BYOD

Konzeptionierung einer Entscheidungsempfehlung für ein mittelständiges Unternehmen

Studienarbeit

für die Prüfung zum

Bachelor of Engineering

Studiengang Informationstechnik

Duale Hochschule Baden-Württemberg Karlsruhe

von

Nicolas Konle, Luka Kröger

Abgabedatum:	6. April 2018
Bearbeitungszeitraum:	12 Wochen
Matrikelnummer, Kurs:	MATRIKELNUMMERN, TINF15B3
Betreuer der Dualen Hochschule:	Ralf Brune

Eidesstattliche Erklärung

Ich versichere hiermit, dass ich meine Studienarbeit mit dem Thema

> *BYOD - Konzeptionierung einer Entscheidungsempfehlung für ein mittelständiges Unternehmen*

selbständig verfasst und keine anderen als die angegebenen Quellen und Hilfsmittel benutzt habe. Die Arbeit wurde bisher keiner anderen Prüfungsbehörde vorgelegt und auch nicht veröffentlicht.

Mir ist bekannt, dass ich meine Diplomarbeit zusammen mit dieser Erklärung fristgemäß nach Vergabe des Themas in dreifacher Ausfertigung und gebunden im Sekretariat meines Studiengangs an der DHBW Karlsruhe abzugeben habe. Als Abgabetermin giltbei postalischer Übersendung der Eingangsstempel der DHBW, also nicht der Poststempel oder der Zeitpunkt eines Einwurfs in einen Briefkasten der DHBW.

Karlsruhe, den 6. April 2018

Nicolas Konle, Luka Kröger

Sperrvermerk

Abstract/Zusammenfassung

Hier bitte den Abstract Ihrer Arbeit eintragen. Der Abstract sollte nicht länger als eine halbe Seite sein. Bitte klären Sie mit Ihrem Studiengangsleiter ab, ob der Abstract in englischer oder deutscher Sprache (oder möglicherweise sogar in beiden Sprachen) verfasst werden soll.

Inhaltsverzeichnis

Abkürzungsverzeichnis

BYOD	Bring Your Own Device
DHBW	Duale Hochschule Baden-Württemberg
EMM	Enterprise Mobility Management
MAM	Mobile Application Management
MCM	Mobile Content Management
MDM	Mobile Device Management
NFO	Near Field Communication
OS	Operating System
OSS	Open Source Software
PKM	Periodic Kernel Measurements
RKP	Real-Time Kernel Protection
SLA	Service Level Agreement
VPN	Virtual Private Network

Abbildungsverzeichnis

Tabellenverzeichnis

1 Einleitung

1.1 Motivation

1.2 Ziel der Arbeit

1.3 Aufbau der Arbeit

1.4 Bring Your Own Device

In der heutigen Arbeitswelt hat die Geschwindigkeit ein Produkt auf den Markt zu bringen so sehr an Wert gewonnen, dass man dem ständigen Wettbewerb gerecht wird und als Unternehmen überlebt. Hierbei ist es nicht nur wichtig schnell zu sein, sondern auch flexibel. Dazu gehört in einem Unternehmen, die Möglichkeit, wo- und wann auch immer, Arbeit zu verrichten, zu den Voraussetzungen und Treibern, Erfolg im Wettkampf mit der Konkurrenz zu sichern. Die Denkweise der Arbeitnehmer heutiger Zeit, hat sich durch Globalisierung und Vernetzung so angepasst, dass es darum geht, welche Arbeit getan werden muss, und nicht wo. Das Equipment, dass von den Unternehmen den Arbeitnehmern aufgezwungen wird ist nicht nutzerfreundlich und veraltet, der Arbeitsplatz soll nicht mehr auf das Büro beschränkt sein und ein Arbeiten von zuhause und unterwegs ist wegen der ständigen Bewegung in der ÖnlineWelt nicht mehr wegzudenken. Die Grenze zwischen Arbeit und Leben der Arbeitnehmer vermischt sich immer mehr.

Bring Your Own Device (BYOD) beschreibt eine IT-Richtlinie, die, wie die deutsche Übersetzung "Bring dein eigenes Gerätöffenbart, Mitarbeitern eines Unternehmens erlaubt, eigene private Geräte im geschäftlichen Umfeld zu nutzen. Zu den Geräten dieser T̈rend-Richtlinie gehören hauptsächlich die Nutzung von Smartphones. Tablets oder Laptops sind ebenfalls umsetzbar, aber werden im Rahmen dieser Arbeit nicht behandelt. Um BYOD umsetzen zu können, werden EMM-Plattformen eingesetzt (siehe Abschnitt 3.4), welche die Trennung einer Arbeits- und Privatwelt auf den Geräten ermöglicht und dabei die Sicherheitsrichtlinien des Unternehmens einhält. Bevor jedoch erklärt wird, wie BYOD Lösungen umgesetzt werden können, gilt zuerst die Frage zu beantworten warum und wie es zu dieser IT-Bewegung kommt.

1.4.1 Vorteile

In einer Studie von Extreme Networks **ext2014** wurden deutsche Unternehmen nach Vorteilen, die sie sich aus dem Nutzen von BYOD erhoffen. Als Ergebnis, siehe Abb. 1.1 sind 43% erhöhte Mitarbeiterzufriedenheit, 32% erhöhte Produktivität der Mitarbeiter, 16% Kosteneinsparungen und 9% andere Gründe zu vermerken. Diese

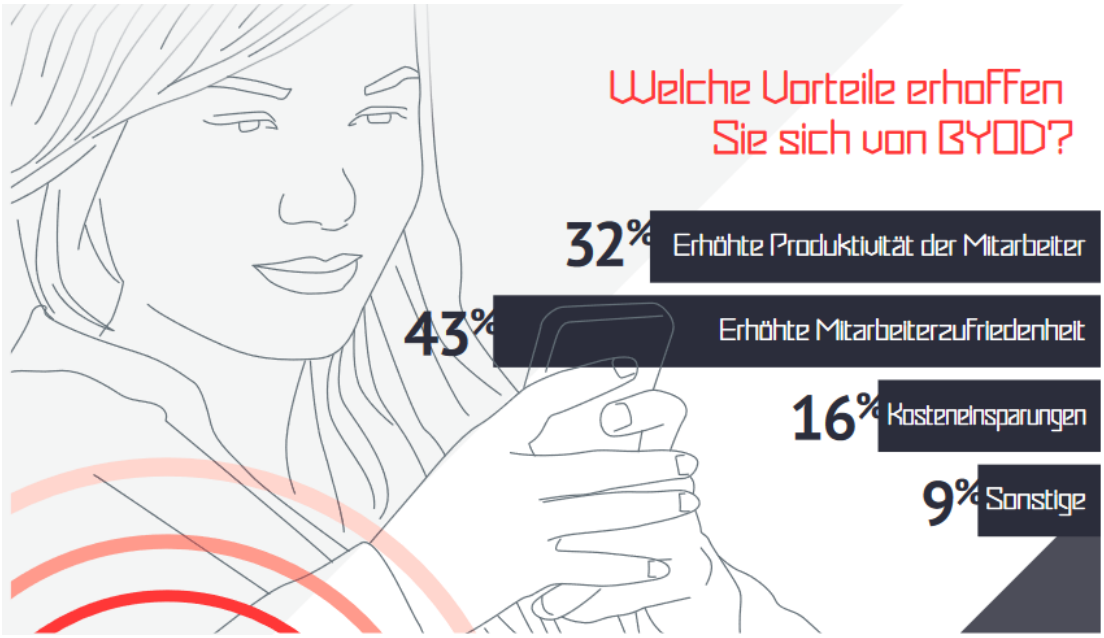

Abbildung 1.1: Umfrage: Erhoffte Vorteile von BYOD

Ziele lassen sich in Vorteile für den Endnutzer und für das Unternehmen unterteilen.[1] Dem Endnutzer bietet die Umsetzung von BYOD den Vorteil, die Freiheit, das Gerät nach ihren Präferenzen auszuwählen. Wie oben beschrieben löst BYOD das Problem der Stationärität des Arbeitnehmers. Das Arbeiten von zuhause und unterwegs ist damit kein Problem mehr. Subjektiv ist, ob BYOD einen positiven Einfluss auf das Work-Life-Balance hat, aber es hat zumindest den Vorteil, dass die Integration von Leben und Arbeit möglich ist. Daraus erhoffen sich die Unternehmen, dass durch das Nutzen eines Gerätes für das private Leben sowie für die Arbeit, die Mitarbeiterzufriedenheit und gleichzeitig das Engagement steigt.

Es ist zu erkennen, dass nicht nur dem Endnutzer aus diesem Aspekt, ein Vorteil geboten ist. BYOD, daraus abgeleitet Mitarbeiterzufriedenheit, hat als weitere Folge, die Attraktivität und das Image eines Unternehmens aufzubessern und so weitere qualifizierte Mitarbeiter zu gewinnen. Denn als Ziel von Unternehmen gilt wie in traditionellerweise die Suche von Talenten. Der Technologiefortschritt und die Flexibilität

[1] Vgl. **fuj2018**

eines Arbeitsplatzes ist im Vergleich zum konventionellen Angebot eines Firmenwagens mittlerweile deutlich attraktiver und erhält immer größere Signifikanz.

Das Mitarbeiter, ihre Arbeit mit dem Privatleben vermischen, bringt Unternehmen weitere Vorteile. Es ist Möglich zusätzlich neben den normalen Arbeitszeiten an Wochenenden zu arbeiten. Dies fördert nicht nur die komplette Produktivität sondern auch die Empfänglichkeit gegenüber der Kunden, welches weiterhin zu erhöhter Kundenzufriedenheit führt. Weiterhin verringert sich dadurch die Antwortzeit auf den Markt, fördert Innovation und sichert damit einen Vorsprung im Wettbewerb.

Wie in der Umfrage beschrieben, erhoffen sich Unternehmen einen Vorteil durch Kosteneinsparungen durch die Einführung von BYOD. Die Frage ob durch die Umsetzung ein Kostenvorteil entsteht und ist nicht direkt ablesbar, da es komplett abhängig von der vorher genutzten Infrastruktur eines Unternehmens ist. Nimmt man ein Unternehmen, welches viel Geld in Firmengelände investiert, damit dort die Mitarbeiter arbeiten können, ist ein großer Kostenvorteil denkbar. Denn lässt dieses mithilfe von BYOD einen Großteil der Mitarbeiter von zuhause arbeiten, können Ausgaben für Gelände und Arbeitsorte gespart werden.

Da Nutzer ihr eigenes Gerät verwenden, steigt die Fürsorge und Vorsicht darum. So können Kosten für Wartung und Ersatzvergabe präventiv klein gehalten werden. Da sich Nutzer mit den Geräten sich ständig auseinandersetzen, steigt die Erfahrung und das Wissen in der Benutzung. Folglich können damit Service Dienste intern gesenkt werden und damit weiter gespart werden.

1.4.2 Herausforderungen

2 Ausgangssituation

Im Rahmen dieser Studienarbeit wird das fiktive Unternehmen „Loco AG“ als Grundlage für die Konzeptionierung der Entscheidungsempfehlung verwendet, um eine konkrete Ausarbeitung zum Themenbereich „Bring your own Device“ zu geben. Im Folgenden wir das Unternehmen vorgestellt: Die „Loco AG“ ist ein mittelständiges Unternehmen ansässig in der Architekturbranche mit dem Hauptsitz in Karlsruhe. Das Unternehmen beschäftigt deutschlandweit 450 Mitarbeiter und hat einen jährlichen Umsatz von XXX€.

Das momentane Geschäftsmodell besteht darin, Kunden zu deren Geschäftsstellen zu bestellen und mit Ihnen in betriebseigenen Meetingräumen Geschäfte abzuschließen. Die „Loco AG“ möchte gerne Ihr Unternehmen erweitern und höherwertige Kunden erreichen. Hierbei evaluieren die Geschäftsführer mehrere Optionen für die Expansion: Die erste Variante wäre ein neues Kundencenter. Als zweite Lösung wäre die Änderung der Geschäftsstrategie auf den Außendienst. Das heißt die Beratung tritt direkt vorort beim Kunden statt.

Das Unternehmen verwendet eine internentwickelte Architektursoftware, welche Anbindung auf die zentralliegende Datenbank benötigt. Die Entwicklungsabteilung hat bereits eine Version für das Smartphone und Tablet entwickelt, aber es findet noch keine richtige Verwendung.

3 Grundlagen

In diesem Kapitel werden Grundlagen zum Thema BYOD gegeben die zum Verständnis der Arbeit benötigt werden.

3.1 Mobile Device Management (MDM)

Mobile Device Management (MDM) ist eine Technologie zur Lebenszyklusverwaltung, mit der die IT Mobilgeräte durch auf den Geräten installierte MDM-Profile einsetzen, konfigurieren, verwalten, unterstützen und sichern kann. MDM Software ermöglicht Anlageninventur, Over-the-Air-Konfiguration von E-Mail, Anwendungen und WLAN, Remotefehlerbehebung sowie Remotesperr- und Remote Wipe-Funktionen zur Sicherung von Geräten und den darauf befindlichen Unternehmensdaten. MDM ist die Grundlage für eine umfassende Enterprise Mobility Management-Lösung (EMM).

3.2 Mobile Application Management

Mobile Application Management-Technologien (MAM) wenden Tools der Verwaltungs- und Richtlinienkontrolle auf individuelle Anwendungen statt auf das gesamte Gerät an. Üblicherweise bieten MAM-Lösungen einen benutzerdefinierten App Store, der die Kontrolle und Bereitstellung von sowohl intern entwickelten als auch Drittanbieteranwendungen erlaubt. IT-Administratoren haben die Möglichkeit, mithilfe von App-Config Community-Standards oder Software Development Kit- oder App Wrapping-Lösungen vom MAM-Anbieter der Anwendung Sicherheits-, Verschlüsselungs- und Kontrollfunktionen hinzuzufügen.

3.3 Mobile Content Management

3.4 Enterprise Mobility Management

Enterprise Mobility Management (EMM) ist eine geräte- und plattformagnostische Lösung, in der die Verwaltung, Konfiguration und Sicherheit aller Geräte – BYO sowie unternehmenseigenen – einer Organisation zusammengefasst werden. EMM erstreckt sich über traditionelle Geräteverwaltung hinaus auf die Verwaltung und Konfiguration von Unternehmensanwendungen und -inhalten. Eine solide EMM-Lösung umfasst

üblicherweise MDM, MAM, Mobile Content Management (MCM), Identitätsmanagement zur Zugriffskontrolle sowie Produktivitätsanwendungen zum mühelosen Zugriff auf E-Mail, Kalender, Kontakte, Inhalts-Repositorys und Intranet-Sites des Unternehmens. Darüber hinaus sollte eine EMM-Lösung es technisch ermöglichen, der IT die Verwaltung und Sicherheit zu erleichtern und gleichzeitig den Mitarbeitern ein angenehmes Benutzererlebnis zu bieten.

3.5 Unified Endpoint Management

Mithilfe von Unified Endpoint Management (UEM) ist die IT endlich in der Lage, sich der unterschiedlichen Tools für die Verwaltung von Mobilgeräten, Desktops und seit Kurzem auch IdD-Geräten (Internet der Dinge) zu entledigen. Durch die Kombination von traditioneller Client-Verwaltung von Desktop- und PC-Systemen mit einem modernen Enterprise Mobility Management Framework (EMM) schaffen UEM-Lösungen die Voraussetzung für einen ganzheitlichen und anwenderorientierten Ansatz zur Verwaltung aller Endpunkte. Eine solide UEM-Lösung befähigt die IT zur Verwaltung von Benutzern und zur Realisierung eines einheitlichen Erlebnisses entlang aller Endpunkte sowie zur Sicherung und Verwaltung des gesamten Gerätelebenszyklus – und alles über eine zentrale, umfassende Plattform.

4 Datenschutz

Durch den Einsatz privater Endgeräte im Unternehmensumfeld kann es zu wechselseitigen Zugriffsmöglichkeiten auf private, personenbezogene Daten oder besonders schützenswerte Unternehmensdaten kommen. Um die Interessen natürlicher Personen zu wahren existieren Rechtsvorschriften. Für den Schutz von Unternehmensdaten hingegen müssen zusätzlich Maßnahmen zur Absicherung ergriffen werden.

4.1 Rechtsrahmen

Vor der Einführung einer Bring Your Own Device Lösung in einem Unternehmen entsteht juristischer Klärungsbedarf bezüglich der Gültigkeit verschiedener Rechtsvorschriften. In der Bundesrepublik Deutschland gelten folgende Gesetzestexte:

4.1.1 Bundesdatenschutzgesetz

Das Bundesdatenschutzgesetz (BDSG) ist wohl das bekannteste Gesetz im Kontext des Datenschutzes. Oberstes Ziel dieser Rechtsvorschrift ist es, das Persönlichkeitsrecht jeden einzelnen im Umgang mit personenbezogenen Daten zu wahren. Hierzu stellt das BDSG einige Grundsätze zum Schutz der personenbezogenen Daten auf. So ist das Speichern, Aufbewahren und Verarbeiten personenbezogener Daten nur in Verbindung eines Zweckes erlaubt, dies kann beispielsweise eine aktive Geschäftsbeziehung sein. Um diesen Zweck rechtfertigen muss die Betroffene Person im Voraus eine wirksame Einwilligung der Datenerhebung und Verarbeitung erteilen. Ist dies nicht der Fall, liegt ein sanktionierbarer Datenschutzverstoß vor. Allgemein ist zur Datenvermeidung bzw. Datensparsamkeit aufgerufen, um nur die für den Zweck der Datenverarbeitung nötigen Daten vorzuhalten. Ebenso darf nicht jeder Mitarbeiter eines Unternehmens, welches personenbezogene Daten speichert auf diese Zugriff haben. Somit muss eine Zugriffsbeschränkung der verschiedenen Personenkreise und ggf. eine Anonymisierung bzw. Pseudonominierung für diese stattfinden. Jede betroffene Person hat zu jeden Zeitpunkt das Recht auf Auskunft über die gespeicherten Daten und das Recht auf Änderung und Löschung. Bei dem Recht auf Löschung gibt es jedoch die Ausnahme, dass Unternehmen die personenbezogenen Daten speichern diese erst nach Ende der Zweckbindung plus die Dauer der gesetzlichen Aufbewahrungsfristen bspw. zehn Jahre bei Rechnungen löschen müssen.

Quelle: BSDG (https://dsgvo-gesetz.de/bdsg-neu/1-bdsg-neu/)

4.1.2 Europäische Datenschutz Grundverordnung

Die ab 25.Mai 2018 inkrafttretende Europäische Datenschutz Grundverordnung (EU-DSGVO) bringt einige Neuerungen im Bezug auf das Datenschutzrecht. Eine europäische Grundverordnung hat die Eigenschaft, dass diese in jedem Mitgliedstaat der Europäischen Union in lokales Recht umgewandelt werden muss. Folglich ergänzt beziehungsweise verstärkt die EU-DSGVO in Deutschland das Bundesdatenschutzgesetz. Neben den neuen gesetzlichen Rahmenbedingungen ändert sich auch der Bußgeldkatalog bei Datenschutzverstößen erheblich. Pro datenschutzrechtlichem Verstoß drohen einem Unternehmen eine Strafe bis zu einer Höhe von 20.000.000 Euro oder bis zu vier Prozent des gesamten weltweiten Jahresumsatzes. Die vom BDSG festgesetzten Bußgelder betragen derzeit maximal 300.000 Euro pro Datenschutzverstoß. Um keinen Datenschutzverstoß zu begehen, müssen sämtliche Unternehmen ihre Verarbeitungs- und Löschprozesse in Zusammenhang mit personenbezogenen Daten an die Neuerungen durch das EU-DSGVO anpassen. Die EU-DGVO schreibt neue Informations- und Transparenzpflichten vor, d.h. allen Betroffenen muss zu jeder Zeit Auskunft gegeben werden können, wohin seine persönlichen Daten hin übermittelt wurden und zu welchem Zweck dies geschah. Durch diese Maßnahme soll unter anderem der unbewusste Datenhandel von personenbezogenen Daten eingebremst werden. Zudem schränkt die EU-DSGVO den Datentransfer an Staaten außerhalb der Europäischen Union ein.

Quelle: https://www.datenschutzbeauftragter-info.de/fachbeitraege/eu-datenschutz-grundverordnung/

4.1.3 Arbeitsrecht

In den meisten Arbeitsverträgen sind neben den Standardinhalten kaum Sonderregelungen beinhaltet. In größeren Unternehmen werden die Arbeitsverträge meist durch Betriebsvereinbarungen ergänzt. Allerdings ist dort meist nur die private Nutzung von geschäftlicher Infrastruktur geregelt. Im Zuge der Einführung einer Bring Your Own Device sollte jedoch auch eine Betriebsvereinbarung für die Nutzung privater Endgeräte für geschäftliche Zwecke geregelt werden. Die Verabschiedung einer Betriebsvereinbarung ist in dem Betriebsverfassungsgesetz klar geregelt und benötigt dazu die Zustimmung des Betriebsrates und dem Arbeitgeber. In öffentlichen Sektor übernimmt der Personalrat die Rolle des Betriebsrates. In der Betriebsvereinbarung sollte auch vertraglich festgelegt werden, welchen Vergütungsanspruch oder Entschädigung der Mitarbeiter für die geschäftliche Nutzung der privaten Hardware erhält. Durch die Möglichkeit über BYOD immer auf geschäftliche Inhalte zugreifen zu können und folglich daraus eine Arbeitsleistung auch außerhalb der regulären Arbeitszeiten entsteht ist auch dies mit einem entsprechenden Zeitmodell oder sonstige Abfindung zu regeln.

4.1.4 Handelsgesetz

4.1.5 Strafrecht

4.1.6 Steuerrecht

4.2 Schützenswerte Daten

Ein Unternehmen hat daran Interesse, dass geheime Unterlagen und Dokumente nicht an die Öffentlichkeit gelangen. Da über ein BYOD System der Zugriff auf die Unternehmensinfrastruktur von privaten Endgeräten erlaubt wird, muss der Zugriff geregelt werden. Die klassische Isolierung von Daten für bestimmte Personenkreise findet meist durch eine entsprechende Berechtigungsstruktur statt. Jedoch kann bei privaten Endgeräten nicht garantiert werden, dass ausschließlich der legitimierte Mitarbeiter physikalischen Zugriff auf das Gerät hat. Folglich muss sowohl technisch als auch datenschutzrechtlich der Zugriff abgesichert werden. Technisch ist dies meist durch passwortgeschützte Containerlösungen realisiert. Damit sich das Unternehmen auch juristisch absichert sollten Verschwiegenheitserklärungen und Zusicherungen der Arbeitnehmer eingeholt werden, dass ausschließlich sie selbst auf die Inhalte zugreifen. Im Umkehrschluss darf auch das Unternehmen keine Möglichkeit erlangen auf die privaten Daten und Inhalte auf den Geräten er Mitarbeiter zu gelangen. Ebenso wenig darf es möglich sein, den Mitarbeiter über technische Mittel zu Kontrollieren. Dies muss ebenfalls vertraglich und technisch geklärt sein.

4.3 Weitere Aspekte

4.3.1 Zivilrecht

-Haftung

5 Systeme

Als Entscheidungsgrundlage für die Auswahl der zu vergleichenden "Bring Your Own Device"Lösungen dient das sogenannte "Magic Qadrant"von Gartner. Das Marktforschungsinstitut Gartner nutzt diese Art der Visualisierung um die Positionen verschiedener Unternehmen in einem Technologie-Markt darzustellen. Hierbei werden die Quadranten in die Bereiche Niche Players, Visionäre, Challengers und Leader unterteilt. Diese Bewertung dient als erste Filterung der in dieser Studienarbeit verglichenen BYOD Lösungen. Alle nachfolgenden Systeme erreichten die höchsten Punktzahlen um in den Quadranten Leader aufgenommen zu werden (Stand Juni 2016) Samsung Knox wurde von Gartner in dieser Auswertung nicht betrachtet. Aufgrund der hohen Marktanteile von Samsung Endgeräten wurde jedoch entschiedenen diese Lösung auch zu untersuchen. Quelle: Gartner Magic Quadrant

Abbildung 5.1: Entscheidungsgrundlage

5.1 MobileIron

5.1.1 Allgemein

Das Unternehmen MobileIron ist ein US-amerikanisches Unternehmen mit Hauptsitz in Kalifornien welches im Jahr 2007 gegründet wurde. MobileIron hat sich von Anfang an auf die Verwaltung von mobilen Endgeräten im Enterprise Umfeld spezialisiert. Das Unternehmen wurde 2017 im siebten Jahr in folge als Leader im Magic Quadrant von der Gartner Inc. neben VMWare, IBM und BlackBerry für MDM/EMM Suites gekürt. Das Softwareentwicklungsunternehmen bietet in Ihrem Produktportfolio verschiedene Bring Your Own Device Pakete mit zahlreichen Funktionen an.

5.1.2 Kompatibilität

Der Hersteller MobileIron unterstützt in seinen Lösungen die mobilen Endgeräte Apple iOS, Google Android und Microsofts Windows Phone. Zusätzlich können klassische Desktop Geräte mit den Betriebssystemen Microsoft Windows (ab 8.1) und Apple OS X (ab 10.9) verwaltet werden.

5.1.3 Paketmodelle

MobileIron bietet die drei verschiedenen Bundles „EMM Silver“, „EMM Gold“ oder „EMM Platinum“ seiner Bring Your Own Device Lösung an. Das Basispaket „EMM Silver“ beinhaltet die Komponenten „Core“ „Sentry „und „Apps@Work“. Das Paket „EMM Gold“ ist um die Module „Email+“, „Docs@Work“ und „Web@Work“ erweitert. Durch die Wahl des Platinum Pakets ergänzt sich dieses wiederum um „Help@Work“, „Tunnel“, „MobileIron Monitor“ und „ServiceConnect-Integration“.

5.1.4 Pakete

5.1.4.1 Core

Das Paket Core ist das zentrale Modul, welches das IT-Backend des Unternehmens einbindet. Hierüber können die erforderlichen Sicherheits- und Verwaltungsrichtlinien der mobilen Endgeräte definiert und verwaltet werden. Über die API Schnittstellen des Cores kann man komfortabel Erweiterungen nutzen. Im Fokus des Cores stehen jedoch die das MDM, MAM und MCM. Der Core bietet für die Administratoren zusätzliche Analyse- und Auswertungsfunktionen. So kann beispielsweise der von den Endgeräten produzierten Netzwerktraffic ausgewertet werden um Infrastrukturprobleme zu lokalisieren. Durch die Möglichkeit Dachboards-Widgets anzulegen kann der Administrator das System und die verschiedenen Gerätestatus komfortabel überblicken.

Mobile Sicherheit:	EMM Silver	EMM Gold	EMM Platinum
Core	✓	✓	✓
Sentry	✓	✓	✓
Apps@Work	✓	✓	✓
AppConnect		✓	✓
Email+		✓	✓
Docs@Work		✓	✓
Web@Work		✓	✓
Help@Work			✓
Tunnel			✓
MobileIron Monitor			✓
ServiceConnect-Integrationen			✓
MobileIron Bridge	Separates Produkt, erfordert MobileIron EMM-Bundles.		
Cloud-Sicherheit:			
MobileIron Access	Separates Produkt, MobileIron EMM Gold Bundle empfohlen.		

Abbildung 5.2: Mobile Iron Paketmodelle

5.1.4.2 Sentry

Die Komponente Sentry ist das Inline-Gateway, das den gesamten Netzwerkverkehr zwischen den Mobilgeräten und dem Unternehmensbackend verschlüsselt, verwaltet und sichert. Sentry setzt die in der Core Komponente definierten Sicherheitsrichtlinien um. Sentry kann beispielsweise E-Mail Anhänge verschlüsseln, sodass nicht autorisierte Applikationen auf diese Daten nicht zugreifen können.

5.1.4.3 Apps@Work

Apps@Work ist ein unternehmenseigener App Store, indem sowohl eigenentwickelte als auch öffentliche, freigegebene Anwendungen für die Benutzer bereitgestellt werden können. Über diesen Weg können Administratoren schnell auswählen, welche Anwendungen erforderlich, zulässig oder verboten sind.

5.1.4.4 AppConnect

Durch AppConnect können auf den Endgeräten installierte Applikationen geschützt werden. Hierbei werden die entsprechenden Anwendungen in Containern gekapselt und sind somit vor unberechtigtem Zugriff geschützt. Alle in Containern befindlichen Apps können durch eine Tunnellösung miteinander kommunizieren um beispielsweise die Funktion eines Single Sign Ons bereitzustellen oder den Austausch von Daten bereitzustellen.

5.1.4.5 Email+

Die gesamte Unternehmenskommunikation über mobile Endgeräte kann über die App Email+ abgewickelt werden. Die Anwendung stellt E-Mails, Kalender und Kontakte dar. Dabei findet eine strikte Trennung von beruflichen und privaten Inhalten statt.

5.1.4.6 Docs@Work

Die Anwendung Docs@Work ist ein Tool um Dokumente auf Endgeräten zu verwalten und zu editieren. Hierbei ist ein besonderes Augenmerk auf die Synchronisation und Sicherung der Daten gelegt.

5.1.4.7 Web@Work

Der Unternehmensbrowser Web@Works bietet dem Benutzer die Möglichkeit auf intern betriebene Webseiten oder Webapplikationen zuzugreifen. Dabei ist die komplette Kommunikation verschlüsselt. Über verschiedene Benutzergruppen können die Zugriffsrechte auf die verschiedenen internen Webressourcen reglementiert werden.

5.1.4.8 Help@Work

Help@Work ist ein Tool für die Fehlerdiagnose. Neben dem Abfragen und Übertragen von Ereignisprotokollen kann unter dem Betriebssystem Android sogar ein Remotezugriff für den IT-Support gewährt werden.

5.1.4.9 Tunnel

Der Tunnel von MobileIron bietet die Möglichkeit die Netzwerkkommunikationen einzelner Apps durch eine VPN Verbindung auf der Basis von Zertifikaten zu schützen.

5.1.5 Abrechnungsmodell

Je nach Tarifplänen bzw. Paketangeboten werden neben den genannten Grundfunktionen weitere Features unterstützt. Das Unternehmen selbst betreibt ein sehr flexibles Abrechnungsmodell, welches auf jegliche Bedürfnisse des Endkunden angepasst werden kann. Dabei kann beispielsweise zwischen einer Lizenzierung pro Benutzer (maximal 3 Endgeräte) oder einem Lizenzierungsmodell je nach Endgerät gewählt werden. Neben der Kaufoption von Lizenzen auf Lebenszeit wird auch ein Abonnement angeboten. Neben der klassischen Installation innerhalb des eigenen Netzwerks betreibt MobileIron auch eine eigene Cloud die für die Bereitstellung der Services genutzt werden kann. Falls sich der Endkunde für die Cloudlösung entscheidet kann direkt ein erweiterter Support (SLA) dazu gebucht werden. Für die Installation auf einem eigenen System kann hierbei nur zwischen einem Standard- und Premiumsupport unterschieden werden.

Abbildung 5.3: Mobile Iron Abrechnungsmodell

5.2 Samsung Knox

5.2.1 Allgemein

Das weltbekannte Unternehmen Samsung hat ebenfalls an einer Sicherheitslösung für die Mobilnutzung im Unternehmen gearbeitet. Als Produkt ist Samsung Knox, in Anlehnung an Hochsicherheitsstützpunkt Fort Knox, im Portfolio von Samsung zu finden. Ist man Besitzer aktueller Samsung-Geräten findet man die Applikation *Sicherer Ordner*[1]als vorinstallierte Standardsoftware vor. Mit Öffnen dieser App können, nach Eingabe eines benutzerdefinierten Sicherheitsverfahren, verschiedene Einstellungen getätigt werden. Es ist möglich Dateien oder Apps in diesen «sicheren Ordner»zu verschieben. Sogar Apps die vorher nicht auf dem Smartphone vorhanden sind, können direkt vom Store geladen und installiert werden.Theoretisch wäre dieser Lösungsansatz genau richtig für die Verwendung von BYOD und zusätzlich sogar kostenlos. Dennoch wäre dies nicht umsetzbar im Enterprise-Umfeld.

Um den Anforderungen an eine BYOD-Lösung der Loco AG gerecht zu werden, benötigt es eine MDM-Möglichkeit. Dafür muss die IT-Administration, die Möglichkeit haben die eingesetzten Geräte zu verwalten und somit an die firmeninternen Sicherheitsanforderungen anzupassen. Eine mögliche Lösung bietet Samsung mit der kostenpflichtigen Variante Samsung Knox Premium, die im Folgenden nach dem Kriterienkatalog belichtet werden soll.

[1]Sicherer Ordner löste am 19. Dezember 2017 den Vorgänger MyKnox ab **sk:myknox**

5.2.2 Knox-Plattform

Die Knox-Plattform ist die technische Umsetzung in Hardware und Software, welche standardmäßig in aktuellen Samsung-Geräten vorzufinden ist. Das Sicherheitsverfahren der Knox-Plattform besteht, wie in Abb. 5.4 sichtbar, aus fünf Komponenten. Die Knox-Plattform setzt bereits in der Hardware-Ebene ein. Der Prozessor ist die

Abbildung 5.4: Samsung Knox Security Solutions Layers

Steuereinheit auf dem bekanntlich das entsprechende Betriebssystem und die Applikationen laufen. Modi bestimmen welche Priorität, welcher Software oder Applikation zugeschrieben werden. So laufen vom Benutzer installierte Apps im Modus *user mode* und haben somit keinen direkten Zugriff auf die Hardware, das Betriebssystem oder auf andere Apps. Die *ARM TrustZone* beschreibt eine Prozessorarchitektur, die von der Knox-Plattform verwendet wird. Hierbei werden die Modi in *Worlds* eingeteilt. Zum einen die *Normal World*, auf dem standardmäßig alle installierte Software landet und die *Secure World*, die durch kryptographische Methoden gesichert wird und

sich in einer isolierten Hardwareumgebung befindet, und somit für das geschäftliche Nutzen des Smartphones eingesetzt werden soll.[2]

Beim Anschalten eines Gerätes, startet für gewöhnlich die Boot-Chain (zu dt. "Hochfahrkette"), die nacheinander die Softwarekomponenten startet. Zum Ausschließen von Fremd- oder Schadsoftware wird ein *Secure Boot* ausgeführt. Jede Komponente in der Kette prüft die Integrität der vorangehenden Komponente durch Abfrage einer Signatur. Wenn die Verifikation einer Signatur fehlschlägt, also eine mögliche Modifikation stattgefunden ist, wird entweder der weitere Startvorgang verhindert oder es wird der *Knox Warranty Fuse* ausgelöst, welcher prüft ob das Gerät vorher jemals einen unzulässigen Status hatte. Allerdings stößt *Secure Boot* beim Unterscheiden von akzeptierten Versionen an seine Grenzen, da er neue Versionen einer Software direkt als gültig sieht. Hierzu wird der *Trusted Boot* hinzugezogen, welcher beim Durchlaufen der Boot-Chain den Hash der nächsten Komponente in die TrustZone Secure World lädt.[3] Es kann also Software nur genehmigt und gestartet werden, die auch als erlaubt in der TrustZone stehen. Das Unternehmen hat die Kontrolle darüber, welche Versionen von welcher Software, sei es öffentlich zugängliche oder eigenentwickelte Software, verwendet werden sollen.

Denkbar wäre natürlich, dass während der Laufzeit, also nachdem die Überprüfung auf richtige Software, eine fälschliche Modifikation stattfindet. Um dem entgegenzuwirken nutzt Samsung Knox die *Real-Time Kernel Protection* (RKP) um Veränderungen am Kernel zu verhindern und die *Periodic Kernel Measurements* (PKM) zum periodischen Überprüfen der Integrität des Kernels.[4]. Diese beiden Sicherheitsverfahren spielen sich ebenfalls in der *TrustZone Secure World* ab und sind somit isoliert und nicht zugänglich vom Kernel. Weitere integrierte Verfahren in die Knox-Plattform sind Google DM Verify, genauer beschrieben in **Goo2017a**, welches überprüft ob das Gerät sich im selben Zustand befindet, wie beim letzten Start und SE for Android, genauer beschrieben in **Goo2017b**, dass *mandatory access control* (MAC) über alle Prozesse vollzieht.

5.2.3 Knox Solutions

5.2.3.1 Knox Configure

5.2.3.2 Knox Mobile Enrollment

Um ein EMM-System aufzubauen, ist es notwendig, dass die Mitarbeiter auch Samsung Knox auf ihrem Endgerät installiert haben. Dies findet häufig per Download vom *Google Play store* statt, dem darauf folgenden Authentifizieren und weiteren Einstellen des Workspaces auf die Unternehmensrichtlinien. Damit diese manuelle Installation

[2] Vgl. **sam2017c**
[3] Vgl. **sam2017d**
[4] Vgl. **sam2017d**

durch den Mitarbeiter vermieden und damit Fehler vermieden werden können, gibt es das *Knox Mobile Enrollment* (KME). Ein Enrollment durch KME funktioniert durch einen Link, der je nach Unternehmensbelangen, bspw. per E-Mail oder Interner Webseite an den Mitarbeiter vermittelt wird. Nachdem dieser Link aufgerufen wird, werden nach entsprechenden Authentifizierungsmaßnahmen, alle Einstellungen und Applikationen automatisch konfiguriert.

5.2.3.3 Knox Manage

5.2.3.4 Knox Workspace

Samsungs Knox Workspace entspricht dem in Abschnitt 5.2.1 beschriebenen «sicheren Ordner»in der Enterprise-Welt. Das heißt, es existiert eine Containerlösung für Mobilgeräte, ersichtlich in Abb. 5.5, auf dem geschäftliche Applikationen und Daten von den eigenen getrennt werden können. Es ist nicht möglich außerhalb des Workspaces auf Daten oder Applikationen innerhalb zuzugreifen, aber von innerhalb auf außerhalb. So ist es beispielsweise nicht möglich Bilder, die innerhalb des Workspaces gemacht wurden, außerhalb in der App Galerie anzuschauen.

Abbildung 5.5: Samsung Workspace Container

Um die Container des Samsungs Workspace zu verwalten, wird das *Mobile Container Management* verwendet. Hierbei können Authentifizierungsmöglichkeiten, Datensicherheit, VPN, Blacklisting und viele weitere Features, die wie andere EMM Lösungen nutzen gemanagt werden.

Um Zugang zum Workspace zu bekommen wird ein doppeltes Authentifizierungsverfahren verwendet. Hierzu muss der Nutzer zuerst den Fingerabdruck oder wenn es das Gerät zulässt, den Iris-Scanner nutzen und als zweites PIN oder Password eingeben. Erst dann ist ihm Zugriff gewährt. Andersrum ist es so möglich den Workplace als Authentifizierung zu nutzen. Hierzu gibt es beispielsweise die Möglichkeit per *Near Field Communication* (NFC) das Smartphone als SmartCard agieren zu lassen und so beispielsweise den Zugriff in Sicherheitsbereiche oder Accounts zu gewähren. Welche Methodiken schlussendlich, wie genutzt werden sollen, kann das IT Management des MCM's je nach Sicherheitsanforderung im Unternehmen anpassen.

5.2.3.5 Samsung E-FOTA

Mit der Samsung E-FOTA-Lösung können alle Geräte mit demselben Betriebssystem betrieben werden.

5.2.4 Kompatibilität

Um Knox Workspace, Knox Mobile Enrollment und Samsung E-FOTA zu nutzen benötigt es eine geeignete EMM-Lösung. In Abb. 5.6 sind einige EMM Lösungen und deren Kompatibilität mit den Samsung Knox Paketen aufgezeigt.

EMM-ANBIETER	KNOX-PLATTFORM, KNOX WORKSPACE	KNOX MOBILE REGISTRIERUNG	SAMSUNG E-FOTA
BlackBerry Enterprise Mobility	✓ Verfügbare Richtlinien anzeigen	✓	-
Citrix XenMobile	✓ Verfügbare Richtlinien anzeigen	✓	✓
DuoSTATION MDM	-	✓	-
FAMOC by FancyFon	-	-	✓
IBM MaaS360	✓ Verfügbare Richtlinien anzeigen	✓	✓
ManageEngine Mobile Device Manager	-	✓	-
Microsoft Intune	✓ Verfügbare Richtlinien anzeigen	-	-
MobileIron EMM	✓ Verfügbare Richtlinien anzeigen	✓	✓
Proget MDM	✓	✓	✓
SAP Cloud Platform	✓ Verfügbare Richtlinien anzeigen	-	-
SOTI MobiControl	✓ Verfügbare Richtlinien anzeigen	✓	-
Samsung SDS EMM	✓ Verfügbare Richtlinien anzeigen	✓	✓
Sophos Mobile	✓ Verfügbare Richtlinien anzeigen	-	-
VMware AirWatch	✓ Verfügbare Richtlinien anzeigen	✓	✓

Abbildung 5.6: Unterstützte EMM-Dienstleister

5.2.5 Kosten

5.3 VM AirWatch

5.3.1 Paketmodelle

5.3.2 Workspace ONE

Vmware Workspace ONE ist eine Enterprise-Plattform, die einen digitalen Workspace zu den entsprechenden und geforderten Bedürfnissen bietet. Dieser bietet dem Nutzer

5.3.3 Workspace Horizon

5.3.4 Kosten

Abbildung 5.7: AirWatch Kosten nach Paket

6 Zusammenfassung

6.1

6.2