

Über die BlackBerry-*Sprachsteuerung* kann man Text diktieren oder Befehle erteilen. Die Sprachanweisungen werden an BlackBerry-Server übertragen. Eine Interpretation der Ergebnisse findet unter anderem mithilfe der Kontakte, mit Namen von Anwendungen und Titeln in den Musikwiedergabelisten, Standortdaten und gerätebezogenen Informationen statt, sodass diese Daten (oder Ausschnitte von ihnen) ebenfalls an BlackBerry-Server übertragen werden.

Aktiviert man die Spracheingabe in den Einstellungen des Smartphones, hat man die Wahl, ob man eine vollständige Spracherkennung nutzen oder nur Unterstützung für sprachgesteuertes Wählen aktivieren möchte.

iOS

POTENZIELL BETROFFENE DATEN: Spracheingabe, Kontakte, Musik

Wird Siri oder die Diktierfunktion genutzt, wird alles Gesagte aufgezeichnet und an Apple gesendet, um die Worte in Text umzusetzen und die Anfrage zu verarbeiten.

Aktiviert der Nutzer Siri, stimmt er zu, dass zusätzlich weitere Informationen an Apple gesendet werden, z.B. der eigene Name und Kurzname sowie die Namen und Kurznamen der eigenen Kontakte sowie die Beziehungen zu den Kontakten oder die Titel in der Musiksammlung.

Windows Phone

POTENZIELL BETROFFENE DATEN: Spracheingabe

Windows Phone bietet Nutzern eine *Sprachfunktion*, mit der z.B. sprachgesteuerte Online-Suchen durchgeführt werden können oder Nachrichten per Sprachbefehl versendet werden können. Zur Realisierung dieser Funktionen setzt Windows Phone einen *Spracherkennungsdienst* ein, dessen Aktivierung ein Nutzer bei erstmaligem Zugriff auf Sprachfunktionen bestätigen muss.[26]

Hat ein Nutzer diesen Dienst aktiviert, werden sowohl die Spracheingaben als auch damit verbundene Informationen wie z.B. Korrekturen des Textergebnisses an Microsoft zu Verbesserungszwecken gesendet. Microsoft ordnet dem übersendenden Endgerät eine eindeutige, zufällig generierte ID zu. So wird laut Microsoft verhindert, dass die Spracheingaben zur Identifikation des Nutzers eingesetzt werden können.

Der Spracherkennungsdienst kann durch den Nutzer deaktiviert werden. Allerdings schränkt dies die Leistungsfähigkeit der Sprachfunktion deutlich ein.

[26] Diese Aussagen beziehen sich auf Windows Phone 8. Der Sprachassistent Cortana, der mit WP 8.1 ausgeliefert wird, wird hier nicht berücksichtigt.

5.4 Einschalten von Ortungsdiensten

Auf rein technischer Ebene dienen Ortungsdienste zur Lokalisierung eines Smartphones. Dazu wird z.B. über einen eingebauten GPS-Empfänger der Standort bestimmt. Viele Apps verwenden Standortdaten dazu, dem Nutzer ortsabhängig Informationen zur Verfügung zu stellen. Navigations-Apps ermöglichen es mit Standortdaten, dem Nutzer nicht nur den Weg zu zeigen, sondern ihn per Turn-by-Turn-Navigation schrittweise zum Ziel zu führen. Andere Apps zeigen dem Nutzer z.B. an, welche seiner Freunde gerade in der Nähe sind.

Bei der Nutzung von Ortungsdiensten wird die Standortbestimmung lokal, d.h. auf dem Endgerät, ausgeführt. Diese Daten werden sodann zu einem Server geschickt, damit dieser die für diesen Standort relevanten Daten zurücksenden kann. So kann ein Bewegungsprofil des Nutzers erstellt werden. Aus einem solchen Profil lässt sich beispielsweise herauslesen, wo der Nutzer arbeitet oder wo er wohnt und welche Orte er regelmäßig besucht.

Alle Betriebssysteme bieten die Möglichkeit an, Ortungsdienste generell zu deaktivieren. Dies hat allerdings zur Folge, dass etwa Turn-by-Turn-Navigations-Apps nicht mehr funktionieren. Die Unterschiede im Umgang mit Ortungsdiensten bei den verschiedenen Betriebssystemen werden im Folgenden vorgestellt.

Android

POTENZIELL BETROFFENE DATEN: Standortdaten, Bewegungssensor, IP-Adresse

Google unterscheidet zwischen drei Arten von Standortdaten, die zur Bereitstellung weiterer Dienste erfasst, verarbeitet sowie gespeichert werden. Im Folgenden werden diese Standortdaten näher beschrieben.

1. **Gerätebasierte Informationen** wie GPS, WLAN-Zugangspunkte sowie Mobilfunkmast-ID ermöglichen in der Regel eine sehr genaue Standortbestimmung eines Gerätes. Darüber hinaus kann auch andere Sensorik wie Beschleunigungsmesser, Kompass, Gyroskop und Barometer genutzt werden, um die Genauigkeit der Standortbestimmung zu erhöhen. Der Nutzer kann die Erfassung gerätebasierter Standortinformationen einschränken (siehe hierzu Kapitel 7.3 für weitere Informationen).
2. **Daten des Internetverkehrs** wie z.B. IP-Adresse können in der Regel bestimmten geografischen Regionen zugewiesen werden und so als Information zur Näherung des Standortes eines Gerätes dienen. Um die Erfassung dieser Standortinformationen einzuschränken, sind fortgeschrittene Anwendungen wie z.B. VPN-Dienste, Anonymisierungs-Proxies, notwendig. Diese werden nicht durch Android bereitgestellt und müssen daher durch den Nutzer installiert bzw. konfiguriert werden.
3. **Implizite Standortinformationen** verraten nicht den Standort des Gerätes, sondern erlauben eine Annahme zum Aufenthaltsort. So kann eine Suchanfrage, etwa nach einem Restaurant in einer bestimmten Stadt, einen Anhaltspunkt über den Standort des Endgerätes liefern. Nutzer können die Erfassung solcher Standortinformationen sehr wenig beschränken.

Um die so erfassten Standortinformationen weiterzuverarbeiten, bietet Google Nutzern die Möglichkeit, aktuelle Standortdaten eines Endgerätes regelmäßig mit einem verknüpften Google-Konto über sogenannte Standortberichte zu synchronisieren.

Davon ausgehend verknüpft die Anwendung *Standortverlauf* die Daten des Standortberichtes und stellt diese Daten wiederum anderen Anwendungen zur Verfügung (z.B. Google Now). Die Daten des Standortverlaufs werden laut Google nicht ohne die Zustimmung des Nutzers weitergegeben. Zur

Bestimmung der Standortinformationen eines mobilen Endgerätes ist keine SIM-Karte, d.h. keine Verbindung mit einem Mobilfunknetz, notwendig.

Weiterhin ist es dem Nutzer möglich, im Nachhinein in den Systemeinstellungen nachzuvollziehen, welche Apps und Systemdienste zuletzt Ortungsdienste genutzt haben.

BlackBerry OS

POTENZIELL BETROFFENE DATEN: Standortdaten

Sobald der Nutzer *Datendienste* in BlackBerry OS aktiviert und standortbezogene Dienste auf dem Gerät verwendet, werden Daten an BlackBerry übertragen. Diese umfassen „anonyme Crowdsourcing-Informationen über Wi-Fi-Hotspots und Sendemasten für eine bessere und schnellere Standorterkennung". BlackBerry weist darauf hin, dass die Speicherung dieser Daten in einer Form erfolgt, „die keine persönliche Zuordnung erlaubt" [8, Abschnitt 4g].

Die Einstellung lässt sich global deaktivieren, sodass keine App Standortdaten verwenden kann. Weiterhin bietet das BlackBerry-Smartphone die Möglichkeit, den Zugriff auf Standortdaten für einzelne Apps zu (de)aktivieren.

Bei der Nutzung der Karten-App von BlackBerry OS, die standardmäßig auf den Geräten installiert ist, werden (anonymisierte) Standortdaten des Telefons an BlackBerry übertragen, um Verkehrsstaus anzuzeigen. Diese Daten werden auch dafür verwendet, um die Routenplanung für den Anwender zu verbessern. Die Einstellung ist deaktivierbar.

Für die Nutzung von standortbezogener *Werbung* wird der Standort des Telefons ebenfalls an BlackBerry übertragen. BlackBerry versichert, dass „keinerlei Daten an dritte Werbeanbieter weitergegeben [werden], anhand derer [der Anwender] persönlich identifizierbar" ist. Standortbezogene Werbung kann in den Systemeinstellungen des Smartphones deaktiviert werden.

iOS

POTENZIELL BETROFFENE DATEN: Standortdaten

Aktiviert der Nutzer auf dem Smartphone die Ortungsdienste, stimmt er damit zu, dass Apple und andere die auf dem Smartphone erhobenen Standortdaten übertragen, speichern, verwalten, verarbeiten und verwenden dürfen, um auf Standortdaten basierende Dienste bereitzustellen und verbessern zu können. Wird es Drittanbieter-Apps erlaubt, auf Ortungsdienste zuzugreifen, unterliegen die der App bereitgestellten Standortdaten nur der Datenschutzrichtlinie des App-Anbieters.

Unter diese Daten fallen laut Nutzungsbedingungen:

- Standortdaten einschließlich der geografischen Echtzeitposition des iPhones
- Informationen zur Fahrgeschwindigkeit auf Straßen
- Ortssuchanfragen (z.B. in der Karten-App)
- Orte, an denen Programme gestartet werden
- Orte, an denen Programme gekauft werden

Um den Standort möglichst genau bestimmen zu können, setzt Apple nicht nur GPS ein, sondern verwendet auch eine durch Crowdsourcing erstellte Datenbank mit WLAN-Hotspots sowie eine durch Crowdsourcing erstellte Datenbank mit Mobilfunkmasten. Bei der Aktivierung der Ortungsdienste auf dem Smartphone werden auch in regelmäßigen Abständen die per Geotagging markierten Positionen von nahe gelegenen WLAN-Hotspots und Mobilfunkmasten in anonymisierter Form an Apple

geschickt. Dies lässt sich auf dem Smartphone einzeln deaktivieren, ohne Ortungsdienste komplett auszuschalten.

Stellt das Smartphone fest, dass es unterwegs ist, sendet es bei aktivierten Ortungsdiensten in regelmäßigen Abständen die GPS-Position und Informationen zur Fahrgeschwindigkeit in anonymisierter Form an Apple zum Aufbau einer Crowdsourcing-Datenbank für den Straßenverkehr.[27] Auch dies lässt sich auf dem Smartphone einzeln abschalten, ohne Ortungsdienste komplett zu deaktivieren.

In regelmäßigen Abständen werden Informationen über Orte an Apple gesendet, an denen Apps gekauft oder gestartet wurden. Die Übertragung geschieht verschlüsselt und laut Apple anonymisiert. Dies lässt sich auf dem Smartphone einzeln deaktivieren, ohne Ortungsdienste komplett zu deaktivieren.

Im Smartphone werden auch Orte gespeichert, die kürzlich besucht wurden, sowie wann und wie oft. Diese Daten bleiben laut Apple nur auf dem Smartphone gespeichert.

An Apple werden auch Standortdaten gesendet, damit geografisch relevante Werbung angezeigt werden kann. Dies lässt sich auf dem Smartphone einzeln deaktivieren, ohne Ortungsdienste komplett zu deaktivieren. Eine Deaktivierung hat nur zur Folge, dass die Werbung nicht mehr „geografisch relevant" ist, es wird jedoch weiterhin Werbung angezeigt.

Für Notrufe sind die Ortungsdienste stets aktiviert, selbst wenn Ortungsdienste vom Benutzer generell abgestellt worden sind.

Damit ein Nutzer erkennen kann, wann Ortungsdienste bzw. Standortdaten verwendet werden, bietet iOS die Möglichkeit, in der Statusleiste des Smartphones ein Symbol anzuzeigen, welches immer beim Zugriff auf Ortungsdienste sichtbar ist. Weiterhin ist es dem Nutzer möglich, im Nachhinein in den Systemeinstellungen nachzuvollziehen, welche Apps und Systemdienste innerhalb der letzten 24 Stunden Ortungsdienste genutzt haben.

Windows Phone

POTENZIELL BETROFFENE DATEN: Standortdaten

Ortungsdienste sind bei Windows Phone standardmäßig aktiviert. Sie können global deaktiviert werden. In diesem Fall hat keine App Zugriff auf Informationen, um Ortungsdienste auszuführen. Nutzer von Windows Phone können den Zugriff auf Standortdaten zudem einzelnen Apps des Telefons gewähren, wenn diese selbst eine Auswahlmöglichkeit anbieten.[28]

Die Grundlage für Ortungsdienste bildet die *Positionsdatenbank*, welche die Daten zur Bestimmung des ungefähren Standortes des Handys auf dem Gerät speichert und anderen Anwendungen des Gerätes bereitstellt. Bei Zustimmung des Nutzers werden hier WLAN-Zugangspunkte, GPS-Koordinaten sowie Informationen der Mobilfunkzelle gespeichert. Diensten des Gerätes werden laut Microsoft allerdings nur Daten bereitgestellt, die keine Identifizierung des Nutzers zulassen. Diese können umfassen: Breitengrad, Längengrad, Geschwindigkeit, Richtung sowie Höhe des Telefons.

Microsoft empfiehlt die einmalige Übermittlung von Standortdaten bei Aktivierung des Gerätes. Der Nutzer muss der Ausführung dieses Dienstes zustimmen.

---

[27] http://support.apple.com/kb/HT5594?viewlocale=de_DE (Letzter Zugriff 29.07.2014)

[28] Inwieweit die in einer App ausgewählte Option vom Betriebssystem durchgesetzt wird, wurde nicht geprüft.

5.5 Erlauben von interessenbezogener Werbung

Mit interessenbezogener Werbung bezeichnet man ein Auswahlverfahren von Werbeanzeigen. Es basiert darauf, nur solche Anzeigen zu präsentieren, die den Interessen des Kunden entsprechen. Grundvoraussetzung dazu sind zwei Dinge: Zum einen muss der Werber den Kunden identifizieren können, und zum anderen muss er seine Interessen kennen.

Ein wichtiger Aspekt bei interessenbezogener Werbung ist die Profilbildung. Je umfassender das Profil ist, desto wertvoller ist es für den Werber. Daher wird hier auch versucht, Informationen aus unterschiedlichsten Quellen zusammenzutragen. So ist z.B. denkbar, dass Werber ein Kundenprofil auf Basis seines Surfverhaltens im Netz erstellt haben und ein zweites Profil bei der Nutzung einer App auf dem Smartphone. Kann der Werber dann verifizieren, dass beide Profile zu dem gleichen Kunden gehören, hat er ein wesentlich genaueres gewonnen.

Auf Smartphones gehört Werbung vor allem bei kostenfreien Versionen von Apps zum Alltag. Viele Apps setzen Werbung ein, um sich zu finanzieren. Bei der Entscheidung für eine App sollte man sich daher bewusst machen, dass man auch Daten von sich preisgibt.

Android

POTENZIELL BETROFFENE DATEN: IP-Adresse, Cookies

Google setzt verschiedene Technologien ein, um Nutzern interessenbezogene Werbung zu präsentieren sowie Remarketing, d.h. Kennzeichnung eines beobachteten Nutzerinteresses und dafür abgestimmte Werbung (z.B. ein Schuhmodell, das sich ein Nutzer auf einer Webseite angesehen hat, wird ihm danach als Werbung präsentiert).

Wird eine Anzeige auf einer besuchten Webseite eines Nutzers eingeblendet, erfasst Google folgende Daten: Webanfrage, IP-Adresse, Browsertyp, Browsersprache, Datum und Uhrzeit der Anfrage sowie ein oder mehrere Cookies, die den Browser des Nutzers u.U. eindeutig identifizieren können.

Ferner kommen zur Schaltung personalisierter Werbung oft Cookies zum Einsatz. Dienste, wie z.B. mobile Apps, unterstützen diese Verfahren nicht. Um auch in diesen Diensten personalisierte Anzeigen schalten zu können, verwendet Google sogenannte *anonyme Kennungen*. Dabei handelt es sich um eine nach dem Zufallsprinzip erstellte Zeichenfolge, welche eine ähnliche Funktionalität wie Cookies bereitstellen.

Android bietet ferner die Möglichkeit, personalisierte Werbung zu deaktivieren. Dies ist in der App *Google-Einstellungen* unter *Anzeigen* ➜ *Interessenbezogene Anzeigen* möglich.

BlackBerry OS

POTENZIELL BETROFFENE DATEN: Standortdaten

BlackBerry gibt an, verschiedene Technologien einzusetzen, um Nutzern interessenbezogene Werbung zu präsentieren sowie Remarketing zu betreiben. BlackBerry verwendet dafür einen eigenen Advertising Service, der mit Ad-Netzwerken zusammenarbeitet und sich merkt, auf welche Werbung ein Nutzer besonders häufig klickt.

Der BlackBerry Advertising Service erlaubt es, Metadaten über den Nutzer der App zu übertragen, um zielgerichtetere Werbung anzuzeigen. Eine Dokumentation über mögliche Metadaten steht nicht zur Verfügung.[29]

[29] In der Dokumentation auf https://developer.blackberry.com/bbos/html5/ documentation/webworks_ad_services_api_1731218_11.html (Letzter Zugriff 29.07.2014) finden sich jedoch Metadaten wie age und activity.

iOS

POTENZIELL BETROFFENE DATEN: Standortdaten, Geräte-IDs

Apple schränkt die Möglichkeiten zur Identifikation des Nutzers ein, indem Apps kein Zugriff auf gängige Hardware-IDs wie IMEI oder MAC-Adresse gewährt wird. Aus Sicht der App-Entwickler kann eine Identifikation des Nutzers wichtig sein, um beispielsweise zu erkennen, dass ein Nutzer mehrere Apps des gleichen Entwicklers benutzt. Damit App-Entwickler und Werber den Nutzer identifizieren können, hat Apple drei Identifikatoren eingeführt, auf welche Apps zugreifen können:

➜ **APPLICATION ID** Dieser Identifikator ist eindeutig über alle Apps auf dem Smartphone. Löscht der Nutzer die App, wird auch der Identifikator vom Smartphone gelöscht.

➜ **VENDOR ID** Dieser Identifikator ist eindeutig für Apps eines Entwicklers auf dem Smartphone. Der Identifikator bleibt erhalten, solange noch eine App des gleichen Entwicklers auf dem Smartphone vorhanden ist.

➜ **ADVERTISING ID** Dieser Identifikator ist eindeutig auf einem Smartphone und bleibt erhalten, bis der Nutzer das Smartphone komplett zurücksetzt. Der Nutzer kann diesen Identifikator auch separat zurücksetzen.

Interessenbezogene Werbung lässt sich unter iOS deaktivieren. Dabei wird ein Flag auf dem Smartphone gesetzt, welches anzeigt, dass Werbefirmen die Advertising ID nicht nutzen dürfen, um interessenbezogene Werbung zu senden [21]. Der Nutzer erhält jedoch die gleiche Menge an Werbeanzeigen, egal, ob interessenbezogene Werbung aktiviert oder deaktiviert wurde.

Windows Phone

POTENZIELL BETROFFENE DATEN: Browserverlauf, Geräte-IDs, Betriebssystemversion, Informationen zum Handybesitzer, IP-Adresse, Cookies, Standortdaten

Microsoft ermöglicht personalisierte Werbung, bei der Nutzern z.B. in Apps Werbung eingeblendet wird, die für sie besonders relevant sein soll. Auch schließt dies Drittanbieter ein, die Nutzern personalisierte Werbung anzeigen. Im letzteren Fall wird eine eindeutige ID für den Nutzer generiert und diese an den Drittanbieter übergeben. Zur Personalisierung von Werbung nutzt Microsoft u.a. folgende Informationen:

- Suchbegriffe, die Nutzer eingeben, und Suchergebnisse, auf die Nutzer klicken, wenn Sie den Bing-Suchdienst nutzen
- die Seiten, die Nutzer sich ansehen, sowie die Links, auf die sie bei der Nutzung der Webseiten und Dienste von Microsoft und deren Werbepartnern klicken
- demografische Daten, die ein Nutzer bei der Erstellung des Microsoft-Kontos bereitstellt, wie z. B. Alter, Beruf und Wohnort

Interagiert ein Nutzer mit Werbung von Microsoft oder Partnern, erfasst Microsoft u.a. folgende Informationen:

- IP-Adresse des Endgerätes
- IDs der Microsoft-Cookies oder Kennung der Werbeanzeigen

- Computer-, Browser- oder Geräteinformationen einschließlich Browsertyp und -sprache, Betriebssystem und URLs
- Informationen über spezifische Werbung, die auf der Seite veröffentlicht wurde, sowie Datum und Uhrzeit der Bereitstellung
- Information über die von Nutzern angezeigten Seiten sowie die Links, auf die sie klicken
- ungefähren Standort des Gerätes

Nutzer von Windows Phone können personalisierte Werbung deaktivieren, indem sie unter http://choice.microsoft.com/de-DE die entsprechende Option abwählen.

5.6 Erhebung von Nutzungs- und Diagnosedaten

Nutzungs- und Diagnosedaten sind Daten, die beim Benutzen eines Smartphones anfallen. Nutzungsdaten werden erhoben, um herauszufinden, ob und wie bestimmte Dienste genutzt werden. Diagnosedaten sind vor allem interessant, wenn Fehler bei der Benutzung auftreten. Beide können dazu beitragen, die auf dem Smartphone vorhandenen Dienste zu verbessern, und bieten daher eine für den Hersteller sehr wertvolle Datenbasis.

Welche Daten genau erfasst werden, ist nicht klar definiert und daher für den Nutzer wenig transparent. Wenn ein Hersteller etwa angibt, dass „technische, nutzungsrelevante und zugehörige Informationen"[30] erhoben werden, so bleibt hier viel Spielraum, welche Daten ein Hersteller darunter verstehen kann. Die Daten lassen Rückschlüsse auf das Nutzungsverhalten des Anwenders zu und könnten daher zur Profilbildung genutzt werden.

Erlaubt der Nutzer die Erhebung von Nutzungs- und Diagnosedaten, trägt er unentgeltlich dazu bei, die Produkte des Herstellers zu verbessern. Dies setzt allerdings das Vertrauen des Nutzers in den Hersteller voraus, dass dieser die gesammelten Daten ausschließlich zur Verbesserung der Produkte nutzt und entsprechend vertraulich behandelt.

Android

POTENZIELL BETROFFENE DATEN: Geräte-IDs, Anrufliste & Anrufstatistik, eigene Rufnummer, anonyme Nutzungsdaten, Gerätetyp, Betriebssystemversion, Netzbetreiber

Bei der Nutzung von Google-Diensten können gerätebezogene Informationen erfasst werden. Dazu zählen: Modell der verwendeten Hardware, Version des Betriebssystems, eindeutige Gerätekennungen wie IMEI sowie Informationen über das Mobilfunknetz einschließlich der Telefonnummer.

Ferner kann Google Einzelheiten darüber erfassen, welche Google-Dienste verwendet werden. Genutzt werden dazu *Serverprotokolle*, d.h. Aufzeichnungen von Aufrufen bestimmter Server, welche die Google-Dienste bereitstellen. Ein Beispiel hierfür sind Suchanfragen, die ein Nutzer auf google.de getätigt hat.

Telefonieprotokoll-Informationen sind eine weitere Kategorie von Daten, die Google erfassen, speichern und verarbeiten kann. Solche protokollierten Daten sind Telefonnummer, Anrufernummer, Weiterleitungsnummern, Datum und Uhrzeit von Anrufen, Dauer von Anrufen, SMS-Routing-Informationen sowie Art der Anrufe. Es geht aus den Angaben von Google nicht hervor, ob diese Daten

[30] Der Text stammt aus den Nutzungsbedingungen, die man sich beim Einrichten eines iPhones durchlesen oder per E-Mail zuschicken lassen kann. Im Internet findet sich nur eine englische Version der Nutzungsbedingungen [3].

generell auf Android-Geräten erfasst und verarbeitet werden oder ob es sich um Daten handelt, die bei der Nutzung Google-eigener Apps mit Telefoniefunktionen wie z.B. Google+ Hangouts, Google Voice bzw. Gmail Voice & Video Chat[31] erfasst werden.

Auch kann Google Informationen über Abstürze, Systemaktivität, Hardware-Einstellungen, Browser-Typ, Browser-Sprache, Datum und Uhrzeit einer Nutzeranfrage sammeln. Solche Geräteereignisse werden ausgewertet und die Ergebnisse für weitere Analysen verwendet.

BlackBerry OS

POTENZIELL BETROFFENE DATEN: Geräte-IDs, Installierte Apps, Region- und Spracheinstellungen, Betriebssystemversion, Gerätetyp, anonyme Nutzungsdaten, Standortdaten

Hat der Benutzer die Übertragung von *Diagnose- und Nutzungsdaten* aktiviert, werden z.B. folgende Daten übertragen, sobald das Telefon eingeschaltet ist:

- Informationen über den Zustand des Geräts
- Akku-Leistung
- Standort unerwartet beendeter Anrufe
- verwendete Anwendungen und Funktionen
- Interaktionen mit unterschiedlichen Medienarten
- aufgetretene Fehler
- Standortdaten

BlackBerry OS bietet zur Erkennung und Behebung von Fehlern *Tools zur Fehlerbehebung* an. Wird solche Software verwendet, kann BlackBerry grundlegende Nutzungsstatistiken oder Informationen zu dem verwendeten Gerät erheben und verarbeiten. Dazu zählen unter anderem Ereignisprotokolle, Anwendungskonfigurationen, Batterielaufzeit, Funk- oder Wi-Fi-Signalstärken, Geräte-Reset- und Speicher- oder Systemleistungsdaten.

iOS

POTENZIELL BETROFFENE DATEN: Geräte-IDs, anonyme Nutzungsdaten, Gerätetyp, Betriebssystemversion, Standortdaten

Erlaubt der Nutzer die Erhebung von Diagnose- und Nutzungsdaten, sammelt Apple diese regelmäßig in einer Form, die angeblich keinerlei Rückschlüsse auf die Person zulässt. Die Daten können u.a. das Modell der verwendeten Hardware, die Version des Betriebssystems, einen Zeitstempel und die Standortdaten zur Zeit der Erhebung umfassen. Wird das Smartphone zum Beispiel an einen Computer zur Synchronisation angeschlossen, können auch Informationen über den genutzten Computer enthalten sein. Gleiches gilt für eventuell genutzte Peripheriegeräte.

Mit der Aktivierung der Erhebung von Diagnose- und Nutzungsdaten stimmt der Nutzer zu, dass Apple diese Daten sammeln, verwalten, verwenden und verarbeiten darf. Außerdem erlaubt er Apple, diese Daten an Partner und Fremdentwickler (z.B. App-Entwickler) weiterzuleiten.

In iOS können die gesammelten Nutzungs- und Diagnosedaten eingesehen werden. Einem Nutzer ohne ausreichend Expertenwissen wird die Bewertung der Daten allerdings schwerfallen.

---

[31] Für weitere Informationen siehe http://www.google.com/googlevoice/about. html (Letzter Zugriff 29.07.2014)

Windows Phone

POTENZIELL BETROFFENE DATEN: Geräte-IDs, Betriebssystemversion, Region- und Spracheinstellungen, Gerätetyp, Netzbetreiber, installierte Apps, Name des Telefons, eigene Rufnummer, Anrufliste & Anrufstatistik, Sperrliste, E-Mails, SMS, MMS, Textnachrichten, anonyme Nutzungsdaten, Kontakte, Termine, Aufgaben, Standortdaten, Bewegungssensor, Weckzeiten, Musik, Videos, Fotos, Foto-Metadaten, Browserverlauf/Favoriten/Lesezeichen, Cookies, Web-Cache, Offline-Inhalte, Web-Formulardaten, IP-Adresse

Sobald ein Windows-Phone-Gerät mit dem Internet verbunden ist, werden sogenannte *Standardinformationen* von Microsoft über dieses Gerät erhoben. Diese umfassen: IP-Adresse des Gerätes, Betriebssystemversion, Browserversion, Region- und Spracheinstellungen, (Teile oder vollständige) International Mobile Subscriber Identity (IMSI) sowie weitere eindeutige IDs für das Gerät und Kennungen, die Handyhersteller, Handynamen, Version sowie Mobilfunkanbieter erfassen.

Windows Phone kann regelmäßig grundlegende Informationen über das Gerät sowie die Verwendung von Apps in Form sogenannter *Handyberichte* festhalten. Die Berichte sind einem Endgerät eindeutig zugeordnet und können Informationen über private Daten eines Nutzers beinhalten. Microsoft weist u.a. darauf hin, dass ein Bericht auch Snapshots des Arbeitsspeichers, also Momentaufnahmen gerade auf dem Gerät verarbeiteter Daten, umfassen kann. Diese können z.B. eine Kontaktliste, Teile von E-Mails oder SMS sowie auch Daten enthalten, die an eine Webseite übermittelt wurden. Da sich prinzipiell ein beliebiges Datum zum Zeitpunkt eines Snapshots im Arbeitsspeicher befinden kann, können potenziell alle – bis auf wenige Ausnahmen[32] – auf dem Gerät verwalteten Daten betroffen sein. Dabei behält sich Microsoft vor, die Berichtinformationen an andere Hersteller und weitere vertrauenswürdige Partner weiterzugeben.

Microsoft *empfiehlt* die Aktivierung der Berichte, wobei die Erfassung und Übertragung der Berichte an Microsoft die Zustimmung des Nutzers voraussetzt. Insgesamt soll dadurch die Dienstgüte verbessert werden. Microsoft betont, die Berichtinformationen nicht zur Identifikation der Nutzer heranzuziehen. Zu den Informationen der Handyberichte zählen im Einzelnen:

- **Handykonfiguration u.a.:** verwendete Netzwerkverbindung, Bildschirmauflösung, Speicherverwendung, Akku-Lebensdauer, Domäneneinstellungen für eingerichtete E-Mail-Konten, Betriebssystemversion
- **Leistungs- und Zuverlässigkeitsmetriken:** Wie schnell reagieren Funktionen des Telefons, wenn ein Symbol ausgewählt wurde, welche Probleme sind mit der Funktion oder Anwendung aufgetreten, und wie schnell werden Daten über eine Netzwerkverbindung gesendet und empfangen
- **Anwendungsverwendung u.a.:** die häufigst verwendeten Funktionen und Apps, welche Anwendungen sind auf dem Startbildschirm verfügbar, wie navigiert ein Nutzer in den Menüs, Häufigkeiten der Änderung von Einstellungen sowie Aktualisierung von Feeds und Kontaktinformationen
- **Softwarebetriebsfehler:** Probleme, welche die Funktionstüchtigkeit des Telefons stören, sowie Fehler, die in Hintergrunddiensten auftreten. Dies kann private (darunter auch personenbeziehbare) Informationen enthalten. Diese werden von Microsoft jedoch nicht verwendet, um einen Nutzer zu identifizieren oder zu kontaktieren.

[32] Zu diesen Ausnahmen zählen beispielsweise in einem Trusted Platform Modul (TPM) gespeicherte kryptografische Schlüssel. Bei einem TPM handelt es sich um eine Hardware-Komponente, die in einem Endgerät integriert sein kann und zur sicheren Speicherung und Verarbeitung von besonders schützenswerten Daten dient.

Weiterhin erhebt Microsoft Informationen, um Textvorschläge bei Tastatureingaben zu verbessern. Dazu zählen diese Daten: Berührungspunkte (Koordination auf dem Bildschirm), eingegebene Zeichen, ausgewählte Vorschläge sowie automatische Korrekturen. Es werden keine Daten für Passwortfelder oder den Startbildschirm (PIN-Sperre) erfasst. Weiterhin werden laut Microsoft Eingaben von E-Mail-Adressen, Telefonnummer oder Kreditkartendaten nicht verwertet. Die Teilnahme an diesem Verbesserungsprogramm wird von Microsoft empfohlen, Nutzer müssen aber ausdrücklich zustimmen.

5.7 Nutzungs- und Datenschutzbestimmungen

Dieses Kapitel beschreibt die Nutzungs- und Datenschutzbestimmungen der unterschiedlichen Betriebssysteme. Die Hersteller stellen diese Bestimmungen auf ihren Webseiten zur Verfügung. Zusätzlich fragen die Smartphones bereits bei der ersten Inbetriebnahme, ob ein Anwender den Datenschutzbestimmungen zustimmt.

Diese Bestimmungen umfassen Informationen darüber, welche Daten auf den Betriebssystemen erhoben werden und wie sie die Daten der Anwender weiterverarbeiten können. Sie verdeutlichen auch, wo die Grenzen der Datennutzung durch den Hersteller liegen.

Für jedes Betriebssystem werden im Folgenden wichtige Aspekte der Nutzungs- und Datenschutzbestimmungen dargelegt. Der erste Abschnitt bietet eine zusammenfassende Übersicht über die datenschutzrechtlichen Aspekte der Betriebssysteme.

Übersicht zu datenschutzrechtlichen Aspekten der Betriebssysteme

Als **Zweck für die Datenerfassung** nennen alle vier Betriebssystemhersteller ähnliche Gründe: Die Erfassung von Daten über das Gerät – darunter personenbezogene Daten – dient dazu, dem Nutzer Dienste für das Gerät bereitstellen zu können. Neben dem Betrieb der Dienste dient die Erfassung und Auswertung der Daten auch Wartungs- und Optimierungszwecken sowie der Entwicklung neuer Dienste.

Die Hersteller weisen darauf hin, dass die **Datenverarbeitung** personenbezogener Daten auf Servern stattfinden kann, die sich nicht im Heimatland des Nutzers befinden.

Alle Betriebssystemhersteller räumen in ihren Datenschutzvereinbarungen Nutzern die Möglichkeit ein, **erfasste Daten einzusehen**. Allerdings gilt dieses Angebot oft nur unter Einschränkungen, etwa falls die Herausgabe der Daten eines Nutzers keinen unverhältnismäßig hohen Aufwand verursacht. Was diese Formulierung im Detail bedeutet, wird nicht genau beschrieben.

Alle Betriebssystemhersteller geben in ihren Nutzungs- und Datenschutzvereinbarungen an, dass sie **personenbezogene Daten so lange aufbewahren**, um die in ihren Datenschutzbestimmungen angegebenen Zwecke zu erfüllen oder um gesetzlich vorgeschriebene Anforderungen zu erfüllen.

Alle vier Betriebssysteme gewähren **Dritten nur Zugriff auf personenbezogene Daten** eines Nutzers, wenn dieser explizit darin eingewilligt hat. Allerdings behalten sich ebenfalls alle vier Betriebssystemhersteller vor, unter bestimmten Voraussetzungen personenbezogene Daten auch ohne Zustimmung des Nutzers herauszugeben. Dabei kann es sich z.B. um rechtmäßige Gründe handeln, etwa um einer vollstreckbaren behördlichen Anordnung nachzukommen.

Android

Google stellt zur Nutzung von Android-Geräten keine speziellen Datenschutz sowie Nutzungsbestimmungen bereit, sondern wendet die generell für Google-Produkte und -Dienste zum Einsatz kommenden an [12]. Es ist im Zuge des Open-Source-Charakters von Android daher möglich, dass modifizierte Versionen des Android-Betriebssystems, wie z.B. spezifische Versionen bestimmter Gerätehersteller (etwa HTC, Samsung, Huawei etc.), eingesetzt werden. Diese können abweichenden Vereinbarungen unterliegen.

Die Erfassung der Daten erfolgt laut Google zur Bereitstellung der angeforderten Dienste, zur Wartung der Dienste, zur Verbesserung der Dienste, zur Entwicklung neuer Dienste sowie zum Schutz von Google und den Nutzern. Das Unternehmen weist darauf hin, dass die Verarbeitung personenbezogener Daten auf Servern stattfindet, die sich in zahlreichen Ländern auf der ganzen Welt befinden.

Google bietet Nutzern an, auf ihre personenbezogenen Daten zuzugreifen, sofern dieser Zugriff mit vertretbarem Aufwand zu realisieren ist und den Schutz personenbezogener Daten Dritter nicht verletzt. Darüber hinaus bietet Google an, Daten, z.B. Gmail, Kontakte, Kalender oder Google Drive, zu exportieren.[33]

Wenn Nutzer Daten in Google-Diensten löschen, werden erstellte Sicherungskopien möglicherweise nicht sofort von aktiven Servern entfernt und nie von den Sicherungssystemen gelöscht. Eine Weitergabe von personenbezogenen Daten an Dritte kann nur mit Einwilligung der Nutzer erfolgen. Handelt es sich dabei um sensible Kategorien personenbezogener Daten (etwa Zugehörigkeit zu einer bestimmten ethnischen Gruppe, politische oder religiöse Gesinnungen oder sexuelle Neigungen), erfordert dies die explizite, d.h. zusätzliche und dezidierte Einwilligung der Nutzer zur Weitergabe dieser Daten.

Bei vorliegender Einwilligung des Nutzers behält sich Google vor, personenbezogene Daten zur Verarbeitung an Unternehmen aus der Google-Unternehmensgruppe und an andere vertrauenswürdige Unternehmen oder Personen weiterzugeben. Darüber hinaus ist eine Weitergabe personenbezogener Daten an externe Unternehmen, Organisationen oder Personen laut Google in folgenden Fällen notwendig:

- um technische Probleme, Sicherheitsmängel oder Betrug aufzudecken, zu verhindern oder anderweitig zu bekämpfen,
- um geltende Nutzungsbedingungen durchzusetzen, einschließlich der Untersuchung möglicher Verstöße,
- um die Rechte, das Eigentum oder die Sicherheit von Google, seinen Nutzern oder der Öffentlichkeit vor Schaden zu schützen, soweit gesetzlich zulässig oder erforderlich, sowie
- um anwendbare Gesetze, Regelungen oder anwendbares Verfahrensrecht einzuhalten oder einer vollstreckbaren behördlichen Anordnung nachzukommen.

BlackBerry OS

BlackBerry stellt eine Vielzahl an Nutzungsbedingungen und -Vereinbarungen auf seiner Webseite [9] zur Verfügung. Zu einzelnen Endgeräten, wie sie in dieser Studie betrachtet werden, gibt es keine speziellen Nutzungsbedingungen. BlackBerry stellt stattdessen Bedingungen für sein gesamtes Serviceangebot zur Verfügung [6] sowie zu einzelnen Komponenten wie der BlackBerry-ID, der

[33] Für weitere Informationen siehe https://www.google.com/settings/takeout? hl=en (Letzter Zugriff 29.07.2014)

BlackBerry App World und anderen. Darüber hinaus veröffentlicht BlackBerry eine allgemeine Datenschutzrichtlinie [8].

BlackBerry gibt an, personenbezogene Daten des Nutzers nur so lange aufzubewahren, wie dies für die Erfüllung der durch BlackBerry identifizierten Zwecke oder anderweitig zur Einhaltung von geltendem Recht erforderlich ist. BlackBerry weist darauf hin, dass Einwohner des Europäischen Wirtschaftsraums in die Übertragung ihrer persönlichen Angaben außerhalb des Europäischen Wirtschaftsraums zwecks Verarbeitung oder Speicherung durch oder im Namen von BlackBerry einwilligen.

In der Datenschutzrichtlinie [8, Abschnitt 5] schreibt BlackBerry, „[w]enn die persönlichen Angaben für die durch BlackBerry identifizierten Zwecke nicht mehr erforderlich oder relevant sind oder gemäß geltendem Recht nicht mehr vorgeschrieben sind, hat BlackBerry alle notwendigen Schritte zu unternehmen, um diese Angaben zu entfernen, zerstören, zu löschen, zu sammeln oder anonym zu machen".

BlackBerry kann darüber hinaus private Angaben des Nutzers auch verwenden, um auf Gerichtsbeschlüsse, Haftbefehle oder sonstige rechtmäßige Anforderungen oder rechtliche Verfahren zu antworten oder um Notfallhilfe in Situationen geben zu können, die lebensbedrohend sind. In diesem Fall benötigt BlackBerry keine Einverständniserklärung des Nutzers.

iOS

Es gibt eine Datenschutzrichtlinie [2] von Apple, die für alle Dienste von Apple gilt und der ein Nutzer durch Akzeptieren der Nutzungsbestimmungen von iOS zustimmt. Mit der Aktivierung eines iPhones ermächtigt der Nutzer Apple und den Mobilfunkprovider zum Austausch der beim Aktivierungsprozess erhobenen Daten. Welche Daten genau ausgetauscht werden, bleibt intransparent, die Datenschutzrichtlinie spricht von „Daten, die Sie während des Aktivierungsprozesses bereitstellen".

In der Richtlinie informiert Apple, dass personenbezogene Daten an Unternehmen weitergegeben werden, die Dienstleistungen für Apple durchführen, wie das Ausführungen von Kundenbestellungen. Weiterhin darf Apple die für die Optimierung und Bereitstellung der verschiedenen Dienste erhobenen Daten an seine Partner, Lizenznehmer und Fremdentwickler weitergeben.

Nutzer, die innerhalb des europäischen Wirtschaftsraums wohnen, weist Apple darauf hin, dass alle ihre privaten (darunter auch personenbezogene) Daten sowie in der iCloud zur Verfügung stehenden Daten „von Apple Distribution International in Cork, Irland überwacht und in dessen Namen von Apple Inc. verarbeitet" werden.

Weiterhin gibt Apple an, dass es für das Unternehmen notwendig sein kann – „aufgrund von gesetzlichen Bestimmungen, rechtlichen Verfahren, Rechtsstreitigkeiten und/oder Aufforderungen von öffentlichen und Regierungsbehörden innerhalb oder außerhalb Ihres Wohnsitzlandes" –, personenbezogene Daten offenzulegen. Außerdem darf Apple Daten eines Nutzers offenlegen, wenn das Unternehmen der Überzeugung ist, „dass dies für die nationale Sicherheit, den Gesetzesvollzug oder andere öffentliche Interessen notwendig oder angemessen ist".

Apple erklärt, dass personenbezogene Daten so lange wie notwendig aufbewahrt werden, um die in dieser Datenschutzrichtlinie beschriebenen Zwecke zu erfüllen, „soweit nicht eine längere Aufbewahrungsfrist durch Gesetze verlangt oder erlaubt ist".

Windows Phone

Die erhobenen Daten können von Microsoft Unternehmen bereitgestellt werden, die im Auftrag von Microsoft z.B. Postwerbesendungen verschicken, Kundenfragen beantworten oder statistische Analysen von Microsoft-Diensten durchführen.

Microsoft weist in seiner Datenschutzerklärung [20] darauf hin, dass Informationen von Nutzern, die durch den Einsatz von Windows Phone erfasst werden, möglicherweise in den USA und weiteren Ländern durch Microsoft, deren Partner, Tochtergesellschaften sowie Dienstanbieter gespeichert und verarbeitet werden.

Weiterhin kann Microsoft zu folgenden Zwecken auf Informationen von Windows-Phone-Nutzern, einschließlich des Inhalts ihrer Kommunikationen, zugreifen oder sie offenlegen:

1. um gesetzliche Bestimmungen oder rechtliche Forderungen zu erfüllen oder laufende Verfahren zu unterstützen,
2. um die Rechte oder das Eigentum von Microsoft oder von Microsoft-Kunden zu schützen, was die Durchsetzung von Verträgen oder Richtlinien umfasst, welche die Verwendung der Dienste regeln,
3. wenn in der begründeten Annahme gehandelt wird, dass ein Zugriff oder eine Offenlegung zum Schutz der persönlichen Sicherheit von Mitarbeitern oder Kunden von Microsoft oder der Öffentlichkeit erforderlich ist.
4. Auch können die Daten von Nutzern im Rahmen einer Unternehmenstransaktion wie einer Fusion oder einem Verkauf von Aktiva offengelegt werden.

Microsoft bietet Nutzern an, Zugriff auf die über sie erhobenen Informationen zu bekommen. Dazu müssen Nutzer ein Webformular ausfüllen.[34]

[34] https://support.microsoft.com/contactus/emailcontact.aspx?scid=sw;en;1213&showpage=1 (Letzter Zugriff 29.07.2014)

6. Grundfunktionen und Kopplung mit der Cloud

Dieses Kapitel betrachtet die *Grundfunktionen* eines Smartphones, die einem Nutzer unmittelbar nach erstmaligem Einrichten des Gerätes zur Verfügung stehen – ohne dass Apps Dritter installiert werden müssen. Zu diesen Grundfunktionen zählen z.B. Telefonieren, Versenden und Empfangen von E-Mails und SMS sowie Surfen im Internet. Im Gegensatz zu den in Kapitel 5 vorgestellten Basisdiensten, die eine Basis für die Grundfunktionen bilden, bieten die Grundfunktionen dem Nutzer einen direkten Mehrwert an. Die Basisdienste hingegen wirken indirekt, so kann der Nutzer Ortungsdienste nicht direkt nutzen, diese ermöglichen aber z.B. Turn-by-Turn-Navigation durch andere Apps.

Realisiert werden die Grundfunktionen durch vorinstallierte Apps, die zusammen mit dem Betriebssystem ausgeliefert werden. Bei der Nutzung dieser Apps fallen verschiedene private Daten an (siehe Kapitel 4). In gewissem Rahmen hat der Nutzer hier die Wahl, wie er mit diesen privaten Daten umgehen möchte. Er kann sich entscheiden, die Apps zu nutzen und seine Daten dort einzupflegen, er kann sie mit verfügbaren Cloud-Diensten synchronisieren lassen, oder er kann sich entscheiden, eine App nicht zu nutzen.

Bei Verzicht auf eine Grundfunktion fallen die entsprechenden Daten nicht an, dies kann aber mit gravierenden Einschränkungen in der Benutzbarkeit einhergehen. Werden z.B. Kontakte nicht auf dem Smartphone gepflegt, so hat dies Einfluss auf diverse andere Funktionen, wie Telefonieren oder das Schreiben von E-Mails. Wesentlich häufiger wird sich ein Nutzer daher nur zwischen lokaler Speicherung der privaten Daten auf seinem Smartphone und einer zusätzlichen Datensynchronisation mit der Cloud entscheiden wollen.

Die folgenden Kapitel betrachten die Grundfunktionen hinsichtlich der Möglichkeit, wie private Daten vom Telefon abfließen können, z.B. durch die Kopplung der Grundfunktion an einen Cloud-Dienst, und ob der Nutzer eine Entscheidungsmöglichkeit besitzt. In der Betrachtung werden nur herstellereigene Cloud-Dienste berücksichtigt. Telefonieren wird dabei aus der Betrachtung ausgeklammert, da diese Funktion nicht an Dienste des Betriebssystemherstellers, sondern an Dienste des Mobilfunkanbieters geknüpft ist, analog zu anderen Mobilfunkgeräten.

6.1 Verwalten von Kontakten

Alle Betriebssysteme bieten eine Möglichkeit, *Kontakte* (vgl. Kapitel 4.5) zu verwalten, meist in Form einer separaten App oder als Teil der Telefonie-App. Trägt ein Nutzer Kontakte in die entsprechende App ein, werden diese Daten bei allen Systemen zunächst nur lokal gespeichert.

Android

Bei Anlegen eines Google-Kontos (für weitere Informationen siehe Kapitel 5.2) wird ein Nutzer unmittelbar dazu aufgefordert, die Kontakte über Cloud-Dienste zu synchronisieren. Die Daten werden nur übertragen, wenn der Nutzer dem zustimmt.

BlackBerry OS

BlackBerry OS bietet keine Möglichkeit der Cloud-Synchronisierung von Kontakten. Sie bleiben daher nur lokal gespeichert.

iOS

Bei der Nutzung des Cloud-Dienstes iCloud werden die Kontakte auf die iCloud-Server geladen. Kontakte sind bei der Aktivierung von iCloud vorausgewählt zur Synchronisierung, können aber abgewählt werden.

Windows Phone

Hat ein Nutzer eines Windows Phones ein Microsoft-Konto (für weitere Informationen siehe Kapitel 5.2) eingerichtet, werden die Kontakte automatisch mit Microsoft-Servern synchronisiert. Der Nutzer kann diese Synchronisierung nicht abwählen.

6.2 E-Mails und Kurznachrichten

Auf allen Betriebssystemen können *SMS, E-Mails und Textnachrichten* (vgl. Kapitel 4.4) empfangen und verschickt werden. Dazu bieten alle eigene Apps an, die Zugriff auf die auf dem Smartphone gespeicherten Kontakte haben.

Die E-Mail-Apps funktionieren ähnlich zu E-Mail-Anwendungen auf Desktop-Computern. Der Nutzer kann E-Mail-Konten von verschiedenen Anbietern einbinden. Auf dem Smartphone geschriebene E-Mails werden dann zum Versand an den jeweiligen E-Mail-Anbieter geschickt. Wird der herstellereigene E-Mail-Dienst genutzt, ist dies der Betriebssystemhersteller.

Kurznachrichten umfassen SMS und Textnachrichten per Instant-Messenger, wie z.B. iMessage bei iOS. SMS werden über den Mobilfunkanbieter abgewickelt, während Textnachrichten über die herstellereigene Infrastruktur verschickt werden. Daher können sie nur an Teilnehmer geschickt werden, die an die Infrastruktur des Herstellers angeschlossen sind. Für die Nutzung des Textnachrichtendienstes gelten die Datenschutz- sowie Nutzungsbedingungen des Herstellers (für weitere Informationen siehe Kapitel 5.7), daher ist es möglich, dass Inhalte der Textnachrichten sowie Metadaten (Zeitstempel der Nachrichten, Größe etc.) vom Hersteller erfasst und verarbeitet werden.

Android

Für Kurznachrichten bietet Android die Kombination von Google+ Hangouts und SMS. *Google+ Hangouts* ist eine App, die bei Android standardmäßig als Teil des Betriebssystems[35] mitgeliefert wird. Diese verknüpft das soziale Netzwerk Google+ mit Gerätefunktionen, die den Zugriff auf die Kontaktdaten sowie SMS-Funktionalität ermöglichen.

BlackBerry OS

BlackBerry OS nutzt für Textnachrichten den BlackBerry Messenger, der auch für die anderen Betriebssysteme als App erhältlich ist. Für das Versenden und Empfangen von SMS gibt es eine eigene App.

[35] Diese Informationen beziehen sich auf um ein LG E960 Nexus 4 Endgerät mit Android 4.4

iOS

In der Kurznachrichten-App kombiniert Apple die Möglichkeit, SMS zu versenden, mit einem Textnachrichten-Dienst, genannt iMessage. Beim Versenden von iMessage-Nachrichten wird dem Empfänger die Telefonnummer des Senders angezeigt, auch wenn dieser eine unterdrückte Telefonnummer verwendet.

Windows Phone

Windows Phone bietet eine Messenger-App an für Kurznachrichten und hat das soziale Netzwerk Facebook integriert. Ist das Windows Phone mit einem Microsoft-Konto verknüpft, kann der Nutzer Kurznachrichten mit einem Cloud-Dienst synchronisieren.

6.3 Surfen im Internet

Alle Betriebssysteme ermöglichen es, im Internet zu surfen. Dies funktioniert ähnlich wie auf Desktop-Computern, anstelle des Browsers wird jedoch eine Browser-App – in der Regel eine Eigenentwicklung des Herstellers – aufgerufen. Genau wie auf Desktop-Computern fallen auch beim Surfen mit dem Smartphone *Internetdaten* (vgl. Kapitel 4.7) an, die zunächst nur lokal auf dem Smartphone gespeichert werden.

Android

Der Standard-Browser unter Android ist über die Browser-App verfügbar. Dieser speichert Browser-Daten sowie Formulardaten und Passwörter nur lokal. Eine Synchronisierung mit einem Cloud-Dienst erfolgt nicht.

Die Browser-App erlaubt nur grobgranulare Cookie-Einstellungen, d.h. vollständige Deaktivierung von Cookies. Das Surfen im privaten Modus ist mit diesem Browser nicht möglich, ebenso wenig unterstützt er die *Do-Not-Track-Option*[36].

BlackBerry OS

Auch BlackBerry OS beinhaltet einen eigenen Browser. Dieser bietet allerdings keine Datensynchronisation, d.h., alle beim Surfen anfallenden Daten bleiben lokal gespeichert.

Der BlackBerry-Browser erlaubt im Umgang mit Cookies nur, diese global zu akzeptieren oder abzulehnen, nicht jedoch pro Webseite oder abhängig von ihrer Herkunft. Er ermöglicht aber, im *privaten Modus* zu surfen, d.h., der Browser zeichnet besuchte Webseiten nicht auf und löscht Cookies nach Schließen der App. Der Browser unterstützt aber nicht die Do-Not-Track-Option.

iOS

iOS beinhaltet eine App-Version des von Apple entwickelten Safari-Browsers. Damit ist in Verbindung mit dem Cloud-Dienst iCloud das Synchronisieren von Browser-Daten möglich. Bei eingerichtetem

[36] Die Do-Not-Track-Option teilt einer Webseite beim Besuch mit, dass der Nutzer nicht will, dass Daten über ihn erhoben werden. Dabei handelt es sich lediglich um eine Bitte des Browsers. Die Do-Not-Track-Option kann nicht gewährleisten, dass tatsächlich keine Daten über den Nutzer erfasst werden.

iCloud-Konto wird per Default die Synchronisierung von Browser-Daten aktiviert. Apple synchronisiert dabei die geöffneten Browser-Tabs, gespeicherte Offline-Webseiten und Lesezeichen. Passwörter und Auto-Fill-Daten können auch synchronisiert werden, allerdings muss hierzu separat die Keychain-Synchronisationsfunktion in iCloud aktiviert werden, die per Default nicht aktiviert wird.

Safari ermöglicht dem Anwender, Cookies immer zu blockieren, nur Cookies von Dritten oder Werbeanbietern zu blockieren oder Cookies nie zu blockieren. Bei der Standardeinstellung werden Cookies von Dritten und Werbeanbietern blockiert. Der Browser unterstützt die Do-Not-Track-Option und bietet einen *privaten Modus* beim Surfen an. Ist dieser aktiviert, werden Cookies blockiert, und der Browser zeichnet keinen Verlauf besuchter Webseiten des Nutzers auf.

Windows Phone

Bei erstmaliger Aktivierung des Internet Explorers wird der Nutzer aufgefordert, zwischen zwei Konfigurationsprofilen des Browsers, *Empfohlen* und *Anpassen*, zu wählen. Die dabei empfohlenen Optionen beinhalten das Senden des Browser-Verlauf an Microsoft und den Einsatz von DataSense.[37]

Außerdem lassen sich der SmartScreen-Filter zum Schutz vor unsicheren Webseiten und die Do-Not-Track-Option aktivieren. Der Internet Explorer bietet grobe Einstellungen für den Umgang mit Cookies. Dabei wird zwischen *alle akzeptieren, alle blockieren* sowie *einige blockieren* unterschieden. Die Angaben von Microsoft machen nicht deutlich, welche Cookies bei der Option *einige blockieren* blockiert werden.

6.4 Termine und Aufgaben

Alle Betriebssysteme bieten Apps an, in denen Nutzer ihre *Termine und Aufgaben* (vgl. Kapitel 4.5) verwalten können. Die Kalender-Apps können in der Regel mehrere Kalender verwalten und auch externe Kalender einbinden. Aufgaben werden üblicherweise in einer eigenen App getrennt von den Terminen verwaltet.

Kalender-Apps bieten einen Standardkalender an, der meist eine Verknüpfung mit dem Kalender-Dienst des Herstellers bietet. Per Default werden neue Termine in den Standardkalender eingetragen und lokal auf dem Smartphone gespeichert. Bietet der Hersteller einen Cloud-Dienst zur Synchronisation der Kalenderdaten an, werden diese Termine an den Hersteller gesendet. Termine in extern eingebundenen Kalendern werden nicht an den Betriebssystemhersteller übertragen.

Android

Termine und Aufgaben werden auf dem Telefon gespeichert und können mit einem verknüpften Google-Konto über den Google-Kalender-Dienst synchronisiert werden. Dafür ist die Zustimmung des Nutzers notwendig.

[37] Funktion, bei der jeder Webseiten-Aufruf zur möglichen Optimierung der Datenübertragung zwischen Endgerät und ausgewählter Webseite an einen Dienst von Microsoft gesendet wird.

BlackBerry OS

Termine sowie Aufgaben werden lokal auf dem Smartphone gespeichert und können mithilfe der BlackBerry-Link-Software mit dem Computer des Anwenders synchronisiert werden. Dies muss der Nutzer jedoch explizit durchführen, eine automatische Synchronisierung von Aufgaben und Terminen bietet BlackBerry OS nicht selbst an.

iOS

Termine und Erinnerungen können, wenn es der Nutzer wünscht, über iCloud synchronisiert werden. Dann werden diese an Apple-Server gesendet. Bei der Aktivierung von iCloud ist die Synchronisierung von Terminen und Aufgaben standardmäßig eingeschaltet, kann aber durch den Nutzer deaktiviert werden.

Windows Phone

Sofern ein Endgerät mit einem Microsoft-Konto verknüpft ist, wird – wie bereits in Kapitel 5.2 beschrieben – laut Microsoft automatisch u.a. von existierenden Kalendereinträgen, die auf dem Endgerät gespeichert sind, eine Sicherung erstellt.

Das bedeutet, Kalendereinträge (und Kontakte) werden auf einen Server von Microsoft hochgeladen und dort gespeichert.

6.5 Fotos, Bilder und Videos

Alle Betriebssysteme bieten Apps an, die es erlauben, Fotos, Bilder und Videos (vgl. Kapitel 4.6) aufzunehmen und zu verwalten. Bilder und Videos können Standortinformationen in den Metadaten enthalten, wobei jedes der vier Betriebssysteme bei erstmaliger Aktivierung der Foto-Funktion den Nutzer auswählen lässt, ob der Aufnahmeort (Geo-Informationen) für Fotos erfasst und gespeichert werden soll.

Android

Bei erstmaliger Aktivierung der Foto- bzw. Video-Funktion kann ein Nutzer auswählen, ob der Aufnahmeort für Fotos erfasst und gespeichert werden soll. Ferner wird ein Nutzer bei der Verknüpfung des Gerätes mit einem Google-Konto aufgefordert, die Synchronisierung von Fotos sowie Videos zu aktivieren.

BlackBerry OS

Der Anwender kann auswählen, ob der Aufnahmeort in den Metadaten der Fotos und Videos gespeichert werden soll. Standardmäßig bietet BlackBerry OS keine Möglichkeit, Fotos und Videos mit einem Online-Speicherdienst zu synchronisieren.

iOS

Bei erstmaligem Öffnen der Kamera-App kann der Nutzer auswählen, ob der Aufnahmeort für Fotos und Videos erfasst und gespeichert werden soll. Diese Einstellung lässt sich jederzeit ändern. Der Nutzer kann die Synchronisation über den Cloud-Dienst iCloud für Bilder und Videos aktivieren, dann werden diese an Apple-Server übertragen. Bei der Aktivierung der iCloud-Funktion werden die Fotofreigabe[38] und Fotostreams per Default aktiviert, können aber ausgeschaltet werden.

Windows Phone

Aktiviert ein Nutzer erstmalig die Foto- bzw. Video-Funktion, kann er auswählen, ob der Aufnahmeort der Fotos erfasst und gespeichert werden soll. Ferner wird einem Nutzer bei der Verknüpfung des Gerätes mit einem Micosoft-Konto die Aktivierung der Synchronisierung von Fotos sowie Videos angeboten.

6.6 Musik

Auf allen Betriebssystemen werden Apps angeboten, die es erlauben, *Musik* (vgl. Kapitel 4.6) abzuspielen und eigene Musiksammlungen zu verwalten. In manchen Fällen muss die Musik nicht einmal auf dem Smartphone selbst gespeichert sein, sondern kann vom Hersteller auf das Smartphone gestreamt werden. Dies spart lokalen Speicherplatz, benötigt aber eine Internetverbindung, damit Musik wiedergegeben werden kann.

Android

Android speichert Musikdateien lokal und synchronisiert diese nicht mit einem Server. Standardmäßig umfasst Android eine App *Play Music*[39], die Nutzern gegen monatliches Entgelt anbietet, u.a. Musikdateien von einem Desktop-PC auf einen zentralen Server zu übertragen und dann auf das mobile Endgerät zu streamen.

BlackBerry OS

Musik wird lokal auf BlackBerry-Smartphones gespeichert. Der Nutzer kann Musik über die BlackBerry-Link-Software mit seinem Computer synchronisieren.[40] BlackBerry OS bietet von Haus aus keine Möglichkeit, Musik mit einem Cloud-basierten Dienst zu synchronisieren oder Musik über einen Dienst zu streamen.

iOS

Bei iOS wird Musik lokal gespeichert. Musik kann über iTunes mit einem Computer synchronisiert oder im iTunes Store gekauft werden. Apple bietet Nutzern gegen ein monatliches Entgelt den Dienst

---

[38] Bei Nutzung der iCloud-Fotofreigabe werden die Fotos und Videos auf Apple-Servern so lange gespeichert, bis die Inhalte vom Nutzer gelöscht werden.

[39] Diese Informationen beziehen sich auf ein LG E960 Nexus 4 Endgerät mit Android 4.4.

[40] Bis zum 21.07.2014 konnte über die BlackBerry App World auch Musik erworben werden.

iTunes Match an, der Streaming von Musik auf das Smartphone möglich. Beim Nutzen von iTunes Match wird die eigene Musiksammlung mit der dem Service zur Verfügung stehenden Musik-Bibliothek abgeglichen. Apple erhebt hier Daten wie Namen, Interpreten und Dauer aller in der Musiksammlung vorhandenen Titel.

Windows Phone

Windows Phone speichert Musikdateien lokal und erlaubt die Synchronisierung von Musikdateien mit dem Desktop-PC eines Nutzers. Ferner kann die auf dem Windows Phone gespeicherte Musiksammlung um die Xbox Music-Cloud erweitert werden. Eine automatisierte Synchronisierung von Musikdateien oder Informationen über Musikbibliotheken mit entfernten Servern findet nicht statt.[41]

6.7 Weitere Cloud-Dienste

In den vorigen Kapiteln wurde auf die Grundfunktionen eines Smartphones eingegangen und dargestellt, wie diese mit Cloud-Diensten verknüpft sind. Zusätzlich bieten einige Betriebssysteme noch weitere Cloud-Dienste an, welche im Folgenden dargestellt werden.

Android

Android stellt mit der App *Drive* die Möglichkeit bereit, beliebige Daten mit einem Google-Server zu synchronisieren. Diese können dann auf andere Endgeräte kopiert werden, welche ebenfalls Zugriff auf *Drive*-Funktionen besitzen (als App oder via Browser), oder mit anderen Nutzern geteilt werden.

➜ **NOTIZEN** Erlaubt die Synchronisation von Notizen aus der Keep-App und wird per Default nach der Einrichtung des Google-Kontos als Synchronisationsoption vorgeschlagen. Der Nutzer kann die Synchronisationsoption abwählen.

➜ **MEINE DATEN SICHERN** Nach der Einrichtung des Google-Kontos wird dies als Synchronisationsoption vorgeschlagen. Sie erlaubt die Synchronisation von App-Daten, WLAN-Passwörtern und anderen Einstellungen auf Google-Servern – welche Einstellungen dies genau sind, ist aus den von Google bereitgestellten Informationen nicht ersichtlich. Der Nutzer kann diese jedoch abwählen.

BlackBerry OS

BlackBerry OS bietet für die aktuelle Betriebssystemversion 10 keinen Cloud-basierten Back-up-Dienst an oder Services, mit deren Hilfe sich die Daten auf mehreren Geräten synchronisieren lassen. BlackBerry Protect erlaubt lediglich das Orten verlorener/gestohlener Geräte sowie deren Deaktivierung, nicht jedoch die Sicherung von Daten auf diesen Geräten.

[41] Eine automatisierte Synchronisierung ist dann möglich, wenn der Nutzer ein Xbox-Konto über ein vorhandenes Microsoft-Konto freischaltet.

iOS

Unter dem Dienst iCloud versammelt Apple alle Cloud-Synchronisierungsdienste, die ein iOS-Nutzer direkt nutzen kann. Die verschiedenen Dienste können einzeln aktiviert oder deaktiviert werden und arbeiten nach Aktivierung größtenteils im Hintergrund, ohne dass eine weitere Nutzerinteraktion notwendig wäre. Zusätzlich zu den bereits in den vorangegangenen Abschnitten besprochenen Diensten können folgende Dienste aktiviert werden:

➜ **NOTIZEN** Erlaubt die Synchronisation von Notizen und ist bei Aktivierung von iCloud per Default deaktiviert.

➜ **PASSBOOK** Kann für die Synchronisation von z.B. Eintrittskarten oder Flugtickets genutzt werden und ist bei Aktivierung von iCloud per Default aktiviert.

➜ **SCHLÜSSELBUND** Ermöglicht es, Passwörter und Formulardaten des Browsers zu synchronisieren. Ist bei der Aktivierung von iCloud per Default ausgeschaltet.

➜ **DOKUMENTE & DATEN** Der Nutzer kann hier nicht selbst Daten und Dokumente hochladen, sondern erlaubt die Synchronisation von Daten und Dokumenten der installierten Apps, sodass auf anderen Geräten – die auch mit seiner Apple-ID verknüpft sind – den Apps dieselben Daten zur Verfügung stehen. Bei Aktivierung von iCloud ist dieser Dienst per Default eingeschaltet.

➜ **BACK-UP** Ermöglicht, Back-ups des iOS-Geräts in der iCloud zu speichern, und ist bei Aktivierung der iCloud per Default aktiviert.

Windows Phone

Auch Microsoft bietet Cloud-Dienste an, mit denen Nutzer Daten speichern, verwalten und mit anderen Nutzern teilen können. Diese Dienste können beliebige Daten synchronisieren (OneDrive), unterstützen aber auch Microsoft-spezifische Dateiformate (Office 365).

➜ **ONEDRIVE** Microsoft bietet Nutzern den Synchronisationsdienst *OneDrive* (vormals SkyDrive) an, welcher ähnliche Funktionen wie iCloud und Google Drive bereitstellt. Nutzer können hier beliebige Daten auf einem Microsoft-Server speichern, Daten zwischen verschiedenen Geräten synchronisieren und Daten mit anderen teilen.

➜ **OFFICE 365 & MICROSOFT SHAREPOINT** Dokumente, Dokumenteinstellungen sowie Notizen können ebenfalls mit Office 365 & Microsoft SharePoint synchronisiert werden. Dabei werden laut Microsoft bestimmte Metadateneigenschaften, wie z.B. letzte Aktualisierung eines Dokumentes sowie Autorenschaft, automatisch synchronisiert, sofern ein Nutzer das Gerät mit einem Microsoft-Konto verbunden hat. Um die Dokumente selbst hochzuladen, muss der Nutzer diese Aktion explizit auslösen, d.h. den entsprechenden Speicherdienst auswählen. Ferner werden OneNote-Dateien automatisch synchronisiert.

7. Funktionserweiterung durch Drittanbieter-Apps

Viele Funktionen auf Smartphones werden erst durch die Installation von Apps Dritter möglich. Kapitel 7.1 stellt die App-Markets der verschiedenen Ökosysteme vor. Diese werden in der Regel vom Betriebssystemhersteller betrieben und sind als Vertriebskanal für Apps konzipiert. App-Entwickler können dort unter bestimmten Bedingungen Apps einstellen, während Nutzer sie von dort beziehen können.

Die Nutzung von Apps hat allerdings auch eine Kehrseite: Ihre Verwendung bedeutet, Software von mehr oder weniger bekannten Dritten auf einem Endgerät zu installieren und auszuführen. Greifen die Apps auf die privaten Daten des Nutzers zu, so muss dieser dem App-Anbieter vertrauen und sich auf dessen Datenschutzrichtlinie verlassen. Nutzer können oft nur schwer erkennen, wie eine App genau arbeitet und auf welche Daten diese tatsächlich zugreift. Zudem sind mittlerweile auch Schädlinge – Trojaner, Viren, Würmer etc. –, wie sie aus der Welt der Desktop-PCs bekannt sind, auf Smartphones vertreten. Diese Schadprogramme werden in Kapitel 7.2 betrachtet.

Wie die Betriebssysteme die privaten Daten des Nutzers schützen, beschreibt Kapitel 7.3. Dazu wird zunächst das Sicherheitsmodell der Betriebssysteme im Hinblick auf deren Umgang mit Apps untersucht. Dabei werden verschiedene Aspekte des Sicherheitsmodells vorgestellt, z.B. der Zugriff von Apps auf private Daten, und deren Realisierung in den verschiedenen Betriebssystemen betrachtet. Inwieweit ein Nutzer diese Zugriffe erkennen, verstehen und kontrollieren kann, unterscheidet sich von Betriebssystem zu Betriebssystem. Im Anschluss werden einige weitere Sicherheitsvorkehrungen der Betriebssysteme beschrieben, die nicht direkt im Zusammenhang mit Apps stehen.

Den Abschluss bildet Kapitel 7.4 mit einer exemplarischen Untersuchung der App *Angry Birds*. Dort wird untersucht, welche Verbindungen die App während des Spielens aufbaut. Einem Nutzer wird dabei nicht unbedingt bewusst sein, dass die App mit externen Servern kommuniziert.

7.1 App-Markets

Um Apps von Drittanbietern auf einem mobilen Endgerät zu installieren, haben die Hersteller im Ökosystem Vertriebswege vorgesehen, die sogenannten App-Markets. Dabei handelt es sich um zentrale Verteilungspunkte, von denen Nutzer Apps beziehen können. In diesem Kapitel werden die korrespondierenden Markets der Ökosysteme vorgestellt. Dabei wird insbesondere auf die folgenden Aspekte und Fragestellungen eingegangen (Stand Juli 2013):

➜ **AUTOMATISCHE ANALYSE VON APPS** Welche Mechanismen setzen die Markets ein, um automatisiert Schwachstellen und bösartige Apps zu identifizieren?

➜ **BEDINGUNG FÜR DIE VERÖFFENTLICHUNG VON APPS** Welche Voraussetzungen müssen Entwickler von Apps erfüllen, um auf den App-Markets Apps zum Download anbieten zu können?

➜ **BESCHREIBUNGSPROFIL** Wie werden die Apps auf den Webseiten eines App-Markets dargestellt? Finden sich hier auch Informationen, die einen Rückschluss auf Sicherheitseigenschaften der App zulassen?

➜ **MELDESSYSTEM** Wie können entdeckte Schwachstellen von Apps dem Market bzw. dem Anbieter gemeldet werden?

Android

➜ AUTOMATISCHE ANALYSE VON APPS Google testet Apps, die von einem Entwickler zur Veröffentlichung auf Googles App-Market, dem Google Play Store, eingereicht wurden, auf schadhaftes Verhalten. Dieser Dienst wird Bouncer genannt und führt sowohl statische als auch dynamische Analysen durch [15].

Im Jahre 2012 ergaben Untersuchungen, dass unter Einsatz eines Android-Emulators dynamische Analysen durchführt werden, die insgesamt fünf Minuten dauern.[42] Wird eine App als bösartig angesehen, so wird diese für die weitere manuelle Inspektion markiert [22].

Android unterstützt zudem die Installation von alternativen App-Markets, sodass Apps von anderen Quellen als dem Google Play Store installiert werden können. Beispiele für alternative Märkte sind f-droid[43] und slideme[44]. Um diese Möglichkeit nutzen zu können, muss ein Nutzer die entsprechende Option in den Systemeinstellungen des mobilen Gerätes aktivieren. Welche Sicherheitsmechanismen in diesen App-Markets eingesetzt werden und ob diese mit dem Google-Bouncer vergleichbar sind, lässt sich pauschal nicht beantworten und muss fallweise untersucht werden.

Auch erlaubt Android sogenanntes *Sideloading*. Darunter versteht man das Kopieren von Daten wie z.B. Apps von einem Desktop-PC oder Notebook via USB-Kabel. Auch diese Option muss ein Nutzer in den Systemeinstellungen des Gerätes aktivieren. Auf diese Weise kann ein Nutzer Apps beliebigen Ursprungs auf dem Endgerät installieren.

➜ BEDINGUNGEN FÜR DIE VERÖFFENTLICHUNG VON APPS Um Apps zu publizieren, muss ein Entwickler einen Publisher Account bei Google eröffnen. Dies kostet 25 USD, welche unter Verwendung des Google Wallet bezahlt werden müssen (hierfür wird für die Registrierung eine Kreditkarte benötigt). In manchen Ländern ist es nicht möglich, einen Google Developer Account zu eröffnen.[45] Um kostenpflichtige Produkte über Google Play zu vertreiben, benötigen Entwickler ferner einen Google Wallet Merchant Account.

➜ BESCHREIBUNGSPROFIL VON APPS Jede App des Google Play Store wird auf einer eigenen Seite beschrieben. Dies umfasst die Absätze

- Beschreibung: Beschreibung der Inhalte und Funktion einer App
- Reviews: Meinungen von Benutzern samt grafischer Übersicht mit einer Punkteskala von 1 – 5 (höher ist besser)
- What's New: Beschreibung neuer oder überarbeiteter Funktionalitäten für neue Versionen der App
- Zusätzliche Informationen: umfasst weitere Eigenschaften der App: Updated (Datum des letzten Updates der App), Content Rating (muss vom Entwickler eingestuft werden und gibt eine Art moralischen Kodex wieder,[46] Size (Gesamtgröße der App), Current Version (aktuelle Versionsnummer), Requires Android (benötigte Android-Version), Required Permissions (benötigte

[42] Inwieweit der Google Play Store die automatisierten Sicherheitstests weiterentwickelt hat, ist nicht bekannt.

[43] Für weitere Informationen siehe https://f-droid.org/ (Letzter Zugriff 29.07.2014).

[44] Für weitere Informationen siehe http://slideme.org/ (Letzter Zugriff 29.07.2014).

[45] Für weitere Informationen siehe https://support.google.com/googleplay/android-developer/answer/136758 (Letzter Zugriff 29.07.2014)

[46] Für weitere Informationen siehe https://support.google.com/googleplay/android-developer/answer/188189?hl=en (Letzter Zugriff 29.07.2014)

Berechtigungen), Flag as Inappropriate (ungeeignete App melden), Contact Developer (Webseite des Entwicklers, E-Mail-Adresse des Entwicklers, Datenschutzrichtlinie) sowie Installs (Anzahl der Installationen).

Die Kategorie *Reviews* kann sicherheitsrelevante Informationen zu einer App enthalten, z.B. in Form von Warnungen anderer Nutzer. Eine explizite Bewertung der Sicherheitsaspekte der Apps, etwa in Form einer eigenen Kategorie, findet nicht statt. Dies gilt sowohl für die Webseite des Google Play Store als auch für die Google Play Store App, welche die Installation von Apps direkt vom Gerät aus erlaubt.

➜ **MELDESYSTEM FÜR SICHERHEITSVERLETZUNGEN** Die Google Play Store App, welche auf dem Endgerät installiert ist, bietet die Möglichkeit, als ungeeignet empfundene Apps zu melden [13]. Auf den Developer-Seiten findet sich eine Definition von Malware sowie eine E-Mail-Adresse, an die verdächtige Apps gemeldet werden können [1].

BlackBerry OS

➜ **AUTOMATISCHE ANALYSE VON APPS** Bevor eine Applikation in der BlackBerry App-World, dem App-Market von BlackBerry, zum Download für andere Nutzer veröffentlicht wird, überprüft BlackBerry diese Applikation. Über den Review-Prozess selbst und die durchgeführten Tests, ob die Richtlinien [7] eingehalten werden, gibt es jedoch keine weiterführenden Informationen.

Wie Android unterstützt auch BlackBerry OS durch die Installation zusätzlicher Software den Zugriff auf alternative App-Markets und Sideloading. Wird der alternative App-Market als App realisiert und ist nicht über die BlackBerry App-World verfügbar, muss diese über Sideloading installiert werden. Dazu muss der Benutzer jedoch eine entsprechende Option in den Systemeinstellungen von BlackBerry OS aktivieren. Eine pauschale Aussage über automatisierte Sicherheitstests dieser Drittmärkte kann jedoch nicht getroffen werden.

➜ **BEDINGUNGEN FÜR DIE VERÖFFENTLICHUNG VON APPS** Bevor ein Entwickler Apps in der BlackBerry App-World veröffentlichen kann, muss er sich kostenlos bei BlackBerry als Entwickler (Vendor) registrieren lassen. Für das Einstellen von Apps und die Veröffentlichung in der BlackBerry App-World fallen ebenfalls keine Gebühren an. Vor Freischaltung einer App wird überprüft, ob diese die von BlackBerry angegebenen Richtlinien erfüllt [7]. Sowohl Screenshots, die als Vorschau in der BlackBerry App-World angezeigt werden, als auch das Icon der eingereichten Applikation müssen dabei für alle Altersklassen freigegeben sein.

➜ **BESCHREIBUNGSPROFIL VON APPS** In der BlackBerry App-World werden zu jeder App allgemeine Informationen wie Screenshots und eine allgemeine Beschreibung der Applikation selbst bereitgestellt, die der Entwickler beim Hochladen der App in die BlackBerry App-World bereitstellt. Darüber hinaus findet der Anwender Informationen zur Versionsnummer der App, deren Größe und Release-Datum.

Zusätzlich gibt es eine Bewertung der Applikation zwischen einem und fünf Sternen, die sich aus dem Durchschnitt des von anderen Anwendern abgegebenen Feedbacks errechnet. Eine dezidierte Sicherheitsbewertung der App bietet BlackBerry App-World nicht an. Zusätzlich zu diesem Bewertungssystem haben Anwender die Möglichkeit, einen Kommentar in Textform zu hinterlassen.

Die einzige Möglichkeit, Informationen zu Sicherheitsschwachstellen zu bekommen, bietet sich durch vorher abgegebene Kommentare anderer Nutzer. Der Anwender hat jedoch keine Möglichkeit, explizit nach Informationen zu den Sicherheitsaspekten einzelner Apps zu suchen.

➜ **MELDESYSTEM FÜR SICHERHEITSVERLETZUNGEN** In der BlackBerry App-World existiert kein eingebautes Meldesystem für Sicherheitsverletzungen.

iOS

➜ **AUTOMATISCHE ANALYSE VON APPS** Apple prüft alle Apps vor einer Veröffentlichung im eigenen App-Market, dem Apple App Store. Über den genauen Ablauf der Reviews gibt es sehr wenig Informationen. Man weiß allerdings, dass Apples Review-Prozess auf zwei Methoden setzt [19]. Einerseits wird jede App manuell von einem Prüfer getestet, der dabei darauf achtet, dass z.B. die App fehlerfrei läuft und dass die App nicht gegen die von Apple aufgestellten Richtlinien für Apps [4] verstößt. Andererseits setzt Apple auf statische Analyse der Apps, um z.B. die Nutzung von privaten Schnittstellen zu entdecken, die von Entwicklern nicht eingesetzt werden dürfen.

➜ **BEDINGUNGEN FÜR DIE VERÖFFENTLICHUNG VON APPS** Um Apps im App Store veröffentlichen zu können, muss der Entwickler einen Apple Developer Account bei Apple erstellen und sich beim iOS Developer Program anmelden, welches 99 USD pro Jahr kostet. Des Weiteren müssen alle Apps den von Apple aufgestellten Richtlinien [4] entsprechen. Apple gibt dort z.B. vor, dass Apps keine anderen Apps installieren dürfen oder dass App-Icons und Screenshots eine Altersfreigabe von 4+ aufweisen müssen.

➜ **BESCHREIBUNGSPROFIL VON APPS** Einkäufe im Apple App Store erfolgen über die App Store App auf dem Telefon oder die Software iTunes. Innerhalb des App Store sind die Informationen über Apps auf einer Seite in iTunes zusammengefasst. Auf einen Blick werden dort einige Screenshots, eine kurze Beschreibung und die Release Notes der letzten Version angezeigt. Des Weiteren kann man dort Informationen zum Entwickler, die aktuelle Versionsnummer, das Datum der letzten Aktualisierung, die Größe der Anwendung, die durchschnittliche Bewertung, Kompatibilitätsinformationen, unterstützte Sprachen und Altersfreigabe einsehen.

Über einen Reiter lassen sich Benutzerbewertungen und Rezensionen einblenden. Dort findet sich neben den Bewertungen und einer kleinen Statistik über diese Bewertungen ein Link zum Support des App-Entwicklers. Es werden zunächst nur die Bewertungen für die aktuelle Version angezeigt, allerdings können auch die Bewertungen für alle Versionen eingesehen werden. Eine dezidierte Sicherheitsbewertung der App ist im App Store nicht verfügbar.

➜ **MELDESYSTEM FÜR SICHERHEITSVERLETZUNGEN** Im Apple App Store existiert kein eingebautes Meldesystem für Sicherheitsverletzungen.

Windows Phone

➜ **AUTOMATISCHE ANALYSE VON APPS** Hat ein Entwickler eine App zur Publikation im Windows Phone Store, dem App-Market von Microsoft, eingereicht, werden eine automatisierte und eine manuelle Prüfung durchgeführt. In der automatisierten Phase wird z.B. kontrolliert, ob alle benötigten Berechtigungen vorhanden sind und ob für alle verwendeten Daten (z.B. das App-Icon) korrespondierende Ressourcen vorhanden sind.

Die manuellen Tests zielen auf die Überprüfungen des Verhaltens der App. Bevor eine App durch Microsoft getestet wird, kann sie durch den Entwickler mit dem Store Test Kit vorbereitend überprüft werden.[47] Die Beschreibung dieser Kontrollen durch das Store Test Kit weisen keine sicherheitspezifischen Aspekte auf, obwohl diese laut Microsoft durchgeführt werden.[48] Daher liegt es nahe, dass das Store Test Kit keine oder nicht alle Sicherheitstests implementiert, die im Falle der Überprüfung einer zu veröffentlichen App von Microsoft tatsächlich durchgeführt werden.

➜ **BEDINGUNGEN FÜR DIE VERÖFFENTLICHUNG VON APPS** Um Apps über den Windows Phone Store zu veröffentlichen, müssen sich Entwickler zunächst registrieren. Die Kosten hierfür belaufen sich auf einmalig 19 USD. Die Registrierung umfasst die Angabe der Adresse sowie valide Kreditkartendaten des Entwicklers. Hier kann ferner zwischen zwei Account-Typen gewählt werden, für einzelne Entwickler (Individual) oder für Unternehmen (Company). Für Letztere ist der Validierungsprozess aufwendiger, da hier unternehmenseigene Zertifikate für das Ausrollen eigener Apps ausgestellt werden.

➜ **BESCHREIBUNGSPROFIL VON APPS** Konkret umfasst das Profil einer App auf der Webseite des Windows Phone Store eine kurze Beschreibung, Hersteller (Publisher), Größe der App, letzte Aktualisierung der App, Versionsnummer, Kompatibilität (Windows Phone 7, 8), Kritiken von Nutzern, die benötigten Ressourcen der App (mit einem Link unterhalb zu einer allgemeinen Erläuterungen zu Capabilities), unterstützte Sprachen, ein Link zur manuellen Installation sowie ein Link zur Datenschutzrichtlinie des App-Anbieters.

Im Falle von *Nutzerkritiken* handelt es sich um Textkommentare, welche sicherheitsrelevante Informationen zu Apps enthalten können. Zusätzlich gibt es eine Bewertung der Applikation zwischen einem und fünf Sternen, die sich aus dem Durchschnitt des von anderen Anwendern abgegebenen Feedbacks errechnet. Dezidierte Bewertungen der Apps nach Sicherheitsaspekten erfolgen fernerweder auf der Webseite des Windows Phone Store noch im Rahmen der internen Store-Anwendungen, über die eine Nutzerin direkt auf dem Endgerät Apps auswählen und installieren kann.

➜ **MELDESYSTEM FÜR SICHERHEITSVERLETZUNGEN** Ein Nutzer hat in der Store-App auf dem Endgerät die Möglichkeit, Bedenken zu einer bestimmten App an Microsoft zu senden. Diese Bedenken umfassen folgende Kategorien:

- Anstößige Inhalte
- Ausbeutung von Kindern
- Malware
- Datenschutzbedenken
- Irreführende Anwendung
- Schwache Leistung

[47] http://msdn.microsoft.com/en-us/library/windowsphone/develop/hh394032%28v=vs.105%29.aspx (Letzter Zugriff 29.07.2014)

[48] http://msdn.microsoft.com/en-us/library/windowsphone/develop/ff402533%28v=vs.105%29.aspx#BKMK_Appsafeguards (Letzter Zugriff 29.07.2014)

Ferner weist ein Eintrag eines offiziellen Microsoft-Blogs auf die Möglichkeit hin, Schadsoftware per E-Mail unter reportapp@microsoft.com zu melden.[49]

7.2 Malware auf mobilen Endgeräten

Malware dient als Überbegriff für unterschiedliche Programme, die schadhaftes Verhalten an den Tag legen. Darunter fallen Softwareanwendungen, die ein Computersystem stören, beschädigen, ausspionieren oder fernsteuern (um weitere, bösartige Aktionen auszuführen, z.B. massenweisen Versand von Werbe-E-Mails (Spam)).

Smartphones, die von Nutzern gerne als Kommunikationszentrale eingesetzt werden, stellen daher ein lohnendes Ziel dar. Während Malware prinzipiell auf allen Betriebssystemen vorkommen kann, ist das Hauptziel heutiger Malware Android. Im Folgenden wird kurz auf die Verteilung von Malware auf den verschiedenen Betriebssystemen eingegangen, dann werden einige Typen von Malware auf mobilen Endgeräten vorgestellt.

App als Infektionsweg

Schädliche Programme gelangen überwiegend als App auf mobile Endgeräte.[50] Vor diesem Hintergrund gilt es zu beachten, dass die Betriebssysteme iOS, Android, BlackBerry OS sowie Windows Phone in technischer Hinsicht profunde Unterschiede aufweisen. Deshalb können Apps, die für z.B. iOS entwickelt wurden, nicht unverändert auf einem Android-Gerät ausgeführt werden. Analog dazu verhält es sich auch mit bösartigen Apps: Auch hier muss der (kriminelle) Entwickler entscheiden, welches Betriebssystem seine Anwendung befallen soll.

Wie bereits in Kapitel 7.1 beschrieben, setzen die App-Markets, die den Betriebssystemen Apps bereitstellen, Sicherheitsmechanismen ein, um schädliche Apps zu detektieren. Bis auf Android und BlackBerry OS erlauben die anderen Betriebssysteme ausschließlich den Bezug über den herstellereigenen App-Market. Aus Sicht eines Malware-Entwicklers bieten diese Systeme prinzipiell mehr Möglichkeiten, die zur Installation schädlicher Apps auf ein Endgerät führen können.

Trojaner auf mobilen Endgeräten

Trojaner bezeichnen Programme, die getarnt als gutartige App heruntergeladen, installiert und ausgeführt werden. Die dem Benutzer suggerierte Programmfunktionalität wird von einem Trojaner in der Regel bereitgestellt, allerdings besitzt das Programm weitere verborgene, bösartige Funktionalität.

➜ **BANKING-TROJANER** Mit Blick auf mobile Endgeräte ist im Umfeld von Trojanern besonders eine Unterform hervorzuheben, die darauf abzielt, Online-Banking-Informationen, wie z.B. Zugangsdaten (Credentials) für Online-Banking-Konten, auszuspähen und an einen zentralen Punkt zu übertragen. Kaspersky, ein russisches Sicherheitsunternehmen, listet vier Beispiele für diese Banking-Trojaner

[49] http://blogs.windows.com/windows_phone/b/windowsphone/archive/2013/08/29/how-windows-phone-guards-against-malware. aspx (Letzter Zugriff 29.07.2014)

[50] Es sind aber auch Fälle bekannt, bei denen Schadprogramme bereits als Teil der Firmware, d.h. des Betriebssystems des Endgerätes, integriert sind. Für weitere Informationen siehe u.a. CarrierIQ.

auf, namentlich sind das *Carberp*, *Citadel*, *SpyEye* sowie *Zeus*.[51] Der Quellcode von Zeus wurde 2011 veröffentlicht, viele der heute bekannten Banking-Trojaner bauen in Teilen darauf auf.

Botnets auf mobilen Endgeräten

Ein weiterer Typ von Malware sind Botnets. Unter einem *Botnet* versteht man Anwendungen, mit denen (in der Regel) sehr viele Computer infiziert sind. Die Anwendungen bekommen von einem zentralen Punkt Anweisungen zur Durchführung bestimmter Aktionen. So können Botnets z.B. eingesetzt werden, um Spam (Massen-E-Mails) zu versenden oder massenweise private Daten der infizierten Geräte auszuspähen.

Der Einsatz von Botnets bei mobilen Endgeräten lohnt deshalb besonders, weil diese sehr selten ausgeschaltet werden. Somit stehen die Endgeräte – im Unterschied zu infizierten Desktop-PCs – stets zur Durchführung bestimmter Aktionen des Angreifers bereit [17].

7.3 Sicherheitsmodelle

Ein Sicherheitsmodell in der IT ist eine Abstraktion zur Beschreibung der Sicherheitseigenschaften eines Systems. Hierunter fällt insbesondere auch der Umgang mit geschützten Ressourcen, z.B. wer Zugriffsrechte erhält, ob diese Rechte geändert werden können und welche Ressourcen das System schützt. Auf einem Smartphone ist ein solches Sicherheitsmodell gerade im Zusammenhang mit Drittanbieter-Apps wichtig. Das jeweilige Betriebssystem regelt anhand des Sicherheitsmodells den Zugriff der Apps auf die Daten. Dadurch hat das Sicherheitsmodell direkten Einfluss auf die Sicherheit der Daten des Nutzers. Eingegangen wird nur auf den Umgang mit Zugriffsrechten auf private Daten, die in Kapitel 4 vorgestellt worden sind.

Eine Betrachtung der Sicherheitsmodelle erlaubt es zudem, die Sicherheitseigenschaften der Betriebssysteme zu vergleichen. Das Sicherheitsmodell eines Betriebssystems gibt einen Rahmen vor, in welchem sich App-Entwickler bewegen müssen. Im Fokus steht bei der Betrachtung die Perspektive eines Nutzers und welche Auswirkungen die verschiedenen Aspekte des Sicherheitsmodells für ihn haben. Eine technisch detaillierte Betrachtung aus Entwicklersicht geht über den Rahmen der Studie hinaus.

Die verwendeten Sicherheitsmodelle lassen sich grob durch die folgenden Aspekte beschreiben:

- Erkennbarkeit benötigter Berechtigungen
- Zeitpunkt der Zugriffserlaubnis
- Selektive Vergabe von Zugriffsrechten
- Granularität von Zugriffsrechten
- Änderungsmöglichkeiten von Zugriffsrechten
- Nachverfolgbarkeit von erfolgten Zugriffen
- Benutzbarkeit

Tabelle 7.1 skizziert die Ergebnisse des Vergleichs der Sicherheitsmodelle anhand der angegebenen Aspekte. Eine detailliertere Beschreibung der Ergebnisse findet sich in den folgenden Abschnitten.

[51] https://blog.kaspersky.com/the-big-four-banking-trojans/ (Letzter Zugriff 29.07.2014)

Tabelle 7.1: Vergleich der Sicherheitsmodelle

● Weniger gut umgesetzt ●● Durchschnittlich umgesetzt ●●● Besonders gut umgesetzt

	Android	BB OS	iOS	Windows Phone
Erkennbarkeit	●●	●●	●	●
Zeitpunkt	Installation	Installation	direkt vor Zugriff	Installation
Selektive Vergabe	●	●●●	●●●	●
Granularität	●	●●	●●	●●
Änderungsmöglichkeit	●	●●●	●●●	●
Nachverfolgbarkeit	●●	●	●●	●
Benutzbarkeit	●	●	●●●	●

7.3.1 Erkennbarkeit benötigter Berechtigungen

Die Sicherheitsmodelle unterscheiden sich durch den Umfang der Daten, die geschützt werden. Der Fokus dieser Betrachtung liegt dabei darauf, ob dies für einen Nutzer ersichtlich ist oder nicht. Das Sicherheitsmodell sieht i.d.R. vor, dass der Nutzer über bestimmte Berechtigungen informiert wird, die eine App anfordert. Einige dieser Berechtigungen betreffen den Zugriff auf vom System verwaltete Daten und helfen so, den Nutzer über mögliche Datenzugriffe zu informieren.

Im Rahmen der Betrachtung wird davon ausgegangen, dass es einem Nutzer nicht zumutbar ist, in technischen Entwicklerdokumentationen nachzulesen, welche seiner Daten geschützt werden. Das Sicherheitsmodell muss ihn über Zugriffe auf private Daten informieren. Dies geschieht über die Präsentation der von der App angeforderten Rechte per Dialogfenster, etwa beim Installationszeitpunkt einer App.

Ein Problemfeld in diesem Zusammenhang stellt die Unterscheidung dar, ob Daten vom Betriebssystem verwaltet werden oder von einer App. Für den Nutzer ist dies nicht unbedingt offensichtlich, kann aber je nach Betriebssystem einen wichtigen Unterschied darstellen. So können z.B. Apps unter Android Datenzugriffe auf von ihnen verwaltete Daten erlauben, während dies unter iOS nicht möglich ist. Im Rahmen der hier durchgeführten Betrachtung werden die vom Betriebssystem geschützten Daten berücksichtigt, nicht jedoch die von Apps bereitgestellten Daten.

Erschwert wird der Vergleich auch dadurch, dass die Sicherheitsmodelle ihre Berechtigungssysteme nicht auf der gleichen Einteilung von Ressourcen bzw. Daten aufbauen. Besonders deutlich wird dies bei Mediendaten. BlackBerry OS und Android nutzen eine vergleichsweise generische Berechtigung, um Apps Zugriff auf den Speicherort zu gewähren, an dem Mediendaten gespeichert sind.[52] iOS und Windows Phone vergeben die Berechtigung auf die Mediendaten unter der Annahme, dass sich diese in den systemeigenen Medienbibliotheken befinden.

Tabelle 7.2 gibt eine Übersicht, welche in Kapitel 4 vorgestellten privaten Daten für den Nutzer ersichtlich vom Sicherheitsmodell geschützt werden. Eine vollständige Betrachtung aller möglichen Daten bzw. Ressourcen sowie korrespondierender Berechtigungen geht über den Rahmen dieser Studie hinaus. Dies gilt insbesondere für den Fall, dass Daten nicht ersichtlich für den Nutzer geschützt werden. Ob diese Daten tatsächlich vom Sicherheitsmodell nicht geschützt werden oder es nur für den Nutzer nicht ersichtlich ist, müsste in einer detaillierten Sicherheitsanalyse untersucht werden.

[52] Wie bereits oben erwähnt, wird keine App-interne Verwaltung von Daten betrachtet.

Tabelle 7.2: Vom Sicherheitsmodell geregelter und für den Anwender erkennbarer Zugriff auf einzelne Daten

👁 Der Nutzer wird über Datenzugriff informiert

✘ Der Nutzer wird über den Datenzugriff nicht informiert – aber ein Zugriff ist möglich – , oder das Sicherheitsmodell gestattet keinen Zugriff auf die Daten

Daten	Android	BB OS	iOS	Windows Phone
KONFIGURATIONSDATEN				
Geräte-IDs	👁	👁	✘[53]	👁
KOMMUNIKATIONSDATEN				
Anrufliste & Anrufstatistik	👁	✘	✘	✘
TRANSFERDATEN				
SMS/MMS	👁	👁	✘	✘
E-Mails	✘	👁	✘	✘
PROFILDATEN				
Eigene Kontaktdaten	👁	👁	✘	✘
Kontakte	👁	👁	👁	👁
Termine	👁	👁	👁	👁
Aufgaben	✘	👁	👁	✘
Standortdaten	👁	👁	👁	👁
Bewegungssensor	✘	✘	👁	👁
MEDIENDATEN				
Musik	👁[54]	👁[55]	✘	👁
Videos	👁[54]	👁[55]	👁[56]	👁
Fotos, Bilder & Fotoalben	👁[54]	👁[55]	👁	👁
INTERNETDATEN				
Verlauf, Lesezeichen	👁	✘	✘	✘
ANDERE DATEN				
SD-Karte	👁[54]	👁[55]	✘[57]	👁

[53] Apple stellt Entwicklern eigens eingeführte IDs mit unterschiedlichen Lebensdauern zur Verfügung, welche zur Identifikation des Nutzers genutzt werden sollen.

[54] Android bietet eine generische Berechtigung, USB-Speicherinhalte zu lesen, die unter anderem den Zugriff auf den „externen Speicher" (nicht notwendigerweise entfernbarer Speicher) regelt, in welchem u.a. Mediendateien gespeichert werden können.

[55] BlackBerry OS bietet nur eine generische Berechtigung „Freigegebene Daten", hinter der sich eine Vielzahl verschiedener Daten verbirgt. Eine feingranulare Steuerung der Zugriffsrechte ist nicht möglich. Einmal erteilt, kann eine App auf alle weiteren Daten ohne Nachfrage zugreifen.

[56] Videos werden unter iOS mit Fotos zusammengefasst. Wurde bspw. der Nutzer einmal um die Erlaubnis für den Zugriff auf Fotos gefragt, wird er nicht erneut um eine Erlaubnis für den Zugriff auf Videos gefragt.

[57] Das iPhone verfügt über keine SD-Karten-Schnittstelle.

7.3.2 Zeitpunkt der Zugriffserlaubnis

Im Sicherheitsmodell stellt der Zeitpunkt, wann ein Nutzer nach Erlaubnis für den Zugriff auf Daten gefragt wird, ein wichtiges Kriterium dar. Auf den untersuchten Betriebssystemen lassen sich zwei unterschiedliche Verfahren feststellen. Die meisten Systeme, darunter Android, BlackBerry OS und Windows Phone, stellen den Nutzer direkt bei der Installation vor die Wahl, den Zugriff auf Daten bzw. Ressourcen zu gewähren. Die Konsequenzen unterscheiden sich allerdings zwischen den Betriebssystemen. Während die Installation einer App auf Android und Windows Phone ohne die Zustimmung eines Nutzers zu benötigten Rechten abgebrochen wird, kann die App auf BlackBerry OS trotz verweigerter Rechte installiert werden. Im Extremfall kann diese aber nicht sinnvoll verwendet werden.

Apples Betriebssystem iOS arbeitet anders. Der Nutzer erhält jedes Mal eine Zugriffserlaubnis-Anfrage, wenn die Drittanbieter-App zum ersten Mal auf ein geschütztes Datum zugreifen möchte. Hat der Nutzer einmal den Zugriff erlaubt, wird er bei weiteren Zugriffen der gleichen App auf das gleiche private Datum nicht mehr darauf hingewiesen.

7.3.3 Selektive Vergabe von Zugriffsrechten

Ein anderer Aspekt des Sicherheitsmodells stellt der Umgang mit der Kumulation von Zugriffsanfragen dar. Oft wollen Drittanbieter-Apps nicht nur auf ein einziges geschütztes Datum eines Typs zugreifen, sondern auf mehrere. In diesem Fall könnte das Sicherheitsmodell den Nutzer jeweils einzeln für jedes private Datum auffordern, seine Erlaubnis zu erteilen, oder in einer kumulierten Anfrage auf einmal die Erlaubnis für alle privaten Daten dieses Typs einholen.

Die einzelnen Betriebssysteme gehen unterschiedlich mit der Zusammenfassung von Zugriffsanfragen um. iOS stellt beim ersten Zugriffsversuch auf ein privates Datum eines Typs eine Anfrage an den Benutzer. Dies erlaubt dem Nutzer natürlich auch, jede Anfrage unterschiedlich zu beantworten, allerdings kann es dann vorkommen, dass direkt hintereinander mehrere Anfragen gestellt werden.

Im Gegensatz hierzu stellen die anderen Betriebssysteme kumulierte Anfragen bei der Installation der Drittanbieter-Apps. Während man bei BlackBerry OS allerdings die Möglichkeit hat, die Anfragen zu selektieren, die man nicht erlauben möchte, muss man bei Android und Windows Phone entweder alle erlauben oder alle ablehnen.

7.3.4 Granularität von Zugriffsrechten

Im Sicherheitsmodell wird auch die Granularität von Zugriffsrechten festgelegt, d.h. wie detailliert bestimmt werden kann, auf welche Daten Zugriffe möglich sind. Am Beispiel eines Adressbuches mit verschiedenen Kontakten lässt sich dies verdeutlichen. Bestimmt das Sicherheitsmodell, dass Zugriffsrechte nur für das Adressbuch allgemein vergeben werden, kann eine App, die dieses Zugriffsrecht erhält, auf alle Kontakte innerhalb des Adressbuches zugreifen. Erlaubt das Sicherheitsmodell aber Zugriffsrechte auf Kontaktebene, könnte der Nutzer der App nur bestimmte einzelne Kontakte zugänglich machen, z.B. indem er die Freigabe für jeden einzelnen Kontakt bestätigt.

Keines der betrachteten Betriebssysteme erlaubt Zugriffsrechte auf Kontaktebene. Dies hat Vorteile für den Nutzer, denn eine zu hohe Granularität der Zugriffsrechte setzt umfangreiches Wissen über die Ressource voraus, erschwert im Allgemeinen die Benutzung und sorgt so schnell für Verdruss beim Nutzer. In der Regel nutzen alle Betriebssysteme eine vergleichbare Granularität.

Eine Besonderheit für die Granularität ergibt sich bei Android: Seit Mai 2014 werden dargestellte Zugriffsrechte von Google Play in Berechtigungsgruppen zusammengefasst. Dies diene laut Google der besseren Darstellung [14] benötigter Zugriffsrechte gegenüber dem Benutzer. Allerdings gehen Berechtigungsgruppen über ein bare Änderung in der Darstellung hinaus: Stimmt ein Nutzer einer Berechtigungsgruppe zu, so können Aktualisierungen der App zu einem späteren Zeitpunkt – ohne einer Bestätigung durch den Nutzer zu bedürfen – weitere Zugriffsrechte der bestätigten Gruppe nutzen. Im Beispiel: Apps, die auf die Anrufstatistik zugreifen dürfen, können zu einem späteren Zeitpunkt unter Umständen Anrufe ohne Nutzerinteraktion führen.

7.3.5 Änderungsmöglichkeiten von Zugriffsrechten

Das Sicherheitsmodell legt auch fest, ob es dem Nutzer gestattet ist, Zugriffsentscheidungen rückgängig zu machen. So können Nutzer bei BlackBerry OS und iOS nachträglich die Zugriffsberechtigungen von Apps entziehen (oder erlauben), bei Android und Windows Phone ist dies nicht möglich.

Alle Betriebssysteme unterstützen für bestimmte Zugriffsentscheidungen den Entzug von Zugriffsberechtigungen. Dazu zählen die globale Deaktivierung der Positionsbestimmung sowie Möglichkeiten der Datenverbindung (Deaktivierung von Datenübertragung via WLAN oder Mobilfunknetze).

7.3.6 Nachverfolgbarkeit von erfolgten Zugriffen

Ein Sicherheitsmodell kann einem Nutzer ermöglichen, nachzuvollziehen, ob und wann Zugriffe auf private Daten erfolgt sind. Die betrachteten Betriebssysteme bieten eine solche Möglichkeit allerdings nicht an. Eine Ausnahme stellen Standortdaten auf Android und iOS dar. Hier kann ein Nutzer nachvollziehen, welche Anwendungen zuletzt auf Standortdaten zugegriffen haben.

7.3.7 Benutzbarkeit

Ein Aspekt eines Sicherheitsmodells, der von den anderen diskutierten Aspekten stark beeinflusst wird, ist die Benutzbarkeit, d.h. wie viel Expertenwissen erforderlich ist, um wirklich entscheiden zu können, ob ein Datenzugriff notwendig ist oder nicht. Den größten Einfluss auf die Benutzbarkeit hat der Zeitpunkt der Zugriffsentscheidung sowie die zu diesem Zeitpunkt vorhandene Information über den Grund des Zugriffs. Bei iOS wird eine Zugriffsanfrage beim ersten Zugriff auf das Datum gestellt. Die Anfrage enthält eine kurze Erklärung der Drittanbieter-App, warum der Zugriff notwendig ist. Solche Anfragen werden im Verlauf der Nutzerinteraktion mit der App gestellt, wodurch sie dem Nutzer zusätzliche Kontextinformationen bieten. Daraus kann er im Allgemeinen ableiten, ob eine Zugriffsanfrage im Zusammenhang mit seiner Interaktion mit der App steht oder nicht.

Bei Android, BlackBerry OS und Windows Phone wird vom Nutzer erwartet, dass er zum Zeitpunkt der Installation entscheiden kann, welche Zugriffe gerechtfertigt sind und welche nicht. Zu den Auflistungen der angefragten Zugriffsrechte werden keine Erläuterungen geliefert, weshalb diese von der App benötigt werden. Auch ein Nutzungskontext ist zu diesem Zeitpunkt nicht vorhanden. Deshalb ist es für Nutzer ohne ausreichendes Expertenwissen schwierig, einen gerechtfertigten Zugriff von einem nicht gerechtfertigten zu unterscheiden.

7.3.8 Weitere Sicherheitsvorkehrungen der Betriebssysteme

➜ **BILDSCHIRMSPERRE** Smartphones bieten die Möglichkeit, eine Bildschirmsperre einzurichten. Diese verwehrt Unbefugten den Zugriff auf das Telefon. Bei einem verlorenen oder gestohlenen Telefon bietet dies eine erste Schutzfunktion für die auf dem Gerät gespeicherten Daten. Ohne diese sind die Daten direkt zugänglich. Zur Entriegelung stehen z.B. folgende Optionen zur Verfügung:

- **PIN:** Eine persönliche Identifikationsnummer, d.h., der Nutzer gibt eine geheime Zahlenkombination ein, um das Telefon zu entriegeln.
- **Passwort:** Ein Nutzer gibt eine geheime Zeichenfolge ein, um das Gerät zu entsperren.
- **Muster:** Dieses Muster setzt sich aus einer individuellen, nur dem Nutzer bekannten Linie zusammen, die neun Punkte auf dem Telefon auf (fast) beliebige Art miteinander verbindet.
- **Face Unlock:** Bei Android kann das Gerät über Gesichtserkennung entriegelt werden. Da dieser Mechanismus z.B. aufgrund der Lichtverhältnisse zum Teil nicht funktionstüchtig sein kann, muss der Nutzer als alternative Entsperrungsoption ebenfalls ein Muster, eine PIN oder ein Passwort setzen.
- **Fingerprint:** Apple iOS bietet in Zusammenhang mit dem aktuellen iPhone-Modell die Möglichkeit, das Telefon über den Fingerabdruck des Nutzers zu entriegeln. Dafür besitzt das Gerät einen Fingerabdruckscanner, über den es den Anwender identifiziert.

Die dritte und vierte Option gibt es nur auf Android-Smartphones. Damit der Nutzer das Smartphone nicht selbst verriegeln muss, existiert bei allen Betriebssystemen die Auto-Lock-Funktion. Durch diese aktiviert sich die Bildschirmsperre nach einer konfigurierbaren Zeitspanne von selbst.

➜ **VERSCHLÜSSELUNG** Bei allen Betriebssystemen lassen sich Daten auf dem Gerät verschlüsseln. Beim Einsatz einer *Geräteverschlüsselung* wird der ganze interne Speicher geschützt. Allerdings ist Geräteverschlüsselung nur bei iOS obligatorisch. Bei den anderen Betriebssystemen kann der Nutzer wählen, ob er die Verschlüsselung aktiviert oder sie deaktiviert lässt. Bei aktiver Verschlüsselung verschlüsselt Android u.a. Daten der Google-Konten, App-Daten, Musik sowie andere Mediendateien.[58] Windows-Phone-Nutzer können die Verschlüsselung nur über den Einsatz einer Exchange Active Sync Policy, wie sie im Unternehmensumfeld zum Einsatz kommt, aktivieren. Privatnutzer ohne eigenen Exchange-Server können daher die Verschlüsselung gar nicht aktivieren.

Ein Problem mit Geräteverschlüsselung bei Smartphones ist, dass diese nur greift, wenn das Gerät ausgeschaltet ist, was bei Smartphones fast nie der Fall ist. Während Android und Windows Phone es dabei belassen, versuchen BlackBerry OS und iOS, dieses Problem mit unterschiedlichen Ansätzen anzugehen. Ist ein BlackBerry-Smartphone gesperrt, liegen auch die Daten verschlüsselt auf dem Gerät und können nicht ausgelesen werden. Daten, die währenddessen empfangen werden, werden vom Gerät sofort verschlüsselt gespeichert.

iOS definiert ein System von Schutzklassen für Daten, welche den Umfang der Verschlüsselung regeln und welche von allen App-Entwicklern genutzt werden können. In der restriktivsten Schutzklasse sind Daten nur entschlüsselt, wenn das Gerät entsperrt ist. Apple nutzt laut eigenen Angaben [5] die restriktivste Klasse bei E-Mails und Standortdaten. Welche Schutzklasse für welche Daten genutzt wird, ist für den Nutzer nicht transparent.

[58] Die Verschlüsselung umfasst die Data Partition des Gerätes. Sofern das Gerät externe Speicher in Form von SD-Karten unterstützt, können Nutzer auch die auf der SD-Karte gespeicherten Daten verschlüsseln.

➜ **REMOTE SERVICES** Alle Betriebssysteme erlauben es dem Nutzer, das Telefon mit einem Benutzer-Account des jeweiligen Herstellers zu verbinden, um Zugriff auf verschiedene Fernwartungsdienste zu erhalten. Die Benutzer können ihre Smartphones orten, einen Ton abspielen, das Smartphone sperren oder die Daten auf dem Smartphone löschen lassen. Dazu müssen in der Regel auf dem Smartphone der Benutzer-Account eingerichtet und die Remote Services auf dem Telefon aktiviert werden.

7.4 Datennutzung am Beispiel von *Angry Birds*

Apps tun mehr, als dem Nutzer eventuell bewusst ist, was hier am Beispiel von *Angry Birds* vom Hersteller Rovio verdeutlicht werden soll. Das Spiel *Angry Birds* ist als App auf allen untersuchten Betriebssystemen erhältlich. Während der aktiven Spielzeit kommuniziert *Angry Birds* mit verschiedenen Servern. Die Kommunikation kann bei Spielen z.B. dazu dienen, Ranking-Listen abzufragen, damit sich Leistungen vergleichen lassen oder um Werbung einzublenden.

Für alle Betriebssysteme bis auf Android ist das Spiel kostenpflichtig, wobei es für iOS zusätzlich eine kostenfreie Version gibt, allerdings mit erheblich eingeschränktem Funktionsumfang. Die kostenfreien Versionen zeigen im Vergleich zu den kostenpflichtigen Versionen mehr Werbung an.

Der nachfolgende Abschnitt fasst die Ergebnisse der praktischen Tests zusammen und hebt wichtige Erkenntnisse hervor. Untersucht wurde, welche Verbindungen während einer durchschnittlichen Nutzerinteraktion aufgebaut wurden. Danach folgt pro Betriebssystem jeweils ein Abschnitt, in dem die Einzelergebnisse detailliert beschrieben werden.

Zusammenfassung der Ergebnisse

➜ **WERBUNG, WERBENETZE & CDNS** Sowohl bei Android als auch bei iOS wurden Werbeanzeigen in Form von Bildern angezeigt. Android tauschte mit einem Volumen von ca. 6 MB mit Abstand die meisten Daten aus. Auch die Anzahl der Endpunkte mit insgesamt 38 war bei Android am höchsten. Es ließ sich für Android feststellen, dass ein komplexes Werbenetzwerk im Hintergrund zum Einsatz kommt, an das neben der App-Nutzung auch Daten wie z.B. aktuelle IP-Adresse des Gerätes, Mobilfunkanbieter, Geräte-Typ, Betriebssystemversion etc. übermittelt werden. Die übermittelten Daten werden von Unternehmen wie http://www.millennialmedia.com gesammelt und ausgewertet. Dabei kommen sowohl bei Android als auch bei iOS Content Delivery Networks (CDN) für die Übertragung von Bildern, z.B. um Werbebanner einzublenden, zum Einsatz.

➜ **SPIELESTATISTIKEN** Bei den Verbindungen des Windows Phone ließ sich beobachten, dass Statistiken über den Spielverlauf der Microsoft-Spieleplattform xboxlive.com bereitgestellt wurden und allgemeine Informationen über die Nutzung von Spielen erhoben wurden.

➜ **KEINE ZUSÄTZLICHEN VERBINDUNGEN** Im Falle von BlackBerry konnten keine Verbindungen identifiziert werden, die speziell auf die Nutzung des Spiels zurückzuführen sind.

Einzelergebnisse der Betriebssysteme

Android

Dem Nutzer wird Werbung in Form von Bannern und Videos eingeblendet, sowohl während des Spielens als auch zwischen einzelnen Levelübergängen.
Zusätzlich zu den Konversationen und Verbindungen, die bereits in den praktischen Tests zu minimalen Einstellungen beobachtet werden konnten (siehe dazu Unterkapitel 5.1.2), etablierte das Gerät **164 Verbindungen** mit insgesamt **38 Endpunkten (IP-Adresse)**, wobei **6,05 Megabyte** Daten ausgetauscht wurden. Weitere Informationen über die Konversationen und Verbindungen:

- 5 der 38 Endpunkte besitzen eine IP-Adresse, die zu Amazon CloudFront gehören, einem Content Delivery Network (CDN)-Angebot von Amazon.
- 1 der 38 Endpunkte spricht direkt mit einem Endpunkt, dessen Adresse cloud.rovio.com lautet.
- 52 der 164 Verbindungen sind mit TLS verschlüsselt.

Das Gerät baut eine Verbindung mit dem Host neptune.appads.com auf, der unter der URL P-ADS-OR-LB04-1773581531.us-west-2.elb. amazonaws.com zu erreichen ist. Die App bzw. das Gerät überträgt folgende Daten in unverschlüsselter Form (via HTTP):

- ausgewählte Sprache
- Geräte-ID sowie MAC-Adresse[59] (verschlüsselt, d.h., diese beiden Felder sind nicht im Klartext lesbar)
- IP-Adresse des Gerätes
- Mobilfunkanbieter
- Gerätetyp
- Betriebssystem des Gerätes sowie Version
- Auslösung des Bildschirms

Ein Teil der Endpunkte, mit denen die *Angry Birds*-App kommuniziert, sind Content Delivery Networks (CDN). Dazu zählen Rovio selbst (ads.cdn.rovio. com), skyrocketapp[60] (cdn.skyrocketapp.com), Google (pagead2. googlesyndication.com), appads (cdn.appads.com), applifier (cdn. applifier.com)[61] sowie cdn.mxpnl.com. Diese Dienste dienen u.a. dazu, Bilder und Videos zu Werbezwecken auszuliefern.

Weiterhin kommuniziert die App mit Adressen, die zu Firmen wie z.B. TRUSTe[62], millennialmedia[63]21, flurry[64], nexage[65] sowie mixpanel[66] gehören. Diese Unternehmen konzentrieren sich auf die Sammlung, Analyse und Verwertung von Daten, die bei der Nutzung einer App mit Werbung entstehen.

---

[59] Eine Media-Access-Control (MAC)-Adresse bezeichnet eine Nummer, die eine Hardware-Komponente eindeutig identifiziert, über die auf ein Netzwerk, z.B. auf ein WLAN, zugegriffen wird.

[60] http://www.skyrocketapp.com/ (Letzter Zugriff 29.07.2014)

[61] http://www.applifier.com/ (Letzter Zugriff 29.07.2014)

[62] http://www.truste.com (Letzter Zugriff 29.07.2014)

[63] http://www.millennialmedia.com (Letzter Zugriff 29.07.2014)

[64] http://www.flurry.com (Letzter Zugriff 29.07.2014)

[65] http://www.nexage.com/ (Letzter Zugriff 29.07.2014)

[66] https://mixpanel.com/ (Letzter Zugriff 29.07.2014)

BlackBerry OS

Während des Untersuchungszeitraums konnte bei der Verwendung der AngryBirds-App keine weitere Netzwerkkommunikation neben den in Kapitel 5.1.2 bereits untersuchten Verbindungen beobachtet werden.

iOS

Neben den aus den vorherigen praktischen Tests (s. Kapitel 5.1.2) bekannten Endpunkten kommunizierte das Gerät mit weiteren **13 Endpunkten (IP-Adressen)** und etablierte dabei **43 Verbindungen**. Ausgetauscht wurden insgesamt **1,11 Megabyte** Daten. Weitere Informationen über die Konversationen:

- 5 der 13 Endpunkte sprechen die Adresse cloud.rovio.com an, die in der Amazon Cloud gehostet werden.
- 6 der 13 Endpunkte besitzen eine IP-Adresse, die zu Amazon CloudFront gehören, einem CDN-Angebot von Amazon.
- 2 der 13 Endpunkte kommunizieren mit der Adresse data.flurry. com, welche der Firma Flurry gehört, einem Anbieter für Datenanalyse und Werbung auf mobilen Betriebssystemen.
- 38 der 43 Verbindungen wurden mit TLS verschlüsselt. Unter den untersuchten Verbindungen sind hervorzuheben:

Bis auf eine der Verbindungen mit dem CDN-Dienst CloudFront waren alle Verbindungen unverschlüsselt und dienten der Bereitstellung von Werbeanzeigen in Form von Bildern. Die erste erfasste Verbindung mit CloudFront war verschlüsselt, daher lässt sich nicht sagen, ob über diese Verbindung Informationen über das iPhone, z.B. ein Identifier, abgeflossen sind.

Die Verbindung mit data.flurry.com war verschlüsselt. Daher bleibt unklar, welche Daten an flurry abgeflossen sind.

Windows Phone

Zusätzlich zu den Konversationen und Verbindungen, die bereits in den praktischen Tests zu minimalen Einstellungen beobachtet werden konnten (siehe dazu Unterkapitel 5.1.2), etablierte das Gerät **52 Verbindungen** mit insgesamt **26 Endpunkten (IP-Adressen)**, wobei **1,44 Megabyte** Daten ausgetauscht wurden. Weitere Informationen über die Konversationen und Verbindungen:

- 10 der 26 Endpunkte besitzen eine IP-Adresse, die alle in der Domäne xboxlive.com liegen.
- 2 der 26 Endpunkte sprechen direkt mit einem Endpunkt, dessen Adresse cloud.rovio.com lautet.
- 39 der 52 Verbindungen sind mit TLS verschlüsselt.

Die Konversationen mit den Endpunkten der Domäne xboxlive.com sind verschlüsselt. Anhand der Namen der Subdomänen kann aber vermutet werden, welche Dienste sich hinter diesen URLs verbergen:

- stats.gtm.xboxlive.com: An diese Stelle scheinen Statistiken über den Spielverlauf übertragen zu werden.

- rewards.xboxlive.com: Dabei handelt es sich um einen Dienst, der Informationen über die Nutzung von Spielen sowie anderen Medien des Angebotes Xbox Live sammelt. Wer das Angebot sehr ausgiebig nutzt, erhält eine Belohnung.[67]
- client-auth.gtm.xboxlive.com: Dieser Dienst scheint die Authentifizierung von Nutzern durchzuführen, wenn ein Spiel auf dem Endgerät gestartet wird.

[67] Für weitere Informationen siehe http://rewards.xbox.com/ (Letzter Zugriff 29.07.2014).

8. Praxishinweise für Smartphone-Nutzer

Vor dem Hintergrund der Kapitel 5, 6 und 7 fasst dieser Abschnitt praktische Hinweise für Nutzer zusammen. Sie dienen der Orientierung und werden für jedes Betriebssystem nachfolgend kurz beschrieben.

8.1 Hinweise für Android-Nutzer

➜ **BILDSCHIRMSPERRE** Das Einstellen der Bildschirmsperre bietet im Verlustfall oder bei Diebstahl des Smartphones einen ersten Schutz vor unberechtigtem Zugriff auf die gespeicherten Daten eines Gerätes.

➜ **VERSCHLÜSSELUNG** Die Aktivierung der Geräteverschlüsselung kann verhindern, dass auf die gespeicherten Daten im Falle eines Diebstahls oder Verlusts zugegriffen werden kann.

➜ **SYNCHRONISIERUNG** Android bietet eine Reihe von Synchronisierungsoptionen, die einzeln aktiviert oder deaktiviert werden können. Je nach Sensibilität kann ein Nutzer hier entscheiden, welche Daten auf Servern von Google gespeichert werden sollen. Dies gilt auch für Cloud-Dienste wie Google Drive.

➜ **INTERESSENBEZOGENE ANZEIGEN** Android bietet Nutzern die Option, interessenbezogene Werbung zu deaktivieren.

➜ **STANDORTBERICHTE & STANDORTVERLAUF** Standortberichte speichern regelmäßig den Aufenthaltsort des Smartphones auf Google-Servern. Der Standortverlauf verknüpft die Informationen verschiedener Geräte des gleichen Nutzers zu einem detaillierten Standortverlauf des Nutzers. Beide können deaktiviert werden.

➜ **ORTUNGSDIENSTE** Der Nutzer kann Ortungsdienste in verschiedenen Modi nutzen, die unterschiedlich genaue Standortbestimmungen ermöglichen. Der Unterschied zwischen den Modi liegt darin, welche Daten zur Standortbestimmung genutzt werden. Bei höchster Genauigkeit werden Daten über WLAN-Netzwerke und Mobilfunkmasten zusätzlich zu GPS genutzt. Ortungsdienste kann ein Nutzer nur global erlauben oder verbieten. Dies ermöglicht eine gewisse Kontrolle, der Nutzer kann z.B. Standortdaten nur im Bedarfsfall einschalten, etwa zur Verwendung einer Navigations-App.

➜ **SPRACHEINGABE** Spracheingaben für die Sprachsuche werden von Google erfasst. Dies gilt auch für sensible Informationen, die auf diese Weise in das Gerät eingegeben werden.

➜ **APPS AUS UNBEKANNTEN QUELLEN** Android erlaubt es Nutzern, Apps aus unbekannten Quellen, d.h. abseits des Google Play Store, zu beziehen und auf dem Gerät auszuführen. Auf diese Weise können Schadprogramme auf das Endgerät gelangen, da Apps aus unbekannten Quellen u.U. keine vergleichbaren Überprüfungsmechanismen wie im Google Play Store durchlaufen haben.

➜ **SUPERUSER** Android bietet die Möglichkeit, Endgeräte zu *rooten*, sodass auf dem Gerät installierte Apps über höhere Privilegien verfügen. Bestimmte Funktionalitäten können Apps nur dadurch ermöglicht werden. Allerdings werden auf diese Weise einige Sicherheitsmechanismen des Betriebssystems ausgehebelt, was weitreichende Konsequenzen haben kann. Diese Privilegien können z.B. von

bösartigen Apps missbraucht werden, um die Daten des Endgerätes auszuspionieren. Durch die umfassenden Berechtigungen des Superusers können die Daten des Anwenders erheblich gefährdet werden.

8.2 Hinweise für BlackBerry-Nutzer

➜ **GERÄTEKENNWORT** Das Festlegen eines Kennworts dient als genereller Zugriffsschutz auf die Daten des Telefons. Darüber hinaus ist es notwendig zur Aktivierung der Datenverschlüsselung. Neben einem normalen Passwort kann der Nutzer ein sogenanntes Bild-Passwort verwenden. Dabei wird eine Matrix aus Ziffern über einem vorher auszuwählenden Bild angezeigt, und der Anwender muss eine bestimmte Ziffer der Matrix in einen bestimmen – vorher festgelegten – Bereich des Bildes ziehen, um das Telefon zu entsperren.

➜ **BILDSCHIRMSPERRE** Die Bildschirmsperre ist nur aktivierbar, wenn zuvor das Gerätekennwort gesetzt wurde. Das Einstellen der Bildschirmsperre bietet im Verlustfall oder bei Diebstahl des Smartphones einen ersten Schutz vor unberechtigtem Zugriff auf die gespeicherten Daten eines Gerätes.

➜ **VERSCHLÜSSELUNG** Die Verschlüsselung ist nur aktivierbar, wenn zuvor das Gerätekennwort gesetzt wurde. Sobald sie aktiviert wird, werden alle Daten auf dem Gerät verschlüsselt. Darüber hinaus kann der Anwender entscheiden, ob er zusätzlich alle auf der Speicherkarte vorhandenen Daten verschlüsseln möchte. Die Verschlüsselung verhindert unberechtigten Zugriff auf die gespeicherten Daten, wenn das Gerät über USB an einen Computer angeschlossen oder die Speicherkarte in einen Kartenleser eingelegt wird.

➜ **DIAGNOSEDATEN** Wird die Erhebung von Diagnosedaten deaktiviert, werden keine Diagnosedaten an BlackBerry übertragen. Dadurch entstehen keinerlei Einschränkungen bei der Benutzung des Geräts.

➜ **APPS AUS UNBEKANNTEN QUELLEN** Standardmäßig erlaubt BlackBerry OS die Installation von Apps nur über die BlackBerry App-World. Da diese Apps vor Veröffentlichung von BlackBerry getestet werden, unterliegen sie einem gewissen Qualitätsstandard. Werden Apps aus anderen Quellen installiert, unterliegen diese womöglich keinen entsprechenden Überprüfungsmechanismen und können so Schadsoftware auf das Telefon bringen.

➜ **ORTUNGSDIENST** Über die Funktion Standortbestimmungsdienste werden bei BlackBerry OS die Ortungsdienste aktiviert. Dabei hat der Anwender die Wahl, ob das Telefon anonyme Systeminformationen bei der Nutzung von Ortungsdiensten an BlackBerry übertragen darf. Unabhängig davon kann er entscheiden, ob er standortbezogene Werbung bekommen möchte. Der Anwender kann die Ortungsdienste auch global abschalten. Dies kann die Funktionalität einzelner Anwendungen jedoch beeinflussen, z.B. Navigations-Apps.

➜ **BERECHTIGUNGEN VON APPS** Eine regelmäßige Prüfung der Berechtigungen durch den Anwender stellt sicher, dass Apps nur die Berechtigungen erhalten, die sie für ihre Ausführung benötigen. In diesen Einstellungen können den installierten Apps auch bereits erteilte Zugriffsrechte wieder entzogen werden.

➜ **SPRACHEINGABE** Bei der Verwendung der Spracheingabe sendet BlackBerry OS Daten an die BlackBerry-Server, um die Anfragen des Nutzers bearbeiten zu können. Dies gilt auch für sensible Informationen, die auf diese Weise in das Gerät eingegeben werden.

8.3 Hinweise für iOS-Nutzer

➜ **BILDSCHIRMSPERRE** Das Einstellen der Bildschirmsperre bietet im Verlustfall oder bei Diebstahl des Smartphones einen ersten Schutz vor unberechtigtem Zugriff auf die gespeicherten Daten eines Gerätes.

➜ **SYNCHRONISIERUNG** Apple bietet mit iCloud viele Synchronisierungsoptionen, die einzeln aktiviert bzw. deaktiviert werden können. Bei der Synchronisierung werden die Daten des Anwenders auf Server von Apple übertragen und dort gespeichert. Der Benutzer kann entscheiden, welche Daten er nicht auf fremde Server übertragen und dort speichern möchte.

➜ **INTERESSENBEZOGENE ANZEIGEN** iOS bietet Nutzern die Option, interessenbezogene Werbung zu deaktivieren.

➜ **NUTZUNGS- UND DIAGNOSEDATEN** iOS bietet Nutzern die Option, das Senden von Nutzungs- und Diagnosedaten zu unterlassen. Dadurch entstehen keinerlei Einschränkungen bei der Benutzung des Geräts.

➜ **SPRACHEINGABE** Spracheingaben werden von Apple erfasst, in Text umgewandelt und dürfen von Apple zur Verbesserung des Spracheingabedienstes genutzt werden. Dies gilt auch für sensible Informationen, die auf diese Weise in das Gerät eingegeben werden.

➜ **ORTUNGSDIENSTE** Ortungsdienste können auf iOS sehr differenziert aktiviert bzw. deaktiviert werden. So können sie z.B. separat für Werbung deaktiviert werden, ohne auf die Möglichkeit zur Navigation verzichten zu müssen. Sobald Ortungsdienste aktiviert werden, sind standardmäßig alle Optionen aktiviert. Aktiviert der Nutzer die Statusanzeige für Ortungsdienste, kann er direkt in der Statusleiste des Smartphones sehen, wenn Standortdaten erhoben werden.

➜ **BERECHTIGUNGEN VON APPS** Eine regelmäßige Prüfung der Berechtigungen durch den Anwender stellt sicher, dass Apps nur die Berechtigungen erhalten, die sie für ihre Ausführung benötigen. In diesen Einstellungen können den installierten Apps auch bereits erteilte Zugriffsrechte wieder entzogen werden.

8.4 Hinweise für Windows-Phone-Nutzer

➜ **BILDSCHIRMSPERRE** Das Einstellen der Bildschirmsperre bietet im Verlustfall oder bei Diebstahl des Smartphones einen ersten Schutz vor unberechtigtem Zugriff auf die gespeicherten Daten eines Gerätes.

➜ **MINIMALE EINSTELLUNGEN** Windows Phone sieht bei der Aktivierung sogenannter *Handyberichte* weitreichende Zugriffe auf die Daten eines Nutzers vor. Da dies sogar Snapshots des Arbeitsspeichers

beinhalten kann, sind selbst verschlüsselte Daten nicht vollständig vor dieser Art des Diagnoseverfahrens geschützt. Die Aktivierung erfolgt bei der Einrichtung des Endgerätes, wenn die *empfohlenen Einstellungen* ausgewählt werden. Die Übertragung von Handyberichten an Microsoft kann vom Nutzer deaktiviert werden.

➜ **ORTUNGSDIENSTE** Der Nutzer kann Standortdaten nur global aktivieren oder deaktivieren. Dies ermöglicht eine gewisse Kontrolle, der Nutzer kann z.B. Standortdaten nur im Bedarfsfall einschalten, etwa zur Verwendung einer Navigations-App.

➜ **MICROSOFT-KONTO** Die Verknüpfung des Endgerätes mit einem Microsoft-Konto führt zur Synchronisation von Terminen und Kontakten, die auf dem Gerät gespeichert sind. Eine Deaktivierung dieser Funktion ist nicht möglich.

➜ **BERECHTIGUNGEN VON APPS** Nutzer eines Windows Phones können Berechtigungen einer App im Windows Phone Store nachlesen. Eine explizite Aufforderung zur Bestätigung der angeforderten Berechtigungen wird dem Nutzer bei der Installation nicht zwingend präsentiert, die Anzeige einer Aufforderung obliegt der jeweiligen App.

➜ **SICHERUNG VON DATEN** Windows Phone bietet verschiedene Sicherungsmechanismen an, um Anwendungsliste und Einstellungen, SMS, Fotos und Videos auf den Servern von Microsoft zu speichern, standardmäßig sind diese Sicherungen nicht aktiviert. Dies setzt die Verknüpfung des Endgerätes mit einem Microsoft-Account voraus. Nach Aktivierung können die aufgeführten Sicherungsmechanismen deaktiviert werden.

9. Fazit und Ausblick

Die Studie zeigt, welche Vielzahl privater Daten auf einem Smartphone vorhanden sind und wie die einzelnen Betriebssysteme mit diesen umgehen. Bei der Untersuchung des Einrichtungsvorgangs stellte sich heraus, dass die Betriebssysteme bereits Netzwerkverbindungen mit verschiedenen Servern im Internet herstellen, bevor der Anwender persönliche Informationen auf das Smartphone eingegeben oder geladen hat. Der Zweck einiger Verbindungen lässt sich nachvollziehen, so werden manche zur Bereitstellung von Funktionalitäten wie beispielsweise Push-Benachrichtigungen oder dem Abgleich der Uhrzeit benötigt. Die Anzahl der in den Untersuchungen festgestellten intransparenten Verbindungen – bereits direkt nach dem Start und vor jeder Nutzerinteraktion – ist dennoch erstaunlich. Erfreulich ist, dass viele der Verbindungen verschlüsselt sind und die dabei übertragenen Daten so beim Transport abgesichert sind. Allerdings blieb dadurch ein potenziell unerwünschter Datenabfluss über diese Verbindungen auch vor den Untersuchungen, die im Rahmen dieser Studie durchgeführt worden sind, verborgen.

Mit steigendem Nutzungsumfang und Personalisierung des Geräts wird eine Vielzahl an Daten erhoben und gespeichert. Insbesondere die beiden Basisdienste Ortungsdienste und Sprachsteuerung dienen den Herstellern auch als Datenquellen, worüber ein Nutzer formell in den Nutzungsbedingungen aufgeklärt wird. Bei den Ortungsdiensten werden beispielsweise WLANs und Mobilfunkantennen kartografiert und an den Hersteller weitergeleitet, während bei der Sprachsteuerung Tonaufnahmen und Metainformationen weitergeleitet werden. Nutzungs- und Diagnosedaten stellen eine weitere wertvolle Datenquelle für die Hersteller dar.

In den Datenschutzbestimmungen erhält der Nutzer grundsätzliche Informationen darüber, welche Daten von den Betriebssystemen erhoben werden und welche Rechte der Nutzer dem Hersteller in Bezug auf diese Daten einräumt. Dies schließt in der Regel die Nutzung der Daten zur Bereitstellung und der Verbesserung der genutzten Dienste ein, ebenso die Weitergabe der Daten an Partner. Insgesamt enthalten die Bestimmungen oft einen gewissen Interpretationsspielraum, sowohl dabei, welche Daten wie lange genau gespeichert werden, als auch, wofür diese genutzt werden dürfen.

Die meisten Betriebssysteme ermöglichen eine Datensynchronisierung mit Cloud-Diensten des Herstellers. Welche Daten dabei synchronisiert werden können, unterscheidet sich von Betriebssystem zu Betriebssystem. Windows Phone synchronisiert die Kontakte seiner Nutzer automatisch, ohne die Möglichkeit, dies zu deaktivieren, sobald ein Microsoft-Konto mit dem Windows Phone verknüpft wurde.

Zum Ökosystem eines jeden Betriebssystems gehört ein Vertriebskanal für Apps, der es ermöglicht, sie auf dem Telefon zu installieren. Diese App-Markets versuchen, eine gewisse Qualität sicherzustellen. Jeder Hersteller veröffentlicht Kriterien, die von den Entwicklern für eine Veröffentlichung eingehalten werden müssen. Deren Einhaltung wird beim Veröffentlichungsprozess des App-Markets überprüft. Fällt eine solche Untersuchung negativ aus, wird die App nicht publiziert. Dies umfasst unter anderem die korrekte Verwendung von Programmierschnittstellen, aber auch inhaltliche Bewertungen, z.B. zur Vermeidung von anstößigen Inhalten.

Die bestehenden Regularien und Prüfungsverfahren der App-Markets bieten einen gewissen, aber mitnichten vollständigen Schutz gegen Missbrauchsmöglichkeiten durch Apps. Mit der Installation und Nutzung von Drittanbieter-Apps verlässt der Nutzer den Raum der Datenschutzbestimmungen des Herstellers und vertraut sich denen des Drittanbieters an. Der Zugriff auf die privaten Daten des Nutzers durch eine App ist oft bedingt durch die angebotene Funktionalität, kann aber auch ohne eigentliche Relevanz für den angebotenen Dienst verlangt werden. Drittanbieter-Apps verwerten Daten der Nutzer oft für kommerzielle Zwecke. Hier ist eine Sensibilisierung des Anwenders wichtig, um

ihm eine bewusste Entscheidung der Erteilung oder der Verweigerung einer Zugriffsberechtigung auf bestimmte Daten zu ermöglichen.

Das Sicherheitsmodell eines Betriebssystems ist verantwortlich dafür, dass die Daten des Nutzers vor unberechtigtem Zugriff durch Drittanbieter-Apps geschützt werden. Die eingesetzten Modelle unterscheiden sich zum Teil erheblich und wurden unter verschiedenen Aspekten, wie z.B. dem Umfang der geschützten Daten oder dem Zeitpunkt der Zugriffserlaubnis, genauer betrachtet. Besonders relevant ist dabei der Aspekt der Benutzbarkeit, der allerdings stark durch die anderen beeinflusst wird. Je leichter benutzbar ein Sicherheitsmodell für den Nutzer ist, desto einfacher fällt es ihm, bewusst Entscheidungen zu fällen, ob der Zugriff auf private Daten gerechtfertigt ist oder nicht.

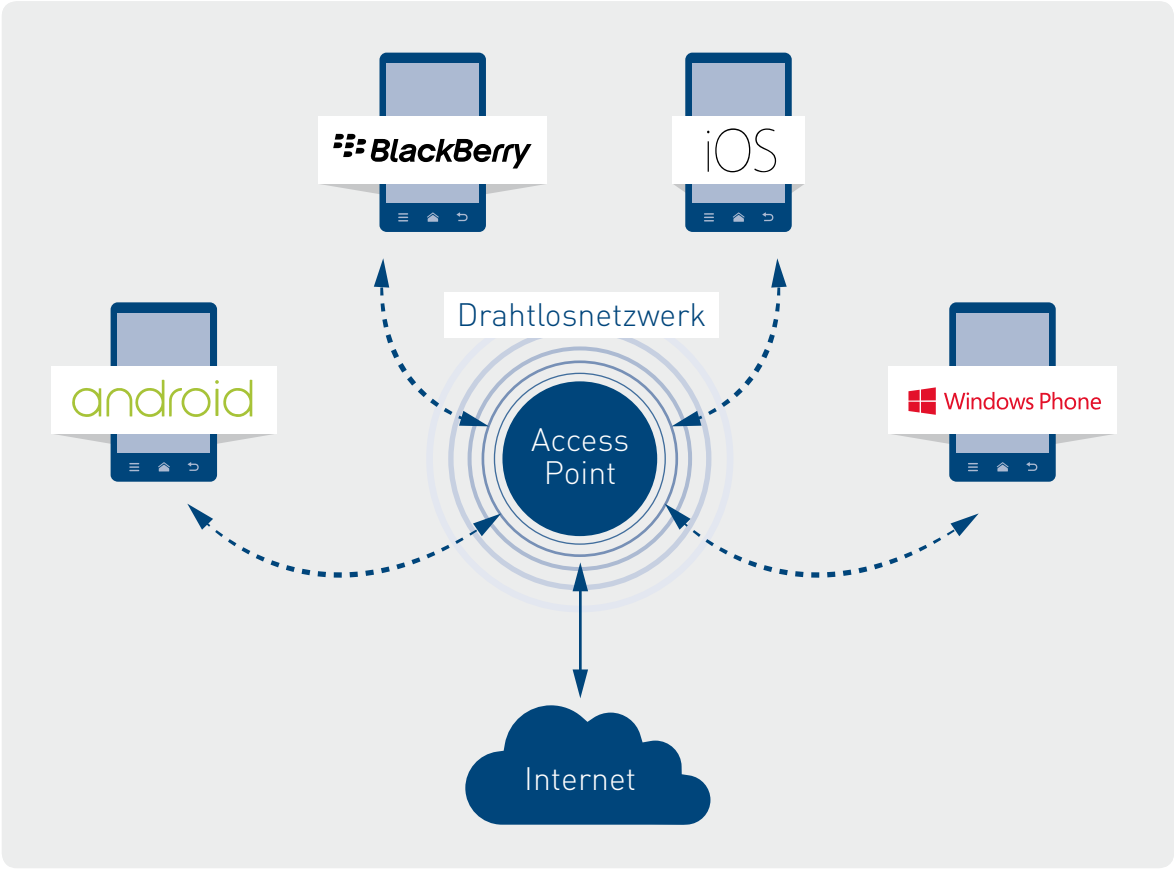
Die Sensibilisierung der Anwender sowie die Darstellung von Implikationen der Datenübertragung an die jeweiligen Betriebssystemhersteller ist umso wichtiger, als dass einige der Betriebssysteme nicht nur auf Smartphones eingesetzt werden, sondern sich bereits auf weiteren Gegenständen unseres täglichen Lebens befinden: Android kommt beispielsweise auf der Datenbrille von Google (Glass) zum Einsatz oder wird auf vielen Set-Top-Boxen eingesetzt, die an Fernseher angeschlossen werden. Auch Apple bietet eine auf iOS basierende Set-Top-Box (Apple TV) an und unternimmt nun Anstrengungen, iOS auch in Autos zum Einsatz zu bringen. Die hier aufgezeigten Zusammenhänge zwischen Funktionalität und Informationsfreigabe und -nutzung sind daher nicht nur für die Nutzung eines Smartphones wichtig, sondern künftig auch bei der Verwaltung privater Daten auf Datenbrillen, im Auto und bei der Nutzung unterschiedlichster App-Angebote auf dem heimischen Fernseher.

A. Anhang

A.1 Aufbau und Vorgehen

Die praktischen Untersuchungen in Kapitel 5.1.2 und Kapitel 7.4 wurden mithilfe der in Abbildung A.1 dargestellten Testumgebung im Labor durchgeführt.

Abbildung A.1: Aufbau der Testumgebung



Die vier Smartphones wurden an einem eigens für die Untersuchung eingerichteten WPA2-gesicherten (verschlüsselten) Drahtlosnetzwerk angemeldet. Der Access Point wird durch einen Linux-Server realisiert, der mit dem Internet verbunden ist und den Datenverkehr der einzelnen Smartphones ins Internet routet. An dieser Stelle besteht die Möglichkeit, den Netzwerkverkehr aufzuzeichnen und im Anschluss daran mit Blick auf die durchgeführten Datenübertragungen zu untersuchen.

Für die Tests in Kapitel 5.1.2 wurden die Telefone auf Werkseinstellungen zurückgesetzt. Die Telefone sind dann bereit für die erste Einrichtung durch den Nutzer. Ab diesem Zeitpunkt wurde der Netzwerkverkehr mitgeschnitten, sodass alle Netzwerkverbindungen ins Internet beim Einrichten des Telefons erkannt wurden. Nach der Einrichtung wurde der Netzwerkverkehr der Telefone ohne weitere Nutzerinteraktion noch mehrere Stunden weiter überwacht.

Für die Tests in Kapitel 7.4 wurde auf den Telefonen nach der ersten Einrichtung ein Kundenkonto eingerichtet und das Spiel *Angry Birds* im jeweiligen App-Market gekauft. Der Netzwerkverkehr wurde ab dem Starten der App mitgeschnitten und für die Dauer einer durchschnittlichen Nutzerinteraktion aufgezeichnet.

Literaturverzeichnis

[1] Android Developers. I think I found a security flaw. How do I report it? https://developer.android.com/guide/faq/security.html#issue. Letzter Zugriff am 31.07.2014.

[2] Apple. Apple-Datenschutzrichtlinie. http://www.apple.com/legal/privacy/de-ww/. Letzter Zugriff am 31.07.2014.

[3] Apple. Apple-Nutzungsbedingungen iOS7. http://images.apple.com/legal/sla/docs/iOS7.pdf. Letzter Zugriff am 31.07.2014.

[4] Apple. App Store Review Guidelines. https://developer.apple.com/appstore/resources/approval/guidelines.html, 2013. Letzter Zugriff am 31.07.2014.

[5] Apple. iOS Security. http://images.apple.com/ipad/business/docs/iOS_Security_Feb14.pdf, February 2014. Letzter Zugriff am 31.07.2014.

[6] BlackBerry. BlackBerry-Lösungslizenzvereinbarung. http://de.blackberry.com/legal/blackberry-solution-licenseagreement.html. Letzter Zugriff am 31.07.2014.

[7] BlackBerry. BlackBerry World Vetting Criteria.

[8] BlackBerry. Datenschutzrichtlinie. http://de.blackberry.com/legal/privacy-policy.html. Letzter Zugriff am 31.07.2014.

[9] BlackBerry. Rechtliche Hinweise. http://de.blackberry.com/legal.html. Letzter Zugriff am 31.07.2014.

[10] Glenn Block, Pablo Cibraro, Pedro Felix, Howard Dierking, and Darrel Miller. Designing Evolvable Web APIs with ASP. NET. O'Reilly Media, Inc., 2014.

[11] Dan Goodin. Stealthy technique fingerprints smartphones by measuring users' movements. http://arstechnica.com/security/2013/10/stealthy-technique-fingerprintssmartphones-by-measuring-users-movements/. Letzter Zugriff am 31.07.2014.

[12] Google. Datenschutzbestimmungen. http://www.google.com/intl/de/policies/privacy/.

[13] Google. Report malicious or inappropriate apps. https://support.google.com/googleplay/answer/2479847?hl=en. Letzter Zugriff am 31.07.2014.

[14] Google Play. App-Berechtigungen prüfen. https://support.google.com/googleplay/answer/6014972?hl=de. Letzter Zugriff am 31.07.2014.

[15] Hiroshi Lockheimer. Android and Security. http://googlemobile.blogspot.de/2012/02/android-and-security.html, February 2012. Letzter Zugriff am 31.07.2014.

[16] Kantar Worldpanel. Smartphone OS market share. http://www.kantarworldpanel.com/smartphone-os-market-share/. Letzter Zugriff am 31.07.2014.

[17] Kaspersky. Kaspersky Security Bulletin 2013. http://media.kaspersky.com/pdf/KSB_2013_EN.pdf, 2013. Letzter Zugriff am 31.07.2014.

[18] Jennifer R Kwapisz, Gary M Weiss, and Samuel A Moore. Activity recognition using cell phone accelerometers. ACM SigKDD Explorations Newsletter, 12 (2): 74–82, 2011.

[19] Marco Tabini. How Apple is improving mobile app security. http://www.macworld.com/article/2047567/howapple-is-improving-mobile-app-security.html, September 2013. Letzter Zugriff am 31.07.2014.

[20] Microsoft. Datenschutzbestimmungen. http://www.windowsphone.com/de-de/legal/wp8/windows-phoneprivacy-statement.

[21] Nick Arnott. What Apples 'Limit Add-Tracking' Means to Users. http://www.doubleencore.com/2013/04/what-apples-limitad-tracking-feature-actually-means-to-users/. Letzter Zugriff am 31.07.2014.

[22] J Oberheide and C Miller. Dissecting the android bouncer. SummerCon 2012, New York, 2012.

Über das Fraunhofer AISEC

Das Fraunhofer AISEC ist eine der international führenden Einrichtungen für angewandte Forschung im Bereich IT-Sicherheit. Mehr als 80 hoch qualifizierte Mitarbeiterinnen und Mitarbeiter arbeiten an maßgeschneiderten Sicherheitskonzepten und -lösungen für Wirtschaftsunternehmen und den öffentlichen Sektor. Dazu zählen Lösungen für eine höhere Datensicherheit sowie für einen wirksamen Schutz vor Cyberkriminalität wie Wirtschaftsspionage und Sabotageangriffe. Das Kompetenzspektrum erstreckt sich von Embedded Security über Automotive, Network und Smart Grid Security bis hin zum Schutz vor Produktpiraterie und Industrial Security sowie die Absicherung von Cloud-Diensten. Zudem bietet das Fraunhofer AISEC in seinen modernen Testlaboren die Möglichkeit zur Evaluation der Sicherheit von vernetzten und eingebetteten Systemen, von Hard- und Softwareprodukten sowie von webbasierten Diensten und Cloud-Angeboten.

Zu den Kunden des Fraunhofer AISEC gehören Hersteller, Zulieferer und Anwender aus den Bereichen der Chipkartensysteme (u.a. Infineon Technologies, Giesecke & Devrient), Telekommunikation (u.a. Deutsche Telekom), dem Automobilbau (u.a. BMW) und deren Zulieferindustrie sowie Logistik und Luftfahrt, Maschinenbau und Automatisierungstechnik, dem Gesundheitswesen, der Software-Industrie wie auch dem öffentlichen Sektor.

Weitere Informationen unter www.aisec.fraunhofer.de.

Über DIVSI

Die Durchdringung von Staat und Gesellschaft mit IT nimmt immer weiter zu. In vielen Bereichen des täglichen Lebens ist das Internet heute nahezu unverzichtbar. Es wird daher künftig entscheidend sein, das Vertrauen der Menschen in das Internet zu fördern und zu sichern. Es geht darum, eine zeitgemäße Technologie sicher einsetzen zu können. Dabei wollen wir als Institut maßgeblich mithelfen.

Das Deutsche Institut für Vertrauen und Sicherheit im Internet (DIVSI) ...

- versteht sich als Forum, das einen offenen und transparenten Dialog zu mehr Vertrauen und Sicherheit im Internet gestaltet und mit neuen Aspekten belebt.
- fördert den interdisziplinären Dialog und die Vernetzung zwischen Wissenschaft, Wirtschaft, Gesellschaft und Politik.
- unterstützt Wissenschaft und Forschung und will so mithelfen, potenzielle Risiken bei der elektronischen Kommunikation und Transaktion zu untersuchen und zu analysieren.
- will durch Aufklärungsarbeit für eine Sensibilisierung auf Seiten der Nutzer zur Steigerung von Vertrauen und Sicherheit im Internet sorgen.

Das Deutsche Institut für Vertrauen und Sicherheit im Internet ist eine gemeinnützige Gesellschaft der Deutsche Post AG.

DIVSI-Kernbegriffe

Vertrauen ist eine wichtige Triebfeder menschlichen Handelns. Das gilt im alltäglichen Leben ebenso wie für spezielle Aktivitäten im Internet. Konkret kann Vertrauen dabei zweierlei bedeuten: Vertrauen in eine Sache oder Vertrauen in eine Person. Neben der Fähigkeit, mit etwas vertraut zu sein, bringt der Begriff also auch die menschliche Empfindung zum Ausdruck, Vertrauen zu haben. Beides ist entscheidend dafür, wie wir das Internet nutzen. Aus diesem Grund ist Vertrauen für DIVSI ein Kernbegriff im Diskurs über Chancen und Risiken des Internets.

Sicherheit ist ein Grundbedürfnis aller Menschen. In unterschiedlicher Ausprägung bestimmt es unser individuelles Handeln und Nutzungsverhalten. Wie sicher die Nutzung des Internets tatsächlich ist, können die wenigsten Menschen beurteilen. Das Sicherheitsempfinden einzelner User hängt zum einen von der Technologie und zum anderen von einem Konsens über sicheres Agieren im Internet ab. Dem Thema Datenschutz kommt dabei eine besondere Bedeutung zu. An einem bestimmten Punkt kann ein „verordnetes" Maß an Sicherheit zur Einschränkung individueller Freiheiten führen. Eine freie und demokratische Gesellschaft muss daher stets die Balance zwischen Sicherheit und Freiheit wahren.

DIVSI Studien

Braucht Deutschland einen Digitalen Kodex? (2014)

Mit dem Projekt „Braucht Deutschland einen Digitalen Kodex?“ lotet DIVSI aus, ob ein Digitaler Kodex ein geeignetes Mittel ist, verbindliche Regeln im Internet auszuhandeln und durchzusetzen. Der Projektbericht steuert nicht nur zu diesem Gedanken Anregungen bei. Er bietet darüber hinaus generelle Anstöße, über die nachzudenken sicherlich lohnt.

DIVSI Studie zu Bereichen und Formen der Beteiligung im Internet (2014)

Das DIVSI-Forschungsprogramm „Beteiligung im Netz“ leistet auf einer breiten theoretischen und empirischen Basis einen Beitrag zum öffentlichen Verständnis der Beteiligungschancen des Internets – und ihrer Voraussetzungen. Die Studie präsentiert einen ersten Schritt in diesem Vorhaben und verschafft einen Überblick über den heutigen Stand der Forschung

DIVSI U25-Studie (2014)

Die DIVSI U25-Studie liefert erstmals fundierte Antworten auf Fragen, die das Verhalten der nachwachsenden Generation im Hinblick auf das Netz betreffen. Über die Nutzungsformen hinaus werden auch die Denk- und Handlungslogiken sowie der lebensweltliche Hintergrund untersucht.

DIVSI Studie zu Freiheit versus Regulierung im Internet (2013)

Wie sicher fühlen sich die Deutschen im Internet? Wie viel Freiheit und Selbstbestimmung wollen sie? Nach wie viel Regulierung wird verlangt? Die Studie zeigt ein detailliertes Bild des Nutzungsverhaltens der Deutschen im Internet und ihrer Wahrnehmung von Chancen und Risiken.

Entscheider-Studie zu Vertrauen und Sicherheit im Internet (2013)

Wie denken Entscheider über das Internet? Welchen Akteuren schreiben sie welche Verantwortung und welche Einflussmöglichkeiten zu? Was sagen sie zu Sicherheits- und Freiheitsbedürfnissen? Die Studie verdeutlicht erstmals, wie diejenigen über das Internet denken, die wesentlich die Spielregeln gestalten und Meinungsbilder prägen.

Meinungsführer-Studie „Wer gestaltet das Internet?“ (2012)

Wie gut kennen sich Meinungsführer im Netz aus? Wie schätzen sie ihre Einflussmöglichkeiten ein? Welche Chancen, Konfliktfelder und Risiken erwachsen daraus? In persönlichen Gesprächen wurden führende Repräsentanten aus Politik, Wirtschaft, Verwaltung, Wissenschaft und Verbänden interviewt.

Milieu-Studie zu Vertrauen und Sicherheit im Internet (2012) + Aktualisierung (2013)

Die Milieu-Studie differenziert erstmals unterschiedliche Zugangsweisen zum Thema Sicherheit und Datenschutz im Internet in Deutschland basierend auf einer bevölkerungsrepräsentativen Typologie.

www.divsi.de