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:	22. Februar 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 22. Februar 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
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

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 Definitionen

3.1 Bring Your Own Device

3.2 Mobile Device Management

Mobile Device Managemen ist der Überbegriff für ....

3.3 Mobile Application Management

3.4 Mobile Content Management

4 Systeme

Die Entscheidungsgrundlage

4.1 MobileIron

4.1.1 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 Unternhemen 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.

4.1.2 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.

4.1.3 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“.

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 4.1: Mobile Iron Paketmodelle

4.1.4 Pakete

4.1.4.1 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 Auswerungsfunktionen. 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.

4.1.4.2 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.

4.1.4.3 Apps@Work

Apps@Work ist ein unternhemenseigener 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.

4.1.4.4 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.

4.1.4.5 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.

4.1.4.6 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.

4.1.4.7 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.

4.1.4.8 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.

4.1.4.9 Tunnel

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

4.1.5 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 4.2: Mobile Iron Abrechnungsmodell

4.2 Samsung Knox

4.2.1 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.

4.2.2 Knox Platform

Das Sicherheitsverfahren der Knox-Plattform besteht, wie in Abb. 4.3 sichtbar, aus fünf Komponenten. Die Knox-Plattform setzt bereits in der Hardware-Ebene ein. Der Prozessor ist die 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 Auschließen von Fremd- oder Schadsoftware wird ein *Secure Boot* ausgeführt. Jede Komponente in

[1]Sicherer Ordner löste am 19. Dezember 2017 den Vorgänger MyKnox ab [Sa17b]
[2]Vgl. [Sa17c]

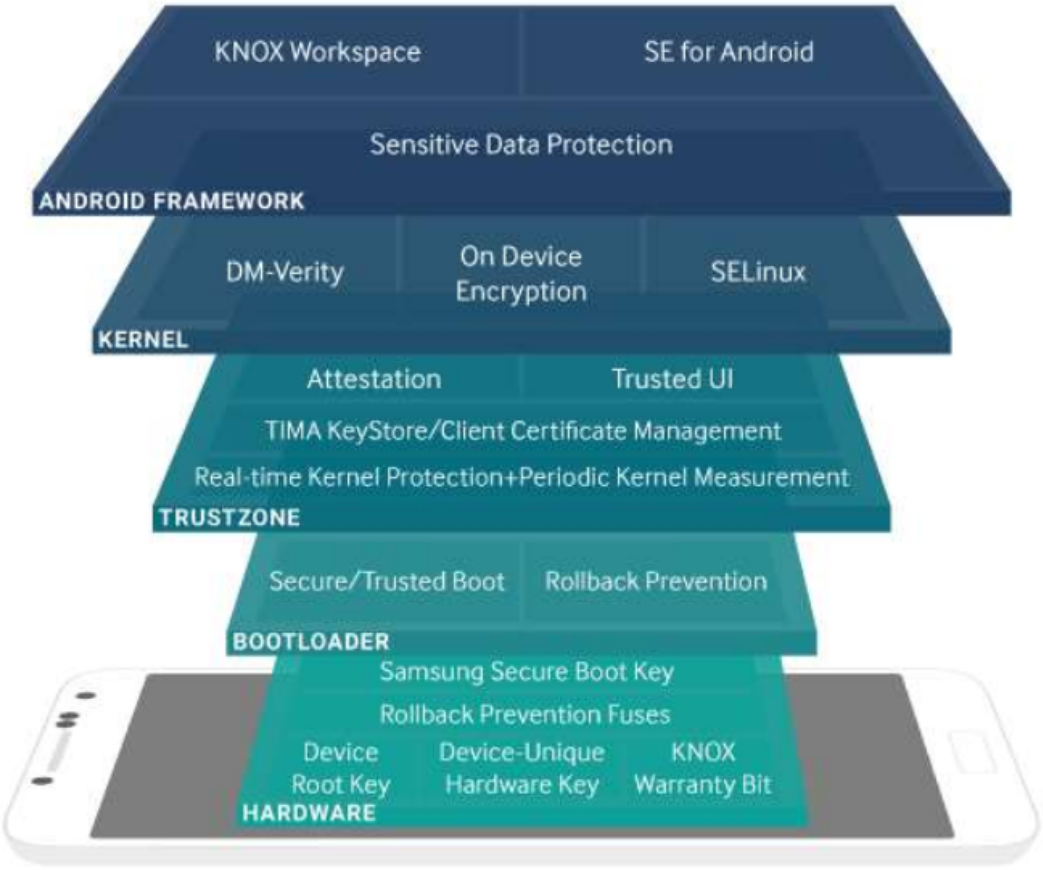

Abbildung 4.3: Samsung Knox Security Solutions Layers

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 öffentlichzugängliche oder eigenentwickelte

[3] Vgl. [Sa17d]

Software, verwendet werden sollen.

Denkbar wäre natürlich, dass während der Laufzeit, also nachdem die Überprüfung auf richtige Software, eine fälschliche Modifikation stattfindet. Um dem gegenzuwirken 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 [Go17a], welches überprüft ob das Gerät sich im selben Zustand befindet, wie beim letzten Start und SE Linux, genauer beschrieben in [Go17b], dass *mandatory access control* (MAC) über alle Prozesse vollzieht.

Android SE

4.2.3 Knox Workspace

Samsung's Knox Workspace entspricht dem in Abschnitt 4.2.1 beschriebenen «sicheren Ordner»in der Enterprise-Welt. Das heißt, es exisitiert eine Containerlösung für Mobilgeräte, 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. So ist es beispielsweise nicht möglich Bilder, die innerhalb des Workspaces gemacht wurden, außerhalb in der App Galerie anzuschauen.

4.2.3.1 Mobile Container Management

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

4.2.3.2 Autentifizierung

Um Zugang zum Workspace zu bekommen wird ein doppeltes Autentifizierungsverfahren 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 im Zugriff gewährt. Andersrum ist es so möglich den Workplace als Autentifizerung zu nutzen. Hierzu gibt es beispielsweise die Möglichkeit

[4] Vgl. [Sa17d]

Abbildung 4.4: Samsung Workspace Container

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 Managagement des MCM's je nach Sicherheitsanforderung im Unternehmen anpassen.

4.2.3.3 Knox Manage

4.2.3.4 Knox Mobile Enrollment

4.2.3.5 Samsung E-FOTA

5 Zusammenfassung

5.1

5.2

Literaturverzeichnis

[Sa17a] Samsung: *Samsung Knox: mobile Sicherheit für Ihr Unternehmen*, 2017. S.4

[Sa17b] Samsung: *Mitteilung über die Einstellung von My Knox* , 2017, https://my.samsungknox.com/

[Sa17c] Samsung: *Whitepaper: Samsung Knox Security Solution*. 2017 S.4

[Sa17d] Samsung: *Whitepaper: Samsung Knox Security Solution*. 2017. S.14

[Sa17e] Samsung: *Whitepaper: Samsung Knox Security Solution*. 2017. S.15

[Go17a] Google: *Verified Boot*. 2017. https://source.android.com/security/verifiedboot/

[Go17b] Google: *Security-Enhanced Linux in Android*. 2017. https://source.android.com/security/selinux/