Mobile Infrastrukturen
Studiengang Informatik

- Dipl.-Inf., Dipl.-Ing. (FH) Michael Wilhelm
- Hochschule Harz
- FB Automatisierung und Informatik
- mwilhelm@hs-harz.de
- Raum 2.202
- Tel. 03943 / 659 338

Inhalt

- **Rechnerstrukturen ohne Tablets (Hardware / Software)**
  - Ebenen der IT-Infrastruktur
  - Rechenzentrum (Desktop-Rechner)
- **Erweiterung auf „Mobile Infrastrukturen“**
  - Rechenzentrum + Mobile Infrastrukturen
- **Komponenten_mobiler_Infrastrukturen**
- **Gesetze**
- **Sicherheitsprobleme bei Smartphones und Tablets**
- **Mobile Device Management**

Mobile Device Management

Vergleichbar mit dem „Local Device Management“ für stationäre Rechner, steht MDM für die umfassende Verwaltung und Überwachung der mobilen Infrastruktur

- Unterschiede
  - Keine festen Standort
  - Netzwerk über WLan oder Funknetz
  - Keine dauerhafte Empfangsqualität
  - Große Datenmengen sind schwer zu transportieren
  - Alle Aktionen, z. B. Notfall, müssen per Netz ausgelöst und kontrolliert werden.
  - Inventarisierung eventuell vor Ort.
  - Audits immer per Netz (ferngesteuert)
  - Manuelle Eingriffe vor Ort sind kaum möglich (die Anwender sind keine IT-Experten)
  - Nach Jahren sehr heterogenes System
  - Möglichst wenig unterschiedliche Geräte

Anforderungen an ein Mobile Device Management

- **Ein MDM hat zwei Komponenten**
  - Einen Server
  - Eine App pro mobiles Gerät (Client für Exchange Active Sync)
- **Kompatibel zu allen marktüblichen mobilen Plattformen und Anwendungen**
- **In allen mobilen Netzen, weltweit, arbeiten**
- **Das MDM sollte direkt „Over the air“ installierbar sein**
- **Mobile Geräte sollten bei Bedarf von Admins aus dem System entfernt oder hinzugefügt werden können.**
- **Es sollte stets die Integrität und Sicherheit der IT-Infratstutur gewährleisten.**
- **Security Policies konsequent durchsetzen.**
- **Transparent für den Anwender. Das MDM sollte möglichst wenig stören.**

Exchange ActiveSync is a proprietary protocol that syncs your mobile device with your Exchange mailbox, so you can access your email, calendar, contacts, tasks, and so much more. It is based on XML and communicates with a mobile device using HTTP or HTTPS.

Funktionsumfang an ein Mobile Device Management

- **Inventarisierung von mobilen Geräten**
- **Incident und problem management**
  - An IT incident is any disruption to an organization's IT services that affects anything from a single user or the entire business . In short, an incident is anything that interrupts business continuity.
- **Verteilung von Patches, Updates und Applikationssoftware**
- **Überprüfung der Compliance mit Sicherheitsrichlinien (Länge der Passwörter)**
- **Backup und Restore**
- **Sperren der Geräte**
- **Echtes Löschen sensibler Daten**
- Zustandsüberwachung der mobilen Geräte
- Auditieren der mobilen Geräte
- **BYOD**
  - Einhaltung der DSVGO
  - Fernmeldegeheimnis (private Daten dürfen nicht gelesen werden)

Inventarisierung von mobilen Geräten

- Die Identizifierung der mobilen Geräte anhand einer eindeutigen Kennung (Device-ID)
- Eine Zusammenstellung der auf diesem Gerät installierten Firmware mit Versionsbezeichnung
- Eine Liste der installierten Apps und Daten
- Die Erfassung der Mobilfunkanbindung über die verwendete SIM-Karte (Middle of the man attack)

Incident und problem management

- Gerade bei Update der Firmeware oder Updates von Apps kann es zu Problemen kommen.
- Lösen kann man es über das MDM
- Man braucht:
  - Informationen über den Systemstatus
  - Logfiles
  - Bildschirmfotos (möglichst automatisch)
  - Speicherauszüge
  - Etc.
- Fehleranalyse und Fehlerbehebung sind in aktuellen Firmware nicht vorgesehen (überprüfen). Dies sollte das MDM können.

Verteilung von Patches, Updates und Applikationssoftware

- Organisatorischer Teil
  - Kenntnisse der aktuell installierten Software
  - Benachrichtigungen über neue Patches und deren Priorität. Die MDM des Gerät senden diese Informationen.
- Technischer Teil
  - Patches (wichtige Änderungen in der Software)
  - Updates (generelle Änderungen in der Software)
- Open Mobile Alliance (OMA)
  - Seit 2002: Entwicklung eines Device Management inkl. „Firmware Updates Over the Air“ (FOTA)
  - Man überträgt nur die Differenz (neu-alt)
- Weiterentwicklung von FOTA ist SCOTA
  - Ansatz geht in Richtung Module, Kundenspezifische Module
- Weiterentwicklung nach „Simple Certificate Enrollment Protocoll“ (SCEP)
- Bei Apple nur über dem App-Store oder inHouse-Apps

Verteilung von Patches, Updates und Applikationssoftware (2)

- Fragen
  - Wie sieht es mit der Erreichbarkeit alle verwendeten Geräte aus?
  - Zu welcher Zeit ist der Anwender zum Patch/Update bereit?
  - Lässt es sich feststellen, wer welche Version erhalten hat?
  - Welche Anforderungen haben die Mobilfunkbetreiber?
  - Was passiert beim Abbruch von Verbindungen? (Testen!!)
  - Werden „Bricked-Zustände“ beim Abbruch verhindert? (Elektronisch oder softwaremäßig defekt)

Überprüfung der Compliance mit Sicherheitsrichlinien

- Aktivierte Benutzersperre
- Freischaltdauer (10 Minuten!?)
- Tolerierten Fehlerversuchen
- Automatische Sperre bei Inaktivität
- Automatische Verschlüsselung bei Inaktivität
- Güte der Passwörter
- Bei negativer Überprüfung muss das MDM das Gerät sperren.
- Verstöße gegen die Richtlinien müssen protokoliert werden.
- Das MDM muss
  - Richtlinien verteilen
  - Die Umsetzung kontrollieren und auditieren.
  - Gruppen und Ausnahmen zulassen (gibt es immer!)
  - Bei Angriffsversuchen das Gerät sperren (nur Fehlversuche?)
  - Verstöße gegen die Richtlinien protokolieren

Backup und Restore

- Abhängig von der Firmware des Gerätes
- Abhängig von Nutzungsart (z. B. BYOD)
- Abhängig vom Aufenthaltsort
- 1. Fall (iOS-Gerät)
  - Man verwendet Apple School Manager oder Apple Business Manager um alles automatisiert zu löschen oder zu konfigurieren.
  - Musik, Apps, Bilder, Videos, Bücher
  - Kalender, Notizen, Kontakte, Mails
  - Geräteeinstellungen
  - App-Daten
  - Home-Screen und Anordnung der Apps
  - Nachrichten (iMessage, SMS und MMS)
  - Alarmtöne

Backup und Restore

- 2. Fall (Android-Gerät)
  - Man verwendet „Android Device Management“ um alles automatisiert zu löschen oder zu konfigurieren.
  - Musik, Apps, Bilder, Videos, Bücher
  - Kalender, Notizen, Kontakte, Mails
  - Geräteeinstellungen
  - App-Daten
  - Home-Screen und Anordnung der Apps
  - Nachrichten (Message, SMS und MMS)
  - Alarmtöne

Sperren eines Gerätes und Löschen sensibler Daten

- Bei Verlust oder der Annahme das es einen unberechtigten Zugriff auf interne Daten des Geräts gibt, müssen die Daten gelöscht oder das Gerät gesperrt werden.
- Sofortige Aktionen:
  - Sofortige Sperre aktivieren
  - Verbindungseinstellungen müssen gelöscht werden.
  - Widerruf von Zertifikaten
  - Löschen von User-ID‘s und Passwörtern.
- Weitere Aktionen (Diebstahl, Verlust):
  - Alle Daten löschen.
  - Meist wird bei Diebstahl sofort die SIM-Karte entfernt. Dies muss der MDM-Client erkennen und dann die Daten löschen!
  - Oder man setzt das Gerät in den Flugmodus (mit Abfrage)!

Zustandsüberwachung und Auditieren der mobilen Geräte

- Durch den MDM-Client lassen sich vielfältige Daten erfassen, welche im Fehlerfall hilfreich sind:
  - Verbindungsnachweise (DSVGO)
  - Speicherstatus
  - Akkustand
  - Installierte App‘s
  - Belegter Speicher
  - Mobilfunkkosten
  - GPS Daten (DSVGO??)
  - Bei Screenshot benötigt man auch die Zustimmung des Anwenders!

Mobile Device Management Lösungen (iOS)

- Alle neuen Apple-Geräte haben ein MDM-Basisframework, welches MDM-Lösungen massiv unterstützt.
  - SCEP-Protokoll
  - Das Gerät kann jederzeit aus dem MDM entfernt oder hinzugefügt werden
- Apple device supervision
  - iPhone with iOS 13 or later
  - iPad with iPadOS 13.1 or later
  - Mac computers with macOS 10.14.4 or later
  - Apple TV with tvOS 13 or later
- Senden eines „configuration profile“
  - Ein Profil ist eine XML-Datei.
  - Die Profile können an einzelne Geräte oder Gruppen gesandt werden.
  - In einem Profile können Rechte (Payloads) an- oder ausgeschaltet oder konfiguriert werden.
- Payloads
  - https://support.apple.com/guide/deployment/review-mdm-payloads-dep5370d089/1/web/1.0

Mobile Device Management Lösungen (iOS)

- **Manage Engine**
  - Android
  - iOS,
  - Windows, Chrome OS
- Eigenschaften
  - Automatische Installation
  - Silent app installation
  - Blocklist app
  - App Katalog
  - Automatisches Updates
  - Container für die Daten (mit Verschlüsselung)
  - VPN
  - Block or allow web content
  - Lost / stolen devices (remote command)

- https://www.manageengine.com/mobile-device-management/

Mobile Device Management Lösungen (iOS)

- **Scalefusion**
  - iOS,
- Eigenschaften
  - Device/User enrollment
  - Application Management
  - Remote Support
  - Remote Commands
  - Location Tracking
  - Content management
  - Reports

- https://scalefusion.com/ios-mobile-device-management

Mobile Device Management Lösungen (Android)

- **ManageEngine Mobile Device Manager Plus**
  - EDITOR'S CHOICE Mobile device management solution for device management that supports Windows, Mac OS, Chrome OS, iOS, and Android. A complete enterprise device management package with both on-premises and cloud-based versions. Start the 30-day free trial.
- **Kandji**
  - (FREE TRIAL) A cloud-based service that reaches out to devices through agents and specializes in Apple devices. Start a 14-day free trial.
- **VMWare Workspace ONE**
  - Mobile device management solution that can configure policies for devices remotely, automatically deploy applications, and more.
- **BlackBerry Unified Endpoint Management**
  - Endpoint management solution design that supports Windows 10, Mac OS, iOS, Android, and Chrome OS.
- **Citrix Endpoint Management**
  - MDM solution that supports Windows 10, Mac OS, iOS, tvOS, iPadOS, Android, Android Enterprise, Chrome OS, and Citrix.

- https://www.comparitech.com/net-admin/mobile-device-management-software/

Mobile Device Management Lösungen (Android)

- **SOTI MobiControl**
  - Endpoint management software that supports Windows XP, Windows CE, Mac OS, iOS, and Android.
- **IBM MaaS360**
  - Enterprise mobility management solution with real-time data usage monitoring, application updates, endpoint device malware detection, and more.
- **Cisco Meraki**
  - Includes a container system to deliver apps to user-owned devices and also has loss protection procedures.
- **Miradore Mobile Device Management**
  - A Cloud-based device manager in both free and paid versions.
- **Jamf Now**
  - A cloud-based service that only manages iOS devices.
- **SimplySecure**
  - A cloud-based MDM that covers iOS and Android mobile devices and portable storage.

ManageEngine Mobile Device Manager Plus

Key features:

- Supports Windows, Mac OS, Chrome OS, iOS, and Android.
- Remote devicecontrol
- Device scanning
- Out-of-the-box reports
- The software's **free for up to 25 devices**.
- Server: Windows

Pros:

- Designed to work right away, features over 200 customizable widgets to build unique dashboards and reports
- Leverages autodiscovery to find, inventory, and map new devices
- Uses intelligent alerting to reduce false positives and eliminate alert fatigue across larger networks
- Supports email, SMS, and webhook for numerous alerting channels
- Integrates well in the ManageEngine ecosystem with their other products

Cons:

- Is a feature-rich tool that will require a time investment to properly learn

Kandji

Key features:

- Macs and mobile devices
- Onboarding features
- Patching
- Data privacy standards compliance

Pros:

- Integrates with third-party systems to create a single sign-on environment
- Allows the creation of Blueprints, which are software profiles for groups of devices
- Lets users switch between on-premises Macs and mobile devices
- Automated the update of software and operating systems

Cons:

- Won’t manage devices running Windows, Linux, or Android.

VMWare Workspace ONE

Key features:

- Configure devices on bulk
- Automatically deploy applications
- Use onboarding workflow to add new devices
- Workspace One is a cloud-based service

Pros:

- Supports platforms like Apple Enrollment as well as Android Zero Touch
- Great for both managed devices as well as BYOD environments
- Can build workflows and policies with little platform knowledge

Cons:

- Can take some time to explore the product

VMWare Workspace ONE is suitable for enterprises of all sizes and comes with a range of pricing options, due to its seven editions. Prices start at $1.66 (£1.33) per device and $3.00 (£2.40) per user. You can try the 30-day free trial to manage up to 100 devices.

BlackBerry Unified EndPoint Management

Key features:

- Manage device policies
- Supports iOS, Android, Chrome OS, Windows, and Mac OS
- Activate uses with a QR code (iOS and Android only)
- Available on-Premises and in the cloud

Pros:

- Sleek highly customizable interface
- Cross platform support with Windows, Mac OS, Linux, Android and iOS
- Available on premise and as a cloud service

Cons:

- Would like to see more options for mobile security
- Better suited for enterprise networks

BlackBerry Unified Endpoint Management is a solid MDM solution that's available on-premises and in the cloud. To view the pricing information you need to request a quote from the sales team directly.

Citrix EndPoint Management

Key features:

- Remote monitoring & device management
- Machine learning and Analytics
- Integrations with Azure Active Directory and Okta

Pros:

- Supports a wide range of monitoring environments from Windows 10 to Citrix
- Monitors user behavior to identify insider threats and block high-risk users proactively
- Best suited for large environments that have to support multiple types of devices

Cons:

- Better suited for enterprise networks

Citrix Endpoint Management is worth considering at if you're looking for cross-platform device management, with compatibility with Citrix infrastructure.

IBM MaasS360

- **Key features:**

  - Real-time data usage monitoring
  - Malware detection and remediation
  - 24/7/365 customer support
  - Single sign-on to web and cloud apps

- **Pros**:

  - Built with enterprises in mind
  - Good fit for those looking to monitor IoT devices
  - Can detect and defend against malware

- Cons:

  - Best suited for MSPs and larger networks

IBM MaasS360

Key features:

- Real-time data usage monitoring
- Malware detection and remediation
- 24/7/365 customer support
- Single sign-on to web and cloud apps

Pros:

- Built with enterprises in mind
- Good fit for those looking to monitor IoT devices
- Can detect and defend against malware

Cons:

- Best suited for MSPs and larger networks

IBM MaasS360

- The device security features included with IBM MaaS360 are one of its greatest assets. The device platform can detect and remediate malware on endpoints. Being able to detect malware on devices provides you with an extra layer of mobile security that helps prevent endpoints from being compromised and putting your data at risk.

- If you’re Looking to monitor IoT devices then IBM MaaS360 is a natural choice. The platform can monitor Google Android, Android Things, Microsoft Windows 10, and Windows IoT devices to deploy security policies to protect the devices from causing security risks.

- IBM MaaS360 is one of the easiest to use tools on this list, with a high-quality console for managing devices that would suit the needs of enterprises of all sizes. IBM MaaS360 pricing starts at $4 (£3.25) per device per month and $8 (£6.50) per user per month.

Mobile Device Management Lösungen (Android)

- **Android**
  - Devices
  - Management
  - Security
  - Enterprise Recommended
  - Employees

- https://www.android.com/enterprise/management/