Technical Report 72

Analyse der Sicherheit geschäftsbezogener Daten auf Android-Endgeräten bei sowohl privater als auch geschäftlicher Nutzung

Daniela Zimmermann

TZI, Universität Bremen

TZI-Bericht Nr. 72
2014

TZI-Berichte

Herausgeber:
Technologie-Zentrum Informatik und Informationstechnik
Universität Bremen
Am Fallturm 1
28359 Bremen
Telefon: +49 421 218 94090
Fax: +49 421 218 94095
E-Mail: hq@tzi.de
http://www.tzi.de

ISSN 1613-3773

Eigenständigkeitserklärung

Ich versichere hiermit, dass die von mir vorgelegte Bachelorarbeit selbstständig und ohne fremde Hilfe verfasst wurde. Alle Stellen, die wörtlich oder sinngemäß aus veröffentlichten oder nicht veröffentlichten Quellen entnommen sind, wurden als solche kenntlich gemacht. Sämtliche Quellen und Hilfsmittel, die ich für die Arbeit benutzt habe, sind angegeben. Die Arbeit hat mit gleichem Inhalt bzw. in wesentlichen Teilen noch keiner anderen Prüfungsbehörde vorgelegen.

Kurzfassung

Der Inhalt dieser Bachelorarbeit ist die Untersuchung der Sicherheit geschäftsbezogener Daten auf Android-Endgeräten, wenn diese privat und geschäftlich eingesetzt werden. Dafür wird das Betriebssystem *Android* auf seine vorhandenen Sicherheitsmechanismen untersucht und anhand bestimmter Sicherheitsmerkmale mit den beiden alternativen mobilen Betriebssystemen *iOS* und *Windows Phone* verglichen. Auf diese Weise soll unter anderem die Einsatztauglichkeit von Android im Rahmen von *BYOD* festgestellt werden. Des Weiteren werden für die Umsetzung von *BYOD* Anforderungen aufgestellt, die zusammen mit den Herausforderungen von *BYOD* und Android für die Bewertung beispielhafter Lösungsansätze herangezogen werden.

Gegen Ende der Arbeit werden abschließend die gesammelten Erkenntnisse zusammengefasst und die Vor- und Nachteile die Android im Rahmen von *BYOD* bietet gegenübergestellt.

Inhaltsverzeichnis

1. Einleitung

Dieses Kapitel geht einleitend auf die Motivation sowie die Zielsetzung und Abgrenzung dieser Arbeit ein. Ebenfalls wird ein Überblick der fünf Hauptkapitel gegeben, bei dem die Vorgehensweisen der einzelnen Kapitel beschrieben werden.

1.1. Motivation

Die Anzahl der Smartphones steigt von Jahr zu Jahr. Dies zeigt sich beispielsweise daran, dass die Milliardengrenze nach Angaben von *Strategy Analytics*[1] bereits überschritten wurde. Dass das Smartphone zum Alltag vieler Menschen gehört, lässt sich nicht mehr abstreiten und mit einem Marktanteil von über 70% in Europa gehört das mobile Betriebssystem *Android* zu dem populärsten unter den Betriebssystemen für mobile Geräte. Grund für diese weite Verbreitung ist womöglich die Tatsache, dass dieses Betriebssystem auf einer Vielzahl von Smartphone-Modellen unterschiedlicher Anbieter läuft. So kann ein potentieller Käufer ein für seine Bedürfnisse entsprechendes Android-Smartphone in einer Menge von Einsteigermodellen bis hin zu High-End-Smartphones wählen [1, 2].

Durch das große Angebot verschiedener Modelle und Marken sowie der starken Verbreitung von Android-Smartphones und Tablet-PCs spielt dieses mobile Betriebssystem bei dem Konzept *Bring Your Own Device* (BYOD) eine immer bedeutendere Rolle. Wie bereits bei der geschäftlichen Nutzung privater Notebooks, entstehen auch in Bezug auf Smartphones und Tablet-PCs für einen Betrieb durch dieses Konzept neue Risikopotentiale. Wird ein privates Smartphone beziehungsweise Tablet-PC für den betrieblichen Gebrauch genutzt, werden nicht mehr nur die eigenen privaten Daten durch eventuelle sicherheitskritische Anwendungen oder andere Bedrohungen gefährdet, sondern gleichermaßen jegliche Geschäftsdaten auf die beispielsweise über das Gerät zugegriffen wird. Dadurch nimmt auch die Relevanz der Sicherheit des Betriebssystems zu. Bereits auf dieser Ebene sollten die Möglichkeiten für einen Angriff minimiert werden, um auf diese Weise ein gewisses Maß an Sicherheit voraussetzen zu können. Gerade in Zeiten der NSA-Skandale ist daher der Schutz von unternehmensbezogenen Daten von höchster Priorität, denn das Risiko einer Wirtschaftsspionage ist trotz der Entwarnung des Verfassungsschutz-Chefs Maaßen erschreckend hoch [3].

[1] Globales und unabhängiges Forschungs- und Beratungsunternehmen mit Hauptsitz in Boston, USA.

1.2. Zielsetzung und Abgrenzung

Das Ziel dieser Bachelorarbeit ist es im Rahmen einer Literaturrecherche und -analyse die Sicherheit von Daten, insbesondere von vertraulichen und geschäftsbezogenen, auf Android-Geräten zu untersuchen, wenn diese sowohl privat als auch geschäftlich genutzt werden. Dabei sollen bereits bestehende Sicherheitskonzepte wie die der Datenseparierung betrachtet werden sowie spezielle Sicherheits-Apps und Custom-ROMs, die die Sicherheit Androids steigern sollen. Bei dieser Betrachtung soll analysiert werden, inwieweit die Sicherheit gewährleistet wird und ob das sogenannte*„Rooten“* im Hinblick auf die Sicherheit förderlich ist oder eher ein Risiko darstellt. Ferner soll die allgemeine Architektur von Android auf ihre Sicherheitsmechanismen untersucht und dabei explizit mit denen anderer mobiler Betriebssysteme verglichen werden. Auf diese Weise soll das Maß der Sicherheit qualitativ bewertet und überprüft werden, ob gegebene Sicherheitslösungen bestehende Schwachstellen abdecken.

Des Weiteren sollen frühere Probleme des „BYOD“-Konzeptes im Hinblick auf die duale Nutzung von Notebooks betrachtet werden, um mögliche Gemeinsamkeiten zu finden und gegebenenfalls damalige Lösungen bzw. Lösungsansätze für das derzeitige Sicherheitsproblem abzuleiten.

Da das Betriebssystem Android sich im Laufe seines Daseins immer weiter entwickelt hat und derzeit mehrere Versionen auf dem Markt sind, wird für die Untersuchung möglicher Lösungsansätze in Kapitel 4 und auch bei dem Vergleich der Sicherheitsmechanismen der Betriebssysteme von der Android-Version 4.3.x ausgegangen. Jedoch wird in dem späteren Fazit in Kapitel 5 auch berücksichtigt, dass viele Geräte mit älteren Android-Versionen im Umlauf sind. Dabei muss beachtet werden, dass bei ihnen Sicherheitsrisiken, die in späteren Versionen nicht mehr anzutreffen sind, dennoch bestehen.

1.3. Vorgehensweise

Diese Bachelorarbeit lässt sich in fünf Kapitel einteilen, die wie folgt definiert sind:

1. Einleitung
2. Grundlagen
3. Sicherheit auf mobilen Betriebssystemen
4. Android im betrieblichen Umfeld
5. Fazit

Zu Beginn wird in der Einleitung die Motivation und Zielsetzung erläutert. Auch die Vorgehensweise, die einen Einblick in den Aufbau der Arbeit bietet, ist in diesem Abschnitt enthalten.

In Kapitel zwei wird anschließend auf die Grundlagen der Informationssicherheit eingegangen und das Konzept *BYOD* erläutert.

In dem Abschnitt „Sicherheit auf mobilen Betriebssystemen“ werden allgemeine, potentielle Gefahren untersucht und beschrieben, welche Mechanismen die Sicherheit bei mobilen Betriebssystemen steigern können und die zuvor genannten Gefahren abdecken. Außerdem wird Android auf seine Sicherheit untersucht. Dabei wird zunächst das sogenannte *Android Sicherheitsprogramm* erläutert sowie dessen Sicherheitsarchitektur. Gleichermaßen werden zusätzliche Sicherheitsmechanismen und -werkzeuge für Android beschrieben. Dabei findet eine Unterscheidung der von Android selbst zur Verfügung gestellten Mechanismen und der von Drittanbietern angebotenen Werkzeuge statt. Ebenfalls wird an dieser Stelle das sogenannte *Rooten* des Geräts kritisch betrachtet, da dieses für bestimmte Werkzeuge vorausgesetzt wird. In diesem Zusammenhang soll analysiert werden, ob *Rooten* und *Custom-ROMs* sich positiv oder negativ auf die Sicherheit des Systems auswirken. Auch die Entwicklung von Android im Zusammenhang mit dessen Sicherheit wird innerhalb des dritten Kapitels kurz dargestellt. Dabei soll insbesondere verdeutlicht werden, dass gerade in den späteren Versionen viele Sicherheitsverbesserungen eingebaut wurden und ältere Versionen, die ebenfalls bei vielen Geräten stark vertreten sind, über ein weniger ausgereiftes Sicherheitsmodell verfügen. Der nächste Abschnitt dieses Kapitels beschäftigt sich mit dem Sicherheitsstand anderer mobiler Betriebssysteme. An dieser Stelle soll ein grober Überblick über die alternativen mobilen Betriebssysteme und deren Sicherheitsmechanismen verschafft werden. Ebenso wird ein direkter Vergleich ausgewählter Sicherheitsmechanismen der anderen vorgestellten Betriebssysteme mit denen von Android vorgenommen, um Stärken und Schwächen der Sicherheit in Android hervorzuheben.

Kapitel vier beschäftigt sich mit dem Einsatz von privaten Android-Geräten im betrieblichen Umfeld. Hierbei werden zu Beginn Anforderungen aufgestellt, die für eine sichere betriebliche Nutzung privater Android-Geräte notwendig sind. Diese Anforderungen werden in funktionale und nicht-funktionale unterteilt. Auch werden diverse Herausforderungen dargestellt, die *BYOD*, insbesondere in Verbindung mit Android-Geräten, mit sich bringt. Des Weiteren werden drei vorhandene Lösungsansätze vorgestellt und anschließend mit Hilfe der aufgestellten Anforderungen und unter Berücksichtigung der Herausforderungen bewertet.

Zuletzt wird im Fazit das Konzept der Datenseparierung im Hinblick auf die Steigerung der Sicherheit beurteilt sowie die Anwendungen und Custom-ROMs, die dieses Konzept beinhalten. In diesem Zusammenhang wird außerdem noch einmal auf die Problematik des *„Rootens“* der Android-Geräte eingegangen. Ebenso wird im letzten Kapitel eine Gegenüberstellung der Vor- und Nachteile von Android in Bezug auf die betriebliche Nutzung vorgenommen. Dies soll einen Eindruck der Tauglichkeit des Betriebssystems in einem solchen Umfeld verschaffen.

2. Grundlagen

Da in den späteren Kapiteln ein gewisses Grundverständnis zu den Themen *Informationssicherheit* und *Bring Your Own Device* vorausgesetzt wird, besteht der Inhalt dieses Abschnittes darin, die relevanten und grundlegenden Begrifflichkeiten einleitend zu erklären.

2.1. Informationssicherheit

Die Informationssicherheit beschreibt in erster Linie den Präventivschutz bei informationsverarbeitenden und -lagernden Systemen. Dort sollen die Kernsicherheitsziele *Verfügbarkeit, Integrität* und *Vertraulichkeit* gewährleistet werden. Die Systeme können dabei technischer oder nicht-technischer Art sein. Der Präventivschutz umfasst den Schutz des Systems vor Bedrohungen beziehungsweise Angriffen, um Schäden möglichst zu vermeiden und das Risiko eines Angriffs so gering wie möglich zu halten. Sollte ein Angriff jedoch glücken, ist das Erkennen des Angriffs und die Eingrenzung möglicher Schäden ebenso Teil der Informationssicherheit [4, 5, 6].

Häufig wird der Begriff *IT-Sicherheit* als Synonym für Informationssicherheit verwendet. Dabei stellt die IT-Sicherheit lediglich einen Bereich der Informationssicherheit dar, der speziell den Schutz von IT-Systemen sowie der darin gespeicherten Daten vorsieht [7].

Um einen tieferen Einblick in die Informationssicherheit und ein besseres Verständnis für deren Relevanz in der heutigen Zeit zu bekommen, werden im Folgenden die wichtigsten Grundbegriffe zu diesem Thema genauer erläutert. Dabei werden die *Sicherheitsziele* eines Systems vorgestellt und die Bedeutung von *Schwachstellen, Bedrohungen, Angriffe* und *Angreifer* anhand von Beispielen erklärt. Außerdem wird prinzipiell auf die Arten der Sicherheitsmaßnahmen eingegangen und die Bedeutung der Informationssicherheit für Unternehmen erläutert.

2.1.1. Sicherheitsziele

Bei den Sicherheitszielen der Informationssicherheit handelt es sich um bestimmte Eigenschaften beziehungsweise Anforderungen, die die Vertrauenswürdigkeit und Sicherheit eines informationsverarbeitenden und -lagernden Systems beschreiben. Dabei lauten die drei grundlegenden Sicherheitsziele (vlg. [6, Seite 21]):

- Vertraulichkeit
- Integrität
- Verfügbarkeit

Sie stellen wie bereits erwähnt die Kernsicherheitsziele der Informationssicherheit dar, denen eine besonders große Bedeutung zukommt. Die Vertraulichkeit beschreibt die Verpflichtung, Informationen anderer geheim zu halten (vgl. [6, Seite 22]). Das bedeutet, dass unbefugten Dritten weder der Zugang zu diesen möglich ist, noch dass sie diese unberechtigter Weise einsehen können. Bei der Integrität handelt es sich um die Eigenschaft, dass Daten vor unautorisierten und unbemerkten Veränderungen geschützt werden (vgl. [6, Seite 24]). Dadurch soll die Vollständigkeit und Korrektheit der Informationen gewährleistet werden. Diese Eigenschaft steht in enger Verbindung mit der Eigenschaft *Verfügbarkeit*. Die Verfügbarkeit von Informationen steht für die Zugänglichkeit dieser, ohne die Beeinträchtigung der Funktionalität jeglicher Komponenten oder Dienste (vlg. [6, Seite 26]). So soll es berechtigten Nutzern möglich sein auf die gewünschten Daten zuzugreifen, welche sich dabei in einem integren Zustand befinden [8].

Neben diesen drei Kernsicherheitszielen existieren noch weitere Sicherheitsziele in der Informationssicherheit. Dazu gehört unter anderem die Geheimhaltung von Informationen. Sie beschreibt das Vorgehen, Zugriffe auf Informationen einzuschränken und nur berechtigten Personen den Zugriff zu gewähren (vgl. [6, Seite 22]). Diese Eigenschaft steht zusammen mit der des Datenschutzes in enger Verbindung zur Vertraulichkeit. Der Datenschutz ist dabei das Recht auf den Schutz von persönlichen Daten, der unbefugten Zugriff und allgemein den Missbrauch der Informationen verhindern soll (vgl. [6, Seite 22]). Ein weiteres Sicherheitsziel ist die Authentizität. Sie beschreibt, dass Informationen, die integer und frisch sind, einer bestimmten Identität eindeutig zugeordnet werden können (vgl. [6, Seite24]). Auf diese Weise soll es möglich sein die Echtheit und Glaubwürdigkeit des Objekts beziehungsweise Subjekts zu überprüfen (vgl. [9, Seite 6 f.]). Dieses Sicherheitsziel ist unter anderem relevant für die beiden weiteren Sicherheitsziele *Zurechenbarkeit* und *Verbindlichkeit*. Während die Zurechenbarkeit für die eindeutige Zuordnung einer durchgeführten Handlung zu einem Kommunikationspartner steht, beschreibt die Verbindlichkeit, dass gewisse durchgeführte Handlungen nicht unzulässig abgestritten werden können (vgl. [6, Seite 25]). Dabei stehen die drei zuletzt genannten Sicherheitsziele jedoch im Widerspruch zu dem Sicherheitsziel *Anonymität*. Dieses fordert, dass Handlungen ohne die Preisgabe der Identität durchgeführt werden können (vgl. [6, Seite 23]) [4].

Somit existieren diverse Sicherheitsziele, die die Anforderungen an ein informationsverarbeitendes und -lagerndes System definieren und sich dabei teilweise widersprechen.

2.1.2. Schwachstellen und Verwundbarkeiten

Die Sicherheit eines Systems ist durch dessen Schwachstellen beeinträchtigt. Beispielsweise können durch deren Ausnutzung die Kernsicherheitsziele gefährdet werden. *Claudia Eckert* definiert den Begriff Schwachstelle in ihrem Werk *IT-Sicherheit* wie folgt:

> *„Unter einer Schwachstelle (engl. weakness) verstehen wir eine Schwäche eines Systems oder einen Punkt, an dem das System verwundbar werden kann.“* ([9, Seite 13]).

Das System wird infolgedessen genau dann verwundbar, wenn die Möglichkeit besteht dessen Sicherheitsmaßnahmen über eine Schwachstelle zu umgehen (vgl. [9, Seite 13 f.]). Ist dies der Fall, so wird aus der Schwachstelle eine Verwundbarkeit des Systems. Als Beispiel für eine Schwachstelle kann man sich die Mobilität von Notebooks vorstellen. Ein Unternehmen kann noch so gut gegen das unrechtmäßige Eindringen von Personen geschützt sein, um den Zugriff auf betriebsinterne Daten zu schützen, wenn dessen Mitarbeiter diese Daten auf ihren Firmen-Notebooks heraustragen. Daraus könnte sich dann die Bedrohung eines Diebstahls ergeben. Neben dieser Bedrohung existiert noch eine Vielzahl von weiteren, denen ein System ausgesetzt werden kann. Der nachfolgende Abschnitt befasst sich mit dem Begriff *Bedrohung* und wird einen groben Überblick der Klassifikation möglicher Bedrohungen bieten.

2.1.3. Bedrohungen

Der Begriff *Bedrohung* (engl. *threat*) stellt die Möglichkeit dar, die Schwachstellen beziehungsweise Verwundbarkeiten eines Systems auszunutzen. Dabei können Bedrohungen in verschiedene Klassen zugeordnet werden, bei denen negative Auswirkungen auf die Sicherheitsziele, wie Verfügbarkeit, Vertraulichkeit oder Integrität, die Folge sein können (vgl [9, Seite 15]). In dem Werk *IT-Sicherheit* verweist Claudia Eckert dabei auf die fünf Klassen *höhere Gewalt, organisatorische Mängel, technisches Versagen, Fahrlässigkeit* und *Vorsatz*, die vom Bundesamt für Sicherheit in der Informationstechnik vorgeschlagen werden. Die nachfolgende Abbildung zeigt diese verschiedenen Bedrohungsklassen und Beispiele für die dazugehörigen Bedrohungen.

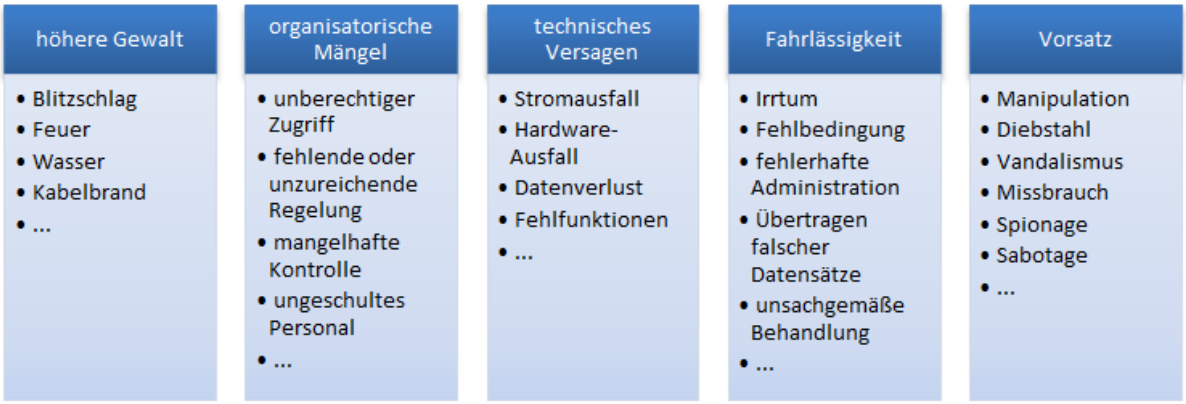

Abbildung 1: Bedrohungsklassifikation[9, 7]

Somit ließe sich die genannte Bedrohung aus Abschnitt 2.1.2 in die Klasse Vorsatz einordnen. Insbesondere in dieser Klasse lassen sich diverse Angriffe feststellen, die von den unterschiedlichsten Angreifertypen durchgeführt werden. Welche verschiedenen Arten von Angriffen und Angreifern dabei vorkommen können, wird in den beiden nachfolgenden Abschnitten beschrieben.

Bevor mit den Angriffstypen in Abschnitt 2.1.4 fortgefahren wird, werden jedoch noch kurz drei spezielle Bedrohungen vorgestellt, auf die in späteren Kapiteln vermehrt verwiesen wird. Gemeint sind *Viren, Würmer* und *Buffer-Overflow-Angriffe*.

Bei den Buffer-Overflow-Angriffen werden Daten in Variablen fester Länge eingelesen oder kopiert, die über den dafür vorgesehenen Speicherbereich (*engl. buffer*) hinaus reichen. Dies kann passieren, wenn keine Längenüberprüfung der Eingaben stattfindet und es zum Überlauf des Speicherbereichs (*Buffer-Overflow*) kommt. Das Ziel bei solchen Angriffen ist zum Beispiel, *„[...] durch einen gezielt konstruierten Eingabestring die auf dem Stack abgelegte Rücksprungadresse des Prozeduraufrufs zu überschreiben“*([9, Seite 47]). Durch das Überschreiben der Rücksprungadresse kann ein Angreifer gegebenenfalls dafür sorgen, dass eingeschleuster Code angesprungen und mit den Berechtigungen des Prozesses ausgeführt wird, der für diese Manipulation genutzt wurde (vgl. [9, Seite 47 f.]).

Diese Art von Angriff machen sich auch die sogenannten *Würmer* zunutze, um in das System des Opfers zu gelangen. Ein Wurm ist dabei ein selbstständiges Programm mit der Fähigkeit sich zu reproduzieren. Je nach Art kann er die Sicherheitsziele *Vertraulichkeit, Integrität* und *Verfügbarkeit* gefährden. So löschte beispielsweise der *ILOVEYOU*-Wurm gezielt Dateien vom lokalen Dateisystems des Opfers und durchsuchte dessen lokale Festplatte nach Passwörtern, welche er daraufhin an seinen Entwickler zu senden versuchte (vgl. [9, Seite 63 ff.]).

Die dritte zu nennende Bedrohung sind die *Viren*. Ein Virus ist dabei vergleichbar mit dem gleichnamigen Begriff aus der Biologie. Dieser ist im Vergleich zum Wurm kein ei-

genständiges Programm und benötigt, wie auch ein echter Virus, einen Wirt für seine Existenz. Er ist lediglich eine Befehlssequenz, die sich in andere Programme einschleust. Bei der Einschleusung spricht man auch von *Reproduktion*, bei der er nach nicht infizierten Programmdateien sucht, um sich zu vervielfältigen und sich somit im System zu verbreiten. Durch eine bestimmte *Viruskennung* in seinem Aufbau prüft er, ob eine Datei bereits von ihm infiziert ist. Diese wird ebenfalls von Viren-Scannern genutzt, um selbiges zu überprüfen. Für diesen Zweck verfügen die Viren-Scanner über eine *Virendatenbank*, die diverse bekannte Virenkennungen beinhaltet und für die Überprüfung des Systems genutzt wird.

2.1.4. Angriffstypen

Bei einem Angriff auf ein System handelt es sich um den Versuch eines unberechtigten Zugriffs auf die dort abgelegten Informationen. Der Versuch kann dabei erfolgreich oder nicht erfolgreich verlaufen, doch ist es in jedem Fall ein Angriff. Es wird zwischen *aktiven* und *passiven Angriffen* unterschieden, wobei passive Angriffe speziell die Vertraulichkeit durch die unautorisierte Informationsbeschaffung gefährden. Diese Informationsbeschaffung kann zum Beispiel durch Lauschangriffe (*sniffen*) vorgenommen werden, bei denen die Kommunikation anderer unberechtigt und unbemerkt durch den Angreifer „mitgehört“ wird. Besonders gefährdet ist dabei die Datenkommunikation in drahtlosen Netzen, weil dort die Kommunikation direkt über die Luftschnittstelle abgefangen werden kann und keine Datenkabel angezapft werden müssen. Bei den aktiven Angriffen ist das Ziel die Integrität der Informationen oder die Verfügbarkeit des Systems zu beeinträchtigen. Besonders bekannt sind in diesem Zusammenhang die sogenannten Denial-of-Service (DoS) und Spoofing-Angriffe. Bei einem DoS-Angriff wird versucht, die Verfügbarkeit eines Systems beziehungsweise eines Dienstes zu beeinträchtigen. Dazu überfluten die Angreifer beispielsweise einen Server mit Anfragen, sodass dieser die Menge der Anfragen nicht mehr bewältigen kann und das System zusammenbricht. Spoofing-Angriffe sind sogenannte Maskierungsangriffe, bei denen der Angreifer eine gefälschte Identität vorgibt. Auf diese Weise ist es ihm zum Beispiel möglich, sich in fremde Kommunikationen einzuschleusen und die Kommunikationsinhalte zu lesen, zu verändern oder sogar nicht weiter zu leiten und sie somit aus dem Informationsfluss verschwinden zu lassen. In dem Fall spricht man auch von einem *man-in-the-middle*-Angriff. Ebenso hat der Angreifer die Möglichkeit durch *E-Mail Address Spoofing* sensible Daten zu erfragen, indem er sich dabei als eine vertrauenswürdige und gegebenenfalls bekannte Person ausgibt [9, Seite 16 f.] [10].

2.1.5. Angreifer

Wie aus den vorigen Abschnitten zu entnehmen ist, gibt es diverse Bedrohungen denen ein System ausgesetzt sein kann. Wer dabei die Angreifer sein können, wird innerhalb dieses Abschnittes genauer erläutert.

Einen besonderen Gefahrenfaktor stellen die Mitarbeiter eines Unternehmens dar. Sie gehören zu dem Angreifertyp *Insider*, der in die drei Bedrohungsklassen *organisatorische Mängel, Fahrlässigkeit* und *Vorsatz* eingeordnet werden kann. Mitarbeiter können Angriffe verursachen, indem sie sich, zum Beispiel aufgrund von Unwissenheit oder Bequemlichkeit, nicht an aufgestellte Sicherheitsrichtlinien halten. Sie können durch Fahrlässigkeit falsche Berechtigungen verteilen und somit die Vertraulichkeit von Informationen gefährden. Genauso können sie auch mit Vorsatz handeln und den Missbrauch oder die unberechtigte Manipulation von Daten vornehmen. Durch sie wird ein hohes Gefahrenpotential ausgestrahlt, gegen das sich das Unternehmen zu schützen wissen muss.

Ein weiterer Angreifertyp sind die sogenannten *Hacker*. Sie sind technisch versierte Angreifer, die ihre Angriffe entwickeln und durchführen, um die Schwachstellen und Verwundbarkeiten von Systemen aufzudecken und der Öffentlichkeit mitzuteilen (vgl. [9, Seite 19]). Im Gegensatz zu dem *Cracker* ist der Anlass seiner Angriffe nicht zu seinem eigenen Vorteil. Vielmehr will er auf die unbekannten und häufig risikoreichen Schwächen von Systemen aufmerksam machen. Besonders häufig sind dabei populäre Systeme und Plattformen im Fokus der Hacker. So kam es beispielsweise auf Mark Zuckerbergs[1] Facebook-Timeline zu einem Post, der eigentlich nicht hätte möglich sein dürfen. Der palästinensische Entwickler *Khalil Shreateh* entdeckte bei Facebook eine Schwachstelle in der Timeline, die er wiederholt an Facebook meldete. Weil auf seine Benachrichtigung nicht reagiert wurde, entschloss Shreateh auf einem anderen Weg auf sich aufmerksam zu machen. Er nutzte die von ihm entdeckte Schwachstelle aus und postete auf der Timeline von Mark Zuckerberg eine Nachricht. Diese Funktionalität ist normalerweise nicht ohne Weiteres gegeben, sondern setzt eine bestehende Freundschaft zwischen den jeweiligen Nutzern voraus. Häufig werden den Entdeckern von Schwachstellen Belohnungen in Form von Preisgeldern übergeben. Da Shreateh allerdings gegen die Bestimmungen von Facebook verstoßen hatte, die besagen, dass gefundene Schwachstellen nicht ausgenutzt werden dürfen, wurde lediglich sein Facebook-Konto vorübergehend gesperrt (siehe [11]).

Wie bereits erwähnt, sind *Cracker* den Hackern sehr ähnlich. Auch sie sind technisch versierte Angreifer, die aber im Gegensatz zu den Hackern ihre Angriffe zu ihrem eigenen Nutzen durchführen oder um Dritten Schaden zuzuführen (vgl. [9, Seite 19]). Aus diesem Grund würden Cracker die von ihnen gefundenen Schwachstellen auch nicht der Öffentlichkeit mitteilen. Um möglichst viel von ihren Angriffen zu profitieren, liegt ihr Fokus

[1] Gründer des Online-Netzwerks Facebook

nicht zwangsläufig auf Systemen, die durch ihre Popularität auffallen. Vielmehr liegt ihr Augenmerk auf jenen, die sich für den Cracker als profitabel erweisen. Weil eine große Popularität jedoch häufig eine gewisse Lukrativität für die Angriffe des Crackers mit sich bringt, handelt es sich bei den Angriffszielen nicht selten um sehr bekannte und stark genutzte Systeme.

Die sogenannten *Skript Kiddies* stellen einen weiteren Angreifertypen in der Informationssicherheit dar. Bei ihnen handelt es sich eher selten um technisch versierte Angreifer, sondern vielmehr um Angreifer die häufig aus Langeweile, Neugier oder Spaß handeln. Skript Kiddies nutzen meist frei verfügbare Exploits, um ihre Angriffe durchzuführen. Exploits sind dabei vorgefertigte Schadprogramme oder Befehlsfolgen, die entwickelt wurden um bestimmte Schwachstellen auszunutzen. Auf diese Weise müssen die Skript Kiddies über keinerlei spezifisches Wissen zu den von ihnen durchgeführten Angriffen verfügen. Weil diese Exploits frei zugänglich sind, kann auf die vorgefundenen Schwachstellen allerdings schnell reagiert werden. Dazu werden Patches bereitgestellt, die diese Schwachstellen schließen und somit das Ausnutzen dieser verhindern sollen [9, Seite 19 f.] [12].

Zu Zeiten der NSA-Spionage-Vorfälle ist ein bestimmter Angreifertyp von besonders großer Bedeutung, nämlich der *professionelle Angreifer*. Dieser kann zum Beispiel in Form von Geheimdiensten vorliegen, die ihre Angriffe hauptsächlich zum Schutz der Bevölkerung ausüben. Diesbezüglich sorgt die NSA in letzter Zeit für große Empörung in Deutschland, aufgrund der Spionage wie beispielsweise bei Internet-Firmen wie Google, Apple und Microsoft, deren Dienste auch von der deutschen Bevölkerung in Anspruch genommen werden (vgl. [14]). Doch soll nicht nur Spionage zum Schutz gegen Terrorismus ausgeübt worden sein. Es bestand sogar der Vorwurf der Wirtschaftsspionage gegen die USA und Großbritannien, welche der Verfassungsschutz-Chef Hans-Georg Maaßen jedoch dementierte (vgl. [3]). Die Wirtschaftsspionage beinhaltet unter anderem *„[..] die staatlich gelenkte oder gestützte, von fremden Nachrichtendiensten ausgehende Ausforschung von Wirtschaftsunternehmen und Forschungseinrichtungen [..]“*([13]), welche wiederum dem Angreifertyp *organisiertes Verbrechen* zugeordnet werden kann. Diese wird in erster Linie zum Vorteil der landeseigenen Unternehmen beziehungsweise zur Ausschaltung von Konkurrenten ausgeübt [6].

2.1.6. Sicherheitsmaßnahmen

Die Sicherheit von Informationssystemen ist von besonderer Wichtigkeit. Um die Einhaltung der Sicherheitsziele wie Vertraulichkeit, Integrität oder Verfügbarkeit sicherzustellen, existiert eine Vielzahl bestimmter Sicherheitsmaßnahmen. Das *Bundesamt für Sicherheit in der Informationstechnik* (BSI) definiert dafür allein 50 Maßnahmen in seinem Werk *Leitfaden Informationssicherheit*. Um nicht alle 50 Maßnahmen dieses Leitfadens aufzuzählen, wurde eine Auswahl der Sicherheitsmaßnahmen vorgenommen, die ebenfalls in einer ausgewählten Menge anderer Quellen anzutreffen sind und durch ihre häufige Nennung als besonders relevant betrachtet werden.

Um den unerwünschten Zugang zu schützenswerten Informationen zu verhindern, gibt es unterschiedliche Maßnahmen die berücksichtigt werden sollten. Zunächst sollten die Räumlichkeiten, in denen sich die Informationssysteme befinden, vor unbefugtem Zutritt mittels Zutrittsberechtigungen geschützt werden. Dafür gibt es verschiedene Möglichkeiten. Zum Beispiel könnte man diese Räume mit Hilfe eines Türschlosses schützen, das nur mit dem entsprechenden Schlüssel, Transponder, Chipkarte, PIN, Passwort oder biometrischen Merkmal zu öffnen ist. Jedoch muss der Angreifer nicht zwangsläufig eine Person sein, die den Zugang durch den unbefugten Zutritt erhält. Es kann ebenfalls ein Mitarbeiter sein der eine Zutrittsberechtigung zu den jeweiligen Räumlichkeiten besitzt. Aus diesem Grund ist es wichtig von einer recht simplen aber dennoch effektiven Maßnahme Gebrauch zu machen. Gemeint ist das Sperren des Computers beim vorübergehenden Verlassen des Arbeitsplatzes. Hierbei wird die Sperrung entweder selbst durchgeführt oder automatisch durch den Bildschirmschoner bei einer gewissen Inaktivität. Das Entsperren ist dann nur noch mit dem Benutzerpasswort möglich. Diese Maßnahme ist jedoch nur so sicher, wie das Passwort des Benutzers. Aus diesem Grund ist die Wahl eines sicheren Passwortes von großer Bedeutung. Ebenso ratsam ist es, dass die Datenzugriffsmöglichkeiten auf das minimal erforderliche Ausmaß beschränkt werden (vgl. [15, Seite 41]). Das BSI nennt in diesem Zusammenhang speziell das sogenannte *Need-to-Know-Prinzip*. Dieses Prinzip besagt, dass nur so viele Zugriffsmöglichkeiten auf Informationen oder Programme vorhanden sein sollten, wie für die Ausführung der täglichen Arbeit benötigt wird. Durch die Verteilung von Zugriffsberechtigungen kann daher der unbefugte Zugriff von Mitarbeitern auf Informationen oder Programme eingeschränkt werden. Jedenfalls solange sie nicht unberechtigterweise an die Rechte anderer gelangen. In dieser Hinsicht ist es ratsam, die Administratorrechte einzuschränken (vgl. [15, Seite 42]). So können größere Schäden durch das unbefugte Erlangen von Administratorrechten, die häufig keinerlei Zugriffseinschränkungen haben, vermieden werden. Wird die Anzahl der Benutzer, denen Zugriffsrechte zugewiesen werden müssen, jedoch zu groß, ist es vorteilhaft verschiedene

Rollen mit Zugriffsberechtigungen zu definieren. Auf diese Weise können Fehlzuweisungen und der allgemeine Aufwand minimiert werden (vgl. [15, Seite 42]).

Sollte ein unberechtigter Zugriff trotz eventueller Maßnahmen erfolgreich verlaufen, kann die Vertraulichkeit der Daten durch eine Verschlüsselung dieser bewahrt bleiben. Gerade im Geschäftsumfeld sind Verschlüsselungen von größter Bedeutung. So kann beispielsweise eine E-Mail mit sensiblen Daten eines Unternehmens ohne eine Verschlüsselung auf dem Weg zum Empfänger von Dritten mitgelesen werden. Aus diesem Grund wird eine unverschlüsselte E-Mail auch gerne mit einer Postkarte verglichen. Doch selbst Verschlüsselungen können geknackt werden. RSA Security warnt derzeit sogar dringend vor dem Einsatz des Zufallszahlengenerators *Dual Elliptic Curve Deterministic Random Bit Generation* (Dual EC DRBG), der neben fünf weiteren Zufallszahlengeneratoren in der Kryptografie-Bibliothek *BSAFE* zur Verfügung steht. Der Grund für die Warnung sind Dokumente des PRISM-Enthüllers Edward Snowden, die den Verdacht aufkommen ließen, dass die *National Security Agency (NSA)* eine Hintertür in den Zufallszahlengenerator eingebaut habe. Diese Warunung ist begründet durch die Mitentwicklung eines NSA-Mitarbeiters bei dem Dual EC DRBG und der derzeitigen NSA-Skandale (siehe [16]).

Eine weitere Maßnahme zum Schutz der Informationssysteme und der darauf befindlichen Informationen sind Viren-Schutzprogramme. Sie können anhand von speziellen Signaturen bekannte Schadsoftware identifizieren. Dabei fungieren die Signaturen als eine Art Fingerabdruck, die die Antiviren-Software in einer Datenbank zum Vergleich sammelt. Wichtig bei Antiviren-Software ist, dass ihre Virendatenbanken regelmäßig aktualisiert werden. Nur so können neue Schadprogramme anhand ihrer Signatur erkannt werden. Doch selbst die aktuellste Antiviren-Software kann keinen absoluten Schutz bieten. Ist die Signatur eines Schadprogamms noch nicht bekannt, können auch die Antiviren-Programme mit aktueller Virendatenbank dieses nicht aufspüren [15, Seite 40 f.].

Weil Schadsoftware Schwachstellen in Betriebssystemen und Anwendungen ausnutzen, ist es ebenfalls wichtig die gesamte Software durch aktuelle Updates und Patches auf dem neuesten Stand zu halten. Dadurch können bestehende Sicherheitslücken der Anwendungen oder des Betriebssystems geschlossen und das Risiko einer „Infektion“ durch Schadsoftware verringert werden [17].

Kommt es dennoch zu einem Übergriff durch Schadsoftware, was möglicherweise den Verlust beziehungsweise die Infektion von Daten mit sich bringt, ist oft die einzige Lösung gegen einen totalen Verlust dieser Daten eine regelmäßige Datensicherung. Solche sogenannten *Backups* können gleichermaßen bei Stromausfällen oder allgemein bei Ausfällen von Systemen oder von Hardware-Komponenten eine effektive Lösung gegen Datenverlust darstellen. Dabei ist es vorteilhaft, wenn die Speichermedien, die für die Backups genutzt werden, an einem gesicherten Ort aufbewahrt werden (vgl. [15, Seite 59 f.]). Auf diese

Weise soll verhindert werden, dass zum Beispiel beim Ausbruch eines Feuers sowohl die Daten auf dem genutzten System als auch die gesicherten Daten des Backup-Mediums verloren gehen.

Da die Effektivität bei allen Maßnahmen insbesondere vom Faktor *Mensch* abhängig ist, ist gerade im geschäftlichen Umfeld die Schulung der Mitarbeiter unverzichtbar. Bei diesen Schulungen sollte in erster Linie das Sicherheitsbewusstsein (engl. *Security Awareness*) der Teilnehmer gefördert werden (vgl. [15, Seite 51 f.]). Ein angemessenes Sicherheitsbewusstsein der Mitarbeiter ist essenziell für die allgemeine Sicherheit von Unternehmensdaten. Das Aufstellen der besten Sicherheitsmaßnahmen bietet nur dann wirkliche Sicherheit, wenn die Mitarbeiter bereit sind diese anzuwenden. Es muss daher klar definiert werden, welche Bedrohungen existieren und welche Maßnahmen dagegen eingesetzt werden sollen. Besonders wichtig ist es den Mitarbeitern klar zu machen, welchen Beitrag sie zu der Informationssicherheit leisten und wie bedeutend dieser in der Gesamtbetrachtung ist (siehe [18]). So soll die Motivation der Mitarbeiter gestärkt werden. Sehen sie nämlich keinen Nutzen in den Maßnahmen oder inwiefern sie zu der Informationssicherheit beitragen, können die Sicherheitsmaßnahmen auf Ablehnung stoßen und daraufhin nicht sachgemäß durchgeführt werden.

2.1.7. Informationssicherheit in Unternehmen

Die Informationstechnik ist ein grundlegendes Werkzeug vieler Betriebe. Weil mit ihr jedoch ein gewisses Sicherheitsrisiko einhergeht, müssen Unternehmen versuchen dieses auf ein kleinstmögliches Minimum zu reduzieren. Besonders problematisch ist dabei, dass Unternehmen nicht nur private Daten der Mitarbeiter, sondern ebenfalls sensible Geschäftsdaten in jeglicher Form besitzen und diese schützen müssen. Aus diesem Grund zählt die Informationssicherheit mit zu den wichtigsten Aspekten der Unternehmensführung. Sie ist insbesondere Aufgabe des Managements, das verantwortlich für die Analyse der Risiken des Unternehmens und die Entwicklung geeigneter Schutzmaßnahmen ist. Für diesen Zweck werden auch sogenannte Sicherheitsrichtlinien (engl. *security policies*) entwickelt. Sie definieren alle technischen und organisatorischen Regeln, Verhaltensrichtlinien und Maßnahmen, um die aufgestellten Sicherheitsziele erreichen zu können. Ebenso legen sie dafür die einzelnen Verantwortlichkeiten und Rollen fest (vgl. [9, Seite 31]). Diese Sicherheitsrichtlinien werden in der Zusammenarbeit zwischen der Unternehmensleitung, den IT-Sicherheitsverantwortlichen, dem Datenschutzbeauftragten, gegebenenfalls mit dem Compliance-Beauftragten und den Mitarbeitern erarbeitet (vgl. [20, Seite 27]). Unternehmen haben ebenfalls die Möglichkeit auf spezielle IT-Sicherheitsstandards zurückzugreifen. Diese verfügen über bewährte Methoden für ein optimales IT-Sicherheitsmanagement und bieten allgemein *„[...] Hilfestellung bei der Entwicklung von generischen Maßnahmen*

auf Management-Ebene bis zu detaillierten technischen Implementierungen an“ ([19, Seite 5]).

2.2. Bring Your Own Device

Dieser Abschnitt befasst sich mit dem Konzept *Bring Your Own Device* (BYOD). Dabei wird zu Beginn das Konzept und dessen Hintergrund einleitend vorgestellt. Daraufhin folgt die Beschreibung der rechtlichen Aspekte von *BYOD* und abschließend eine Gegenüberstellung der Vor- und Nachteile, die dieses Konzept mit sich bringt.

2.2.1. Definition und Hintergrund

Das Konzept *Bring Your Own Device* beschreibt das Vorgehen, bei dem die Mitarbeiter von Unternehmen ihre privaten Geräte mit zu ihrem Arbeitsplatz nehmen und für den geschäftlichen Gebrauch nutzen. Dabei verbinden sie die Geräte mit dem Firmennetzwerk, um auf Geschäftsdaten und Arbeitsmaterial zugreifen zu können (vgl. [21, Seite 5]). Der Ursprung dieses Konzeptes findet sich in dem sogenannten Home-Office Trend wieder (vgl. [22]). Dabei wurden private Rechner mit Hilfe eines *Virtual Private Networks* (VPN) mit dem Firmennetz verbunden. Weil durch die zusätzliche Mobilität der Notebooks auf diese Weise sowohl im Betrieb als auch von zu Hause aus gearbeitet werden konnte, bot es sich an, lediglich ein Gerät für die Arbeit zu verwenden. Doch macht die Nutzung eines einzigen Rechners nicht das BYOD-Konzept aus. Viel mehr ergab es sich durch die Tatsache, dass die meisten Privatpersonen bereits über ein Notebook verfügen, welches nach ihren Ansprüchen und Bedürfnissen ausgewählt wurde. Diese Gegebenheit nutzen daher einige Unternehmen und lassen ihre Mitarbeiter mit privaten Notebooks am Arbeitsplatz und von zu Hause aus arbeiten. Im Laufe der Zeit wurden weitere mobile Geräte, wie zum Beispiel Tablet-PCs und Smartphones, mit in das BYOD-Konzept eingebunden.

Nach Angaben von *Bitkom* (vgl. [21, Seite 5]) erlauben ca. 43 Prozent der ITK - Unternehmen ihren Mitarbeitern private Smartphones, Tablet-PCs, Notebooks etc. mit auf ihren Arbeitsplatz zu nehmen und diese zusätzlich mit dem Firmennetzwerk zu verbinden. Von diesen ITK-Unternehmen stellen lediglich ca. 60 Prozent gewisse Regeln für die Nutzung privater Geräte im Firmennetz auf. Dabei sind gerade diese Regelungen von höchster Wichtigkeit für die Sicherheit jeglicher Daten des Unternehmens. Auch sogenannte *Mobile Device Management (MDM) Systeme* können die Sicherheit der IT-Infrastruktur und der geschäftsbezogenen Daten auf den Geräten steigern. Dabei wird mit Hilfe der MDM-Software eine Inventarisierung der gesamten Geräte vorgenommen sowie der Überwachung und Aktualisierung der Software und Daten der mobilen Geräte. Ebenfalls können Fernzugriffe (remote control) durch die Administratoren durchgeführt werden, um beispielsweise beim Geräteverlust Unternehmensdaten zu löschen [23].

2.2.2. Rechtliche Aspekte

Das BYOD-Konzept bringt einige rechtliche Anforderungen mit sich, die ein Unternehmen beachten muss. Dabei spielen insbesondere das Telekommunikationsgesetz (TKG) und das Bundesdatenschutzgesetz (BDSG) eine bedeutende Rolle.

Um private Geräte geschäftlich nutzen zu können, ohne gegen das BDSG zu verstoßen, ist es sinnvoll private Daten auf den Geräten von den geschäftlichen zu trennen. Das Unternehmen muss die Möglichkeit haben, geschäftliche Daten auf diesen Geräten kontrollieren zu können. Dabei stehen insbesondere personenbezogene Daten des Unternehmens im Vordergrund der Kontrolle, die auf eine sachgemäße Erhebung, Verarbeitung und Nutzung überprüft werden müssen [21]. Damit diese Kontrolle durchführbar ist und zum Beispiel nicht gegen das Fernmeldegeheimnis aus §88 des Telekommunikationsgesetzes (genauere Erläuterung siehe Abschnitt 2.2.3) verstößt, ist die Separierung der Daten notwendig [21]. Nach §9 des BDSG muss das Unternehmen dabei die technischen und organisatorischen Maßnahmen treffen, die erforderlich sind, um die Vorschriften und die in den Anlagen genannten Anforderungen des BDSG zu gewährleisten (vgl. [21, Seite 6]). Die Anforderungen aus der Anlage zu §9 Satz 1 sind dabei folgende:

1. „... Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren (Zutrittskontrolle),“

2. „... zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können (Zugangskontrolle),“

3. „... zu gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können (Zugriffskontrolle),“

4. „... zu gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist (Weitergabekontrolle),“

5. „... zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind (Eingabekontrolle),“

6. „. . . zu gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können (Auftragskontrolle),“

7. „. . . zu gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind (Verfügbarkeitskontrolle),“

8. „. . . zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.“

Das BDSG stellt mit dieser Anlage demnach Anforderungen an die Zutritts-, Zugangs-, Zugriffs-, Weitergabe-, Eingabe-, Auftrags- und Verfügbarkeitskontrolle auf. Während bei der Zutrittskontrolle in Bezug auf BYOD nicht zwangsläufig zusätzliche Maßnahmen ergriffen werden müssen, sind bei der Zugangskontrolle wichtige Vorkehrungen zu treffen. Bei privaten Geräten wie zum Beispiel Smartphones und Tablet-PCs ist es durchaus möglich, dass Personen aus der eigenen Familie oder dem Bekanntenkreis diese für private Anliegen nutzen und Zugang zu diesen haben. Sollten sich auf diesen Geräten jedoch personenbezogene Daten des Unternehmens befinden, die nicht zusätzlich gesichert sind, wäre selbst die genannte Nutzung als unbefugte Nutzung anzusehen. Auch im Hinblick auf die Zugriffskontrolle müssen gewisse Maßnahmen getroffen werden, um den Datenschutz gewährleisten zu können. Zum Beispiel dürfen Unternehmensdaten nicht von privaten Anwendungen aus geöffnet werden, die diese eventuell an Dritte versenden können. Die Anforderung an die Weitergabekontrolle ist insofern für BYOD interessant, weil auf privaten Geräten zusätzlich Anwendungen anzutreffen sind, die auf Firmengeräten nicht installiert werden dürften. Diese könnten dann die in Punkt 4 genannten Risiken zulassen. Bezüglich der Eingabe- und Auftragskontrolle müssen Unternehmen auch beim BYOD-Konzept gewisse Kontrollmaßnahmen, wie zum Beispiel eine Protokollierung, vornehmen. Hierbei ist jedoch wichtig, diese Kontrollbefugnis mit den Mitarbeitern auszumachen, insbesondere dann, wenn dabei ebenfalls Bereiche der privaten Daten betroffen sind. Bei der Verfügbarkeitskontrolle ist bei BYOD wieder eine klare Datenseparierung von Relevanz. Um die Daten gegen Zerstörung oder Verlust zu schützen, müssen regelmäßig Backups durchgeführt werden. Dabei entstehen allerdings ohne strikte Trennung der Daten zwei Probleme. Werden die Geschäftsdaten auf Unternehmensservern abgesichert, werden wahrscheinlich auch gleichzeitig die privaten Daten des Mitarbeiters gespeichert. Dafür müssten zusätzlich Regelungen mit den Mitarbeitern vereinbart werden, die diese Speicherung und das Löschen der privaten Daten beinhaltet. Sichert der Mitarbeiter seine Daten eigenständig und nicht auf den unternehmenseigenen Servern, muss auch hier klar geregelt werden, welche Sicherheitsmaßnahmen für die Speicherung der geschäftlichen Daten vorzunehmen sind. Beispielsweise sollten Cloud-Dienste wie Apples iCloud oder Dropbox möglichst nicht verwendet werden. Auch die zuletzt genannte Anforderung verweist auf eine Trennung der

privaten und geschäftlichen Daten [21, Seite 6 ff.].

Ein weiterer rechtlicher Aspekt bei dem BYOD-Konzept ist die Problematik der Softwarelizenzen. Wird zum Beispiel Unternehmenssoftware, die ausschließlich für gewerbliche Zwecke verwendet werden darf, privat genutzt oder umgekehrt, kann der Lizenzgeber urheberrechtliche Unterlassungsansprüche fordern. Im schlimmsten Fall ist der Lizenzgeber sogar berechtigt Schadensansprüche geltend zu machen. Deshalb sollten sämtliche Unternehmenslizenzen auf bestimmte Nutzungseinschränkungen überprüft und die Mitarbeiter darauf hingewiesen werden, dass sie private Software nicht für geschäftliche Zwecke nutzen sollen(vgl. [21, Seite 10 ff.]).

Das BDSG legt weiterhin fest, dass bei einer unrechtmäßigen Übermittlung beziehungsweise dem Verlust von personenbezogenen Daten, die Unternehmen diesen Vorfall unverzüglich bei der zuständigen Aufsichtsbehörde und den Betroffenen melden müssen (siehe §42a BDSG). Aus diesem Grund sollten die Mitarbeiter bei dem Verlust ihres Geräts, das solche Daten beinhaltet, diesen umgehend melden und eventuell Maßnahmen zur Geräteortung oder Fernlöschung der Daten vornehmen [24].

2.2.3. Vor- und Nachteile

Die Beschreibung und die rechtlichen Anforderungen des *BYOD*-Konzepts wurden eingehend erläutert. Um das Thema abschließen zu können, folgen die Vor- und Nachteile, die dieses Konzept mit sich bringt.

Bezüglich der Vorteile von *BYOD* steht besonders die positive Auswirkung auf die Mitarbeiter im Vordergrund. Haben die Mitarbeiter die Möglichkeit, ein Gerät zu verwenden was sie nach ihren Anforderungen und Geschmack ausgesucht haben, steigert dies ihre Zufriedenheit. Auch die Vertrautheit mit dem Gerät wirkt sich positiv auf die Zufriedenheit aus, da Probleme mit der Bedienung meist seltener vorkommen. Durch eine zufriedene Einstellung wird wiederum die Motivation der Mitarbeiter erhöht, sodass diese häufig effizienter arbeiten. Dazu kann ebenfalls die meist bessere Ausstattung der Geräte beitragen. Während Unternehmen dazu tendieren, die Geräte so auszusuchen, dass sie den Anforderungen der Arbeitsaufgaben entsprechen, wählen viele Mitarbeiter ihre privaten Geräte nach dem aktuellen Stand der Technologie. Auf diese Weise können die Unternehmen Kosten für die Anschaffung der Geräte sparen und gleichzeitig das Image des Unternehmens durch die meist neuen Geräte verbessern. Weil es sich bei den Geräten um die privaten Geräte der Mitarbeiter handelt, neigen diese oft zu einem schonenderen Umgang. Das bewirkt wiederum weniger Reparaturkosten für den Arbeitgeber und eine allgemein längere Lebensdauer der Geräte. Nicht zu vergessen ist, dass Mitarbeiter nicht

mehrere Geräte mitführen müssen. Wird das private Smartphone auch geschäftlich genutzt, so muss lediglich ein Mobiltelefon mitgetragen werden [21, Seite 31] [25, 26].

Doch bietet BYOD nicht nur Vorteile. Es bringt gleichermaßen eine Reihe von Nachteilen mit sich, die bei der Entscheidung zur Einführung des Konzeptes berücksichtigt werden sollten.

Ist es den Mitarbeitern gestattet ihre privaten Geräte mit in die Unternehmen zu nehmen und diese mit dem Firmennetz zu verbinden, führt dies schnell zu einer stark heterogenen Infrastruktur und einem hohen Verwaltungsaufwand. Es muss dabei gewährleistet werden diese Geräte so in die Unternehmensinfrastruktur einzubinden, dass sie keine Gefahr für andere Geräte oder Geschäftsdaten darstellen. Würde sich Schadsoftware auf einem privaten Gerät befinden, könnte diese andernfalls die gesamte Unternehmensinfrastruktur angreifen (vgl. [25]). Somit muss eine sichere Integration privater Geräte vorgenommen werden, gegebenenfalls mit Hilfe einer Mobile Device Management Lösung. Weil dieses Vorhaben allerdings wieder mit Kosten verbunden ist, muss an dieser Stelle geprüft werden, ob die Einsparungen höher als die nötigen Ausgaben sind und die Einführung dieses Konzepts somit wirtschaftlich ist. Auch die rechtlichen Aspekte, die sich eher nachteilig auf das Konzept BYOD auswirken, müssen berücksichtigt werden. Besonders im Hinblick auf den Datenschutz lassen sich Nachteile des Konzepts finden. Zum Beispiel ist nach §7 des Bundesdatenschutzgesetzes (BDSG) das Unternehmen verantwortlich für eine ordnungsgemäße Erhebung, Verarbeitung oder Nutzung von personenbezogenen Daten und kann bei Verstoß zu Schadensersatz verpflichtet werden (siehe [27]). Daher ist es dringend notwendig, die angemessene Datenverarbeitung und IT-Compliance zu kontrollieren. Die Kontrolle gestaltet sich jedoch schwierig, sofern keine Trennung der privaten und geschäftlichen Daten auf den Geräten vorgenommen wird. Der Arbeitnehmer muss bei seiner Überwachung, insbesondere in Bezug auf private E-Mails, das sogenannte Fernmeldegeheimnis berücksichtigen, welches untersagt, sich *„Kenntnis vom Inhalt oder den näheren Umständen der Telekommunikation zu verschaffen“* (§88 Abs. 3 Telekommunikationsgesetz) [24, 25].

3. Sicherheit auf mobilen Betriebssystemen

Mobile Betriebssysteme haben wie auch andere Betriebssysteme bestimmte Schwachstellen, die sich auf die Sicherheit des Systems selbst und auf dessen Daten negativ auswirken können. Um im Rahmen dieser Bachelorarbeit die Sicherheit des Betriebssystems *Android* beurteilen zu können, werden zunächst allgemeine potentielle Gefahren mobiler Betriebssysteme und die jeweiligen Sicherheitsmaßnahmen genannt. Daraufhin wird speziell Android vorgestellt, samt des Android-Sicherheitsprogramms, seiner Sicherheitsarchitektur und anderer Sicherheitsmechanismen und -werkzeuge. Diese werden für die spätere Gegenüberstellung mit den Betriebssystemen *iOS* und *Windows Phone* herangezogen, die im Vorfeld ebenfalls kurz auf ihre Sicherheitsmechanismen untersucht werden.

3.1. Potentielle Gefahren

Um die Sicherheit von mobilen Betriebssystemen zu untersuchen, müssen zunächst diverse Gefahren, denen das Gerät und die Daten und Anwendungen ausgesetzt sind, betrachtet werden. Weil jedoch Unmengen an Gefahren für Smartphones und Tablet-PCs existieren, werden lediglich zehn Gefahren vorgestellt, die von der *European Network and Information Security Agency* (ENISA) als die zehn wichtigsten Informationssicherheits-Risiken definiert werden (siehe [28]).

Ein großes Problem mit Smartphones oder Tablet-PCs ist deren Mobilität und ihre meist relativ kleine Größe. Diese Eigenschaften erhöhen das Risiko des Geräteverlusts sowie des Gerätediebstahls enorm. Dieser Verlust führt schlimmstenfalls nicht nur zu einem materiellen Schaden durch das verloren gegangene beziehungsweise gestohlene Gerät, sondern gleichzeitig zu dem Verlust sensibler Daten. Ist der Speicher des Gerätes oder das Gerät selbst ungeschützt, kann der Dieb oder der Finder problemlos auf die darauf befindlichen Daten zugreifen.

Dasselbe Problem besteht, wenn das Gerät entsorgt, weiterverkauft oder möglicherweise an einen Mitarbeiter weitergegeben wird ohne die darauf befindlichen Daten zu löschen. Der neue Besitzer könnte dann Zugriff auf die persönlichen Daten des Vorgängers haben, die auch Login-Daten und andere Informationen beinhalten können. Selbst bei einer Reperatur des Gerätes muss berücksichtigt werden, dass eventuell Unbefugte Zugriff auf die eigenen Daten haben (siehe auch [29]).

Viele Smartphone-Apps besitzen sogenannte *Privatsphäre-Einstellungen*, um bestimmte Daten anderen nicht offenzulegen. Weil der Funktionsumfang dieser Apps allerdings sehr groß und unübersichtlich sein kann, wissen viele Anwender nicht, dass es diese Privatsphäre-Einstellungen überhaupt gibt. Häufig interessiert es die Anwender auch gar nicht, was mit ihren Daten geschieht. Ohne die Rücksicht auf diese Einstellungsmöglichkei-

ten können die Applikationen beispielsweise Positionsinformationen über einen Anwender sammeln und eine Art Bewegungsprofil erstellen. Die ENISA verweist bei dieser Gefährdung auf die Seite `icanstalku.com`, die auf die Offenlegung von GPS-Daten in Bildern eingeht (siehe [30]).

Wie bereits bei der Nutzung von PCs, existiert auch bei dem Gebrauch von Smartphones und Tablet-PCs die Gefahr von Phishing-Angriffen. Dabei ist diese Gefahr bei den mobilen Geräten noch größer, weil die Nutzer dazu neigen, unüberlegt Elemente und Links anzuklicken und viele mobile Internetbrowser nicht den gesamten URL der Webseite anzeigen. Auf diese Weise kann der Angreifer über *Fake-Apps, -Nachrichten* oder *-Webseiten* leicht an die Anmeldeinformationen, Kreditkartennummern oder andere geheime Daten des Opfers gelangen.

Eine weitere Gefährdung bei Smartphones und Tablet-PCs ist *Spyware*. Sie sammelt unbemerkt Informationen über den Nutzer des Gerätes und dessen Aktivitäten. Die gesammelten Informationen werden häufig für wirtschaftliche Zwecke, wie für gezielte Werbung, eingesetzt. Der Nutzer merkt häufig nicht, dass eine App Informationen sammelt und diese an den Entwickler oder an ein Unternehmen weiterschickt. Die für diese Absicht von der App geforderten Berechtigungen (engl. *permissions*) werden für vermeintlich harmlose und unverdächtige Zwecke gefordert, sodass der Benutzer keinen Verdacht schöpft.

Weil Smartphones und Tablet-PCs für gewöhnlich eine Internetverbindung beanspruchen, um diverse Applikationen nutzen zu können und Webseiten zu besuchen, nennt die ENISA in diesem Zusammenhang die Gefahr von *Netz-Spoofing*-Angriffen. Dabei verbindet sich ein Nutzer mit einem nicht vertrauenswürdigen Access Point des Angreifers, der dann die Kommunikation des Nutzers abfängt um Informationen für spätere Angriffe zu sammeln. Die gesammelten Informationen kann der Angreifer beispielsweise für Phishing-Angriffe nutzen.

Während die zuvor genannte *Spyware* eine eher ungezielte „Überwachung“ von bestimmten Informationen wie Internetaktivitäten vornimmt, existiert noch eine weitere ähnliche Gefahr. Es handelt sich um die gezielte Überwachung des Smartphone- beziehungsweise Tablet-PC-Nutzers. Weil die Geräte über diverse Sensoren verfügen, wie zum Beispiel Kamera, Mikrofon, Accelerometer und GPS, kann ein Angreifer diese für seine Überwachung nutzen, sofern das Opfer seine bösartige App installiert hat. Diese tarnen sich oftmals als gewöhnliche Anwendungen wie zum Beispiel Spiele, sodass das Opfer bestenfalls von sich aus die Schadsoftware installiert.

Um dem Opfer einen finanziellen Schaden zuzufügen, gibt es sogenannte *Dialerware*-Angriffe. Bei diesen Angriffen werden bestimmte *API-Calls* vorgenommen, die für das Opfer kostenpflichtig sind, sofern dessen Mobilfunkvertrag diese nicht durch eine *Flatrate* abdeckt. Es werden durch diese *API-Calls* zum Beispiel SMS versendet, gegebenenfalls sogar *Premium-SMS*. Ebenfalls können ohne die Kenntnis des Opfers Anrufe getätigt oder

Datenverbindungen hergestellt werden, die ohne WLAN-Verbindung über das Mobilfunknetz laufen und gegebenenfalls Kosten verursachen können.

In diesem Zusammenhang nennt die ENISA ebenfalls die sogenannten *Financial-Malware*-Angriffe. Diese Art von Malware wird speziell dafür entwickelt, um zum Beispiel Anmeldeinformationen für Online-Banking oder Kreditkartennummern zu „stehlen“. Dies können die Angreifer beispielsweise mittels *man-in-the-middle*-Angriffen durchführen, indem sie eine Online-Banking-App in den App-Store stellen, die die Anmeldedaten abfängt. Solche Angriffe werden ebenfalls als Phishing-Angriff bezeichnet.

Die ENISA nennt als zehntes Risiko die Netzüberlastung. Weil die Auswirkungen und das Risiko selbst nach Angaben der ENISA nicht besonders groß sind, wird stattdessen auf eine andere Gefahr eingegangen, die für diese Arbeit einen größeren Mehrwert hat. Gemeint ist das Problem, dass Smartphones standardmäßig über keinen Mehrbenutzer-Betrieb verfügen. Windows Phone 8 bietet zwar eine *Kinderecke* mit selbst freigegebenen Anwendungen und Daten, jedoch ist dies nicht mit einem Mehrbenutzerbetrieb, wie man ihn von seinem Desktop-PC oder Notebook kennt, vergleichbar. Seit Android 4.2 (*Jelly Bean*) können Tablet-Nutzer mehrere Benutzerkonten auf ihrem Gerät anlegen. Bei Android-Smartphones ist dies jedoch nicht möglich, weil ein Nokia-Patent für diese Technik die Umsetzung auf Smartphones verhindert (vgl. [31]). Der Android-Entwickler *Dan Morrill* schrieb jedoch bei Reddit:

> *„[...] it is not at all clear how it should work on a phone, specifically with respect to SMS and phone calls. Suppose you have device sharing enabled and then a call comes in. Who gets it? Do you punch through to the current user? Only the owner gets it? If only the owner can answer, does it ring for the second user? Is it worse to annoy the current user with a ringing phone they can't answer, or worse for dad to miss a call from his boss because Junior was playing Angry Birds? What about call log, does it appear in the log of the user who happened to be active at the time, only the owner, or both? User research showed that if you ask 5 people how this should work, you get 6 answers.“*([32])

Diese Aussage lässt daher vermuten, dass nicht zwangsläufig das Nokia-Patent der Grund für die Nicht-Unterstützung des Mehrbenutzerbetriebs auf Android-Smartphones ist. Problematisch an dem nicht vorhandenen Mehrbenutzerbetrieb ist dabei, dass alle Daten und Anwendungen vermischt auf dem Gerät liegen und somit zugänglich für einander sein können. Auf diese Weise könnten private Anwendungen (möglicherweise bösartige Anwendungen) auf sensible Geschäftsdaten zugreifen (vgl.[33], [34, Seite 4]).

3.2. Mögliche Sicherheitsmechanismen und -maßnahmen

Nach der Nennung diverser Gefahren für Smartphones beschäftigt sich dieser Abschnitt mit möglichen Sicherheitsmechanismen beziehungsweise -maßnahmen, die diese Gefahren abdecken. Für diesen Zweck werden in erster Linie die Vorschläge der ENISA aus dem zuvor genannten Bericht betrachtet.

Um den durch einen Diebstahl oder das Verlorengehen des Gerätes resultierenden ungewollten Zugriff auf die eigenen Daten beziehungsweise dessen Verlust zu verhindern, existieren verschiedene Maßnahmen. Um einen kompletten Datenverlust zu verhindern, ist es ratsam, wie bereits in Kapitel 2.1.6 erwähnt, regelmäßig die Daten durch ein Backup zu sichern. Durch diese regelmäßige Datensicherung kann ein Großteil der verlorengegangenen Daten wieder hergestellt werden, bestenfalls sogar alle. Damit ein Dieb oder ein Finder des Gerätes keinen Zugriff auf die Daten hat, sollte das Gerät so eingerichtet werden, dass nach einer bestimmten Zeit der Inaktivität eine Art Bildschirmschoner mit Passwort-/PIN-Abfrage erscheint. Dabei ist es besser ein längeres Passwort zu nutzen anstatt einer vierstelligen PIN, weil bei dieser Art der Authentifizierung teilweise beliebig viele Versuche möglich sind. Zwar sind bei einer vierstelligen PIN immerhin 10^4 (= 10.000) Zahlenkombinationen möglich, jedoch stellt ein mehrstelliges alphanumerisches Passwort eine höhere Sicherheit dar. Im Falle eines Geschäfts-Smartphones hat das Unternehmen möglicherweise in seinen Sicherheitsrichtlinien bestimmte Vorgaben zu einer Passwortnutzung definiert, die unbedingt berücksichtigt werden sollten. Eine noch höhere Sicherheit kann zum Beispiel durch eine Mehrfach-Authentifizierung erfolgen, bei der zusätzlich ein Bluetooth-fähiger Smartcard-Leser genutzt wird. Bestenfalls sollte es jedoch ganz vermieden werden, geschäftsbezogene und möglicherweise in Geheimhaltungsstufen (*confidential, secret, top secret*) zugeordnete Daten auf dem Smartphone oder Tablet-PC zu speichern oder auf solche zuzugreifen.

Auch die Verschlüsselung des Speichers kann die Daten vor unbefugten Zugriffen schützen. Dabei muss jedoch die Sicherheit der Verschlüsselungstechnik berücksichtigt werden, die von Algorithmus zu Algorithmus unterschiedlich sein kann. Ist die Verschlüsselung eher schwach und sind die Daten auf dem Gerät sensible Geschäftsdaten, sollte per Fernzugriff eine Löschung der Daten (*Remote Wipe*) erfolgen oder eine automatische Löschung zum Beispiel nach drei erfolglosen Entsperr- beziehungsweise Entschlüsselungsversuchen stattfinden.

Vor der Weitergabe eines Smartphones oder Tablet-PCs oder vor dessen Entsorgung sollte dringend eine Systemzurücksetzung und eine komplette Entfernung der gespeicherten und persönlichen Daten vorgenommen werden.

Damit die eigenen Daten nicht ungewollt über bestimmte Apps offengelegt werden, existieren zwei wichtige Maßnahmen, die grundsätzlich berücksichtigt werden sollten. Zum

einen sollten vor der Nutzung, wenn möglich noch vor der Installation, die von der App geforderten Berechtigungen genau überprüft und bei fraglichen Berechtigungsforderungen diese entfernt oder nicht installiert werden. So können unnötige Zugriffe, wie zum Beispiel auf die gespeicherten Kontakte, den Kalender oder auf andere schützenswerte Informationen, verhindert werden. Zum anderen ist es ratsam, die standardmäßigen Privatsphäre-Einstellungen von Apps zu überprüfen. Dort kann (meistens) festgestellt werden, welche Informationen preisgegeben werden und eingestellt werden, ob diese Preisgabe überhaupt erwünscht ist.

Um Phishing-Angriffen entgegenzuwirken, hilft in erster Linie ein gewisses Misstrauen gegenüber Nachrichten, Anwendungen und Webseiten, die Anmeldedaten, Kreditkartennummern oder ähnliche Informationen anfordern. Dieses Misstrauen ist insbesondere dann empfehlenswert, wenn es sich bei den Nachrichten um einen unbekannten Absender handelt. Aber auch Antiviren-Apps können Nachrichten auf solche Angriffe überprüfen.

Malware-Angriffe durch Spyware, Dialerware oder Financial-Malware kann der Smartphone- beziehungsweise Tablet-PC-Nutzer vorbeugen, indem er vor der Installation von Apps deren Ruf überprüft. Häufig sind zu bösartigen Anwendungen Berichte oder Foreneinträge zu finden, die die versteckten Angriffe aufdecken. Bei geschäftlich genutzten Geräten ist es ratsam, eine Whitelist mit Apps zu führen, die sich ohne Bedenken installieren lassen. Hier ist es wichtig, dass das Unternehmen die Apps aus der Whitelist genau überprüft und testet. Auch die Pflege der Liste ist wichtig, damit die Nutzer der Geräte in gewisser Weise davon abgehalten werden, andere Apps zu installieren, die nicht auf der Whitelist zu finden sind. Ist die Malware bereits auf dem Gerät, lässt sich das bösartige Verhalten durch die Beobachtung (engl. *monitoring*) der Ressourcennutzung feststellen. Kostenpflichtige Services können zum Beispiel von der Telefonrechnung abgelesen werden.

Um Netz-Spoofing-Angriffe zu verhindern, sollten Smartphones und Tablet-PCs so eingestellt werden, dass sie sich nicht automatisch mit öffentlichen Netzen verbinden. Werden öffentliche WLAN-Hotspots dennoch genutzt, dann sollte bestenfalls auf Online-Banking, das Versenden von E-Mails oder andere Aktivitäten, bei denen der Nutzer sensible Daten preisgibt, verzichtet werden. Auch die Verschlüsselung der Kommunikation ist in einem öffentlichen Netz empfehlenswert. Hierfür könnte zum Beispiel ein *Virtual Private Network* (VPN) verwendet werden. Dabei ist anzumerken, dass selbst ein VPN keine hundertprozentige Sicherheit bietet. Spoofing-Angriffe müssen allerdings nicht zwangsläufig im Internet erfolgen, auch das Mobilfunknetz ist vor „Lauschangriffen“ nicht sicher. Deshalb sollten vertrauliche Telefonate und SMS zusätzlich mit einer geeigneten Software verschlüsselt werden.

3.3. Sicherheit in Android

Die System-Plattform *Android* wurde beziehungsweise wird von der *Open Handset Alliance (OHA)* entwickelt. Die *OHA* ist ein Konsortium, welches zu Beginn aus 34 Firmen bestand und *Google* stellt dabei das Hauptmitglied dar. Android ist eine freie und quelloffene Software, die auf einem Linux-Kernel basiert. Sie wurde im Laufe der Zeit rasant weiterentwickelt, sodass seit der ersten Veröffentlichung im Jahr 2008 bis heute mit Android 4.4 die 36. Version herausgebracht wurde. Bei dieser Weiterentwicklung wurden nicht nur an neuen Funktionalitäten und verbesserter Benutzerfreundlichkeit gearbeitet, sondern ebenfalls Fehler im System behoben, die sich teilweise negativ auf die Sicherheit des Systems und der Daten ausgewirkt haben (vgl. [37, Seite 22 f.], [35], [36]). Um die Sicherheit in Android genauer zu untersuchen, wird in diesem Abschnitt auf das Android-Sicherheitsprogramm und dessen Sicherheitsarchitektur eingegangen. Auch zusätzliche Sicherheitswerkzeuge werden kurz vorgestellt sowie die Entwicklung der Sicherheit von Android mit einer Übersicht der Versionen und der jeweiligen Sicherheitsverbesserungen.

3.3.1. Android-Sicherheitsprogramm

Das Android-Betriebssystem läuft auf einer Vielzahl von Gerätemodellen und -typen. Um ein stabiles System zu bieten, das die Verbindung von Anwendungen mit der heterogenen Masse an Geräten ermöglicht, erkannte das Android-Entwicklerteam, dass ein robustes Sicherheits-Modell benötigt wird (vgl. [38]). Dabei durchlief das System bereits während der Entwicklung ein spezielles Sicherheitsprogramm, um Schwächen und Verwundbarkeiten so früh wie möglich aufzudecken. Die Seite `source.android.com` nennt bei dem *Android-Sicherheitsprogramm* folgende vier Hauptmerkmale: (vgl. [38])

- **Design Review**:
  In der frühen Entwicklungsphase wird mit der Erstellung eines mächtigen und konfigurierbaren Sicherheitsmodells und -designs begonnen. Dabei wird jede wichtige Funktion überprüft und mit entsprechenden Sicherheitskontrollen in die Architektur des Systems integriert.

- **Penetration Testing and Code Review**:
  Sowohl interne als auch unabhängige externe Sicherheitsteams und -gutachter überprüfen die Sicherheit der Plattform während der Entwicklung. Dabei sollen bereits vor der Veröffentlichung mögliche Schwachstellen und Verwundbarkeiten identifiziert und bestimmte Arten von Analysen simuliert werden, die von externen Sicherheitsexperten nach der Freigabe durchgeführt werden.

- **Open Source and Community Review**:
  Um eine zusätzliche Überprüfung der Sicherheit durchzuführen, ist es jeglichen interessierten Teilnehmern erlaubt eine solche Sicherheitsüberprüfung abzuhalten. Ebenfalls wird für Android auf Open-Source-Technologien zurückgegriffen, die sich bereits ausführlichen externen Sicherheitsüberprüfungen unterzogen haben, wie zum Beispiel der Linux-Kernel. Auch wird durch das *Google Play*-Forum Nutzern und Unternehmen die Möglichkeit geboten, den Nutzern Informationen zu einer bestimmten Anwendung auf direktem Weg anzubieten.

- **Incident Response**:
  Weil trotz aller Vorsichtsmaßnahmen Sicherheitsprobleme auch nach der Veröffentlichung auftreten können, existiert ein *Android-Sicherheits-Team*, das durchgängig Diskussionen in der Android- und der allgemeinen Sicherheits-Community überwacht. Dabei wird Ausschau nach potentiellen Verwundbarkeiten gehalten, die eine schnelle Reaktion erfordern. Das Android-Team hat dafür einen speziellen Cloud-basierten Reaktionsprozess, der eine schnelle Entschärfung der Verwundbarkeiten ermöglicht. Inhalt dieser Reaktionen kann dann beispielsweise das Updaten der Android-Plattform, das Löschen von Applikationen aus *Google Play* oder sogar das Löschen von Applikationen auf Geräten sein.

Demzufolge werden während des gesamten Lebenszyklus des Systems Sicherheitsüberprüfungen von sowohl internen als auch externen „Gutachtern“ durchgeführt, was zur Steigerung der Sicherheit beitragen soll.

3.3.2. Sicherheitsarchitektur

Die Android-Plattform verfügt über einen besonderen Aufbau und eine spezielle Sicherheitsarchitektur, um Benutzerdaten und Systemressourcen zu schützen. Der Aufbau der Plattform umfasst die fünf Komponenten *Linux Kernel, (native) Libraries, Android Runtime, Application Framework* und *Applications* (siehe Abbildung 2) [38]. Aufgrund dieses Aufbaus verfügt diese Plattform über eine besondere Sicherheitsarchitektur die im folgenden genauer betrachtet wird.

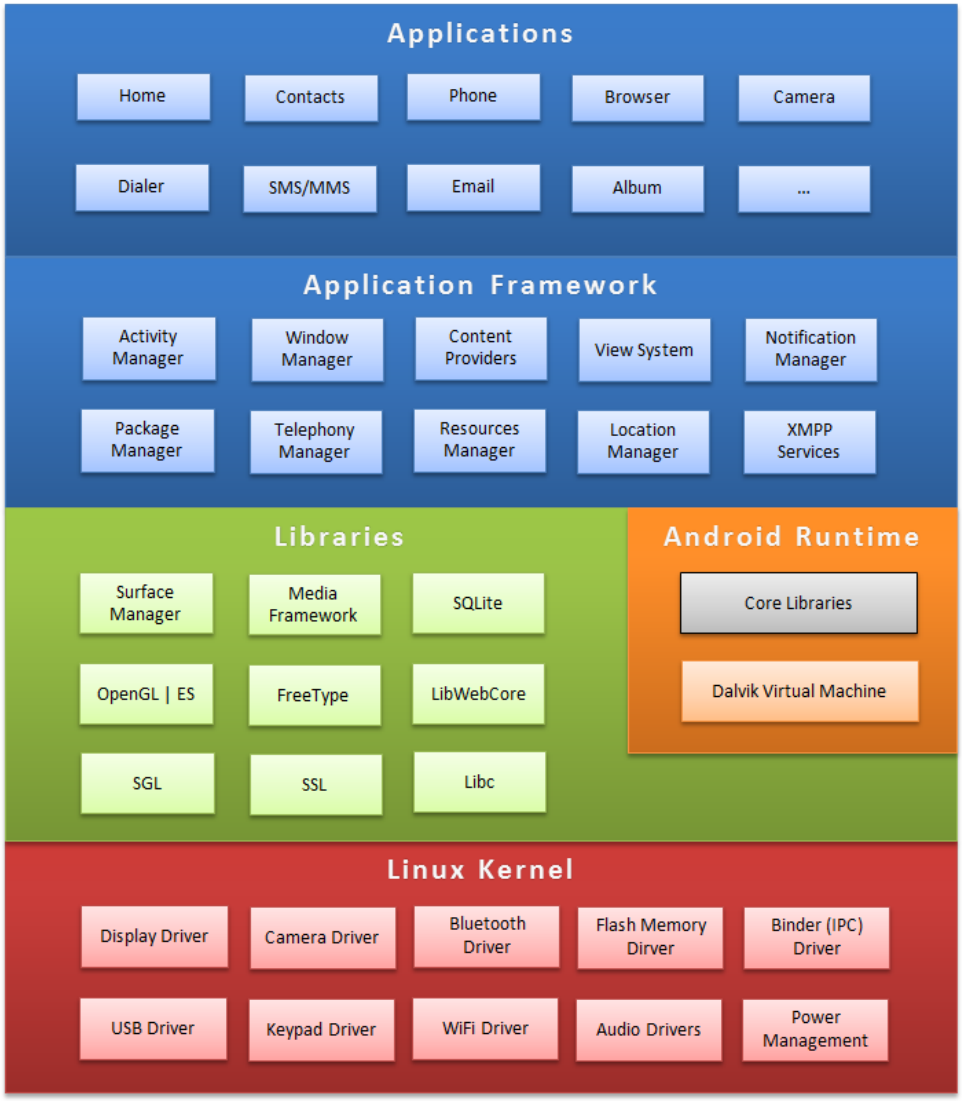

Abbildung 2: Die allgemeine Architektur von Android[38]

Die Sicherheitsarchitektur lässt sich in zwei Ebenen einteilen, auf denen bestimmte Sicherheitsmechanismen anzutreffen sind. Auf der untersten Ebene der Architektur befindet sich die *Kernel-Ebene*, die insbesondere Linux-spezifische Mechanismen zur Absicherung der Daten enthält. Die zweite Ebene ist die *Anwendungs-Ebene*. Sie sorgt unter anderem

für eine sichere Kommunikation zwischen den Anwendungen sowie für den Zugriffsschutz auf gewisse sicherheitskritische APIs.

Sicherheit auf Kernel-Ebene

Wie in der obigen Abbildung zu erkennen ist, basiert Android auf einem Linux Kernel. Dieser stellt Android zusätzliche Sicherheitsfunktionen zur Verfügung, wie zum Beispiel Prozessisolation durch eine Anwendungs-Sandbox auf Kernel-Ebene. Der Linux Kernel stellt normalerweise sicher, dass in einem Mehrbenutzersystem die Nutzer nicht auf die Ressourcen der anderen zugreifen können (ohne die Berechtigung dazu). Das Prinzip sorgt demnach für eine klare Trennung der Daten und Ressourcen aller Nutzer. Um bei Android die Anwendungen isoliert (in einer Sandbox) auszuführen, ohne dass sie unerlaubt auf Daten anderer Anwendungen beziehungsweise auf die persönlichen Daten des Nutzers oder Systemressourcen zugreifen können, werden Anwendungen als einzelne Benutzer betrachtet. Dabei wird jeder Anwendung eine eindeutige User-ID (UID) zugewiesen und als dieser Nutzer in einem eigenständigen Prozess ausgeführt. Diese UID wird bei der Installation einer Anwendung vergeben und bleibt bis zur Deinstallation dieselbe, um die Anwendung identifizieren zu können [38].

Anwendungen bekommen zusätzlich ein gesichertes Heimatverzeichnis, in dem nur sie Lese- und Schreibrechte haben. Um anderen Anwendungen den Zugriff auf dieses Verzeichnis zu erteilen, muss es für „Alle“ freigegeben werden. Außerdem werden Standardanwendungen und Systemdateien in dem */system*-Verzeichnis abgelegt, auf welches lediglich mit Leserechten zugegriffen werden kann (vgl. [40]).

Sicherheit auf Anwendungsebene

Auf der Anwendungs-Ebene verfügt Android über ein spezielles Berechtigungsmodell. Anwendungen haben standardmäßig nur sehr begrenzten Zugriff auf Systemressourcen. Auf bestimmte Ressourcen, wie zum Beispiel Kamera, GPS-Modul, Bluetoothfunktionen oder Telefonfunktionen, können die Anwendungen nur über bestimmte APIs zugreifen. Für diese müssen sie jedoch Berechtigungen anfordern, um erfolgreich auf sie zugreifen zu können [38]. Dies geschieht, indem der Entwickler in der sogenannten *Manifest-Datei* einer Anwendung die benötigten Berechtigungen hinterlegt. Als Beispiel für eine solche Berechtigungsanforderung dient das folgende Listing.

```
1 <manifest xmlns:android="http://schemas.android.com/apk/res/android"
2     package="com.android.app.myapp" >
3     <uses-permission android:name="android.permission.SEND_SMS" />
4     ...
5 </manifest>
```

Listing 1: Manifest-Datei mit der Berechtigung SMS zu senden [41].

Bei der Installation einer Anwendung werden dann dem Nutzer die geforderten Berechtigungen aufgelistet. Dieser muss für sich entscheiden, ob die Berechtigungen für den jeweiligen Anwendungszweck gerechtfertigt sind oder diese möglicherweise ein Sicherheitsrisiko darstellen. Somit liegt die gesamte Sicherheit des Gerätes und der darauf befindlichen Daten in der Hand des Benutzers. Versucht eine Anwendung ohne die Angabe von benötigten Berechtigungen dennoch auf bestimmte abgesicherte Ressourcen zuzugreifen, stürzt diese ab.

Ein weiterer Sicherheitsmechanismus auf der Anwendungsebene stellt die Anwendungs-Signatur dar. Mit der Signatur einer Anwendung wird deren Autor identifiziert. So kann jede Anwendung eindeutig einem Entwickler zugeordnet werden und landet nicht anonym oder verändert in *Google Play*. Sollte ein Entwickler jedoch versuchen eine unsignierte Anwendung in *Google Play* bereitzustellen, wird diese abgewiesen. Auch das Installieren einer unsignierten Anwendung ist bei Android nicht möglich, weil der *Paketmanager* bei der Installation die Signatur abfragt und ohne diese den Vorgang abbricht. Die Anwendungen werden dabei mit einem vom Entwickler selbsterstellten Zertifikat signiert [38].

Seit der Android-Version 4.2 existiert zusätzlich eine optionale Anwendungsüberprüfung, die vor der Installation einer Anwendung stattfindet. Hat der Nutzer diese Überprüfung eingeschaltet, wird er bei eventuell bösartigen Anwendungen benachrichtigt. Handelt es sich um eine sicherheitskritische und als bösartig identifizierte Anwendung, kann die Installation dieser sogar geblockt werden [38].

3.3.3. Zusätzliche Sicherheitsmechanismen und -werkzeuge

Für die Android-Plattform existiert eine Vielzahl an Sicherheitswerkzeugen von Drittanbietern und Sicherheitsmechanismen, die das Betriebssystem selbst bietet. Dieser Abschnitt wird nun einen kurzen Einblick in die Menge der Möglichkeiten zur Steigerung der Sicherheit geben. Hierfür werden zunächst die von Android zur Verfügung gestellten Mechanismen betrachtet, bevor zusätzliche Sicherheitswerkzeuge von Dritten vorgestellt und untersucht werden.

Möglichkeiten des Android-Betriebssystems:

Wie bereits erwähnt bietet Android neben seiner speziellen Sicherheitsarchitektur ebenfalls diverse Mechanismen, die die Sicherheit des Gerätes und der Daten gewährleisten sollen.

Zu diesen Sicherheitsmechanismen gehört zum Beispiel die zusätzliche Authentifizierung durch ein Passwort, PIN, Muster, Gesichts- oder Spracherkennung in Verbindung mit dem Sperrbildschirm. Dieser zusätzliche Mechanismus kann unerwünschte Zugriffe auf das Gerät verhindern, falls es bei kurzer oder längerer Abwesenheit unbeobachtet ist. Dabei ist es empfehlenswert, dass der Sperrbildschirm sich automatisch nach einer kurzen Zeit einschaltet.

Ebenso bietet Android eine Geräteverschlüsselung. Dabei wird das gesamte Dateisystem auf einer 128-Bit AES-Basis verschlüsselt, wobei der Schlüssel das Benutzerpasswort des Gerätes ist [38]. Durch die Eingabe dieses Passworts kann das Gerät wieder entschlüsselt werden, sodass bei dem Verlust des Gerätes die Daten nicht in die falschen Hände geraten, sofern es sich nicht im entschlüsselten Zustand befindet.

Um auch in WLAN-Hotspots „sicher“ Datenübertragungen, wie zum Beispiel zum Versenden von E-Mails, durchzuführen, bietet Android die Möglichkeit das Gerät mit einem VPN zu verbinden. Dabei kann der Nutzer unter anderem zwischen den Protokollen *PPTP, L2TP/IPsec* und *IPsec* wählen. Mit Hilfe dieser Protokolle wird ein sicherer *Tunnel* zwischen dem Gerät und dem Ziel-VPN-Gateway aufgebaut, um bei der Datenübertragung die Sicherheitsziele *Vertraulichkeit, Integrität* und *Authentizität* sicherzustellen. Die Verbindung ist dabei jedoch nur so sicher, wie es das Protokoll und die Verschlüsselung zulässt. Dabei sollen VPN-Verbindungen über das Point-to-Point Tunneling Protocol (PPTP) innerhalb eines Tages geknackt werden können (vgl. [45]).

In Bezug auf bösartige oder fehlerhafte Apps bietet das Betriebssystem Android eine besondere Möglichkeit, um solche von dem Gerät zu entfernen, selbst wenn diese eine normale Bedienung des Systems verhindern. Gemeint ist der abgesicherte Modus bei Android, der vergleichbar mit dem abgesicherten Modus von Windows ist. Im abgesicherten Modus sind lediglich die Standard-Apps und Funktionen vorhanden und keinerlei nach-

träglich installierte Anwendungen. Dennoch ist es in diesem Modus möglich, die Problem-Anwendungen vom Gerät zu entfernen. Auch können über diesen Modus Daten gerettet werden, falls das System im normalen Modus nicht mehr ausführbar ist [46].

Sicherheitswerkzeuge durch Drittanbieter:
Ein zusätzliches Werkzeug, das zu der Steigerung der Sicherheit beitragen soll sind Antiviren-Apps. Je nach Anwendung bieten sie ein unterschiedlich großes Spektrum an Sicherheitsfunktionen. Was sie jedoch alle gemeinsam haben, ist die Überprüfung auf Viren bei Anwendungen nach ihrer Installation. Auch das Scannen von Apps und gegebenenfalls von der SD-Karte kann mit ihnen zu beliebigen Zeitpunkten durchgeführt werden. Zusätzliche Funktionalitäten können das Überprüfen von Nachrichten auf Phishing-Angriffe sein oder allgemein SMS- und Anruffilter. Doch auch Anti-Diebstahl-Funktionen werden häufig geboten, bei denen zum Beispiel der Standort des Gerätes geortet werden kann. Sperrfunktionen sind bei diversen Antiviren-Apps ebenfalls vorhanden, die das Absichern von bestimmten Anwendungen durch ein Passwort ermöglichen. Dies ist besonders nützlich, um sicherheitskritische Anwendungen wie *Google Play* von Android vor unerlaubten Zugriffen zu schützen und so zu verhindern, dass Malware durch Dritte unbemerkt heruntergeladen wird. Häufig bieten Antiviren-Apps auch den Einsatz von Firewalls an. Hierfür benötigt die Anwendung jedoch Root-Rechte, die das Berechtigungssystem aushebeln und es der Anwendung ermöglichen, auf eigentlich geschützte Bereiche zuzugreifen. Handelt es sich bei der Antiviren-App um eine Fake-Antiviren-App, ist ihren Schadfunktionen keine Grenze gesetzt. Dies ist auch mit ein Grund, warum das sogenannte *Rooten* des Geräts und die Zuweisung von Root-Rechten an Anwendungen möglichst kritisch betrachtet werden sollte.

Trotz der Risiken des Rootens, wie zum Beispiel dem Zerstören des Gerätes durch das Übertakten der CPU (vgl. [47]) oder die Zuweisung von Root-Rechten an Malware, kann es ebenso gewisse Vorteile in Bezug auf die Sicherheit eines Gerätes haben. Wie bereits erwähnt können mit Root-Rechten Firewalls genutzt werden. Diese überwachen den Zugriff auf bestimmte Netzdienste und können somit beispielsweise die Infektion des Systems durch einen Wurm oder das Eindringen eines Angreifers verhindern. Ebenso können auf gerooteten Geräten spezielle *Custom-ROMs* aufgespielt werden. Bei diesen Custom-ROMs handelt es sich um alternative Android-Betriebssysteme, die auf Grundlage des freizugänglichen Source-Codes von Android oder einer originalen Firmware eines Android-Gerätes entwickelt werden. Diese bieten insofern eine Steigerung der Sicherheit, weil sie auch jene Android-Geräte mit Sicherheitsupdates versorgen, bei denen die Hersteller Updates auf neuere Android-Versionen nicht mehr unterstützen. Darum sollten gerade Nutzer von Modellen, die nur ältere Android-Versionen unterstützen, den Einsatz von Custom-ROMs und das damit verbundene Rooten in Betracht ziehen [48]. Auch die

Möglichkeit der Trennung von privaten und geschäftlichen Daten und Anwendungen kann mit einem Custom-ROM realisiert werden (siehe zum Beispiel [49]).

Ein weiteres Sicherheitswerkzeug können spezielle Monitoring-Anwendung darstellen. Damit sind Anwendungen gemeint, die die Nutzung von bestimmten Ressourcen, wie CPU, Speicher oder Datenvolumen, überwachen. Mit ihnen kann der Nutzer sehen, welche Anwendungen laufen und ob sie im Hintergrund arbeiten und möglicherweise sogar Daten über das Internet übertragen. In gewissem Maß kann eine solche Überwachung auch über bestimmte Funktionen des Betriebssystems erfolgen, jedoch bieten darauf spezialisierte Anwendungen meist einen übersichtlicheren und detaillierteren Überblick.

Um neben der Geräteverschlüsselung von Android einzelne Daten zu verschlüsseln und abzusichern, gibt es diverse Verschlüsselungsanwendungen, die diese Möglichkeit bieten. Auch sollte im Hinblick auf Verschlüsselung auf E-Mail-Anwendungen zurückgegriffen werden, die eine Verschlüsselung der Nachrichten ermöglichen. Anwendungen zur Verschlüsselung von Nachrichten gibt es ebenfalls für SMS (siehe [51]).

In Bezug auf das BYOD-Konzept existieren für Android sogenannte *Mobile Device Management*-Anwendungen. Sie bieten meist einen großen Umfang an Funktionen zur Verwaltung der Geräte und um deren Daten zu schützen. Zum Beispiel bieten einige die Ortung und Sperrung von Geräten, die Fernlöschung der Daten, Datensicherungen oder setzen bestimmte Sicherheitsrichtlinien durch, wie beispielsweise Passwortrichtlinien. Auch können einige die Konfiguration von Geräteeinstellungen *over-the-air* durchführen. Ebenfalls werden häufig eigene *App-Kataloge* geboten, bei denen nach dem Whitelist-Prinzip nur sichere und geprüfte Anwendungen angeboten werden [50]. Solche Anwendungen sind jedoch eher für den Einsatz in Unternehmen gedacht, bei denen eine größere Menge an Geräten verwaltet werden muss. Für private Zwecke reichen Antiviren-Lösungen, die ähnliche Funktionalitäten bieten.

3.3.4. Entwicklung der Sicherheit

Android ist ein Betriebssystem, welches im Laufe seines Daseins häufig überarbeitet wurde. Diese Überarbeitungen brachten nicht selten diverse Verbesserungen des Systems mit sich, die sich auf dessen Sicherheitsmechanismen bezogen. Um die Entwicklung des Systems im Hinblick auf dessen Sicherheit zu betrachten, folgt nun eine Sammlung diverser sicherheitsspezifischer Änderungen und Erweiterungen, die in bestimmten Versionen vorgefunden werden konnten. Hierbei sind lediglich die Versionen vertreten, bei denen solche Änderungen festgestellt werden konnten. Der Fokus bei der Recherche nach solchen Sicherheitsverbesserungen lag primär auf den *Memory Management Security Enhancements* des *Android Security Overview* auf `source.android.com` sowie auf den Angaben zu den jeweiligen Versionen, die auf der Seite `developer.android.com` gefunden werden konnten.

Android-Version	**Sicherheitsspezifische Änderungen**
1.5 *„Cupcake“*	• Einsatz von Canaries durch *ProPolice*, um Buffer-Overflows zu verhindern [38]. • Verwendung der *safe_iop*-Bibliothek, um Integer-Overflows zu verhindern [38]. • Erweiterungen des OpenBSD Memory Allocator (Speicherverwalter) *dlmalloc* um die potentielle *double free()*-Sicherheitslücke zu schließenc[38] . • Verwendung der OpenBSD *calloc*-Funktion, um Integer-Overflows zu verhindern [38].
1.6 *„Donut“*	• Möglichkeit zur Konfiguration und Verbindung mit einem Virtual Private Network [52].
2.2.x *„Froyo“*	• Bereitstellung von Device Policy Management APIs zur Erstellung von Geräte-Administrator-Anwendungen [53]. • Möglichkeit einen numerischen PIN oder ein alphanumerisches Passwort zum Entsperren des Gerätes zu nutzen [53]. • Möglichkeit zur Durchsetzung von Passwortrichtlinien durch einen Geräte-Administrator [53]. • Möglichkeit durch einen Geräte-Administrator das Gerät aus der Ferne auf Werkzustand zurück zu setzen [53].
2.3.x *„Gingerbread“*	• Schutzmaßnahmen gegen Formatstring-Angriffe [38]. • Nutzung des NX-Bit der ARM-Architektur [38].
3.x *„Honeycomb“*	• Möglichkeit sämtliche Nutzerdaten zu verschlüsseln [54].
4.0.x *„Ice Cream Sandwich“*	• Erschweren der Ausnutzung von Sicherheitslücken im System durch Zufallsgestaltung des Adressraumaufbaus (Address Space Layout Randomization) [38]. • Entsperren des Gerätes über Gesichtserkennung (bietet jedoch keine große Sicherheit) [55].

Tabelle 1: Android-Versionen und ihre Sicherheitserweiterungen - Teil 1

Android-Version	**Sicherheitsspezifische Änderungen**
4.1.x *„Jelly Bean“*	• Unterstützung von *Position Independent Executable* (PIE), einer Technik zur Zufallsgestaltung des Adressraums [38][56]. • RELRO-Mechanismus, zur Schadensbegrenzung bei Speicherkorruption [38] [60] [61]. • Sicherheitserweiterungen, um ungewollte Zugriffe auf bestimmte Informationsquellen des Systems zu verhindern, die ein Angreifer nutzen könnte, um Schwachstellen beim Kernel zu finden und diese auszunutzen [38] [61].
4.2.x *„Jelly Bean“*	• Unterstützung von Benutzerkonten (nur bei Tablets) [35]. • Unterstützung einer App-Überprüfung vor der Installation von Apps, die bei möglicherweise schädlichen Apps den Nutzer alarmiert oder bei besonders bösartigen Apps die Installation sogar blockiert [57]. • Benachrichtigung des Nutzers, wenn eine Anwendung Premium-SMS versenden will, und die Möglichkeit, diesen Vorgang zu blockieren [57]. • Unterstützung von *always-on VPN*, sodass Anwendungen erst Zugriff auf ein bestimmtes Netz haben, wenn eine VPN-Verbindung aufgebaut ist, um Daten nicht durch andere Netze zu schicken [57]. • Benachrichtigung des Nutzers, wenn eine Anwendung Premium-SMS versenden will, und die Möglichkeit, diesen Vorgang zu blockieren [57]. • (weitere siehe [57])
4.3.x *„Jelly Bean“*	• Unterstützung von eingeschränkten Benutzerkonten (zum Beispiel für Kinder) [35]. • Verbesserung der Android Sandbox durch Verwendung des *Mandatory-Access-Control*-Systems SELinux [58]. • Verkleinerung der Root-Angriffsfläche durch das Entfernen aller setuid/setguid-Programme [58]. • Keychain API, die Benutzern erlaubt, Anwendungen den Zugriff auf den System-Key-Store und den dort befindlichen Anmeldeinformationen zu gewähren [58] [59]. • (weitere siehe [58])

Tabelle 2: Android-Versionen und ihre Sicherheitserweiterungen - Teil 2

Wie aus den beiden oberen Tabellen 1 und 2 zu entnehmen ist, wurden besonders in den beiden letzteren Versionen (4.2 und 4.3) viele neue Sicherheitserweiterungen hinzugefügt. Zurückzuführen ist dies möglicherweise auf die steigende Relevanz des Themas *Sicherheit* im Bereich der Informationstechnik, welche durch die Spionageangriffe der Geheimdienste

in diesem Jahr vermutlich noch weiter gewachsen ist. Welche Sicherheitserweiterungen die Version 4.4 (*KitKat*) aufweist, wird kurz am Ende dieser Bachelorarbeit im Fazit genannt, da diese Version erst gegen Ende der Bearbeitungszeit dieser Arbeit erschien.

3.4. Sicherheitsstand anderer mobiler Betriebssysteme

Um die von Android bereitgestellte Sicherheit beurteilen und bewerten zu können, werden im Folgenden die beiden alternativen mobilen Betriebssysteme *iOS* von Apple und *Windows Phone* von Microsoft zusammen mit ihren Sicherheitsmechanismen vorgestellt. Auf Grundlage der gesammelten Sicherheitsmerkmale werden die drei Betriebssysteme vergleichend gegenüber gestellt, um auf diese Weise das Sicherheitspotenzial des Android-Betriebssystems beurteilen zu können.

3.4.1. Überblick

Der Markt der mobilen Betriebssysteme umfasst mehrere verschiedene Anbieter. Neben *Android, iOS* und *Windows Phone* existieren ebenfalls *Symbian, Blackberry OS, Bada, Firefox OS, Ubuntu for Phones* und diverse andere. Um den Fokus dieser Arbeit jedoch etwas einzugrenzen, werden lediglich die drei Betriebssysteme *Android, iOS und Windows Phone* betrachtet.

iOS Sicherheitsmechanismen

Die von Apple entwickelte Plattform *iOS* spielt auf dem Markt der Smartphones und Tablet-PCs eine wichtige Rolle. Es ist das Betriebssystem der *iPhones* und *iPads*, welche lange Zeit eine Art Statussymbol in unserer Gesellschaft darstellten [64]. Doch neben ihrer Beliebtheit bieten Apples Geräte mit iOS gleichermaßen diverse Sicherheitsmechanismen, die nun kurz und eher oberflächlich vorgestellt werden. Diesbezüglich nennt Apple in ihrem Bericht *iOS Security* folgende Sicherheitsmerkmale der iOS-System-Architektur:

- ***Secure Boot Chain***
  Beim Boot-Vorgang werden sämtliche Komponenten, wie Bootloader, Kernel, Treiber und Baseband-Firmware, anhand der kryptographischen Signatur Apples überprüft. Sie soll die Integrität der Komponenten prüfen und beim Fehlschlagen den Boot-Vorgang anhalten und in den Recovery-Modus wechseln. Die Kette der Überprüfungen startet bei dem Boot-ROM (*Root of Trust*). Der Code des Boot-ROM ist unveränderbar und wird bei der Chip-Erzeugung festgelegt. Er beinhaltet den Public Key von Apples Root CA (*Certificate Authority*). Dieser wird benutzt um den ersten Schritt der Überprüfung der Signaturen vorzunehmen. Sollte jedoch bereits die erste Überprüfung fehlschlagen, wird das Gerät in den sogenannten DFU

(Device Firmware Upgrade)-Modus versetzt. Sowohl beim Recovery- als auch beim DFU-Modus muss das Gerät über USB mit iTunes verbunden werden, um es in den Werkszustand zurückzusetzen [65] [66].

- ***System Software Personalization***
  Um zu verhindern, dass zum Beispiel auf ein Gerät eine ältere Softwareversion aufgespielt wird, hat Apple einen besonderen Mechanismus entwickelt. Dabei werden während der Installation oder des Upgrades von iOS eine Liste von kryptographischen Kennzahlen, eine Nonce und die Geräte-ID (ECID) an den Signatur-Server `gs.apple.com` geschickt. Anhand dieser Angaben wird daraufhin überprüft, ob es sich um eine Installation einer autorisierten Systemsoftware handelt und ob eine Server-Antwort nicht von einem Angreifer gespeichert wurde, um das Gerät später auf eine ältere Version zurückzusetzen [65].

- ***App Code Signing***
  Um sicherzustellen, dass alle Apps von einer bekannten und vertrauenswürdigen Quelle stammen und nicht manipuliert wurden, wird der ausführbare Code einer App mittels eines von Apple bereitgestellten Zertifikats signiert. Third-Party-Apps signieren ihre Apps mit einem Zertifikat von dem sogenannten *iOS Developer Program*, bei dem die Entwickler ihre echte Identität hinterlegen. Built-In-Anwendungen werden direkt von Apple signiert [65].

- ***Runtime Process Security***
  Alle Third-Party-Apps werden in einer Sandbox ausgeführt, um den Zugriff auf andere Anwendungsdaten einzuschränken. Dabei hat jede App ein eindeutiges Homeverzeichnis, in dem ihre Daten liegen. Die Kommunikation mit anderen Apps kann lediglich über APIs und Services erfolgen, die von iOS bereitgestellt werden. Systemdateien und -ressourcen werden von den Built-in-Anwendungen und den Apps von Drittanbietern abgeschirmt, indem diese als der nicht-privilegierte Nutzer *mobile* ausgeführt werden. Um einer Anwendung Zugriff auf Nutzerdaten zu ermöglichen, können ihr bestimmte Berechtigungen zugewiesen werden, die ansonsten Administratorrechte benötigen würden. Diese Berechtigungen können nachträglich nicht mehr geändert werden. Da auf diese Weise keine Administratorrechte benötigt werden, kann auch die Gefahr, dass eine kompromittierte App Zugriff auf das System erlangt, reduziert werden. Neben diesen Sicherheitsmechanismen wird in iOS ebenfalls ASLR (*Address Space Layout Randomization*) angewendet um Softwarefehler nicht so leicht erfolgreich ausnutzen zu können. Auch der Gebrauch der Never-Execute-Funktion von ARM soll zusätzliche Sicherheit bieten, der Teile des Flash-Speichers als nicht-ausführbar markiert und somit verhindern soll, dass nicht-autorisierter Code auf dem Gerät ausgeführt wird [65] [67].

Weitere Sicherheitsfunktionen von Apples iOS sind unter anderem die Dateiverschlüsselung aller Daten und der Zugangscode zum Entsperren des Gerätes, der die Basis der Schlüsselhierarchie (*Keychain*) darstellt. Außerdem bietet iOS die Möglichkeit eines *Remote Wipe* bei zu vielen Falscheingaben des Zugangscodes sowie die Klassen-Zuordnung von Dateien, bei denen die Klassen Richtlinien definieren, wann Dateien zugänglich sind und auf welche Weise sie geschützt werden. Ebenso verfügt es über ein Built-in-MDM-Framework, Built-in-VPN-Client und *Per App VPN*. Des Weiteren wird *S/MIME*-E-Mail, SSL/TLS bei Internetanwendungen, wie Safari, Kalender oder Mail, und seit iOS7 *Touch ID* unterstützt. Dabei handelt es sich bei *Touch ID* um einen Fingerabdruck-Sensor zum schnellen Entsperren des Gerätes. Gleichermaßen bedeutend für die Sicherheit ist die neue Auto-Update-Funktion, die Anwendungen automatisch aktualisiert und das *App Configuration Management*, das das Erstellen von Black- und Whitelists von Anwendungen zulässt [65] [66].

Windows Phone Sicherheitsmechanismen

Nachdem die Sicherheitsmechanismen von iOS vorgestellt worden sind, folgt nun eine kurze Betrachtung der gebotenen Mechanismen bei dem Betriebssystem *Windows Phone*. Dabei werden in erster Linie die Sicherheitsmerkmale aus dem *Windows Phone 8 Security Guide* für den Überblick herangezogen.

- ***Trusted Boot***
  Es werden beim Boot-Vorgang alle Binärdateien überprüft, beginnend mit dem ersten Boot-Loader, auf eine Signatur von einer vertrauenswürdigen Instanz. Auch sie baut auf einer *Root of Trust* auf, die während der Herstellung in das Gerät eingefügt wurde [68].

- ***Code and App Signing***
  Der gesamte Code des Windows Phone Betriebssystems sowie OEM-Treiber und -Anwendungen sind von Microsoft signiert. Auch Third-Party-Anwendungen müssen geeignet signiert sein, um ausgeführt werden zu können. Dabei können Apps lediglich aus dem *Windows Phone Store* heruntergeladen werden oder von Unternehmensseiten, die *line-of-business Apps* anbieten und mit Enterprise-Zertifikaten signiert sind [68].

- ***Chambers and Capabilities***
  Jede App läuft in ihrer eigenen isolierten *Chamber*, für welche bestimmte Sicherheitsrichtlinien definiert sind. Die Sicherheitsrichtlinien einer *Chamber* definiert wiederum die *Capabilities* des Betriebssystems, die von dem Prozess in dieser *Chamber* genutzt werden können. Zu diesen *Capabilities* gehören zum Beispiel Kamera-

und Mikrofon-Funktionen, Netzzugriff und geografische Aufenthaltsinformationen. Durch dieses Konzept sind Apps voneinander isoliert und können nicht auf die Daten anderer Apps zugreifen [68].

Neben diesen Sicherheitsmerkmalen der Systemarchitektur von Windows Phone existieren noch weitere Mechanismen zur Steigerung der Sicherheit des Gerätes und dessen Daten. Beispielsweise lässt sich auch hier eine Gerätesperrung mit Passwortabfrage nutzen, bei der nach einer bestimmten Anzahl von Fehlversuchen die Daten vom Gerät gelöscht werden. Bei einem Geräteverlust oder -diebstahl ist es möglich das Gerät zu orten und um unberechtigte Zugriffe auf diese zu verhindern, lassen sich die Daten aus der Ferne löschen. Für den Datenverkehr zwischen Gerät und unternehmenseigenen Mail-Server kann eine SSL-Verschlüsselung verwendet werden. Um Sicherheitsrichtlinien eines Unternehmens auf dem Gerät durchzusetzen, können *Exchange ActiveSync (EAS)*-Richtlinien verwendet werden, die umzusetzen sind, wenn sich ein Gerät mit einem Exchange-Server verbinden will. Mit ihnen lassen sich zum Beispiel Passwortlänge und -komplexität festlegen. Benutzerkonten werden bei Windows Phone lediglich in Form der sogenannten *Kinderecke* unterstützt, die bestimmte Zugriffseinschränkungen auf Daten und Anwendungen vornimmt [68].

3.4.2. Vergleich mit Android

Um die betrachteten Betriebssysteme miteinander vergleichen und somit die Sicherheit von Android in einem gewissen Maß beurteilen zu können, werden bestimmte Merkmale benötigt anhand dieser sie sich gegenüber gestellt werden können. Für diesen Zweck werden einige von den der ENISA aufgestellten Maßnahmen und Mechanismen aus Kapitel 3.2 herangezogen, die die zehn bedeutendsten Gefahren* bei Smartphones und Tablet-PCs verhindern sollen. Ebenfalls werden diverse Maßnahmen aus Kapitel 2.2 betrachtet, die für das BYOD-Konzept berücksichtigt werden sollten.

Diese Auswahl an Merkmalen wird für eine prinzipielle Beurteilung der gebotenen Sicherheit der Betriebssysteme herangezogen. Dabei werden insbesondere die Sicherheitsmerkmale betrachtet, die in dieser Arbeit eine gehobenere Rolle spielen.

Die nachfolgende Tabelle 3 zeigt die Gegenüberstellung der drei Betriebssysteme zu bestimmten Sicherheitsmerkmalen. Für eine ausführlichere Darstellung kann auf das Kapitel *Betrachtung der Sicherheitsmerkmale* im Anhang zurückgegriffen werden, welches die Gegenüberstellung in Textform vornimmt.

*Nach Angaben der European Network and Information Security Agency

Mechanismus	**Android**	**iOS**	**Windows Phone**
Datensicherungen	Ja	Ja	Ja
Gerätesperrung mit Passwortabfrage nach gewisser Inaktivität	Ja	Ja	Ja
Automatische Löschung der Daten bei wiederholter Falscheingabe des Passwortes	Nein	Ja	Ja
Möglichkeit Sicherheitsrichtlinien aufzustellen und durchzusetzen	Ja	Ja	Ja
Verschlüsselung des Speichers	Ja, internen Speicher & SD-Karte	Ja, internen Speicher	Ja, *nur* intern
Remote Wipe	Ja	Ja	Ja
Whitelists für geeignete Anwendungen führen	Nein*	Nein*	Nein*
Verschlüsselter und authentifizierter E-Mail-Verkehr	Ja	Ja	Nein
VPN-Client	Ja	Ja	Nein
Datenseparation	Nein*	Nein*	Nein*
Benutzerkonten	Ja, nur auf Tablet-PCs und diversen Smartphones	Nein	Ja, nur in beschränkter Form (*Kinderecke*)
Over-The-Air Updates des Betriebssystems	Ja	Ja	Ja

(Nein = nur mit zusätzlicher Software von Drittanbietern realisierbar.)*

Tabelle 3: Gegenüberstellung der Sicherheitsmechanismen der Betriebssysteme

Die Gegenüberstellung zeigt, dass sich die Betriebssysteme bei fünf Merkmalen unterscheiden. Während sowohl bei iOS als auch bei Windows Phone die Daten des Gerätes automatisch gelöscht werden können, sobald der Entsperrcode zu häufig falsch eingegeben wurde, existiert diese Funktionalität bei Android nicht. Da oft nur vierstellige PINs genutzt werden, um das Handy schneller entsperren zu können, kann ein Angreifer bei Android-Geräten daher so lange Zahlenkombinationen probieren, bis er die vier Zahlen richtig errät. Lediglich ein Timeout nach mehreren Versuchen, der 30 Sekunden andauert, zögert das Erraten des Entsperrcodes hinaus.

Während Windows Phone lediglich den internen Speicher verschlüsseln kann, bietet Android die Möglichkeit sowohl den internen als auch den zusätzlichen Speicher (SD-Karte) zu verschlüsseln. Dies ist besonders nützlich, da viele Anwendungen ihre Daten ebenfalls auf der SD-Karte speichern und diese von potentiellen Angreifern ebenfalls leicht entfernt werden kann. Auf diese Weise wird einem Dieb der SD-Karte zumindest der Zugriff auf die Daten erschwert, sofern es sich um eine sichere Verschlüsselung handelt. Da beim iPhone und iPad keine Speichererweiterung durch SD-Karten vorgesehen ist, reicht bei iOS die Verschlüsselung des internen Speichers.

Ein weiteres wichtiges Sicherheitsmerkmal, welches besonders für den geschäftlichen Einsatz des Gerätes relevant ist, ist die Möglichkeit, eine Verschlüsselung und Authentifizierung bei E-Mails nutzen zu können. Android und iOS stellen diese Funktionalität mit ihren Standard-Clients zur Verfügung, lediglich Windows Phone kann dies standardmäßig nicht bieten. Dasselbe gilt für VPN-Funktionalitäten. Nur Android und iOS unterstützen die Verbindung mit einem VPN, sodass sich Nutzer sogar über den built-in VPN-Client und ohne Apps von Drittanbietern mit einem VPN verbinden können.

Weil die Trennung von privaten und geschäftlichen Daten im Hinblick auf die geschäftliche Nutzung von Geräten eine der wichtigsten Anforderungen ist, wurde als weiteres Merkmal die Unterstützung von Benutzerkonten gewählt. Diese Eigenschaft kann keines der drei Betriebssysteme wirklich aufweisen, wobei Android immerhin bei Tablet-PCs Benutzerkonten unterstützt. Die *Kinderecke* von Windows Phone und der Gästemodus bei diversen Android-Geräten ist nur im entferntesten Sinn ein zusätzliches Benutzerkonto. Hierbei werden lediglich Einschränkungen auf den Zugriff bestimmter Daten und Anwendungen vorgenommen und kein eigenes Benutzerprofil mit eigenen Daten und Anwendungen geboten. Um bei Smartphones eine vollständige Trennung von Daten vorzunehmen, müssen daher Lösungen von Drittanbietern genutzt werden.

Nach dieser prinzipiellen Betrachtung bestimmter Sicherheitsmerkmale lässt sich erkennen, dass Android im Vergleich zu iOS und Windows Phone keine großen Defizite aufweist. Lediglich den automatischen Löschvorgang nach einer bestimmten Anzahl von Fehlversuchen kann Android im Gegensatz zu iOS und Windows Phone nicht bieten. Dieses

Kriterium ist jedoch nur von Bedeutung, wenn das Gerät mit einer einfachen PIN oder Muster gesperrt ist. Bei der Verwendung eines komplexen und längeren Passworts verliert es wiederum an Bedeutung, da dort das Erraten nicht mehr in einer hinnehmbaren Zeit möglich ist (siehe [86]). Wichtige Eigenschaften wie zum Beispiel das Signieren und Verschlüsseln von E-Mails sowie die Unterstützung von VPN sind auch unter Android gegeben und bieten eine solide Grundlage für die Sicherheit sensibler Daten.

4. Android im betrieblichen Umfeld

Dieses Kapitel befasst sich im Rahmen des BYOD-Konzepts mit der Einsatztauglichkeit von Android-Geräten im betrieblichen Umfeld. Dafür werden zunächst bestimmte Anforderungen für die Umsetzung von *BYOD* mit Smartphones und Tablet-PCs aufgestellt, die für eine spätere Bewertung von speziellen Lösungsansätzen herangezogen werden. Bevor jedoch die Lösungsansätze sowie deren Bewertung vorgestellt werden, wird auf diverse Herausforderungen eingegangen, die *BYOD*, insbesondere in Verbindung mit Android-Geräten, mit sich bringt.

4.1. Anforderungen für eine sichere Nutzung

Um das Konzept *BYOD* in einem Unternehmen umzusetzen, sollten Anforderungen aufgestellt werden. Diese können dafür sorgen, dass das zu realisierende Projekt den Zweck erfüllt, für den es angedacht war. Insbesondere bei der Einführung von *BYOD* muss der Aspekt *Sicherheit* im Vordergrund der Planung stehen. Denn neben der Sicherheit sensibler Geschäftsdaten auf den mobilen Geräten könnte auch die gesamte Unternehmensinfrastruktur gefährdet werden.

Für die Aufstellung allgemeiner Anforderungen wird in dieser Bachelorarbeit auf die Dokumente der *Bitkom* (siehe [21]) und des *BSI* (siehe [87]) zum Thema *BYOD* zurückgegriffen. Um einen Bezug zu einem reellen Fallbeispiel zu bekommen, werden ebenfalls diverse Anforderungen eines deutschen Automobilherstellers genannt und in der Bewertung der Lösungsansätze berücksichtigt. Das Unternehmen plante in einem seiner Werke, neben dem Einsatz von Geschäftssmartphones den Mitarbeitern die Möglichket zu bieten, ihre privaten Geräte für geschäftliche Zwecke einsetzen zu können. Im persönlichen Gespräch konnten die hierfür aufgestellten Anforderungen für die Umsetzung von *BYOD* erfasst werden.

Die nachfolgenden Anforderungen an eine BYOD-Lösung werden in *funktionale Anforderungen* und *nicht-funktionale Anforderungen* unterteilt. Unter funktionalen Anforderungen versteht man all jene Anforderungen, die die Fähigkeiten beziehungsweise Funktionalitäten des Systems beschreiben [88]. Nicht-funktionale Anforderungen beschreiben hingegen, *wie* das System arbeiten soll. Hierzu gehören beispielsweise Anforderungen an die Ergonomie sowie Kompatibilitätsanforderungen [89].

4.1.1. Funktionale Anforderungen

Aus den Dokumenten der Bitkom und des BSI konnten verschiedene funktionale Anforderungen abgeleitet werden, die für eine BYOD-Lösung relevant sein könnten. Zuvor werden jedoch die vom Automobilhersteller aufgestellten Anforderungen genannt, die bereits viele der abgeleiteten Anforderungen abdecken.

Die speziellen funktionalen Anforderungen des Automobilherstellers sind dabei folgende:

- **Datentrennung**
  Das System ist zuständig für eine klare Trennung zwischen den privaten und den geschäftlichen Daten und Anwendungen auf dem Gerät.

- **Passwortschutz für Geschäftsdaten**
  Der Zugriff auf Geschäftsdaten soll durch ein Passwort geschützt sein, sodass Dritte nicht ohne Weiteres darauf zugreifen können. Auf diese Weise sollen Daten in bestimmten Bereichen oder Anwendungen vor unbefugtem Zugriff geschützt werden.

- **Passwortrichtlinien**
  Die vom Unternehmen aufgestellten Passwortrichtlinien sollen umsetzbar sein, sodass der Schutz der Daten und Anwendungen über ein sichereres Passwort als eine vierstellige PIN erfolgt. Dabei soll bereits beim Setzen eines neuen Passworts überprüft werden, ob es den Richtlinien des Unternehmens entspricht.

- **Ortung, Sperre und Löschen aus der Ferne**
  Das Unternehmen sowie der Mitarbeiter selbst sollen in der Lage sein, beim Verlust oder Diebstahl des Geräts dieses aus der Ferne zu orten und zu sperren oder gegebenenfalls die gesamten Daten darauf zu löschen.

- **Schutz der Geschäftsdaten bei privatem Backup**
  Bei einem privaten Backup der Daten auf dem Gerät sollen sämtliche Geschäftsdaten ausgeschlossen und nicht mit abgesichert werden.

- **Schutz von verschlüsselten und vertraulichen E-Mails**
  Der Automobilhersteller fordert explizit, dass verschlüsselte Geschäfts-Mails auf den privaten Smartphones und Tablet-PCs nicht entschlüsselt werden können. Um solche vertraulichen E-Mails zu entschlüsseln, sollen die Mitarbeiter ihre Desktop-PCs nutzen.

Dies waren zunächst die funktionalen Anforderungen, die das Beispielunternehmen für die Einführung von *BYOD* in ihrem Unternehmen aufgestellt hat. Aus den hierfür herangezogenen Berichten der Bitkom und des BSI zu diesem Thema können jedoch noch

weitere, allgemeine Anforderungen abgeleitet werden, die ebenfalls von einem Unternehmen gefordert werden sollten. Zu diesen weiteren Anforderungen gehören folgende:

- **Whitelists beziehungsweise Blacklists für Anwendungen**
  Um die Gefahr der Installation bösartiger Anwendungen zu reduzieren, soll das Unternehmen in Form von Whitelists beziehungsweise Blacklists festlegen können, welche Anwendungen für die Geräte erlaubt beziehungsweise verboten sind [87].

- **Verschlüsselte Verbindungen**
  Die Verbindungen zwischen Gerät und Unternehmen sollen durch eine Verschlüsselung abgesichert werden, um zu verhindern, dass Unbefugte diese abhören können [87].

4.1.2. Nicht-funktionale Anforderungen

Bei den nicht-funktionalen Anforderungen stellte der Automobilhersteller lediglich Anforderungen an die Benutzbarkeit, sodass die BYOD-Lösung intuitiv einsetzbar sein soll. Dies ist gefordert, weil das Unternehmen aus Kostengründen den Mitarbeitern keine zusätzliche Unterstützung zu der BYOD-Lösung bereitstellen will.

Als weitere nicht-funktionale Anforderungen wurden folgende aufgestellt:

- **Android-Version**
  Die Anwendung der BYOD-Lösung muss auch zu älteren Android-Versionen kompatibel sein. Sie soll mindestens auf den 2.3.x-Versionen laufen, da diese die meistverbreiteten Versionen sind [90].

- **Keine Root-Rechte**
  Die Anwendung muss auf den Android-Geräten ohne Root-Rechte ausführbar sein, da ansonsten die Garantieansprüche der privaten Geräte erlöschen können.

- **Kompatibilität zu anderen Betriebssystemen**
  Die Anwendung muss auch auf anderen Betriebssystemen ausführbar sein, um neben den Android-Nutzern auch weiteren Nutzern die Möglichkeit zu bieten, ihr privates Gerät geschäftlich zu verwenden. So soll verhindert werden, mehrere Lösungen für die verschiedenen Betriebssysteme einsetzen zu müssen.

4.2. Herausforderungen

Neben den Anforderungen an eine BYOD-Lösung existieren weitere Herausforderungen, die in diesem Zusammenhang berücksichtigt werden sollten. Dazu gehören unter anderem allgemeine Herausforderungen, die bereits bei der privaten und geschäftlichen Nutzung von Notebooks bestanden, und Android-spezifische Herausforderungen.

Wie bereits in Kapitel 2.2.2 erwähnt, ist die strikte Trennung der privaten Daten von den Geschäftsdaten von großer Bedeutung. Ohne diese Trennung kann das Unternehmen zum Beispiel gegen das Telekommunikationsgesetz verstoßen, wenn es bei der Kontrolle der ordnungsgemäßen Erhebung, Verarbeitung und Nutzung von personenbezogenen Daten auch Zugriff auf private Daten des Mitarbeiters hat (siehe Kapitel 2.2.2). Ohne diese Kontrolle kann das Unternehmen jedoch nicht feststellen, ob der Mitarbeiter die Vorgaben für personenbezogene Daten einhält und ob das Unternehmen eventuell gegen das Bundesdatenschutzgesetz verstößt.

Ebenfalls problematisch ist es mit den auf dem Gerät genutzten Softwarelizenzen. Dabei muss sichergestellt werden, dass die Software nicht für einen Anwendungszweck verwendet wird, der gegen die jeweilige Lizenz verstößt (siehe Kapitel 2.2.2).

Herausforderungen, die insbesondere Android mit sich bringt, sind unter anderem der hohe Aufwand, der betrieben werden muss, um die Geräte auf ihre Einsatztauglichkeit zu überprüfen. Eine Besonderheit ist dabei, dass eine Vielzahl an verschiedenen Modellen von unterschiedlichen Anbietern existiert. Diese haben verschiedene Funktionalitäten und verschiedene Android-Versionen. So muss das Unternehmen für jedes Modell, welches im Rahmen von *BYOD* eingesetzt werden soll, genau überprüfen, ob es den Sicherheitsanforderungen entspricht und für die gewählte BYOD-Lösung verwendet werden kann. Dabei spielt ebenfalls eine Rolle, ob das Gerät *gerootet* wurde. Verstößt ein Gerät gegen bestimmte Sicherheitskriterien, sollte der Mitarbeiter dieses nicht geschäftlich nutzen.

Bei Android besteht des Weiteren das Problem, dass Sicherheitspatches und Updates auf eine neuere Version mit eventuell geschlossenen Sicherheitslücken nicht jedes Gerät gleichzeitig oder sofort erreichen. Schlimmstenfalls werden einige Geräte gar nicht mehr mit Updates versorgt. Es ist dabei sowohl vom Gerätemodell als auch von dem jeweiligen Hersteller abhängig, wann und ob das Gerät ein Update erhält. Laut *heise online* ist die Android-Version 2.3 mit einem Marktanteil von knapp 40% die am weitesten verbreitete Version [90]. Die Hersteller versorgen ihre Geräte meist erst nach mehreren Monaten mit den Updates, weil sie zunächst diese an ihre Hardware anpassen müssen. Lediglich Googles Nexus-Geräte bekommen meist nach nur einigen Wochen die Updates bereitgestellt [90]. Diese Eigenschaft sollte stets berücksichtigt werden, da selbst Geräte, die derzeit auf dem

neusten Stand sind, in Zukunft ebenfalls schlecht mit Updates versorgt werden könnten und aus dem Unternehmensnetz ausgeschlossen werden müssten.

4.3. Überblick diverser Lösungsansätze

Das *BSI* definiert in seinem *Überblickspapier* zum Thema *BYOD* (siehe [87]) drei verschiedene Lösungsansätze. Zum einen stellt es die Datentrennung und -absicherung über *Containerisierung* auf Anwendungsebene sowie die Verwendung von *Thin Clients* beziehungsweise serverbasierten Lösungsansätzen vor, bei denen lediglich die Informationen auf dem Gerät dargestellt, jedoch nicht gespeichert werden. Zum anderen nennt es den Lösungsansatz der Virtualisierung, bei der die Trennung des privaten und geschäftlichen Bereichs auf Betriebssystemebene stattfindet.

Bei diesen Arten von Lösungsansätzen handelt es sich um solche, die bereits für den Anwendungsbereich *BYOD* in Verbindung mit Notebooks eingesetzt werden konnten. Es wurden auch Android-Lösungen für diese drei Arten gefunden, die derzeit erhältlich sind. Hierfür werden im Folgenden drei Beispiellösungen kurz vorgestellt, um einen Eindruck solcher Lösungsansätze zu erhalten.

Containerlösung auf Anwendungsebene

Der erste mögliche Lösungsansatz ist die Verwendung einer Containeranwendung, die die dienstlichen Daten und Zugänge verwaltet und somit eine Trennung der privaten und geschäftlichen Daten und Anwendungen vornimmt. Ein Beispiel für eine solche Lösung ist die App *Good for Enterprise* von *Good Technology* [91]. Sie bietet in einer Anwendung eine Art verschlüsselten Container, der den Zugriff auf E-Mails, Kalender, Dokumente und einen Programmkatalog des Unternehmens erlaubt [92]. Des Weiteren verfügt *Good for Enterprise* über einen eigenen Browser, der einen sicheren Zugang in das Unternehmens-Intranet ermöglicht [93]. Diese Eigenschaften und Funktionalitäten decken bereits einen großen Teil der Anwendungsmöglichkeiten ab, die für die Arbeit mit den mobilen Geräten benötigt wird.

Die Verschlüsselung der Applikations-Sandbox wird von *Good Technology* als *Containerisierung* bezeichnet. Sie soll den Austausch von Daten zwischen Corporate Apps und Consumer Apps verhindern. Lediglich ein sicherer *app-to-app*-Austausch von Daten zwischen *containerisierten* Anwendungen ist möglich, wobei dieser durch eine Verschlüsselung geschützt ist. Damit ein Unternehmen selbst entwickelte Apps sicher nutzen und *containerisieren* kann, bietet *Good Technology* einen speziellen *App Wrapper*. Dieser tauscht die standardmäßigen Systemaufrufe durch equivalente und sichere Aufrufe der *Good Dynamics security libraries* aus [94].

Abbildung 3: App Wrapper[94]

Die *containerisierten* Apps laufen anschließend in ihren eigenen Containern, sodass sie und ihre Daten sicher von anderen Anwendungen und Daten getrennt sind. Es können jedoch nur selbst entwickelte Apps *containerisiert* werden. Werden Business-Apps von Drittanbietern benötigt, können Unternehmen auf den *Good Dynamics Marketplace* (siehe [95]) zurückgreifen. Dieser bietet eine Auswahl verschiedenster *containerisierter* Apps, deren Code bereits überprüft wurde und die somit den Sicherheitsstandards der Plattform entsprechen [96].

Neben der Datentrennung und den zuvor genannten Eigenschaften bietet *Good for Enterprise* ebenfalls eine Reihe von Sicherheitsfunktionalitäten für den Bereich der Administration. Die Aufzählung dieser wird aus dem Dokument *Protect mobile collaboration* (siehe [93]) von *Good Technology* entnommen.

- Schutz der Daten auf dem Gerät und während der Übertragung durch den Einsatz einer FIPS zertifizierten AES-Verschlüsselung
- Fernlöschen und -sperren eines gestohlenen oder verloren gegangenen Geräts
- Sperren diverser Funktionalitäten wie Kamera, WLAN und Bluetooth
- Erzwingung starker Passwörter, indem Passwortrichtlinien des Unternehmens durchgesetzt werden.
- Unterstützung eines firmeneigenen Enterprise-AppStore
- Unterstützung von Firmen- sowie BYOD-Richtlinien
- Beibehaltung der privaten Daten bei einer Fernlöschung
- Unterstützung einer rollenbasierten Administration und einer webbasierten Management-Konsole zur Verwaltung einer Vielzahl von verschiedenen Geräten
- Unterbindung der Copy-and-Paste-Funktionalität, um die Datenübergabe in unsichere Anwendungen zu verhindern

Serverbasierte Lösung

Eine weitere Lösung für eine sichere Verwendung privater mobiler Geräte im Geschäftsumfeld ist *Nubo*. Hierbei handelt es sich um einen *Remote Workspace*, bei dem die Mitarbeiter auf Anwendungen und Daten des Unternehmens über ihre Smartphones und Tablet-PCs zugreifen können, ohne dass sich diese auf dem Gerät befinden. Das Gerät wird demnach lediglich als Anzeige-Medium verwendet, während sich die Daten in dem jeweiligen Datenzentrum des Unternehmens befinden. Diese werden dort in einer extra Android Umgebung ausgeführt und verarbeitet (siehe Abbildung 4) [97].

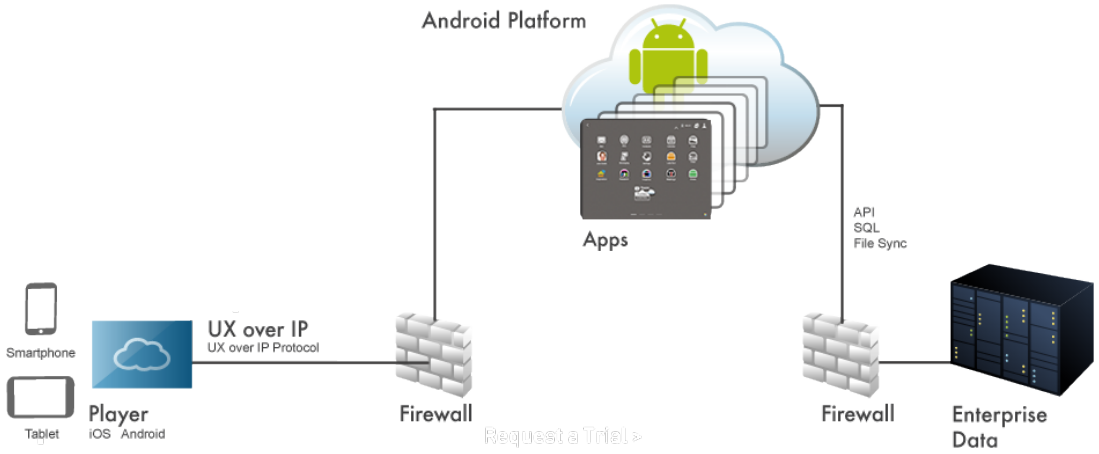

Abbildung 4: Nubo Funktionsweise[97]

Die Kommunikation zwischen dem *Nubo-Player*, der die Display-Funktion übernimmt, und der Android-Plattform auf dem Server findet über Nubos *UX Over IP*-Protokoll statt. Dieses spezielle *Remote-Display*-Protokoll passt die Ausgabe an die jeweilige Display-Größe des Geräts an und erlaubt die Kommunikation mit den geräteigenen Sensoren [97].

Die Daten und Anwendungen der einzelnen Nubo-Nutzer werden nicht miteinander vermischt. Jeder von ihnen arbeitet in einer getrennten Sandbox innerhalb der virtuellen Maschine, wobei ebenfalls der Speicher von dem der anderen Nutzer getrennt ist. Durch den Login des Nutzers wird seine Sandbox automatisch mit seinem eigenen Speicher verbunden, sodass nur er Zugriff auf diese Daten hat [97].

Zusätzliche Eigenschaften bezüglich der Sicherheit bei Nubo sind folgende:

- **Zwei-Faktor-Authentifizierung**
  Für den Aufbau einer Nubo-Session, muss ein Nutzer neben einem zulässigen Passwort auch über ein einzigartiges Security-Token verfügen, um über das Gerät Zugriff auf die Geschäftsdaten zu erlangen. Dieses Token wird auf dem Gerät abgelegt, nachdem es für den Zugriff auf die Unternehmensdaten freigeschaltet worden ist. So lässt sich verhindern, dass unbefugt eine Nubo-Session von einem anderen Gerät aufgebaut wird, falls der Angreifer an das Passwort des Opfers gelangt ist [98].

- **SSL Sicherheit**
  Die gesamte Kommunikation zwischen den Geräten und der Nubo-Plattform findet auf verschlüsseltem Weg statt. Hierfür wird das Verschlüsselungsprotokoll *SSL* verwendet, welches sicherstellen soll, dass selbst in unsicheren WLAN-Netzen eine sichere Verbindung zum Unternehmens-Server besteht [98].

Virtualisierungslösung

Den letzten Lösungsansatz stellt *VMware Horizon Workspace* von *VMware* dar. Hierbei wird auf dem Gerät eine zusätzliche Arbeitsumgebung durch einen virtualisierten Container zur Verfügung gestellt. Dieser Container beinhaltet ein eigenes Betriebssystem mit eigenen Anwendungen, Daten und Richtlinien. Über das zusätzliche Betriebssystem beziehungsweise den Container erhält der Mitarbeiter Zugriff auf die vom Unternehmen freigegebenen Anwendungen und Daten. Dabei werden den Nutzern bestimmte Identitäten zugewiesen, die den Zugriff auf die Unternehmensressourcen und -anwendungen bestimmen, sodass eine anwenderbasierte Zugriffskontrolle stattfindet. Jegliche Unternehmensdaten liegen somit innerhalb des virtualisierten Containers. Auf diese Weise findet eine strikte Trennung der privaten und geschäftlichen Daten statt, die mögliche Datenschutzprobleme verhindert. Dies ermöglicht die Anwenderaktivitäten zu protokollieren, um überprüfen zu können, ob gegen aufgestellte Anforderungen und Richtlinien auf einzelnen Geräten verstoßen wird [99].

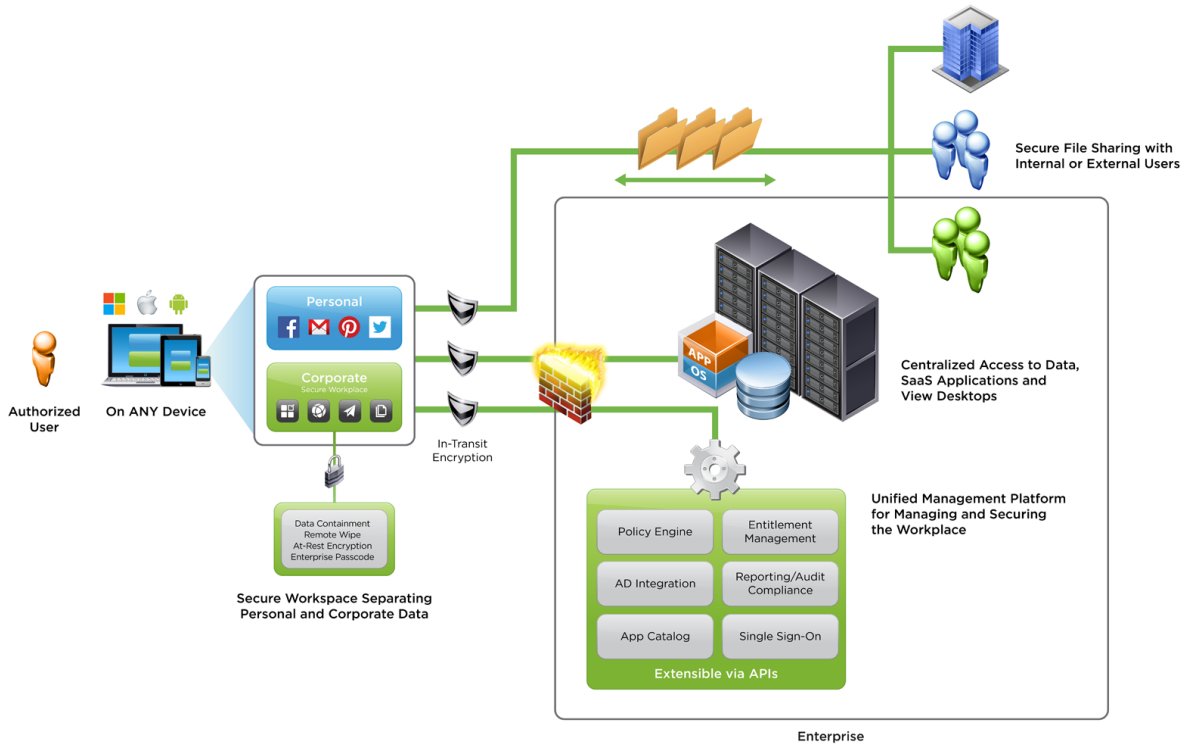

Abbildung 5: VMware Horizon Workspace Funktionsweise [99].

Die obige Abbildung stellt die Funktionsweise von *VMware Horizon Workspace* dar. Dabei ist auf der linken Seite dieser Abbildung zu erkennen, dass die Daten und Anwendungen auf den jeweiligen Geräten des Nutzers in einen *Personal-* und einen *Corporate-*Bereich getrennt werden.

Des Weiteren bietet *VMware Horizon Workspace* eine Vielzahl zusätzlicher Sicherheitsfunktionalitäten, zu denen unter anderem folgende gehören:

- **Detaillierte Richtlinienverwaltung**
  Richtlinien zur Datennutzung können detailliert und gruppenbasiert festgelegt werden. Dies ermöglicht individuellere Zuweisungen von Richtlinien, die bestimmte Kriterien der jeweiligen Benutzerkategorien berücksichtigen. Änderungen von Richtlinien können dabei dynamisch an die Anwender verteilt werden [99].

- **Anwendungsmanagement**
  Es kann ein Anwendungskatalog geführt werden, mit dem sämtliche Klassifizierungen, Veröffentlichungen, Versionierungen und Verteilungen von Anwendungen verwaltet werden können. So können verschiedenen Nutzern anhand ihrer Identität bestimmte Anwendungen zugeteilt werden [99].

- **Verschlüsselung**
  Die gesamte Kommunikation zum Horizon Workspace Server wird durch die Verwendung des Verschlüsselungsprotokolls *SSL* abgesichert. Zusätzlich wird der Inhalt der Anwendung verschlüsselt aufbewahrt. Hierfür wird der *AES*-Algorithmus mit einer Schlüssellänge von 256 Bit verwendet [100].

- **Remote Wipe**
  Beim Verlust oder Diebstahl des Geräts können die Daten per Fernlöschung vom Gerät entfernt werden. Dabei werden jedoch lediglich die Daten der Horizon Workspace Anwendung gelöscht, sobald sich die Anwendung mit dem Server verbindet. Die privaten Daten des Nutzers müssen bei Bedarf zusätzlich auf einem anderen Weg entfernt werden [100].

- **Kennwortabfrage**
  Die Administratoren des Unternehmens können *VMware Horizon Workspace* so einstellen, dass die Nutzer vor der Ausführung ein Passwort eingeben müssen. Das Passwort muss dabei numerisch sein, mit mindestens vier Zahlen. Ebenfalls lässt sich eine automatische Sperrung einstellen, sodass nach einer gewissen Zeit der Inaktivität das Passwort erneut eingegeben werden muss [100].

4.4. Bewertung der Lösungsansätze

Die drei zuvor vorgestellten Lösungsbeispiele werden in diesem Abschnitt anhand der aufgestellten funktionalen und nicht-funktionalen Anforderungen sowie der gesammelten Herausforderungen in Kapitel 4.2 bewertet. Dabei wird insbesondere überprüft, welche Lösung sich für das Beispielunternehmen eignet und ob die derzeit eingesetzte Lösung möglicherweise durch eine andere ersetzt werden sollte.

Good for Enterprise

Diese Container-Anwendung wird derzeit von dem Automobilhersteller eingesetzt, der in dieser Arbeit als Beispielunternehmen betrachtet wird. Durch ihre spezielle *Containerisierung* werden private und geschäftliche Daten von einander getrennt. Dabei wird innerhalb der Anwendung ein extra E-Mail-Client, ein Kontaktebuch, ein Kalender und ein sicherer Browser für den Zugriff auf das Unternehmens-Intranet bereitgestellt. Auch können innerhalb der Anwendung geschäftliche Dokumente sicher aufbewahrt werden. Durch das Verbot der *Copy-and-Paste*-Funktion kann dabei sichergestellt werden, dass diese Dokumente nicht an einen unsicheren Ort außerhalb des Containers verschoben beziehungsweise kopiert werden. Außerdem kann bei der Anwendung ein Passwortschutz eingestellt werden, sodass sie nur durch die Eingabe des korrekten Passworts gestartet werden kann. Hierfür können ebenfalls die Passwortrichtlinien des Unternehmens durchgesetzt werden, um die Wahl eines sicheren Passworts zu gewährleisten. Sollte das Passwort des Anwenders nicht diesen Richtlinien entsprechen, wird er durch eine Fehlermeldung benachrichtigt [101]. Für den Fall, dass ein Gerät verloren geht oder von Dritten entwendet wird, bietet *Good for Enterprise* eine Fernlösch-Funktionalität. Das Orten des Geräts ist über die Anwendung nicht möglich, auch wenn die von der Anwendung geforderte GPS-Berechtigung eine solche Funktionalität vermuten lässt. Diese benötigt *Good for Enterprise* lediglich für ihren internen Browser (siehe [92]). Daten aus dem Repository innerhalb der Anwendung werden bei einem Backup nicht mit abgesichert [102]. Es besteht allerdings die Gefahr, dass die geschäftlichen E-Mail-Kontakte der Anwendung mit den privaten E-Mail-Kontakten des Geräts synchronisiert werden und daraufhin auf den Google Servern abgelegt werden, falls die Synchronisation mit Google aktiviert ist [103]. Auf diese Weise würden private und geschäftliche Daten vermischt und auf den Speichern von Google abgelegt werden. Dies kann sich als Problem herausstellen, da im Gegensatz zur Europäischen Union, bei der der Schutz personenbezogener Daten ein Grundrecht ist, in den Vereinigten Staaten der Datenschutz kaum gesetzlich geregelt ist [104]. Deshalb muss sichergestellt werden, dass keine Synchronisation mit Google oder anderen Cloud-Anbietern aktiviert ist. Im Hinblick auf den Schutz durch Verschlüsselung wird die Anwendung auf *Google Play* mit folgenden Worten vermarktet:

> *„Sie können sich darauf verlassen, dass Good for Enterprise™ die Übertragung, Verarbeitung und Speicherung von Daten auf Android-Geräten durch eine Verschlüsselung schützt, die auch den Anforderungen von Regierungsbehörden genügt.“* [92]

Diese Aussage und die FIPS-Zertifizierung geben Anlass zu der Annahme, dass die Daten ausreichend sicher auf dem Gerät geschützt sind, selbst während der Übertragung. Ein wirklicher Schutz ist allerdings nur dann gegeben, wenn die verwendete Verschlüsselung auch korrekt eingesetzt wird.

Was *Good for Enterprise* jedoch nicht bietet, ist eine Verschlüsselung der E-Mails. Da das Fallbeispielunternehmen jedoch explizit gefordert hat, dass verschlüsselte E-Mails auf den Smartphones und Tablet-PCs nicht entschlüsselt werden sollen, stellt die Nichterfüllung dieser allgemeinen Anforderung eine positive Eigenschaft dar. Dies ist allerdings nur im Hinblick auf die Anforderungen des Automobilherstellers positiv. Sollte eine E-Mail-Verschlüsselung gefordert sein, existiert die zusätzliche Anwendung *Good Vault*. Diese stellt eine S/MIME-E-Mail-Signatur und -Verschlüsselung für *Good for Enterprise* bereit [106]. Allerdings werden bei den technischen Vorraussetzungen lediglich iPhone und iPad genannt und keine Android-spezifischen Vorraussetzungen. Dies weist darauf hin, dass *Good Vault* nicht für den Einsatz auf Android-Geräten ausgelegt ist (siehe [106]).

Eine besondere Eigenschaft bei der Verwendung von *Good for Enterprise* ist, dass die Nutzer auf ihren Geräten keine Einschränkungen bei der Auswahl und Installation von privaten Apps machen müssen. Durch die spezielle *Containerisierung* der Good-Anwendungen sind diese vor den *„normalen“* Anwendungen geschützt. Wichtig ist allerdings, dass nur *containerisierte* Anwendungen für geschäftliche Zwecke verwendet werden, um den Schutz der Daten sicherzustellen. Dafür bietet *Good for Enterprise* einen internen Anwendungskatalog, den das Unternehmen verwaltet und dort den Nutzern an *Good* angepasste (*containerisierte*) Enterprise-Anwendungen bereitstellen kann. Auf diese Weise wird eine Art *Whitelist* von Anwendungen für die geschäftliche Nutzung zur Verfügung gestellt.

Bezüglich der Usability lässt sich behaupten, dass die Verwendung der App relativ simpel ist. Die Grundfunktionalitäten wie E-Mail, Kalender, Kontakte, App-Katalog und Dokumente sind sichtbar in einer Leiste am Boden der Anzeige mit entsprechenden Icons dargestellt (siehe Anhang, Kapitel A.2). Sollten dennoch Unklarheiten bei der Verwendung der Anwendung bestehen, können die Nutzer das von *Good Technology* bereitgestellte Dokument *Android Handheld and Tablet User's Guide* zur Hilfe nehmen. Dies entspricht demnach den Anforderungen des Automobilherstellers, der seinen Mitarbeitern keinen Support für die Verwendung der BYOD-Lösung bieten will, um Kosten zu sparen.

Im Hinblick auf die aufgestellten nicht-funktionalen Anforderungen kann *Good for Enterprise* die geforderte Minimum-Android-Version abdecken. Die Anwendung soll auf Ge-

räten mit der Android-Version ab 2.0 lauffähig sein [107]. Auf *Google Play* wird jedoch darauf hingewiesen, dass die erforderliche Android-Version je nach Gerät variieren kann (siehe [92]). So muss die Herausforderung berücksichtigt werden, die einzusetzenden Geräte auf ihre Einsatztauglichkeit zu überprüfen. Dies kann je nach Anzahl der Geräte einen entsprechend großen Aufwand mit sich bringen. Ebenfalls kann *Good for Enterprise* auf mehreren mobilen Betriebssystemen verwendet werden. Es werden neben Android auch iOS und Windows Phone unterstützt. Außerdem benötigt die Anwendung keine Root-Rechte, sodass die Gefahr des Verlusts der Garantieansprüche auch wegfällt.

Die Anwendung *Good for Enterprise* deckt die meisten aufgestellten Anforderungen ab und eignet sich dadurch besonders gut für das Beispielunternehmen. Für dieses ist die Problematik der fehlenden Verschlüsselungsmöglichkeit von E-Mails nicht relevant, sodass keine offensichtlichen Sicherheitsgefährdungen bestehen und das Unternehmen diese Anwendung weiterhin ohne große Bedenken als BYOD-Lösung einsetzen kann. Lediglich die Kontrolle des ordnungsgemäßen Umgangs mit personenbezogenen Geschäftsdaten kann mit dieser Lösung nicht realisiert werden.

Nubo

Durch die Bereitstellung eines *Remote-Workspace* werden keine Geschäftsdaten und -anwendungen auf dem Gerät abgelegt. Dies bewirkt eine strikte Trennung privater und geschäftlicher Informationen, da die privaten Daten und Anwendungen von dem *Remote-Workspace* aus nicht erreichbar sind. Dasselbe gilt für die andere Richtung. Diese Eigenschaft lässt die Anforderung, die Daten des Geräts aus der Ferne löschen zu können, überflüssig werden, da es keine Geschäftsdaten auf dem Gerät gibt beziehungsweise geben sollte.

Der Zugriff auf den *Remote-Workspace* wird durch ein Passwort und ein Security-Token geschützt, sodass eine Zwei-Faktor-Authentifizierung für mehr Sicherheit stattfindet. Ob bei der Wahl des Passworts die Passwortrichtlinien des Unternehmens durchgesetzt beziehungsweise überprüft werden können, konnte aus den betrachteten Quellen nicht entnommen werden. Jedenfalls kann durch diese Art der Authentifizierung verhindert werden, dass ein Angreifer von seinem Gerät mit dem Passwort des Opfers eine Verbindung zu dessen Workspace aufbauen kann. Für dieses Vorhaben müsste der Angreifer auch das Gerät des Opfers besitzen, wobei bei Verlust des Geräts der Zugang des jeweiligen Mitarbeiters gesperrt werden kann.

Ebenfalls positiv ist, dass sämtliche Verbindungen zwischen dem Gerät und der Nubo-Plattform durch eine Verschlüsselung geschützt sind. Dies wird durch das SSL-Protokoll realisiert.

Diese BYOD-Lösung ist nicht nur für Android-Geräte gedacht. Sie kann auch mit iPhones und iPads genutzt werden. iOS wird ab der iOS-Version 5.0 unterstützt und auf Android-Geräten läuft *Nubo* ab der Android-Version 2.3.3 [108]. Dies entspricht den aufgestellten Anforderungen im Hinblick auf die minimal vorausgesetzte Android-Version und die Möglichkeit, die Lösung auf Geräten mit einem anderen Betriebssystem verwenden zu können. Jedoch unterstützt sie weniger Betriebssysteme als die zuvor bewertete Lösung, die auch auf Windows Phone eingesetzt werden konnte.

iPhone- beziehungsweise iPad-Nutzer könnten die Verwendung von *Nubo* als ungewohnt empfinden, weil sie durch diese Anwendung auf eine Android-Umgebung zugreifen. Auch konnten bei der Recherche keine Dokumente gefunden werden, die eine Art Anleitung für diese Anwendung darstellen. Dies könnte sich als Problem erweisen, sofern die Bedienbarkeit nicht intuitiv ist, da die Nutzer in diesem Fall durch Ausprobieren und Raten ihre Schwierigkeiten selbst lösen müssten. Denn zusätzlicher Support soll für die BYOD-Lösung nicht bereitgestellt werden.

Bei *Nubo* wird ein Enterprise-App-Store bereitgestellt, der es ermöglicht, dieselben Apps für geschäftliche Zwecke zu nutzen, die Anwender sonst auch privat nutzen [109]. Dazu gehören zum Beispiel *Facebook, Twitter, Evernote, TripAdvisor* [110]. Dies ermöglicht den Nutzern kaum Einschränkungen bei ihrer Arbeit. Jedoch ist dabei fraglich, ob die verfügbaren Anwendungen einer ausreichenden Sicherheitsüberprüfung unterzogen wurden. So könnten geschäftliche Daten trotz eines separaten Workspaces gefährdet werden. Auch konnte in den untersuchten Quellen kein Hinweis dafür gefunden werden, ob das Unternehmen bei der virtuellen Android-Umgebung eine Art Blacklist beziehungsweise Whitelist führen kann. Es wurde nur die Anmerkung gefunden, dass Unternehmen ihre eigenen Anwendungen allen Mitarbeitern bereitstellen können, durch eine einmalige Installation auf dem zentralen Server [111].

Diese nicht vorhandene Einschränkung bei der Auswahl von Apps bringt zwar den Vorteil mit sich, dass wahrscheinlich auch bestimmte E-Mail-Apps genutzt werden können, die zum Beispiel *PGP* zur Verschlüsselung und Signierung einsetzen, was jedoch für das Beispielunternehmen eher als Nachteil anzusehen ist. An dieser Stelle muss allerdings auch berücksichtigt werden, dass diese Anforderung eventuell bei der Tatsache, dass sämtliche Daten auf einem Server des Unternehmens abgelegt werden, als unbedeutend betrachtet werden kann. Denn die Gefahr eines unbefugten Zugriffs ist bei dieser Lösung durch die gegebenen Sicherheitsmechanismen relativ gering. Doch für den Fall, dass die Anforderung bestehen bleibt, stellt dieser Lösungsansatz hier einen deutlichen Nachteil dar.

Ein weiterer Nachteil ist, dass für die Verwendung von *Nubo* eine *„ausreichend dimensionierte Internetverbindung“*[87] benötigt wird. Dies könnte bei einer Internetverbindung über das mobile Internet zu starken Performance-Einbußen führen bis hin zur Nicht-Nutzbarkeit von *Nubo*.

Somit stellt *Nubo* lediglich mit einer schnellen Internetverbindung einen guten Lösungsansatz dar. Das Problem mit den vielen Anwendungen, die für geschäftliche Zwecke genutzt werden können und möglicherweise ein Risiko für die Sicherheit der Geschäftsdaten darstellen, muss dennoch berücksichtigt werden. Für das Beispielunternehmen ist dieser Lösungsansatz im Vergleich zu *Good for Enterprise* daher weniger geeignet. Die Möglichkeit, vertrauliche E-Mails auf den Geräten zu entschlüsseln, kann hier durch die Menge diverser Enterprise-Anwendungen gegeben sein. Die Wahrscheinlichkeit, dass dort E-Mail-Anwendungen mit solcher Funktionalität vorhanden sind, ist aufgrund der Menge von Anwendungen relativ hoch.

VMware Horizon Workspace

Die dritte BYOD-Lösung, *VMware Horizon Workspace*, stellt über eine zusätzliche Arbeitsumgebung mit eigenem Betriebssystem, Daten und Anwendungen eine strikte Trennung von privaten und geschäftlichen Daten zur Verfügung. So werden auf einem Gerät zwei virtuelle Telefone abgebildet [112]. Dabei wird der Inhalt des virtualisierten Containers mit dem Horizon Workspace Server synchronisiert, damit der Nutzer auf sämtlichen Geräten Zugriff auf seinen persönlichen *Workspace* und Datenbestand hat. Diese Lösung bietet ebenfalls die Möglichkeit, Anwenderaktivitäten zu protokollieren. Durch das separate Betriebssystem werden auf diese Weise keine Aktivitäten mitprotokolliert, die privat außerhalb des Containers stattfinden. Durch diese Protokollfunktion kann kontrolliert werden, ob die Mitarbeiter eine ordnungsgemäße Erhebung, Verarbeitung und Nutzung personenbezogener Daten vornehmen und nicht gegen das Datenschutzgesetz verstoßen. Auch kann dadurch, im Gegensatz zu den beiden anderen Lösungen, das Lizenzproblem bei dem BYOD-Konzept verhindert werden. Sollten Mitarbeiter Enterprise-Anwendungen privat nutzen und dadurch gegen bestimmte Lizenzen verstoßen, kann das Unternehmen dies mit der Protokoll-Funktion feststellen.

Das Unternehmen kann seinen Mitarbeitern aufgrund von zugewiesenen Benutzerrollen durch einen Anwendungskatalog verschiedene Anwendungen bereitstellen. So können Mitarbeitern aus verschiedenen Abteilungen jeweils die von ihnen benötigten Anwendungen zur Verfügung gestellt werden.

Für eine sichere Kommunikation mit dem Horizon Workspace Server verwendet auch *VMware Horizon Workspace* SSL. Dabei kommt der AES-Algorithmus mit einer Schlüssellänge von 256 Bit zum Einsatz, um die Kommunikation zwischen Client und Server zu verschlüsseln. So ist auch bei diesem Lösungsansatz ein gewisses Maß an Sicherheit bei der Kommunikation sichergestellt.

Weniger positiv ist der Passwortschutz von *VMware Horizon Workspace*. Hier kann lediglich ein numerisches Passwort eingestellt werden, was den Zugriff auf das zusätzliche

Betriebssystem absichern soll. Es wird zwar eine Mindestlänge von vier Zahlen gefordert, jedoch können so Passwortrichtlinien des Unternehmens nicht durchgesetzt werden und der Schutz vor unbefugtem Zugriff ist ebenfalls höher als bei den beiden anderen Lösungen. Deshalb kommt der Fernlösch-Funktionalität, die *VMware Horizon Workspace* bietet, eine besondere Bedeutung zu. Diese kann bei dem Verlust des mobilen Geräts und einer schnellen Reaktion verhindern, dass Unbefugte auf den virtualisierten Container und die darin befindlichen Daten zugreifen können.

Auch *VMware Horizon Workspace* ist für verschiedene Betriebssysteme einsetzbar. Bei den mobilen Betriebssystemen lässt sich diese Anwendung auch auf iOS-Geräten eingesetzen. Zusätzlich ist sie auch für Windows und Mac OS erhältlich, sodass selbst der Einsatz von privaten Notebooks dadurch abgesichert werden kann [100]. Während auf Android-Geräten durch *VMware Horizon Workspace* ein zweites Betriebssystem zur Verfügung gestellt wird, wird bei iOS lediglich eine abgesicherte App bereitgestellt, deren Inhalt von den Administratoren verwaltet werden kann [112]. Somit ähnelt die iOS-Variante eher der Container-Lösung von *Good Technology* und stellt weniger die Virtualisierung eines Betriebssystems dar.

Bezüglich der Lauffähigkeit auf älteren Android-Versionen, kann *VMware Horizon Workspace* bereits auf Android-Geräten mit der Version 2.2 verwendet werden. Somit deckt auch diese Lösung die aufgestellte nicht-funktionale Anforderung mit der Lauffähigkeit auf einer minimal erforderlichen Android-Version von 2.3.x ab.

Nach Betrachtung dieser Eigenschaften lässt sich feststellen, dass *VMware Horizon Workspace* eine gute Alternative zu der bisher eingesetzten Lösung *Good for Enterprise* ist. Der große Vorteil gegenüber *Good for Enterprise* ist die Protokollfunktion. Mit ihr können Lizenz-Missbrauche aufgedeckt und bekämpft werden. Außerdem kann dadurch eine ordnungsgemäße Erhebung, Verarbeitung und Nutzung personenbezogener Daten sichergestellt werden. Der Nachteil gegenüber der derzeit eingesetzten Lösung ist der schwache Passwortschutz, bei dem die Passwortrichtlinien des Unternehmens nicht berücksichtigt werden können. Außerdem konnten während der Recherche keine wirklichen Anleitungen für die Verwendung von *VMware Horizon Workspace* gefunden werden, was den gewünschten Self-Support erschweren könnte. Möglicherweise werden diese jedoch bei dem Erwerb der Anwendung beziehungsweise der Lizenz den Anwendern bereitgestellt.

5. Fazit

Bei dem Thema *BYOD* teilen sich die Meinungen vieler Unternehmen und IT-Experten. Bei einer von der *Dell Software Group* durchgeführten Umfrage zu *BYOD* gaben ca. 70% der Befragten[1] an *„[...] mit BYOD ihre Arbeitsprozesse zu verbessern um in der Zukunft erfolgreicher zu sein“*([114]). 59% sind dabei der Meinung, ohne *BYOD* im Wettbewerb mit der Konkurrenz Vorteile einbüßen zu müssen [114]. Entgegen dieser positiven Einstellung zu dem Thema existieren ebenfalls BYOD-Kritiker. So übersetzt der Geschäftsführer der *Aretas*[2], Peter Bergmann, den Begriff *„BYOD“* mit den Worten *„Bring Your Own Disaster“* [115]. Nach seiner Ansicht lagern die Firmen ihre Kosten und Mühen mit diesem Konzept lediglich auf die Mitarbeiter um. Außerdem behauptet er, dass bei BYOD viele organisatorische und rechtliche Fragen beantwortet werden müssten, die schnell zu einem unwirtschaftlichen Mehraufwand führten [115]. Ob *BYOD* für ein Unternehmen nun einen Mehrwert oder eine unnötige und unwirtschaftliche Belastung darstellt, muss jedes Unternehmen für sich herausfinden. Dabei sollte das Unternehmen analysieren, ob es dadurch tatsächlich Geld einsparen kann und ob die Produktivität der Mitarbeiter gesteigert wird [116]. Ebenfalls wichtig ist es, passende Software zur Realisierung dieses Konzepts zu finden, die den Ansprüchen des Unternehmens genügt. Beispiele für solche Software wurden im Kapitel 4.3 vorgestellt. Bei der jeweiligen Lösung muss zusätzlich geprüft werden, mit welchem Aufwand die Umsetzung verbunden ist und ob sich dieser für das Unternehmen als akzeptabel gestaltet [116]. Sollte bei *BYOD* im Zusammenhang mit Smartphones keine zusätzliche Rufnummer für geschäftliche Zwecke vorhanden sein, ist außerdem grundlegend zu klären, ob der Mitarbeiter bereit ist, seine private Nummer an Kunden weiter zu geben und gegebenenfalls am Ende seiner Beschäftigung dem Unternehmen zu überlassen. Dies sind einige Anhaltspunkte, um festzustellen, ob *BYOD* sich für ein Unternehmen als vorteilhaft erweist. Es existieren jedoch noch diverse Dokumente und Leitfäden, die sich die Unternehmen bei der Planung zu Hilfe nehmen können. So wurde beispielsweise in dieser Arbeit der Fokus auf die Dokumente der Bitkom (siehe [21]) und des BSI (siehe [87]) gelegt, die zu diesem Thema hilfreiches Material bereitstellen.

Im Verlauf dieser Arbeit wurde immer deutlicher, dass das Fundament für *BYOD* eine klare Trennung der privaten und geschäftlichen Daten ist. In den Kapiteln 2.2.2 und 4.2 wurde diesbezüglich auf das *Bundesdatenschutzgesetz* und das *Telekommunikationsgesetz* verwiesen, die ohne eine solche Trennung ein Hindernis für das Unternehmen darstellen könnten. So könnte beispielsweise ein Unternehmen bei der Kontrolle zur sachgemäßen Erhebung, Verarbeitung und Nutzung von personenbezogenen Daten ohne eine Trennung der Daten gegen das Fernmeldegeheimnis aus §88 des TKG verstoßen. Es reicht allerdings

[1] Ca. 1.500 IT-Verantwortliche.
[2] Beratungsgesellschaft für Unternehmen zur Verbesserung der eigenen Services

nicht, sich auf die Trennung der Daten durch eine Softwarelösung für dieses Konzept zu verlassen. Die drei in dem Kapitel 4.3 vorgestellten Lösungsansätze bieten zwar jeweils eine solche Trennung durch einen zusätzlichen *geschäftlichen Bereich* auf den Smartphones und anderen Geräten, jedoch nur so lange, wie die Nutzer sich an die getrennte Verwendung halten. Damit ist gemeint, dass getrennte Bereiche auf den Geräten existieren können, diese aber nur dann ihren Zweck erfüllen, wenn der Nutzer den privaten Bereich für private Angelegenheiten und den geschäftlichen Bereich für geschäftliche Vorhaben nutzt. Es liegt demnach auch an den Mitarbeitern, ob sich *BYOD* ohne rechtliche Schwierigkeiten, wie zum Beispiel Lizenzverstöße, umsetzen lässt.

Einen weiteren interessanten Lösungsansatz für *BYOD*, stellt *BizzTrust* dar. Es handelt sich um eine Lösung, die auf einem modifizierten Android-Betriebssystem aufbaut und Anwendungen und Daten in einen privaten und einen geschäftlichen Bereich trennt. Es wurde in Zusammenarbeit von dem *Fraunhofer Institut für sichere Informationstechnologie*, *CASED* und der *Sirrix AG* entwickelt. Da für die Verwendung von *BizzTrust* allerdings eine spezielle Vorbereitung des Smartphones benötigt wird, eignet sich diese Lösung aufgrund des Aufwands nur bedingt für *BYOD*. Es müsste jedes Smartphone vorbereitet werden, was schnell zu einem sehr hohen Aufwand führen kann. Außerdem wird das Betriebssystem des Smartphones durch das modifizierte Android-Betriebssystem ausgetauscht, sodass die Garantieansprüche zu dem Gerät erlöschen könnten [87]. Aufgrund dieser Eigenschaften wurde *BizzTrust* nicht in die Auswahl der vorgestellten Lösungen in Kapitel 4.3 aufgenommen, sondern lediglich in diesem Kapitel kurz vorgestellt.

Da das Thema dieser Bachelorarbeit *BYO(Android)D* lautet, wurden in den Kapiteln 3.3 und 3.4 die Sicherheitsmechanismen von Android vorgestellt und mit denen anderer mobiler Betriebssysteme verglichen. Es sollte dabei prinzipiell festgestellt werden, ob sich Android im Vergleich zu iOS und Windows Phone anhand seiner Sicherheitsmechanismen genauso gut für *BYOD* eignet oder möglicherweise sogar besser. Dazu wurden die drei Betriebssysteme tabellarisch gegenüber gestellt (siehe Tabelle 3). Es stellte sich heraus, dass Android bei diesem Vergleich positiver abschnitt als seine beiden Konkurrenten. Während Android zwar keine automatische Löschung der Daten bei wiederholter Falscheingabe des Passwortes vornimmt, weist es im Gegensatz zu Windows Phone die Eigenschaften *„Verschlüsselter und authentifizierter E-Mail-Verkehr“* und *„VPN-Client“* auf. iOS wird von Android bei der Eigenschaft *„Benutzerkonten“* übertroffen, da Android diese Funktionalität ab der Version 4.2 auf Tablet-PCs und auf diversen Smartphones (zum Beispiel auf dem LG G2) in Form eines *Gästemodus* bereitstellt. Es kann anhand dieser Gegenüberstellung prinzipiell behauptet werden, dass Android durchaus einen soliden Schutz für Daten aller Art bieten kann und sich durch Funktionalitäten wie VPN-Unterstützung besonders gut für den geschäftlichen Einsatz eignet.

In Kapitel 3.3.3 wurde außerdem auf mögliche Sicherheitswerkzeuge für Android durch Drittanbieter eingegangen. Dabei wurden speziell Antiviren-Apps zur Steigerung der Sicherheit genannt. Sie können Anwendungen scannen, bieten häufig einen Passwortschutz für den Zugang zu Anwendungen und verfügen teilweise über einen Anruf- und SMS-Filter. Auch eine Firewall lässt sich bei vielen Antiviren-Apps einrichten. Hierfür werden jedoch Root-Rechte benötigt. Durch solche Root-Rechte unterliegt die jeweilige Anwendung keinen Einschränkungen und kann ungehindert auf das System zugreifen. Bereits in Kapitel 3.3.3 wird auf die dadurch entstehende Gefahr verwiesen. Denn selbst wenn durch die Zuweisung von Root-Rechten eine Anwendung sicherheitsfördernde Maßnahmen durchsetzen kann, wie zum Beispiel eine Firewall, können die Rechte ebenso einer vermeintlich gutartigen Anwendung zugewiesen werden. Diese könnte daraufhin einen noch größeren Schaden im System anrichten und auf Daten zugreifen, zu denen sie ohne diese Rechte keinen Zugriff gehabt hätte. Es ist somit wichtig, die Vergabe von Root-Rechten mit Bedacht vorzunehmen. Im Rahmen von *BYOD* ist es häufig von den Unternehmen untersagt, *gerootete* Geräte geschäftlich zu nutzen. Daher sollte auf das *Rooten* des Geräts bestenfalls ganz verzichtet werden, wenn dieses neben der privaten Nutzung auch geschäftlich eingesetzt werden soll. Dies würde auch bedeuten, dass auf solchen Geräten kein Custom-ROM zum Einsatz kommen kann, da hierfür das Gerät wieder gerootet werden müsste. Es wird allerdings auch in diversen Foren darauf hingewiesen, dass das Aufspielen eines Custom-ROM beziehungsweise das *Flashen* des Geräts auch ohne Rooten möglich ist (siehe [118] und [119]). Genaue Anleitungen von vertrauenswürdigen Quellen konnten dazu allerdings nicht gefunden werden. Somit können im Rahmen von *BYOD* die Vorteile von Custom-ROMs meist nicht genutzt werden. Zu diesen Vorteilen gehört beispielsweise die bereits in Kapitel 3.3.3 genannte bessere Versorgung älterer Android-Modelle mit Sicherheitsupdates.

Gegen Ende der Bearbeitungszeit dieser Bachelorarbeit erschien die neuste Android-Version *KitKat* (Version 4.4). Sie beinhaltet Sicherheitserweiterungen, die Android noch sicherer machen sollen. Beispielsweise wurde die Android-Sandbox durch SELinux weiter verbessert. So werden im Vergleich zu der Version 4.3 nicht nur Benachrichtigungen bei bestimmten *Events* geschickt, sondern unerlaubte Handlungen von Anwendungen ganz geblockt [120][121]. Es steigt demnach mit jeder neuen Version die Sicherheit des Betriebssystems. Dennoch muss berücksichtigt werden, dass, wie schon in Kapitel 4.2 erwähnt, die am meisten verbreitete Android-Version die Version 2.3 ist. So sind auf vielen Android-Geräten neue Sicherheitserweiterungen noch nicht vorhanden. Dies ist ein wichtiger Faktor bei der Umsetzung von *BYOD* in einem Unternehmen, denn dadurch können unnötige Sicherheitsrisiken entstehen. Außerdem könnte die einzusetzende BYOD-Lösung von einer zu niedrigen Android-Version nicht unterstützt werden, sodass viele Geräte aus diesem Konzept ausgeschlossen werden. Zusätzlich besteht bei Android im Rahmen von *BYOD*

wie bereits erwähnt der Nachteil, dass der Aufwand bei der Einsatztauglichkeitsprüfung sehr hoch ausfallen kann, sofern viele verschiedene Android-Geräte genutzt werden. Diesen Nachteilen stehen jedoch die Vorteile des Einsatzes von Android im Rahmen von *BYOD* gegenüber. Wie bereits bei der Gegenüberstellung der Betriebssysteme (siehe Tabelle 3) erkannt, weist Android bestimmte Sicherheitsmerkmale auf, die iOS und Windows Phone nicht besitzen. Diese bekräftigen die Einsatztauglichkeit von Android im betrieblichem Umfeld. Außerdem kann die Zufriedenheit der Mitarbeiter gesteigert werden, wenn diese die Verwendung von Android-Geräten vorziehen. Auch die große Auswahl an Android-Geräten kann diese Zufriedenheit der Mitarbeiter zusätzlich erhöhen. Sie haben dadurch die Möglichkeit ein Gerät zu nutzen, das ihren Ansprüchen entspricht. Durch die Steigerung der Zufriedenheit kann ebenfalls die Produktivität der Mitarbeiter positiv beeinflusst werden. Auf diese Weise kann selbst das Unternehmen neben möglichen Einsparungen von diesen Vorteilen profitieren.

Ob Android seinen Mehrbenutzerbetrieb von Tablet-PCs auch auf Smartphones überträgt, bleibt abzuwarten. Es würde das Problem der Datentrennung bei *BYOD* jedenfalls größtenteils lösen, ohne durch spezielle Software virtuelle Bereiche erzeugen zu müssen.

Unter Berücksichtigung der in dieser Arbeit vorgestellten Aspekte können Unternehmen bewerten, ob ihnen das Konzept *BYOD* in Verbindung mit Android-Geräten einen wirtschaftlichen Vorteil bei hinnehmbarem Risiko bietet.

A. Anhang

A.1. Betrachtung der Sicherheitsmerkmale

Datensicherung

- **Android:** Multimedia-Dateien können auf die SD-Karte oder über das USB-Kabel auf den Rechner verschoben und gesichert werden. Um Anwendungsdaten, WLAN-Passwörter und andere Einstellungen zu sichern, kann dies mit einem Google-Account auf den Google-Servern vorgenommen werden. Auch Lösungen von Geräteherstellern auf diversen Geräten vorhanden. Ansonsten Apps von Drittanbietern.[69]

- **iOS:** Multimedia-Dateien, Apps, Einstellungen etc. können über iTunes gesichert werden, wenn das Gerät mit dem Computer verbunden ist. Ebenso kann über die iCloud ein Backup erzeugt werden, wenn das Gerät über WLAN mit dem Internet verbunden, es an die Stromversorgung angeschlossen und der Bildschirm gesperrt ist.[70]

- **Windows Phone:** Auch hier können unter anderem Multimedia-Dateien und Einstellungen automatisch in die Cloud von Microsoft gespeichert werden über das Microsoft-Konto.[71]

Geräte-Sperrung mit Passwortabfrage nach gewisser Inaktivität

- **Android:** Vorhanden.

- **iOS:** Vorhanden.

- **Windows Phone:** Vorhanden. Extra-Funktion: Einstellen von *Kennwort abfragen nach*, um nicht bei jedem Entsperren den Code eingeben zu müssen, sondern nu alle 30 Sekunden bis 30 Minuten.[72]

Automatische Löschung der Daten bei wiederholter Falscheingabe des Passwortes

- **Android:** Nicht vorhanden.

- **iOS:** Vorhanden (siehe Kapitel 3.4.1).

- **Windows Phone:** Vorhanden (siehe Kapitel 3.4.1).

Möglichkeit Sicherheitsrichtlinien aufzustellen und durchzusetzen

- **Android:** Exchange ActiveSync-Postfachrichtlinien oder mit zusätzlichen Anwendungen zum Beispiel von Google realisierbar (siehe [82])

- **iOS:** Exchange ActiveSync-Postfachrichtlinien und built-in Support für MDM-Lösungen durch Drittanbieter (siehe [83], [85]).
- **Windows Phone:** Vorhanden durch Exchange ActiveSync-Richtlinien (siehe Kapitel 3.4.1 oder [84])

Verschlüsselung des Speichers

- **Android:** Vorhanden. Sowohl Verschlüsselung des internen Speichers als auch der SD-Karte.
- **iOS:** Vorhanden.[74]
- **Windows Phone:** Interne Speicher ja, SD-Karte nicht.[73]

Verschlüsselter und authentifizierter E-Mail-Verkehr

- **Android:** Verschlüsselung und Signatur vorhanden im standard E-Mail-Client. RSA und DSA als Schlüsselangorithmus. Ansonsten extra Apps von Drittanbietern.
- **iOS:** Verschlüsseln und Signieren über S/MIME. Um PGP nutzen zu können, benötigt man Apps von Drittanbietern.
- **Windows Phone:** S/MIME und PGP wird standardmäßig nicht unterstützt (siehe [75]). Um Mails mittels OpenPGP verschlüsseln und signieren zu können gibt es Apps von Drittanbietern.

Remote Wipe

- **Android:** Vorhanden über Android Geräte-Manager.[81]
- **iOS:** Vorhanden über iCloud.[80]
- **Windows Phone:** Vorhanden.[68, Seite 6]

Whitelists für geeignete Anwendungen führen

- **Android:** Standardmäßig nicht vorhanden. Nur mit Software von Drittanbietern (siehe z.B. [79])
- **iOS:** Standardmäßig nicht vorhanden. Nur mit Software von Drittanbietern (siehe z.B. [79])
- **Windows Phone:** Standardmäßig nicht vorhanden. Nur mit Software von Drittanbietern (siehe z.B. [79])

VPN-Client

- **Android:** Wird standardmäßig unterstützt (siehe Kapitel 3.3.3).
- **iOS:** Wird standardmäßig unterstützt (siehe Kapitel 3.4.1).
- **Windows Phone:** (Noch) nicht vorhanden (siehe [76]).

Datenseparation (geschäftlich/privat)

- **Android:** Standardmäßig nicht vorhanden.
- **iOS:** Standardmäßig nicht vorhanden.
- **Windows Phone:** Standardmäßig nicht vorhanden.

Benutzerkonten

- **Android:** Ab Version 4.2, jedoch nur auf Tablet-PCs (siehe Kapitel 3.3.4).
- **iOS:** Standardmäßig nicht vorhanden.
- **Windows Phone:** In eingeschränkter Form vorhanden (siehe *Kinderecke* in Kapitel 3.4.1)

Over-The-Air Updates des Betriebssystems

- **Android:** Vorhanden.
- **iOS:** Vorhanden.[78]
- **Windows Phone:** Vorhanden.[77]

A.2. Screenshots von Good for Enterprise

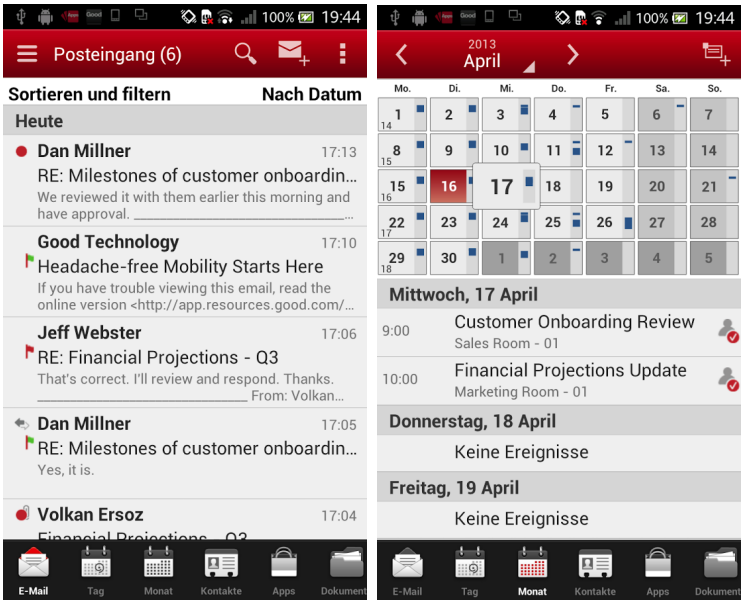

Abbildung 6: E-Mail-Client und Kalender[92]

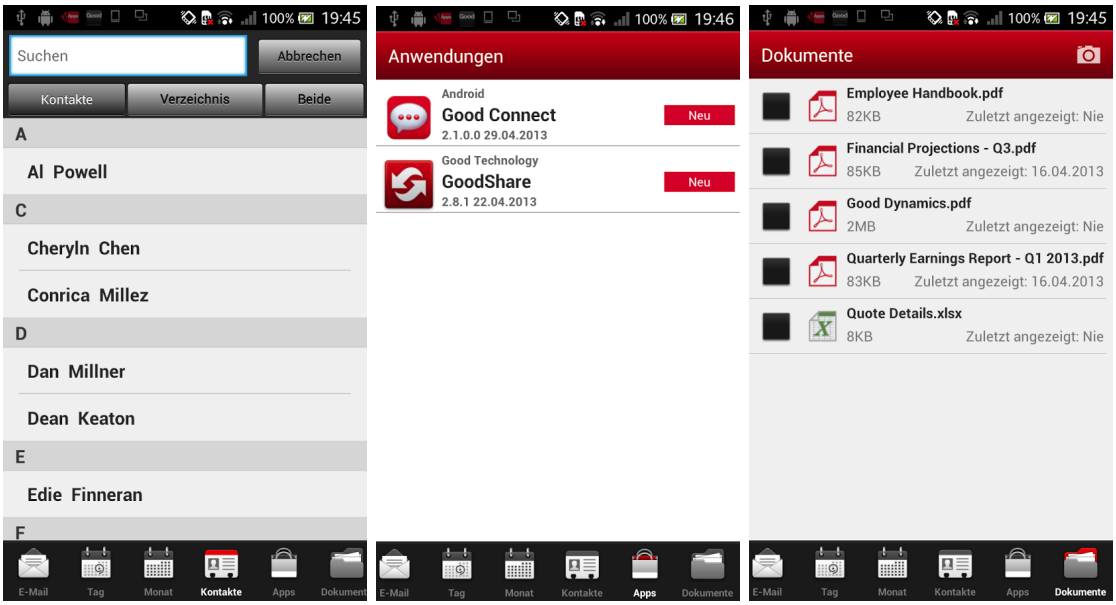

Abbildung 7: Kontakte, Anwendungskatalog und Dokumente[92]

Abbildungsverzeichnis

Tabellenverzeichnis

Abkürzungsverzeichnis

App	Application (dt. Anwendungssoftware)
API	Application Programming Interface (dt. Programmierschnittstelle)
BDSG	Bundesdatenschutzgesetz
BSI	Bundesamt für Sicherheit in der Informationstechnik
BYOD	Bring Your Own Device
Dual EC DRBG	Dual Elliptic Curve Deterministic Random Bit Generation
DoS	Denial of Service
ENISA	European Network and Information Security Agency
GPS	Global Positioning System
IT	Informationstechnik
MDM	Mobile Device Management
NSA	National Security Agency
PC	Personal Computer
PIN	Personal Identification Number
RPC	Remote Procedure Communication
RSA	Rivest, Shamir, Adleman
SMS	Short Message Service
TKG	Telekommunikationsgesetz
URL	Uniform Resource Locator
VPN	Virtual Private Network
WLAN	Wireless Local Area Network

Glossar

Advanced Encryption Standard (AES) Der Advanced Encryption Standard ist ein von dem National Institute of Standards bekanntgegebener Standard, der von Joan Daemen und Vincent Rijmen entwickelt wurde. Es handelt sich dabei um einen deterministisches Verschlüsselungsverfahren, was eine Blockverschlüsselung vornimmt (vgl. [122]). 35, 52, 55, 60**API-Call** Aufruf einer von einer Programmierschnittstelle (API) bereitgestellten Routine. Beispielsweise kann durch eine Programmierschnittstelle auf Datenbanken oder sogar Hardware zugegriffen werden. 26

Boot-ROM Ein spezieller Speicherchip mit der Eigenschaft eines Nur-Lese-Speichers (ROM). Er wird bei Geräten für den Bootvorgang, also für den Start- und Initialisierungsvorgang, eingesetzt. Dabei enthält er den dafür benötigten Bootloader, der auch als Startprogramm bezeichnet wird (vgl. [123] und [124]). 40

Canary Als Canary wird ein Zufallswert bezeichnet, der zum Schutz der Rücksprungadresse und zum Aufdecken eines Overflows eingesetzt wird. Dabei wird bei einem Overflow der Canary überschrieben, sodass beim Rücksprung aus der Funktion bei dem Integritätstest des Canary festgestellt wird, dass dieser Zufallswert geändert wurde. Daraufhin wird die Ausführung abgebrochen (vgl. [125]). 38

Compliance Auch als Regelkonfirmität bekannt, bezeichnet es die Einhaltung von Gesetzen und Richtlinien in Unternehmen (vgl. [126]). 19

Custom-ROM Ein Custom-ROM bezeichnet ein alternatives Betriebsprogramm, das das des Herstellers eines Geräts ersetzt. Custom-ROMs bieten häufig weitere Funktionalitäten, die sich durch das Aufheben von standardmäßigen Einschränkungen, die bei der Originalversion des Herstellers vorhanden sind, ergeben (vgl. [127]). 7–9, 36, 64

Exchange ActiveSync (EAS) Bei EAS handelt es sich um ein XML-basiertes Protokoll. Es wird genutzt, um E-Mails, Kalendereinträge, Kontakte etc. von einem Server mit einem mobilen Endgerät zu synchronisieren (vgl. [128]). 43

Formatstring-Angriff Bei diesem Angriff wird eine Sicherheitslücke ausgenutzt, die durch Formatierungsfehler in ungeprüften Benutzereingaben in diversen C-Funktionen entsteht. Ein Formatstring ist dabei ein String, der neben Text ebenfalls Formatierungsparameter enthält. Wird also eine Format-Funktion, zum Beispiel `printf()`,

in Verbindung mit bestimmten Formatierungstoken verwendet, kann sich ein Angreifer Daten vom Stack ausgeben lassen, sofern sein Angriff erfolgreich verläuft (vgl. [129] und [130]). 38

Integer-Overflow Bei einem Integer-Overflow beziehungsweise einem Ganzzahlüberlauf handelt es sich um das Überschreiten eines vordefinierten Wertebereichs. So kann bei einer Berechnung mit zu hohen Zahlen ein verfälschtes Ergebnis resultieren, da nicht alle Stellen berücksichtigt werden können. Diese Art von Überlauf kann Pufferüberläufe verursachen und dadurch das jeweilige System unter anderem zum Absturz bringen oder Daten verfälschen (vgl. [132] und [133]). 38

Internet Protocol Security (IPsec) Bei Internet Protocol Security handelt es sich um eine Erweiterung des bekannten Internet-Protokolls (IP). IPsec besitzt Verschlüsselungs- und Authentisierungsmechanismen, die es ermöglichen Daten auf „sicherem“ Weg über ein unsicheres Netz zu übertragen (vgl. [134]). 35

Kernel Der Kernel, auch Betriebssystemkern genannt, ist der Bestandteil des Betriebssystems, der direkten Zugriff auf die Hardware hat. Es ist somit der Hauptbestandteil des Systems (vgl. [135]). 30–33

Layer 2 Tunneling Protocol (L2TP) Bei diesem Protokoll handelt es sich um ein spezielles Netzwerkprotokoll, das eine Tunnel-Lösung mit den Vorteilen des Point-to-Point Tunneling Protocols (PPTP) und des Layer 2 Forwarding (L2F) darstellt. Mit Hilfe dieses Protokolls kann dann ein virtuelles privates Netzwerk erzeugt werden (vgl. [136]). 35

Line of Business (LOB) Unter dem Begriff Line of Business versteht man die Art beziehungsweise den Bereich, denen die Produkte und Dienstleistungen eines Unternehmens zugeordnet werden können (vgl. [137]). 42

Mandatory-Access-Control Es beschreibt eine systembestimmte Zugriffskontrolle, bei der Zugriffberechtigungen anhand bestimmter Regeln verteilt werden. Ein Beispiel für Mandatory Access Control ist das Bell-LaPadula-Modell, bei dem Subjekte und Objekte eine Sicherheitsmakierung (label) erhalten, die ihre Vertraulichkeitsstufe darstellt. Je nach Sicherheitsstufe können Subjekte auf bestimmte Objekte zugreifen (vgl. [138]). 39

National Security Agency (NSA) Die National Security Agency gehört zu den Geheimdiensten der Vereinigten Staaten und hat unter anderem die Aufgabe die Telekommunikation weltweit zu überwachen und auszuwerten. Des Weiteren ist die

NSA zuständig für das nationale Verschlüsselungswesen sowie für den Schutz der nationalen Telekommunikationswege (vgl. [139]). 6, 18

Nonce In der Kryptographie versteht man unter einer Nonce einen Wert, der nur einmal für eine bestimmte Sitzung bezieuhungsweise in einem bestimmten Kontext verwendet wird. Der Begriff Nonce steht dabei als Abkürzung für *number use once* oder *used only once* (vgl. [141] und [142]). 41

NX-Bit Das NX-Bit stellt eine Sicherheitserweiterung in Prozessoren dar, die zum Schutz gegen das Einschleusen von Code auf dem Stack durch Buffer-Overflow-Angriffen dienen. Dabei steht das NX-Bit für *No-Execution*-Bit und wird in vielen AMD-Prozessoren verwendet. Diverse Intel-Prozessoren verwenden ebenfalls diese Technik, nur heißt es dort XD- (Execute-Disable-) Bit (vgl. [140]). 38

Point-to-Point Tunneling Protocol (PPTP) Hierbei handelt es sich um ein Protokoll zum Errichten eines Virtual Private Networks. Es bietet eine Verschlüsselung und Authentisierung, die allerdings als unsicher gelten (vgl. [143]). 35

Prism Es handelt sich hierbei um ein Programm zur Überwachung von elektronischen Medien und wird von der National Security Agency geleitet (vgl. [154]). 18

Rivest Shamir und Adleman (RSA) RSA ist ein asymmetrisches Verschlüsselungsverfahren, das von R. Rivest, A. Shamir und L. Adleman während des Versuchs, eine Theorie zur Public-Key-Kryptografie zu widerlegen, entdeckt wurde. Es basiert auf einem Schlüsselpaar, das aus einem privaten und einem öffentlichen Schlüssel besteht. Während der private Schlüssel zum Entschlüsseln und Signieren von Daten verwendet wird, wird der öffentliche Schlüssel zum Verschlüsseln und zur Überprüfung der Signatur genutzt (vgl. [145] und [146]). 18

Root CA Die Certificate Authority (CA) beziehungsweise die Zertifizierungsstelle für digitale Zertifikate beschreibt eine Organisation, die solche Zertifikate herausgibt beziehungsweise diese unterzeichnet (beglaubigt) (vgl. [147]). Solche digitalen Zertifikate durchlaufen dabei eine Vertrauenskette (*chain of trust*), bei der unterschiedliche Zertifizierungsstellen das Zertifikat signieren.[148] Die Root CA ist dabei die *Wurzel des Vertrauens (Root of Trust)*, also die Instanz bei der diese Kette beginnt. 40, 42

Rooten Unter *Rooten* versteht man im Zusammenhang mit Android das Erlangen der Root-Rechte. *Root* steht dabei für den Nutzer mit den meisten Rechten in einem System. Er stellt somit den Administrator des Systems dar.[149] Durch das Erlangen dieser Rechte können die Zugriffsbeschränkungen des Herstellers eines Geräts

ausgehebelt werden und man bekommt uneingeschränkten Zugriff auf das System. 7–9, 36, 39, 49, 50, 58, 64

Sandbox Eine Sandbox beschreibt in der Informatik einen abgetrennten Bereich, in dem zum Beispiel Software ausgeführt wird, die keine Auswirkungen auf das gesamte System haben soll. 33

Secure Sockets Layer/Transport Layer Security (SSL/TLS) Bei SSL handelt es sich um die Vorgängerbezeichnung von TLS und wird häufig an dessen Stelle genannt. Dabei ist das SSL-Protokoll seit der Version 3.0 als TLS weiterentwickelt worden. Es ist ein hybrides Verschlüsselungsprotokoll mit dem Zweck, die Übertragung von Daten im Internet abzusichern (vgl. [151]). 42, 43, 54, 55, 58, 60

Secure/Multipurpose Internet Mail Extensions (S/MIME) Es handelt sich hierbei um einen Standard für die Verschlüsselung und Signatur von E-Mails. S/MIME basiert auf einer hybriden Verschlüsselung (also symmetrische und asymmetrische Verschlüsselung). Für die asymmetrische Verschlüsselung wird ein Schlüsselpaar benötigt, was oft zusammen mit einem S/MIME-Zertifikat von einer Zertifizierungsstelle generiert wird. Das Zertifikat enthält dabei den öffentlichen Schlüssel eines Kommunikationspartners und dient zur Bestätigung der jeweiligen Identität (vgl. [150]). 42

Thin Client Bei einem Thin Client handelt es sich um einen Netz-Computer, dessen Betriebssystem und Anwendungssoftware auf einem zentralen Server liegen (vgl. [152]). 51

Tunnel Ein Tunnel beschreibt in der Informatik die zusätzliche Kapselung einer Kommunikation in ein weiteres Kommunikationsprotokoll während der Übertragung zwischen zwei Kommunikationspartnern. So kann die Kommunikation bei der Verwendung eines entsprechenden Tunnelprotokolls gegen Abhören und Manipulation gesichert werden (vgl. [153]). 35

Literaturverzeichnis

[1] Beiersmann, Stefan (2012): „Zahl der Smartphone-Nutzer übersteigt erstmals die Milliardengrenze“. URL: http://www.zdnet.de/88127635/zahl-der-smartphone-nutzer-uebersteigt-erstmals-milliardengrenze/ [Stand: 11.07.2013]

[2] Beiersmann, Stefan (2013): „Android erreicht 70 Prozent Marktanteil in Europa“. URL: http://www.zdnet.de/88160639/android-erreicht-70-prozent-marktanteil-in-europa/ [Stand: 11.07.2013]

[3] heise online (2013): „Verfassungsschutz-Chef sieht keine NSA-Wirtschaftsspionage in Deutschland“. URL: http://www.heise.de/ix/meldung/Verfassungsschutz-Chef-sieht-keine-NSA-Wirtschaftsspionage-in-Deutschland-1943975.html [Stand: 15.09.2013]

[4] Wikipedia: „Informationssicherheit“. URL: http://de.wikipedia.org/wiki/Informationssicherheit [Stand: 06.09.2013]

[5] ITWissen: „Informationssicherheit“. URL: http://www.itwissen.info/definition/lexikon/Informationssicherheit-information-security.html [Stand: 06.09.2013]

[6] Universität Bremen, Kurs: Informationssicherheit WS 12/13. isec12-0.pdf.

[7] Elschner, Helmut (2009): „DIN ISO/IEC 27001:2005 Informationssicherheits-Managementsysteme“. URL: http://hitforum.de/iso27001-hit.pdf. [Stand: 06.09.2013]

[8] Weigmann, Matthias (2012): „Kurz erklärt: Informationssicherheit“. URL: http://www.anmatho.de/kurz-erklaert-informationssicherheit/ [Stand: 15.09.2013]

[9] Eckert, Claudia: *IT-Sicherheit. Konzepte – Verfahren – Protokolle.* Auflage: 5. München: Oldenbourg Wissenschaftsverlag, 2007.

[10] Bundesamt für Sicherheit in der Informationstechnik: „Denial-of-Service-Attacken“. URL: https://www.bsi-fuer-buerger.de/BSIFB/DE/GefahrenImNetz/DoS/dos_node.html [Stand: 21.09.2013]

[11] Kolokythas, Panagiotis (2013): „Facebook-Schwachstelle nach falschem Zuckerberg-Post behoben“. URL: http://www.pcwelt.de/news/Facebook-Schwachstelle_nach_falschem_Zuckerberg-Post_behoben-Sicherheit-8154281.html [Stand: 22.09.2013]

[12] Mag. Dr. Siller, Helmut: „Exploit“. URL: http://wirtschaftslexikon.gabler.de/Definition/exploit.html [Stand: 22.09.2013]

[13] Bundesamt für Verfassungsschutz: „Wirtschaftsspionage“. URL: http://www.verfassungsschutz.de/de/service/glossar/_lW#wirtschaftsspionage [Stand: 22.09.2013]

[14] heise online (2013): „NSA-Spionage: Empörung in Deutschland“. URL: http://www.heise.de/newsticker/meldung/NSA-Spionage-Empoerung-in-Deutschland-1884873.html [Stand: 22.09.2013]

[15] Bundesamt für Sicherheit in der Informationstechnik: *Leitfaden Informationssicherheit. IT-Grundschutz kompakt.*.

[16] Kling, Bernd (2013): „NSA-Affäre: RSA warnt vor eigenem Produkt“. URL: http://www.zdnet.de/88170660/nsa-affaere-rsa-warnt-eigenem-produkt/ [Stand: 26.09.2013]

[17] Bundesamt für Sicherheit in der Informationstechnik: „Updates halten den Großteil von Schadsoftware ab“. URL: https://www.bsi-fuer-buerger.de/BSIFB/DE/Wissenswertes_Hilfreiches/Service/Aktuell/Meldungen/Updates_gegen_Schadsoftware_20110718.html;jsessionid=105029EE58AE8E099CA6912DC326E948.2_cid360 [Stand: 26.09.2013]

[18] All About SECURITY: „Security Awareness - der Faktor Mensch zwischen technischen Lösungen“. URL: http://www.all-about-security.de/security-artikel/organisation/mensch-und-security/artikel/11016-security-awareness-der-faktor-mensch-zwischen-technischen/ [Stand: 26.09.2013]

[19] BITKOM, DIN: *Kompass der IT-Sicherheitsstandards. Leitfaden und Nachschlagewerk*. Auflage 4.

[20] SAP AG: *SAP Pocketseminar. IT-Sicherheit für kleine und mittlere Unternehmen.* Auflage 2. SAP AG - Government Relations 2010.

[21] BITKOM: *Bring Your Own Device*. BITKOM 2013.

[22] ITWissen: „ByoD (bring your own device)“. URL: http://www.itwissen.info/definition/lexikon/ByoD-bring-your-own-device.html [Stand: 26.09.2013]

[23] Schlede, Frank-Michael und Bär, Thomas (2012): „MDM-Anforderungen und -Lösungen. Ratgeber: Mobile Device Management - den mobilen Geräte-Zoo im Griff behalten “. URL: http://www.tecchannel.de/netzwerk/management/2039192/ratgeber_mobile_device_management_mdm/index2.html [Stand: 26.09.2013]

[24] Jentzsch, Jana: „Bring Your Own Device – Rechtliche Aspekte“. URL: http://www.fides-it-consultants.de/fileadmin/content/bilder/IT/docs/Vortrag_Datenschutz_20120911_BYOD_Dr._Jentzsch.pdf [Stand: 26.09.2013]

[25] Datenschutzbeauftragter INFO: „Bring Your Own Device (BYOD) – Nutzen und Risiken des neuen Trends aus Unternehmensperspektive“. URL: https://www.datenschutzbeauftragter-info.de/bring-your-own-device-byod-nutzen-und-risiken-des-neuen-trends-aus-unternehmensperspektive/ [Stand: 26.09.2013]

[26] Schlenker, Roman: „Bring Your Own Device“. URL: http://www.google.de/url?sa=t&rct=j&q=&esrc=s&source=web&cd=5&ved=0CIMBEBYwBA&url=http%3A%2F%2Fwww.it-sa.de%2FFilestore.aspx%2FAU_Do_13_40_Schlenker.

pdf%3Ffair%3Ditsa%26type%3Ddissertation%26key%3Df18b1d41-8464-440b-9c7e-699de5ae2eec%26language%3Dde%26filegroup%3Dfa23bae7-8eb5-4d15-a034-2e42fbf51f23%26filetype%3Dfile%26indexfile%3Dtrue&ei=_xlIUs40xpWzBvTjgagN&usg=AFQjCNGSwtYdQ3w-BGzWhhUQyuFBZf2luw&sig2=lekBwjZToObS9YE9JUjv2A&bvm=bv.53217764,d.Yms [Stand: 26.09.2013]

[27] Bundesministerium der Justiz: „Bundesdatenschutzgesetz“. URL: http://www.gesetze-im-internet.de/bdsg_1990/__7.html [Stand: 26.09.2013]

[28] European Network and Information Security Agency: *Smartphones: Information security risks, opportunities and recommendations for users*. Dezember 2010.

[29] Bundesamt für Sicherheit in der Informationstechnik: *Überblickspapier Smartphones*.

[30] European Network and Information Security Agency: „Unintentional disclosure of data“. URL: http://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-applications/smartphone-security-1/top-ten-risks/unintentional-disclosure-of-data [Stand: 03.10.2013]

[31] Beiersmann, Stefan (2012): „Bericht: Nokia-Patent verhindert Multi-User-Support auf Android-Smartphones“. URL: http://www.zdnet.de/88129537/bericht-nokia-patent-verhindert-multi-user-support-auf-android-smartphones/ [Stand: 03.10.2013]

[32] reddit: „Official Android 4.3 Questions And Answers Thread [...]“. URL: http://www.reddit.com/r/Android/comments/1j0lo5/official_android_43_questions_and_answers_thread/cb9wu70 [Stand: 03.10.2013]

[33] android tv: „Google: Multi-User-Option bei Android-Smartphones“. URL: http://www.go2android.de/google-multi-user-option-bei-android-smartphones/ [Stand: 03.10.2013]

[34] Dwivedi, Himanshu / Clark, Chris / Thiel, David: *Mobile Application Security*. USA: McGraw-Hill, 2010.

[35] Wikipedia: „Liste von Android-Versionen“. URL: http://de.wikipedia.org/wiki/Liste_von_Android-Versionen [Stand: 05.10.2013]

[36] Wikipedia: „Android (Betriebssystem)“. URL: http://de.wikipedia.org/wiki/Android_%28Betriebssystem%29 [Stand: 05.10.2013]

[37] Künneth, Thomas: *Android 4. Apps entwickeln mit dem Android SDK* Auflage 2. Bonn:Galileo Press, 2012.

[38] Android: „Android Security Program Overview“. URL: http://source.android.com/devices/tech/security/index.html#android-security-program-overview [Stand: 06.10.2013]

[39] Becker, Arno: „Innenansichten. Die Architektur von Android“. URL: http://www.heise.de/ct/artikel/Innenansichten-1176816.html [Stand: 07.10.2013]

[40] Obeid, Pascal / Kunz, Michael / Jelitto, Marcel: „Sicherheitsaspekte von Google Android“. URL: http://winfwiki.wi-fom.de/index.php/Sicherheitsaspekte_von_Google_Android#cite_note-32 [Stand: 07.10.2013]

[41] Android Developers: „Permissions“. URL: http://developer.android.com/guide/topics/security/permissions.html# [Stand: 08.10.2013]

[42] Computerwoche: „Das Android-Sicherheitskonzept“. URL: http://www.computerwoche.de/a/das-android-sicherheitskonzept,1233419 [Stand: 09.10.2013]

[43] Privacy-PC: „Bypassing the Android Permission Model 7: Exploiting Open Interfaces to Steal Permissions “. URL: http://privacy-pc.com/articles/bypassing-the-android-permission-model-7-exploiting-open-interfaces-to-steal-permissions.html [Stand: 09.10.2013]

[44] ITWissen: „XAUTH (extended authentication)“. URL: http://www.itwissen.info/definition/lexikon/extended-authentification-XAUTH-Extended-Authentification-Protokoll.html [Stand: 10.10.2013]

[45] heise Security: „Der Todesstoß für PPTP “. URL: http://www.heise.de/security/artikel/Der-Todesstoss-fuer-PPTP-1701365.html [Stand: 10.10.2013]

[46] mobiFlip: „Schon gewusst? Android im abgesicherten Modus starten“. URL: http://www.mobiflip.de/android-abgesicherter-modus/ [Stand: 10.10.2013]

[47] gamona: „Nach Root oder Flash: Gewährleistungsansprüche bleiben bestehen“. URL: http://www.gamona.de/hardware/android,nach-root-oder-flash-gewaehrleistungsansprueche-bleiben:news,2181579.html [Stand: 20.11.2013]

[48] Chip: „Custom-ROMs für Ihren Androiden“. URL: http://www.chip.de/artikel/Custom-ROM-fuer-Android-CyanogenMod-Paranoid-Android-AOKP-und-mehr_63228054.html [Stand: 10.10.2013]

[49] Sirrix AG: „TrustedMobile BizzTrust“. URL: http://www.sirrix.de/content/pages/63769.htm [Stand: 10.10.2013]

[50] airwatch: „Vollständige Mobilitätsverwaltung“. URL: http://www.air-watch.com/de/ [Stand: 10.10.2013]

[51] Google Play: „PGP SMS“. URL: https://play.google.com/store/apps/details?id=com.woodkick.pgpsms&hl=de [Stand: 10.10.2013]

[52] Android Developers: „Android 1.6 Platform Highlights“. URL: http://developer.android.com/about/versions/android-1.6-highlights.html [Stand: 11.10.2013]

[53] Android Developers: „Android 2.2 Platform Highlights“. URL: http://developer.android.com/about/versions/android-2.2-highlights.html [Stand: 11.10.2013]

[54] Wikipedia: „Android version history“. URL: http://en.wikipedia.org/wiki/Android_version_history [Stand: 11.10.2013]

[55] GIGA Android: „Das ist Android 4.0 Ice Cream Sandwich“. URL: http://www.giga.de/apps/android-ice-cream-sandwich/news/das-ist-android-4-0-ice-cream-sandwich/ [Stand: 11.10.2013]

[56] Murphy, Finnbarr P.: *Position Independent Executables*. URL: http://blog.fpmurphy.com/2008/06/position-independent-executables.html?output=pdf [Stand: 11.10.2013]

[57] Android: „Security Enhancements in Android 4.2“. URL: http://source.android.com/devices/tech/security/enhancements42.html [Stand: 11.10.2013]

[58] Android: „Security Enhancements in Android 4.3“. URL: http://source.android.com/devices/tech/security/enhancements43.html [Stand: 11.10.2013]

[59] TNW: „Google's KeyChain API makes Android more attractive for the enterprise“. URL: http://thenextweb.com/dd/2012/03/13/googles-keychain-api-makes-android-more-attractive-for-the-enterprise/ [Stand: 15.10.2013]

[60] DFN-CERT Portal: „DFN-CERT-2013-1375: Schwachstelle in GPM“. URL: https://portal.cert.dfn.de/adv/DFN-CERT-2013-1375/ [Stand: 15.10.2013]

[61] Duo Security : „Exploit Mitigations in Android Jelly Bean 4.1“. URL: https://blog.duosecurity.com/2012/07/exploit-mitigations-in-android-jelly-bean-4-1/ [Stand: 15.10.2013]

[62] International Buisiness Times: „Sony Xperia Z2 Avatar Specs: 10 Upgrades Including IGZO Display, Android 4.4 KitKat, Xenon Flash, 20.7MP/3.5MP Sony G Lens Camera“. URL: https://blog.duosecurity.com/2012/07/exploit-mitigations-in-android-jelly-bean-4-1/ [Stand: 15.10.2013]

[63] heise online: „Nato lässt Blackberrys für vertrauliche Kommunikation zu“. URL: http://www.heise.de/newsticker/meldung/Nato-laesst-Blackberrys-fuer-vertrauliche-Kommunikation-zu-1971256.html [Stand: 15.10.2013]

[64] FOCUS online: „Gerüchte um das iPhone 5S. Gibt es das iPhone 5S auch in Gold?“. URL: http://www.focus.de/kultur/vermischtes/iphone-5s-blueht-dem-iphone-5s-eine-goldene-zukunft_aid_1075953.html [Stand: 15.10.2013]

[65] Apple: *iOS Security*. Oktober 2012.

[66] Technische Universität München: „Vorlesung Sichere Mobile Systeme. Kapitel 6: Sicherheitsarchitekturen mobiler Endgeräte“. URL: http://www.sec.in.tum.de/assets/lehre/ss13/sms/sms-kap6-mobdev-teil2.pdf [Stand: 16.10.2013]

[67] apple.com: „System architecture“. URL: http://www.apple.com/iphone/business/it/security.html [Stand: 16.10.2013]

[68] Microsoft: *Windows Phone 8 Security Guide*. September 2013.

[69] netzwelt: „Android-Backup ohne Root: So gelingt die Sicherung“. URL: http://www.netzwelt.de/news/96723_3-android-backup-ohne-root-so-gelingt-sicherung.html [Stand: 19.10.2013]

[70] Apple Support: „iOS: Ihre Inhalte sichern und wiederherstellen“. URL: http://support.apple.com/kb/HT1766?viewlocale=de_DE&locale=de_DE [Stand: 19.10.2013]

[71] Windows Phone: „Grundlagen. Sichern von Daten“. URL: http://www.windowsphone.com/de-de/how-to/wp8/basics/back-up-my-stuff [Stand: 19.10.2013]

[72] Tippscout.de: „So sichern Sie Ihr Windows Phone 8 mit einer Kenn-Nummer“. URL: http://www.tippscout.de/windows-phone-8-sperre_tipp_6082.html [Stand: 19.10.2013]

[73] com!: „Wie sicher ist Windows Phone 8?“. URL: http://www.com-magazin.de/news/sicherheit/wie-sicher-ist-windows-phone-8-65498.html [Stand: 19.10.2013]

[74] Der Hessische Datenschutzbeauftragte: „Infoblatt zum Umgang mit iOS- und Android-Geräten“. URL: http://www.datenschutz.hessen.de/tf016.htm [Stand: 19.10.2013]

[75] Windows Phone: „How to create an S/MIME message in Windows Phone 8?“. URL: http://social.msdn.microsoft.com/Forums/wpapps/en-US/f7f9d05c-1273-440d-8406-021e2ffaa8c1/how-to-create-an-smime-message-in-windows-phone-8 [Stand: 19.10.2013]

[76] ZDNet: „Microsoft to add VPN support to Windows Phone 8 in 2014?“. URL: http://www.zdnet.com/microsoft-to-add-vpn-support-to-windows-phone-8-in-2014-7000017903/ [Stand: 19.10.2013]

[77] Windows Phone Centralt: „Microsoft's first OTA update for Windows Phone 8 OS now live for HTC 8X“. URL: http://www.wpcentral.com/first-ota-update-windows-phone-8-os-now-live-htc-8x [Stand: 19.10.2013]

[78] CHIP online: „iOS 7-Update: Drahtlos installieren via OTA“. URL: http://www.chip.de/news/iOS-7-Update-Drahtlos-installieren-via-OTA_64446759.html [Stand: 19.10.2013]

[79] Pretioso Blog: „datomo Mobile Device Management (MDM) 3.8“. URL: http://pretioso-blog.com/datomo-mobile-device-management-mdm-3-8-21-neue-features-im-neuen-master-release-fuer-android-blackberry-iphone-ipad-und-windows-mobile/ [Stand: 19.10.2013]

[80] Apple: „iCloud. Find My iPhone, iPad, and Mac“. URL: http://www.apple.com/icloud/find-my-iphone.html [Stand: 19.10.2013]

[81] androidcentral: „Hands-on with the Android Device Manager remote wipe feature“. URL: http://www.androidcentral.com/hands-android-device-manager-remote-wipe-feature [Stand: 19.10.2013]

[82] Google Play: „Google Apps Device Policy“. URL: https://play.google.com/store/apps/details?id=com.google.android.apps.enterprise.dmagent [Stand: 19.10.2013]

[83] Apple: „Managing iOS devices“. URL: http://www.apple.com/ipad/business/it/management.html [Stand: 19.10.2013]

[84] Windows Phpne: *Windows Phone 8 Device Management Overview.* Oktober 2012.

[85] Apple: „iOS: Setting up Exchange ActiveSync“. URL: http://support.apple.com/kb/HT2480 [Stand: 19.10.2013]

[86] PC Welt: „So lange dauert das Passwort-Knacken“. URL: http://www.pcwelt.de/ratgeber/So-lange-dauert-das-Passwort-Knacken-172195.html [Stand: 19.10.2013]

[87] Bundesamt für Sicherheit in der Informationstechnik: *Überblickspapier Consumerisation und BYOD.* Version 1.2. Juli 2013

[88] IABG: „Das V-Modell XT. Teil 5: V-Modell-Referenz Produkte“. URL: http://v-modell.iabg.de/v-modell-xt-html/14794f684e963e8.html [Stand: 01.11.2013]

[89] Dr.-Ing. Schaefer, Ina: *Anforderungsanalyse. Software Engineering I.* WS 2010/2011. TU Braunschweig.

[90] heise online: „Google will das Android-Update-Problem lösen – mal wieder“. URL: http://www.heise.de/newsticker/meldung/Google-will-das-Android-Update-Problem-loesen-mal-wieder-1865491.html [Stand: 30.10.2013]

[91] Good Technology: „Secure Mobility Solutions. Unlock your mobile potential“. URL: http://www1.good.com/secure-mobility-solution/ [Stand: 01.11.2013]

[92] Google play: „Good for Enterprise™“. URL: https://play.google.com/store/apps/details?id=com.good.android.gfe&hl=de [Stand: 01.11.2013]

[93] Good Technology: *Protect mobile collaboration. Good for Enterprise.* 2012

[94] Good Technology: *Wrapping or Coding: Pros and Cons of Containerization Choices.* 2013

[95] Good Technology: „Good Dynamics Marketplace“. URL: https://begood.good.com/marketplace.jspa#/?categoryFilter=10000&partnerFilter=-1 [Stand: 01.11.2013]

[96] Chip online: „Mobile Allzweckwaffe: Good for Enterprise“. URL: http://business.chip.de/artikel/Smartphones-und-Tablets-im-Unternehmen-verwalten-4_54343862.html [Stand: 01.11.2013]

[97] Nubo: „How it Works“. URL: http://www.nubosoftware.com/howItWorks.html [Stand: 01.11.2013]

[98] Nubo: „Security“. URL: http://www.nubosoftware.com/security.html [Stand: 01.11.2013]

[99] VMware: „VMware Horizon Workspace. Funktionen“. URL: http://www.vmware.com/de/products/horizon-workspace/features.html [Stand: 01.11.2013]

[100] VMware: *VMware Horizon Workspace Security Features*. 2013

[101] Good Technology: *Good for Enterprise: Android*. 2012

[102] Good Technology: *Android Handheld and Tablet User's Guide*. Version 2.1.0. 2013

[103] The Gadget Gurus: „How good is Good for Enterprise?". URL: http://thegadgetgurus.net/2012/04/25/how-good-is-good-2/ [Stand: 02.11.2013]

[104] Wikipedia: „Datenschutz". URL: http://de.wikipedia.org/wiki/Datenschutz#Regelungen [Stand: 02.11.2013]

[105] beGood Communities: „What's New in Good for Enterprise - Android v2.0". URL: https://begood.good.com/blogs/product_blog/2012/08/18/whats-new-in-good-for-enterprise--android-v20 [Stand: 02.11.2013]

[106] Good Technology: „Good Vault. Starke Zwei-Faktor-Authentifizierung und S/MIME-Signatur und -Verschlüsselung für E-Mails". URL: http://de.good.com/applications/collaboration-suite/good-for-enterprise/good-vault [Stand: 02.11.2013]

[107] Amazon: „Good for Enterprise". URL: http://www.amazon.com/Good-Technology-Inc-for-Enterprise/dp/B0072HDUJC [Stand: 02.11.2013]

[108] Nubo: „MOBILE DEVICES". URL: http://www.nubosoftware.com/mobiledevices.html [Stand: 02.11.2013]

[109] Nubo: „Benefits. Select Your Apps and Feel at Home While at Work". URL: http://www.nubosoftware.com/benefits.html [Stand: 02.11.2013]

[110] TechRepublic: „Nubo virtualizes Android for the BYOD win". URL: http://www.techrepublic.com/blog/tablets-in-the-enterprise/nubo-virtualizes-android-for-the-byod-win/ [Stand: 02.11.2013]

[111] Nubo: „Nubo Launches World's First Android™- Based Remote Work Environment". URL: http://www.nubosoftware.com/newsDetail.html [Stand: 02.11.2013]

[112] golem.de: „VMware Horizon. Eine Art Virtualisierung für iOS". URL: http://www.golem.de/news/vmware-horizon-eine-art-virtualisierung-fuer-ios-1208-94156.html [Stand: 03.11.2013]

[113] Google play: „VMware Horizon Workspace". URL: https://play.google.com/store/apps/details?id=com.vmware.horizon.android&hl=de [Stand: 03.11.2013]

[114] Presse Box: „Dell-Umfrage zu BYOD: Unternehmen sehen positives Potential und Wettbewerbsvorteile". URL: http://www.pressebox.de/pressemitteilung/dell-gmbh/Dell-Umfrage-zu-BYOD-Unternehmen-sehen-positives-Potential-und-Wettbewerbsvorteile/boxid/572828 [Stand: 09.11.2013]

[115] Lead Digital: „Private Hardware in der Firma: BYOD bedeutet "Bring your own disaster"". URL: http://www.lead-digital.de/aktuell/work/private_hardware_in_der_firma_byod_bedeutet_bring_your_own_disaster [Stand: 09.11.2013]

[116] CIO: „5 entscheidende Fragen bei BYOD“. URL: http://www.cio.de/knowledgecenter/mobile_it/2877542/index2.html [Stand: 10.11.2013]

[117] nfon: „BYOD - BRING YOUR OWN DEVICE“. URL: https://www.nfon.net/fileadmin/user_upload/content_data/Studien/nfon_WhitePaper_BYOD.pdf [Stand: 10.11.2013]

[118] Android-Hilfe: „Custom-ROM ohne Root usw. möglich?“. URL: http://www.android-hilfe.de/root-hacking-modding-fuer-htc-one-x/347769-custom-rom-ohne-root-usw-moeglich.html [Stand: 11.11.2013]

[119] XDA Developers: „[Q] can I flash a custom rom without root???“. URL: http://forum.xda-developers.com/showthread.php?t=2312108 [Stand: 11.11.2013]

[120] CITE World: „Android KitKat security: Some nice additions, and one mind-boggling blunder“. URL: http://www.citeworld.com/security/22651/android-kitkat-security-blunder [Stand: 12.11.2013]

[121] android: „Security Enhancements in Android 4.4“. URL: http://source.android.com/devices/tech/security/enhancements44.html [Stand: 12.11.2013]

[122] Wikipedia: „Advanced Encryption Standard“. URL: http://de.wikipedia.org/wiki/Advanced_Encryption_Standard [Stand: 13.11.2013]

[123] Wikipedia: „Boot-ROM“. URL: http://de.wikipedia.org/wiki/Boot-ROM [Stand: 13.11.2013]

[124] Wikipedia: „Bootloader“. URL: http://de.wikipedia.org/wiki/Bootloader [Stand: 13.11.2013]

[125] Vorlesung Informationssicherheit: „Bösartige Software“. URL: http://www2.htw-dresden.de/~robge/is/vl/is-05-malware-6up.pdf [Stand: 14.11.2013]

[126] Wikipedia: „Compliance (BWL)“. URL: http://de.wikipedia.org/wiki/Compliance_%28BWL%29 [Stand: 14.11.2013]

[127] Wikipedia: „Custom-ROM“. URL: http://de.wikipedia.org/wiki/Custom-ROM [Stand: 14.11.2013]

[128] Wikipedia: „Exchange ActiveSync“. URL: http://de.wikipedia.org/wiki/Exchange_ActiveSync [Stand: 14.11.2013]

[129] Wikipedia: „Formatstring-Angriff“. URL: http://de.wikipedia.org/wiki/Formatstring-Angriff [Stand: 14.11.2013]

[130] Scut, Team Teso: *Exploiting Format String Vulnerabilities*. Version 1.2. September 2001.

[131] Wikipedia: „Hot Spot (WLAN)“. URL: http://de.wikipedia.org/wiki/Hot_Spot_%28WLAN%29 [Stand: 14.11.2013]

[132] Wikipedia: „Ganzzahlüberlauf“. URL: http://de.wikipedia.org/wiki/Ganzzahl%C3%BCberlauf [Stand: 14.11.2013]

[133] Wikipedia: „Pufferüberlauf“. URL: http://de.wikipedia.org/wiki/Puffer%C3%BCberlauf [Stand: 14.11.2013]

[134] Elektronik Kompendium: „IPsec - Security Architecture for IP“. URL: http://www.elektronik-kompendium.de/sites/net/0906191.htm [Stand: 14.11.2013]

[135] Wikipedia: „Kernel (Betriebssystem)“. URL: http://de.wikipedia.org/wiki/Kernel_%28Betriebssystem%29 [Stand: 14.11.2013]

[136] Wikipedia: „Layer 2 Tunneling Protocol“. URL: http://de.wikipedia.org/wiki/Layer_2_Tunneling_Protocol [Stand: 14.11.2013]

[137] SearchCIO: „LOB (line-of-business)“. URL: http://searchcio.techtarget.com/definition/LOB [Stand: 14.11.2013]

[138] Universität Bremen, Kurs: Informationssicherheit WS 12/13. *IT-Sicherheit: Zugriffskontrolle*. isec05-1a.pdf.

[139] Wikipedia: „National Security Agency“. URL: http://de.wikipedia.org/wiki/National_Security_Agency#cite_note-5 [Stand: 14.11.2013]

[140] Tec Channel: „No eXecute: CPU-Erweiterungen schützen vor Angriffen“. URL: http://www.tecchannel.de/server/prozessoren/402344/no_execute_cpu_erweiterungen_schuetzen_vor_angriffen/ [Stand: 14.11.2013]

[141] Wikipedia: „Nonce“. URL: http://de.wikipedia.org/wiki/Nonce [Stand: 14.11.2013]

[142] Phillip Rogaway: „Nonce-Based Symmetric Encryption“. URL: http://www.cs.ucdavis.edu/~rogaway/papers/nonce.pdf [Stand: 14.11.2013]

[143] Elektronik-Kompendium: „PPTP - Point-to-Point Tunneling Protocol“. URL: http://www.elektronik-kompendium.de/sites/net/0906141.htm [Stand: 14.11.2013]

[144] Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein: „PGP? Noch so eine Abkürzung...“. URL: https://www.datenschutzzentrum.de/selbstdatenschutz/internet/pgp/wasdas.htm [Stand: 14.11.2013]

[145] Uni Magdeburg: „Allgemeines zum RSA-Verfahren und Mathematische Grundlagen“. URL: http://fma2.math.uni-magdeburg.de/~bessen/krypto/krypto61.htm [Stand: 14.11.2013]

[146] Wikipedia: „RSA-Kryptosystem“. URL: http://de.wikipedia.org/wiki/RSA-Kryptosystem [Stand: 14.11.2013]

[147] Wikipedia: „Zertifizierungsstelle“. URL: http://de.wikipedia.org/wiki/Zertifizierungsstelle [Stand: 15.11.2013]

[148] Wikipedia: „Root certificate“. URL: http://en.wikipedia.org/wiki/Root_certificate [Stand: 15.11.2013]

[149] AndroidPit: „Root“. URL: http://www.androidpit.de/de/android/wiki/view/Root [Stand: 15.11.2013]

[150] t3n: „Mails verschlüsseln: Was ist eigentlich S/MIME und wie richte ich es ein?“. URL: http://t3n.de/news/mails-verschlusseln-eigentlich-482381/ [Stand: 15.11.2013]

[151] Wikipedia: „Transport Layer Security“. URL: http://de.wikipedia.org/wiki/Transport_Layer_Security [Stand: 15.11.2013]

[152] ITWissen: „Thin-Client“. URL: http://www.itwissen.info/definition/lexikon/Thin-Client-TC-thin-client.html [Stand: 15.11.2013]

[153] Wikipedia: „Tunnel (Rechnernetz)“. URL: http://de.wikipedia.org/wiki/Tunnel_%28Rechnernetz%29 [Stand: 15.11.2013]

[154] Wikipedia: „PRISM“. URL: http://de.wikipedia.org/wiki/PRISM [Stand: 15.11.2013]