

SYSTEMATIC ADMINISTRATION OF MOBILE DEVICES (SMARTPHONES/TABLETS)

Lodged with:



Author:

Roland Schellhorn

Supervisor:

Prof. (FH) Dipl.-Informatiker Böhm Karsten

Submission Date:

16.12.2014

DECLARATION OF ACADEMIC HONESTY

I hereby declare that this thesis is my own work and has not been submitted in any form for another degree or diploma at any university or other institute. Information derived from the published and unpublished work of others has been acknowledged in the text and a list of references is given in the bibliography.

York Pennsylvania, 16. December 2014



Roland Schellhorn

TABLE OF CONTENTS

| | |
|---|------|
| Declaration of academic honesty | II |
| Table of Contents | III |
| List of figures | VI |
| List of tables..... | VII |
| Abstract..... | VIII |
| 1. Introduction | 1 |
| 1.1 Initial Situation | 1 |
| 1.2 Statement of the problem | 1 |
| 1.3 Purpose..... | 2 |
| 1.4 Methodical approach..... | 2 |
| 1.5 Structure of the work | 2 |
| 2. How is it done currently based on examples..... | 3 |
| 2.1 Example University of Applied Sciences Kufstein | 3 |
| 2.1.1. Hand Out..... | 3 |
| 2.1.2. Return System..... | 3 |
| 2.1.3. Storage..... | 3 |
| 2.1.4. Troubleshooting | 4 |
| 2.2 Example York College of Pennsylvania | 4 |
| 2.2.1. Hand Out..... | 4 |
| 2.2.2. Return System..... | 4 |
| 2.2.3. Storage..... | 5 |
| 2.2.4. Troubleshooting | 5 |
| 3. Device Management Key-Terms..... | 5 |
| 3.1 Local Device Management (LDM) | 5 |

| | | |
|--------|---|----|
| 3.2 | Mobile Device Management (MDA)..... | 5 |
| 3.3 | Choose your own Device (CYOD)..... | 6 |
| 3.4 | Bring your own Device (BYOD)..... | 6 |
| 4. | Mobile Platforms and Stores..... | 7 |
| 4.1 | Apple iOS..... | 7 |
| 4.2 | Android | 8 |
| 4.3 | Symbian | 8 |
| 4.4 | BlackBerry OS..... | 8 |
| 4.5 | Windows Phone..... | 9 |
| 4.6 | Open WebOS..... | 9 |
| 5. | Requirements..... | 9 |
| 5.1 | Core Criteria..... | 9 |
| 5.1.1. | User Group Management..... | 9 |
| 5.1.2. | OTA Configuration Management | 10 |
| 5.1.3. | Automated Compliance | 10 |
| 5.1.4. | Remote Support..... | 10 |
| 5.1.5. | Self-service | 10 |
| 5.1.6. | Logging and Reporting..... | 10 |
| 5.2 | Security Management | 11 |
| 5.2.1. | Remote data lock and wipe..... | 12 |
| 5.2.2. | Selective data wipe..... | 12 |
| 5.2.3. | Localization | 12 |
| 5.2.4. | Password/Pin enforcement | 12 |
| 5.2.5. | Jailbreak/Root Detection and Notification | 12 |
| 5.2.6. | Separate personal and business data..... | 12 |
| 5.2.7. | Restrictive Functions cut-off | 12 |

| | |
|---|----|
| 5.2.8. Data encryption and Time-based access..... | 13 |
| 5.2.9. SIM monitoring..... | 13 |
| 5.2.10. VPN..... | 13 |
| 5.3 Mobile Application Management..... | 14 |
| 5.3.1. Remote software control..... | 14 |
| 5.3.2. Whitelist and Blacklist | 14 |
| 5.3.3. App store restrictions..... | 14 |
| 5.3.4. Enterprise App store..... | 15 |
| 5.4 Diversity Criteria | 16 |
| 5.4.1. Supported mobile platforms | 16 |
| 5.4.2. Supported PC platforms & Peripherals | 16 |
| 5.4.3. Data-Mart..... | 16 |
| 5.4.4. Telecom Expense Management | 17 |
| 5.4.5. Global availability | 17 |
| 6. Costs | 20 |
| 7. Criteria weights | 20 |
| 8. Physical Storage | 21 |
| 9. Replacement Device | 23 |
| 10. Take devices out of service | 23 |
| 11. Requirements analysis | 23 |
| 11.1 Ideal requirements | 24 |
| 11.2 Questions..... | 24 |
| 12. Conclusion and Summary | 25 |
| 13. Bibliography..... | 27 |
| Attachment A – Questions..... | A |

LIST OF FIGURES

| | |
|---|----|
| Figure 1 - Employees using personal devices at work | 7 |
| Figure 2 - Smartphone OS Market Share, Q3 2014 | 16 |
| Figure 3 - Criteria weights | 21 |
| Figure 4 - Small physical storage and charging system | 22 |

LIST OF TABLES

| | |
|--|----|
| Table 1: Core Criteria | 11 |
| Table 2: Security Management | 13 |
| Table 3: Mobile Application Management | 15 |
| Table 4: Diversity Criteria | 17 |
| Table 5: Costs & Versions | 20 |

ABSTRACT

York College of Pennsylvania

University of Applied Sciences Kufstein

Web Business & Technology

SYSTEMATIC ADMINISTRATION OF MOBILE DEVICES

Schellhorn Roland

Prof. (FH) Dipl.-Informatiker Böhm Karsten

This in order of the Austrian Marshall Plan Foundation elaborated thesis deals with the systematic administration of mobile devices. First the reader will get information how it is often currently done based on examples. Thereafter key terms of modern device management are listed and described as well as common mobile platforms and their App stores. Followed by a list of requirements divided by different criteria's and additional subdivisions will be summed up. Next some current prices of Mobile Device Management software solutions are shown. The criteria weights belong to the costs show a common way to find good useable versions out of a quantity. Besides the digital storage some different ways and a possible look into the future of physical storage will be discussed. Next a short look how to take devices out of Service and why some replacement devices should be available is given. Last but not least the term "requirements analysis" shows ideal MDMs requirements and questions to find the right MDMs solution.

16.12.2014

1. INTRODUCTION

In the rapidly increasing change of technology, mobile devices are increasingly used in larger companies. As a result of this, companies are confronted with some problems. For example how to we ensure our inventory of equipment? How can we find the current owners and their residence?

Also security and maintenance represents an important topic. Software developer companies are publishing patches and updates to their software very often.

The challenge hereby is to manage a wide variety of mobile devices in a way to make security and service updates quickly and easily on all devices.

1.1 Initial Situation

Mobile devices improved and accelerated business acts. They are essential for modern firms. Many firms also allow their employees to connect their own device to the business network. All these create several requirements to secure data and device.

1.2 Statement of the problem

Since mobile devices getting an essential part of modern companies, the IT department has a much larger range of devices and platforms which they have to support. Employees often want to bring their own device at work and want to connect them to the business network. It is a part of comfort it helps to bring a good atmosphere and at least an increased performance. Companies want to stay connected to their employees all the time.

The IT department has to solve a lot of requirements to secure data and device. Sensitive data should never leave the company without permission. Employees take their device home it could be stolen or lost, this requires restore and backup solutions as well as the ability to track and wipe the device. The amount of devices is too big to handle without an artful system. Firms need an artful system to manage all devices without losing track.

1.3 Purpose

With this work I will show which challenges a company has to expect by using a mobile solution in comparison to the currently used established infrastructures such as the location of the devices. Which solutions are already available on the market, what are the advantages and disadvantages of these different solutions and to what extent these can be distinguished.

1.4 Methodical approach

First the interviews for an example how some bigger enterprises administrate their mobile devices. Afterwards analyse actually Mobile Device Management software compare with the statement of the problem give us a list of requirements and what each MDMs contains.

1.5 Structure of the work

Following the Introduction, chapter two shows the interview results, chapter three tells key information about mobile device management terms and four about mobile platforms and their App stores. Chapter five indicates requirements for modern mobile device management systems. MDMs costs are shown in chapter six and criteria weights in chapter seven. Chapter eight displays physical storage options. Next in chapter nine a short look how to take devices out of Service and why some replacement devices should be available is given. Chapter eleven tells about requirements analysis including ideal MDMs requirements and questions to find the right MDMs solution. At least in chapter twelve the summary and conclusion are discussed.

2. HOW IS IT DONE CURRENTLY BASED ON EXAMPLES

Many companies or schools loan devices to their employees or students. They permit access to sensitive data. It is important to act fast and well-considered to keep your company safe.

2.1 Example University of Applied Sciences Kufstein

The „Fachhochschule“ Kufstein loans devices to employees as well as to students. Students loan devices for courses and labs like software development or practice projects to test their program and also for presentations to hand out a project prototype. Kufstein has a range of Tablets and Smartphones and supports iOS and Android.

2.1.1. Hand Out

If someone wants to loan a device he has to ask the course assistant if there is one available to loan. If the answer is yes, he can directly take it with him after a short check and list it. The assistant notes the device type, ID, employees name as well as date and time. Afterwards both have to sign like a contract. The short check includes the function of the device and all including like for example cables and operating instructions.

2.1.2. Return System

The process of returning includes an inspection of an assistant which means a simple check similar to the loan proceeds. If everything is okay the borrower get cleared form the list and the device gets back to the storage.

2.1.3. Storage

Loan Units are stored in a lockable cabinet at the course assistant office as well as at the engineering lab.

2.1.4. Troubleshooting

If a problem occurs either software or hardware first the IT department tries to repair it. Otherwise they let it repair especially if there is still warranty. The school pays unless no one acts carelessly.

2.2 Example York College of Pennsylvania

The College supports all devices on the YCP network such as smartphones, tablets from apple, android and windows. The college loan devices only to employees, students have to bring their own device. The range of available devices is limited to Apple devices such as iPhones and iPads.

The college prefers employees who have a device or a computer but not both. It is possible to add your private iTunes account to install personal software which is not possible with a college account. Devices are loosely locked down, however YCP requires passwords on all devices.

2.2.1. Hand Out

All devices are owned by the college, paid with college funds. Before an employee gets a device the device type and ID as well as the employees name are stored in a Mobile Device Management (MDM) system called “Casper”. This system allows the IT department to monitor a device, remotely wipe them and monitor application loaded and security.

Additional adapters for smart classrooms or for charging are available at the Help Desk department. Every additional stuff loan is linked within this software as well.

2.2.2. Return System

When an employee leaves the college, the inventory of devices held by the employee is given to the Human Resources Department, and the employee is required to return all devices upon exit. Software purchased by the employee can be kept by the employee through iTunes or iCloud backup.

2.2.3. Storage

When the College supplies a device to an employee, it is deployed from the IT Desktop Group and is charged and ready to use. The employee stores the unit. If a problem is encountered, the Help Desk will determine. If the Desktop Group needs to be involved in repair, the Help Desk corrects the issue.

2.2.4. Troubleshooting

If a device gets damaged in term of the software, employees use iCloud or iTunes backup to restore their data. In term of hardware usually Apple repair or replace it. If it happens in the period of warranty there is no charge. Otherwise the college pays unless there is abuse of the device.

3. DEVICE MANAGEMENT KEY-TERMS

Well used key-terms in the case of managing devices which are time and time again occur by the process of developing a device management system.

3.1 Local Device Management (LDM)

A well-known term in managing devices is called “Local Device Management” system used to central administrate desktop computers to create a safe and efficient infrastructure. LDMs sometimes include peripherals like printers and computer mouses as well. It is in a way a pioneer for a Mobile Device Management (MDM) system. Modern MDMs often additional include functionality’s of a Local Device Management system. (Heinrich Kerston, 2012)

3.2 Mobile Device Management (MDA)

MDM is a computer science term for central administration of mobile devices such as smartphones, tablets, PDAs and notebooks by using software and managed by one or more administrators. The administration contains systematic hardware storage as well as software controlling, data sharing and security for devices and data. Great Mobile Device Management software includes much functionality. They include configuration settings and data for all devices, over-the-air distribution of

applications, including smartphones, tablets, mobile printers, other mobile computers, etc.

Companies recently add their laptops and desktop computer to the system. Mobile Device Management systems become more and more a basic device management as just for mobile devices itself. Systems are optimized for both company-owned and employee-owned (Bring your own Device (BYOB)) devices. (Rouse, 2013) MDM provide BYOD recently in a bigger effort and improved the security for both sides. (Ford, 2014) This is useful since employees and employers have different imaginations of restrictions. (Ellis, 2014)

A mobile device management can control configuration settings as well as control and protect data for all devices in a network in real-time. The goal of MDM is to reduce costs and risks by optimising functionality and security of a mobile communications network. (InformationWeek, 2011)

More than 100 players share the fast growing market estimated at over 500 million dollar. (Monica Basso, 2012)

3.3 Choose your own Device (CYOD)

As distinct from “Bring your own Device” is “Chose Your Own Device” where employees can choose their device from a much broader assortment. As it is still a company device you have to decide whether or not to give an employee the permission to use it for private. (Bitkom, 2013)

3.4 Bring your own Device (BYOD)

BYOD is the possibility or rather permission for employees to bring personally owned mobile device to their workspace and use them to access to confidential internal information and application.

As a consequence companies expect an increase of satisfaction and efficiency because employees are familiar with their own devices. But on the other hand more than 50 percent assume safety issues depending on much different software. (Bitkom, 2013)

The following figure shows how employees use their personal devices for a variety of work-related tasks.

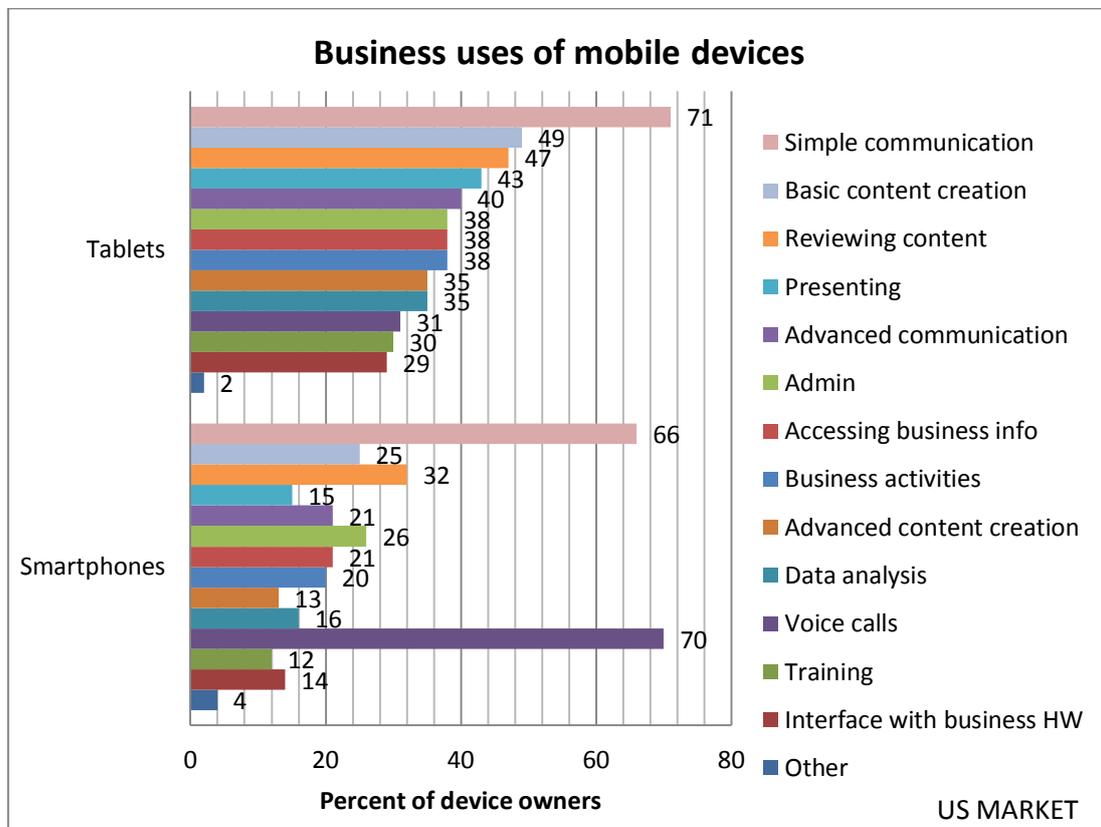


Figure 1 - Employees using personal devices at work

(Own representation based on McKinsey 2012 iConsumer survey on the consumerization of mobile devices)

4. MOBILE PLATFORMS AND STORES

Smartphones and Tablets are distributed with different operating systems (OS) whereby it isn't possible, in a normal safe way to change the OS on a device.

4.1 Apple iOS

Introduced in June 2007 when the first iPhone was developed. Used only by Apple own devices like iPhones and iPads. The current version is iOS 8.2 and works with devices down to iPhone 4s, iPad 2 and iPod touch. (Hein, 2013) To jailbreak an iOS

device means to get root access to the OS which further unprotect the devices security. (theiphonewiki, 2014)

Applications for Apple devices are only available at their own App Store by using access with an iTunes application. Every new application is checked by an Apple employee for compatibility and safety before it gets published at the store.

4.2 Android

Android Inc. was usually a software developer and was bought by Google in 2005. Together in 2007 newly founded to create the “Android Open Source Project” (AOSP) which is up to today responsible for service and advancement. Since Android is open source many other alternative version are available. Unfortunately most android users are using old versions which makes including the fact of an open source software android to a likely unsafe OS than iOS for example. (Heinrich Kerston, 2012)

Googles App store is called “Google Play Store”. Google renounces to review each application. They only search for common Malware and check the developer’s identity. Therefore Trojan and Malware are widespread and additionally many “low-quality” applications are available. (Heinrich Kerston, 2012)

In 2014 over 97% of mobile Malware is count on Android. Compared to other platforms, Symbian 3% and Apple iOS, BlackBerry OS, Windows Phone are together less than one percent. (Kelly, 2014)

4.3 Symbian

Symbian is owned by Nokia and mostly deployed only in Nokia own devices like Nokia E6 or Nokia 701. Unfortunately Symbian is overtaken by the popularity of iOS and Android. (Guru, 2014) Nowadays the whole platform is closed including their own App Store. (Kluczniok, 2013)

4.4 BlackBerry OS

BlackBerry OS was first-time released in 1999 and current property of Research In Motion (RIM). Developed only for BlackBerry own devices as for example BlackBerry Torch or BlackBerry Bold. BlackBerry App World is BlackBerry’s App

store, new Applications become a BlackBerry secure check before it assumed into the store. (Heinrich Kerston, 2012)

4.5 Windows Phone

Microsoft starts his mobile development in 1998 with Windows CE. In 2002 Windows created in advanced the operating system Windows Mobile and published in 2010 the version Windows Phone OS7 (WP7) which current is up to version 8.2.

Windows AppStore for mobile devices is named “Windows Phone Store”. The store included until September 2014 more than 340,000 apps.

4.6 Open WebOS

Open WebOS or also often called Hp WebOS or just WebOS is property of LG. First launched in 2009, basically developed by Palm Inc. and for a short-term property of Hewlett-Packard HP. Apps are available at different stores like LG WebOS, HP WebOs or WebOSnation for example. (Guru, 2014)

5. REQUIREMENTS

Which requirements are the most important and which are just a kind of gadgets. The following requirements are construed by analysing the needs of companies and the offer of MDM vendors.

5.1 Core Criteria

Core criteria's of a Mobile Device Management system are those who help to inventory devices and organize them from support to report. It keeps the number of supporters and costs down.

5.1.1. User Group Management

Allow to create and edit user groups and allocating them different policies. Review and modify policies. This is also an important security part which does not give anyone more rights as he truly need.

5.1.2. OTA Configuration Management

Over-the-air (OTA) configuration allows administrators to manage, control and update devices no matter where their locations are. Every device should at least have all prescribed updates to work safe and solid.

5.1.3. Automated Compliance

An engine monitors information about all devices and performs escalating actions to prevent noncompliance. By detecting a noncompliant device, automatically performed, preconfigured escalating actions bring the device back into compliance.

5.1.4. Remote Support

Very time efficient for both the help requester and the IT professional is the possibility to take control of an employee's device and see what he sees to understand much faster what he means and allows solving the problem quickly.

5.1.5. Self-service

A self-service portal is an important part of reducing time and costs by pare down IT service personnel for mobile device support. Employees can use it around the clock for troubleshooting, get new applications, review policies, change settings or backup and restore data.

5.1.6. Logging and Reporting

Capture detailed information for system monitoring by record both device and console events. Export reports or view them in the directly. Reports provide IT with actionable, result-driven statistics about their deployment. Predefined or creating custom reports, scheduled or recurrent, depending on environment and requirements of each company.

Table 1: Core Criteria

| Vendors | (1) | (2) | (3) | (4) | (5) | (6) |
|-----------------------|-----|-----|-----|-----|-----|-----|
| 2X MDM | X | X | - | X | - | - |
| 7P MDM * | X | X | - | - | - | X |
| Absolute Manage | X | X | - | - | - | X |
| AirWatch | X | X | X | X | X | X |
| Casper | X | X | - | X | X | X |
| FancyFon | X | X | X | X | X | X |
| Fiberlink MaaS360 | X | X | X | X | X | X |
| Good Technology | X | X | X | X | X | X |
| Kaseya | X | X | X | X | X | X |
| Kony | X | X | X | - | - | X |
| Mobile Active Defence | X | X | X | X | X | X |
| MobileIron | X | X | X | X | X | X |
| Notify Technology | X | X | - | - | X | X |
| SAP Afaria | X | X | X | X | X | X |
| SpiceWorks | X | X | X | X | X | X |
| Symantec | X | X | X | X | - | X |
| Tangoe MDM | X | X | - | X | X | X |
| Virtela | X | X | - | X | X | X |
| Wavelink | X | X | - | X | X | X |
| XenMobile | X | X | X | X | X | X |

Legend: (1) Group Management (2) OTA Management
 (3) Automated Compliance (4) Remote Support
 (5) Self-service (6) Logging and Reporting
 * Not at all platform

5.2 Security Management

Security is an important part of modern device management. The rapid increasing of mobile devices and platforms bring a huge size of challenges. Not only different platforms also different versions of each platform must be considered. The ability to bring your own device and separate business and personal data pose a big challenge for IT security.

5.2.1. Remote data lock and wipe

The opportunity to lock or wipe an employee's device remotely, assumes a confirmation.

5.2.2. Selective data wipe

Wipe data from an employee's device when he leaves the company or losing his device is one thing but the possibility to wipe just business data without touching personal data another, especially for users how use their own device.

5.2.3. Localization

For some reason it would be great to track a device. (E.g. If an employee can't find his device, it might be stolen.)

5.2.4. Password/Pin enforcement

To prevent unauthorized access to a device and therefore to sensitive data a strong password policy such as PINs and secure passwords are indispensable. It is one of the most important parts for preventing to create a secure password which cannot be easily attacked.

5.2.5. Jailbreak/Root Detection and Notification

Well-known methods like iOS Jailbreak or Android root to get around the management and remove IT control. Detecting these on a device and blocking them for accessing again to the network is a main security necessity.

5.2.6. Separate personal and business data

Splitting personal and business data to store, backup and control basically just business data. Employees must backup their private data for BYOD user. It saves company backup storage and protects firm access to private data.

5.2.7. Restrictive Functions cut-off

The ability to restrict or freeze functions like Camera, Browser, WLAN, Bluetooth etc. on an employee's device helps secure the system much more. (E.g. Freeze the

| | | | | | | | | | | |
|------------|---|---|---|---|---|---|---|---|---|---|
| SAP Afaria | X | X | X | X | X | X | X | X | X | X |
| SpiceWorks | X | X | X | X | X | X | X | X | - | X |
| Symantec | X | X | X | X | X | X | X | X | X | X |
| Tangoe MDM | X | X | X | X | - | X | X | X | - | X |
| Virtela | X | X | X | X | X | X | X | X | - | X |
| Wavelink | X | X | X | X | - | X | X | X | - | X |
| XenMobile | X | X | X | X | X | X | X | X | - | X |

Legend: (1) Remote data lock and wipe (2) Selective data wipe
 (3) Localization (4) Password/Pin enforcement
 (5) Jailbreak/Root Detection (6) Separate personal and business data
 (7) Restrictive Functions cut-off (8) Data encryption and Time-based access
 (9) SIM monitoring (10) VPN
 * Not at all platform

5.3 Mobile Application Management

Nothing works without applications. Control, manage and update applications centralised from one place with a few people this is what clients expect from a modern MDM system.

5.3.1. Remote software control

Many companies develop their own software to get the best geared to the needs application. The ability to control, manage, and update these applications is a need for employees effectiveness and productiveness.

5.3.2. Whitelist and Blacklist

The ability for administrators to create app whitelists and blacklists, configure compliance policies and restrict native applications. Whitelist applications are approved applications on a specific list provided by an administrator, while a Blacklist keeps undesirable application from installing.

5.3.3. App store restrictions

Again for productivity and effectivity some companies like to disable access to the consumer app store. Especially for platforms who allow people publish their own

application in stores without checking them for bad and unsafe code. This is on one hand very safe but could be on the other hand creating a bad atmosphere.

5.3.4. Enterprise App store

Companies want employees to use specific software which they often develop by their own or holding licenses for these applications. An enterprise app store helps to give employees a fast overview of all required applications and help administrators to manage and provision all at once.

Table 3: Mobile Application Management

| Vendors | (1) | (2) | (3) | (4) |
|-----------------------|-----|-----|-----|-----|
| 2X | - | X | - | - |
| 7P MDM * | X | X | X | X |
| Absolute Manage | X | X | X | - |
| AirWatch | X | X | X | X |
| Casper | - | X | X | X |
| FancyFon | X | X | X | X |
| Fiberlink MaaS360 | X | X | X | X |
| Good Technology | X | X | X | X |
| Kaseya | X | - | X | - |
| Kony | X | X | X | X |
| Mobile Active Defence | X | X | X | X |
| MobileIron | X | X | X | X |
| Notify Technology | X | X | X | - |
| SAP Afaria | X | X | X | X |
| SpiceWorks | X | X | X | X |
| Symantec | X | X | X | X |
| Tangoe MDM | X | - | - | - |
| Virtela | X | X | X | X |
| Wavelink | X | X | X | X |
| XenMobile | X | X | X | X |

Legend: (1) Remote software control (2) Whitelist and Blacklist
 (3) App store restrictions (4) Enterprise App store
 * Not at all platform

5.4 Diversity Criteria

Opportunities of Mobile Device Management Systems are huge, almost every known mobile operating system is supported and nowadays PC platforms like Windows, Mac and Linux are supported as well including the administration of printers and peripherals. Service integration, Telecom Expense Management and Global availability are also part of this topic.

5.4.1. Supported mobile platforms

Which mobile operating systems are supported? There are many different platforms on the market like Google Android, Apple iOS, Windows Phone 7, BlackBerry OS, Mozilla Firefox OS and much more unknown others. And there are many different models and versions as well. The following picture shows the current smartphone market share.

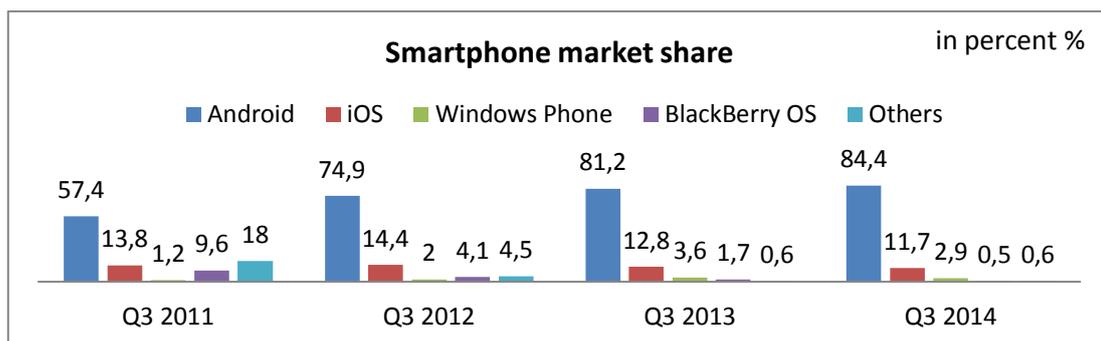


Figure 2 - Smartphone OS Market Share, Q3 2014

(Own representation based on IDC, 2014 Q3)

5.4.2. Supported PC platforms & Peripherals

Since MDM software getting more and more to basic administration software for all electronic devices, many vendors add incessantly new extensions to support other platforms or devices, as for example Windows, Mac and Linux computers or printers and other peripherals.

5.4.3. Data-Mart

This is the ability to export data like specific key data snapshots to third-party business intelligence solutions.

5.4.4. Telecom Expense Management

A constantly analyse followed by adjustment of internal telecommunications procedures and costs to maximize savings. (Auditelinc, 2011)

5.4.5. Global availability

There are many firms who offer Mobile Device Management systems lately but how they are available around the globe. This could be an important requirement for companies whose employees for example need to access the system everywhere they are currently.

Table 4: Diversity Criteria

| Vendors | (1) | (2) | (3) | (4) | (5) |
|-----------------|--|---|------------|------------|------------|
| 2X MDM | Android | - | - | - | - |
| 7P MDM | Android, Apple iOS, Symbian, Windows Mobile, Windows Phone | - | - | - | - |
| Absolute Manage | Android, Apple iOS, Windows Phone | Mac OS X, Windows PC/RT, Linux, Apple TV | x | - | x |
| AirWatch | Android, Apple iOS, BlackBerry, Symbian, Windows CE, Windows Mobile, Windows Phone | Mac OS X, Windows PC/RT, Peripherals | x | x | x |
| Casper | Apple iOS | Mac OS X, Apple TV | - | - | x |
| FancyFon | Android, Apple iOS, BlackBerry, Symbian, Windows Mobile, | - | x | x | - |

| | | | | | |
|-----------------------|---|-----------------------------|---|---|---|
| | Windows Phone | | | | |
| Fiberlink MaaS360 | Android, Apple iOS, BlackBerry, Symbian, webOS, Windows Mobile, Windows Phone | Mac OS X, Windows PC/RT | x | x | x |
| Good Technology | Android, Apple iOS, BlackBerry, Windows Phone, Windows Pro | - | x | - | x |
| Kaseya | Android, Apple iOS | - | - | - | x |
| Kony | Android, Apple iOS, BlackBerry, Windows Mobile, Windows Phone | Mac OS X, Windows PC/RT, | x | x | - |
| Mobile Active Defence | Android, Apple iOS, Symbian, Windows Mobile | - | x | - | x |
| MobileIron | Android, Apple iOS, BlackBerry, Symbian, webOS, Windows Mobile, Windows Phone | - | x | x | x |
| Notify Technology | Android, Apple iOS, BlackBerry, Symbian, webOS, Windows Mobile, Windows Phone | - | x | x | x |
| SAP Afaria | Android, | - | x | x | x |

| | | | | | |
|------------|---|---------------------------------------|---|---|---|
| | Apple iOS, BlackBerry, Windows Mobile | | | | |
| SpiceWorks | Android, Apple iOS, BlackBerry, Symbian, webOS, Windows Mobile, Windows Phone | Mac OS X, Windows PC/RT | x | x | x |
| Symantec | Android, Apple iOS, BlackBerry, Symbian, Windows Mobile, Windows Phone | Mac OS X, Windows PC/RT, Linux, | - | - | x |
| Tangoe MDM | Android, Apple iOS, BlackBerry | - | x | x | - |
| Virtela | Android, Apple iOS, BlackBerry, Symbian, webOS, Windows Phone | - | x | x | x |
| Wavelink | Android, Apple iOS, Symbian, Windows CE, Windows Mobile, Windows Phone | Mac OS X, Windows PC/RT, Linux, | x | x | x |
| XenMobile | Android, Apple iOS, Symbian, Windows Mobile, Windows Phone | - | x | x | x |

Legend:

(1) Supported mobile platforms

(2) Supported PC platforms & Peripherals

(3) Data-Mart

(4) Telecom Expense Management

(5) Global availability

6. COSTS

Mobile Device Management software helps to reduce costs but the software itself creates also costs. The following costs are composed by their own website if they were available. Costs viewed between the first October and 30th December 2014. The most vendors offer different bundles including different options like licence per user or device, Cloud connected or on Premise with or without support.

Table 5: Costs & Versions

| Vendors | | HQ |
|-----------------|---|-----|
| 2X MDM | \$5/device/month, minimum 25 licences | USA |
| 7P MDM | 2,5 - 4€ user/month by up to 2 devices each | GER |
| Absolute Manage | no viewable pricing | USA |
| AirWatch | 51 - \$110 device/month or 102 - \$220 user/month by up to 3 devices each / minimum 15 licences | USA |
| Casper | e.g. cloud \$75/OS X \$40/iOS device/month minimum 25 licences | USA |
| Kaseya | \$1.0/user/month by unlimited devices | CH |
| SpiceWorks | \$4.5/month/device | USA |

All other vendors don't show their price to public. An example of a buy model by using the vendor 7P MDM would cost onetime for a the server software 1298 euros plus 200 euros each year maintenance charges plus for a 50 client licence package onetime 2689 euros plus again maintenance charges 484 euros per year. Altogether 3987 euros onetime plus 684 maintenance charges a year.

7. CRITERIA WEIGHTS

To figure out which MDM systems are suitable for a company. A good method might be to first find all important requirements and creating a criteria weight chart like shown below in figure 3. For example use points between zero and ten for each criteria part and eventually it shows one or more possible MDM systems. (Heinrich Kerston, 2012)

| Criteria | Weight |
|--|--------|
| Functionality | 30% |
| Costs | 20% |
| Usability for User and Administrator | 30% |
| Architecture, Scalability, Infrastructure requirements | 20% |

(Heinrich Kerston, 2012)

Figure 3 - Criteria weights

8. PHYSICAL STORAGE

Also an important part of mobile device management is how to storage all devices. If employees bring their own device there is no storage required at least maybe one of them needs a charging cable which should definitely available. If employees get their device by their firm they can usually take it home and so there is again no permanent storage required. To get a device in first-time a simple locked storage with pre charged devices should be enough.

As we saw previously most MDMs include device tracking so it shouldn't be a problem to track and wipe or lock devices for some reason.

Otherwise if companies lend devices for example tablets for waiter to take order and payments or at schools who offer devices to their student to develop and present.

By using a MDM solution it requires adding and deleting a barrower name or creating a group of users who are responsible, permanently when a device leaves or returns the physical storage. A solution could be to use a barcode or near field communication (NFC) scanner to automat this part by including date into the system form a mobile device and a user ID card/chip.

When devices are reaching a huge size at least a charging system where devices can charge by ones and locked would support the staff to save time and money. Figure 4 shows an example of a small physical storage and charging system for tablets.



Figure 4 - Small physical storage and charging system

(Foreign representation from Ergotron.com)

A much more expensive solution could be creating an automat like a vending machine. It needs a system in the background that administered a lent device and is connected to the MDM system. Therefore you could create for example rules where someone can lend only one device at the same time and create time schedule messages if a devices didn't come back by time.

When someone lend a device out of the automat, he has to sign on a display to confirm the device is ok and as well when he brings back the device to be responsible until the device is signed by someone else as ok or after a certain time when a device longer was not lent an admin should get automatically a message to look after it and sign it as ok.

They only safe way to charge devices without someone needs to plug in a charging cable would be a wireless charging which is unfortunately not that common at the moment.

All in all exterior material condition like the devices display and back as well as additional material from devices like cables etc. are the most unimaginable things by lent a device without personal optical inspection.

To protect devices it would be recommendable to use a Full Body or Screen Protector Film or Shockproof cases. Not required material like headphones and user manual should be not handed over.

9. REPLACEMENT DEVICE

Mobile device can be lost, stolen and unfortunately as well destroyed. To be prepared in the case of a destroyed device, some pre-configured devices should be ready to taken. After restoring a backup file to a pre-configured device it should be ready in a few minutes. (Heinrich Kerston, 2012)

10. TAKE DEVICES OUT OF SERVICE

After a certain time hardware needs to be replaced by newer ones. Old data needs to be deleted out of the MDM system. Flash memory of each device which is taken out of service has to be overwritten as well to ensure no undesirable dataflow. By only deleting the firmware, data on the flash memory is still available. (Heinrich Kerston, 2012)

11. REQUIREMENTS ANALYSIS

When a company decides to implement a Mobile Device Management system it is important to figure out which are the most important requirements for them and which are possible required in the future.

To reduce complexity of the management solution, only a few devices and supported platforms should be provided. But the biggest question by deciding to find the right MDMs is the question to support Bring Your Own Device which hardly affects the range of possible solutions because in this case are many different devices and platforms as well as much more security has to considered. (Heinrich Kerston, 2012)

The possibility to take devices and therefore sensitive data outside the company near unauthorized persons which could take a look at it or steal it requires a lot security functions from a MDMs.

11.1 Ideal requirements

Ideal requirements for a MDMs solution are, compatible to all common platforms and applications, workable to all common cellular networks, fully over-the-air configuration by isolating different affiliations, as necessary add or remove a device by an administrator to the system, always ensure integrity and safety to the IT infrastructure, establish consequently all security policies and is invisible and unrecognized for the user. (Heinrich Kerston, 2012)

11.2 Questions

Some questions to figure out an ideal MDMs solution can help. Mainly MDMs must manage a list of mobile inventory but what have to be included?

Questions for device inventory:

- Which physical devices are needed to administrate?
- How we want to classify or group those devices?
- How do we want to update, change and delete on devices and is selective acting required to wipe just a part of a device for example?
- Do we want to know where our Devices located? Modern devices support GPS already for a long time.
- Do we need to integrate into an already existing database or want we integrate existing data into the new system? Like for example including desktop Pcs and peripherals into the MDMs.

Questions for device provisioning:

- Which platforms and related versions must be supported?
- How devices are getting registered for example by administrators or by themselves? And how will we install first-time the MDM agent on a device?

Questions for software distribution:

- Do we want allow download form public app stores?
- Do we want to create our own enterprise app store?
- Should we have the possibility to allow updates only by using fast WIFI connections with low-cost?

- How we bundle applications and configurations?

Questions for security:

- Do we need password/pin enforcement?
- Want we wipe devices remotely?
- How will we authenticate users by getting access to firm data?
- Do we need de possibility to restrict device functions?
- Want we create white and blacklists to allow and forbid some applications?

Questions for data protection:

- How will we backup and restore data?
- Want we track data transfer between devices?
- How will sensitive firm data be protected and how we want to ensure safe data encryption?

Questions for monitoring and support:

- Want we offer a self-service portal to allow users support their own device in a restricted and simple way?
- Want we can to remote control devices?
- Do we need logging and activity reports and which kind?
(Phifer, 2012)

12. CONCLUSION AND SUMMARY

It is not a condition to support a great many amount of devices to implement a Mobile Device Management solution. By including mobile devices into intern confidential firm data a system who secures data form unauthorized distribution is essential required.

Modern MDMs are broad developed to replace other IT management or inventory systems including PCs, Printer and other Peripherals. Help to reduce time and costs by reduce administrative activities. Optimize processes by monitoring and analysing data which again reduce time and costs. In a generation of computer familiar users

MDM systems they include a self-service portal could reduce support requests next to nought.

The devices operating system and installed applications are always up-to-date for employees without doing anything or big technology knowledge just over-the-air. As well for settings like connection access to E-Mail accounts or WIFI can be predefined or OTA configured. Every device is controllable by the system which allows blocking access or wiping selective data from an employee's device every time and wherever the device is located.

Every system has disadvantages if the system failures the company is incapable of acting or updates are fast shared unfortunately as well by errors.

There are many valuable solutions are available but of course as already addressed not every solution fits for every company. Companies have first to figure out what personal firm requirements they have, by asking themselves questions like do we allow our employees to bring their own device to work? Do we want to support as many as possible platforms or want we isolate our system maybe just for one platform like iOS or BlackBerry OS.

Without consider of personal firm requirements and costs by using the previous shown criteria weight chart two vendors are outstanding. First AirWatch and second MaaS360 both support almost all requirements and platforms. Including obvious costs the cost effectiveness vendors are SpiceWorks and Kaseya.

The best way for physical storage depends again on what a company requires. At least when the mount of devices increases a system where devices can charge by ones and locked would support the staff to save time and money.

13. BIBLIOGRAPHY

Auditelinc, 2011. *auditelinc.* [Online]
Available at: <http://www.auditelinc.com/telecomexpensemanagement.aspx>
[Zugriff am 26 10 2014].

Bitkom, 2013. *BITKOM.* [Online]
Available at:
http://www.bitkom.org/files/documents/20130404_LF_BYOD_2013_v2.pdf
[Zugriff am 28 10 2014].

Ellis, L. J. S. a. P. W., 2014. *mckinsey.* [Online]
Available at:
http://www.mckinsey.com/~media/mckinsey/dotcom/client_service/High%20Tech/PDFs/BYOD_means_so_long_to_company-issued_devices_March_2012.ashx
[Zugriff am 9 10 2014].

Ford, G., 2014. *Cybersecurity HQ.* [Online]
Available at: <http://cybersecurity-hq.blogspot.co.at/2014/02/byod-consumer-demand-and-information.html>
[Zugriff am 8 10 2014].

Guru, 2014. *shoutmeloud.com.* [Online]
Available at: <http://www.shoutmeloud.com/top-mobile-os-overview.html>
[Zugriff am 9 10 2014].

Hein, B., 2013. *cultofmac.com.* [Online]
Available at: <http://www.cultofmac.com/191340/the-evolution-of-ios-from-iphone-os-to-ios-6-gallery/>
[Zugriff am 9 10 2014].

Heinrich Kerston, G. K., 2012. *Mobile Device Management.* 1 Hrsg. München: mitp.

InformationWeek, 2011. *Informationweek.* [Online]
Available at: <http://www.informationweek.com/mobile/byod-requires-mobile-device-management/d/d-id/1097576?>
[Zugriff am 9 9 2014].

Kelly, G., 2014. *forbes.com.* [Online]
Available at: <http://www.forbes.com/sites/gordonkelly/2014/03/24/report-97-of-mobile-malware-is-on-android-this-is-the-easy-way-you-stay-safe/>

[Zugriff am 10 10 2014].

Kluczniok, J., 2013. *netzwelt.de.* [Online]
Available at: <http://www.netzwelt.de/news/104571-nokia-app-store-symbian-meego-schliesst-1-januar-2014.html>

[Zugriff am 11 10 2014].

Monica Basso, P. R., 2012. *Gartner.* [Online]
Available at: <https://www.gartner.com/doc/2110815>

[Zugriff am 15 10 2014].

Phifer, L., 2012. *techtarget.com.* [Online]
Available at: <http://searchconsumerization.techtarget.com/tip/Mobile-device-management-checklist>

[Zugriff am 17 11 2014].

Rouse, M., 2013. *techtarget.* [Online]
Available at: <http://searchmobilecomputing.techtarget.com/definition/mobile-device-management>

[Zugriff am 7 11 2014].

theiphonewiki, 2014. *theiphonewiki.com.* [Online]
Available at: <https://theiphonewiki.com/wiki/Jailbreak>

[Zugriff am 6 10 2014].

ATTACHMENT A – QUESTIONS

1. Which different kinds of devices does the school offer?
2. Who can borrow a device? Student? Employee?
3. How do you hand out a device? Software? Paper? What about additional stuff like cables or the description?
4. If Software. What do you if the Software is out of order?
5. How does the return system work? Which checks do you make? For example check software, hardware, additional stuff.
6. Can or do you trace borrowed devices?
7. Are there any limitations for a borrowed device, like for example lesser admin rights?
8. What if a Device gets damaged in terms of the hardware?
9. What if a Device gets damaged in terms of the software?
10. How do you store loan units? Are they always ready to use? Charged?