Android im Unternehmenseinsatz

Max Johenneken

anderScore trust in competence

- Seit 2013 bei anderScore
- Studiert Informatik im sechsten Semester Schwerpunkt Embedded Systems an der HBRS
- Entwicklungen im mobile App Umfeld vorrangig Android und iOS

Inhalt

Begriffsdefinitionen, Geräteeinrichtung, BYOD

Welche Daten

- Telefonprotokolle
- Mails
- Dokumente
- Kontakte
- Standortdaten
- Aktivitätsdaten
- Browserverlauf
- ...

Intresse des Mitarbeiters vs. des Unternehmens

Firmenhandy

- Alle Daten auf dem Gerät "gehören" dem Unternehmen.
- Zwangsläufig auch Daten des Mitarbeiters auf dem Gerät die nicht umbedingt unternehmensspezifisch sind.
- Bewegungsprofile

Privat Handy

- Viele Private Daten auf dem Gerät
- Vermischung der privaten Daten mit Firmen Daten
- Dadurch wird Löschung der Firmendaten erschwert

BYOD

- "Bring your own Device" Buzzword
  - Der MA bringt sein Handy mit und er benutzt es sowohl für Private als auch Firmen Zwecke
    - Schwierige Situation für SysAdmins, da einbinden potentiell unsicherer Geräte in Unternehmensnetzwerk
    - Bringt das Problem mit sich, in welchem Umfang kann man die geschäftliche Nutzung der privaten SIM zulassen.
  - Rechtlich immernoch schwierig

Warum sollte man die Dualnutzung wollen?

- MA hat immer zwei Handys dabei
- Erhöhter Komfort
- Bessere Erreichbarkeit
- Einsatz von Dual Sim Handys löst das Problem der SIM Karten Nutzung
- Rufumleitungen

Einrichtung eines Firmenhandys

- Initialer Konfigurationsaufwand ist nötig
  - Bei nicht-Root Geräten, muss der Durchgang manuell durchlaufen werden.
    - Durchlaufen des Einrichtungsassistenten
    - Enrollment in EMM
    - Alternativ: weitere Konfiguration der Komponenten
    - Problempunkt: Google Accounts werden auf Einzelpersonen registriert. Somit kann die Registrierung nicht vom Sysadmin aus erfolgen.
      - Mitarbeiter muss bei der Einrichtung anwesend sein oder sein Gerät zu Ende konfigurieren
      - Bei der Einrichtung des Google Accounts müssen die richtigen Datenschutzeinstellungen gesetzt werden
    - weiteres Problem: je nach OS Version und Hersteller ist der Einrichtungsassistent anders

Android Sicherheitskonzepte, EMM und weitere Konzepte

Sicherheitsmechanismen erschweren Administration

anderScore trust in competence

Android ist Linux basiert. Root Zugriff haben nur Systemprozesses/Apps Ändern der Einstellungen nur durch solche möglich

- Als Entwickler kann man den User bestimmte Einstellungsseiten anzeigen, sonst muss er aber manuell die Einstellungen setzen

Man kann Handys rooten

- erlöschen der Herstellergarantie
- Vertrauenswürdigkeit der ROM(Custom OS) Entwickler
- Möglich wäre aber ein modifiziertes Stock/Vanilla(Orginal) Android welches Richtlinien/Anwendungen des Unternehmens direkt mitbringt.

Google Device Policy Controller

- Erster Schritt um Unternehmensrichtlinien auf Android Geräten durchzusetzen
  - Historisch gesehen wird es von Android for Work abgelöst bzw. ergänzt
    - EMM Lösungen die darauf aufbauen bzw. andere Teile/APIs des Systems verwenden
  - Gibt es auch erst nutzbar ab Android 3.0
  - In dem Kontext kann man die Historische Entwicklung von Android in Unternehmen unterbring. z.B. die Tatsache,das iOS und Blackberry wesentlich früher auf den Unternehmensseinatz bereit/grüstet waren
  - Löst das Problem grundlegender Sicherheitsbedürfnisse für das Geräte
    - Passwortrichtlinie für Komplexität, Länge, Erneuerung, Prompten zu PW Einstellung
    - Verschlüsselung des Geräts erzwingen
    - Kamera sperren
    - Remote sperren, Remote Wipe
  - Anforderungen um die App zu installieren
    - Praktisch ausprobieren

Container wie Samsung Knox

anderScore trust in competence

Container wie Samsung Knox

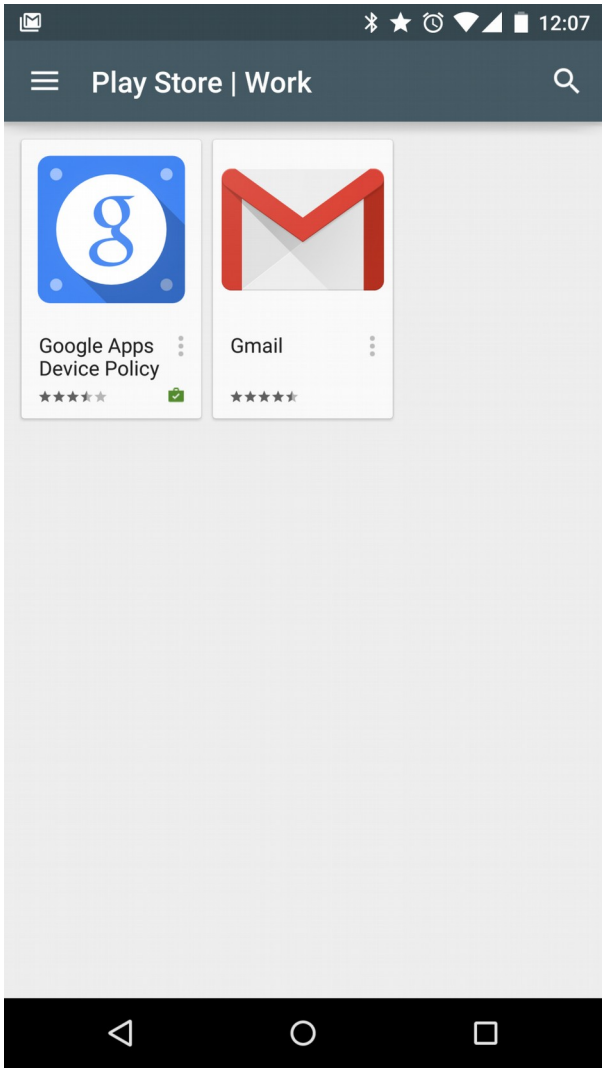
- Stichpunkte
  - Sicherheit wurde infrage gestellt, siehe verlinkte Blog posts

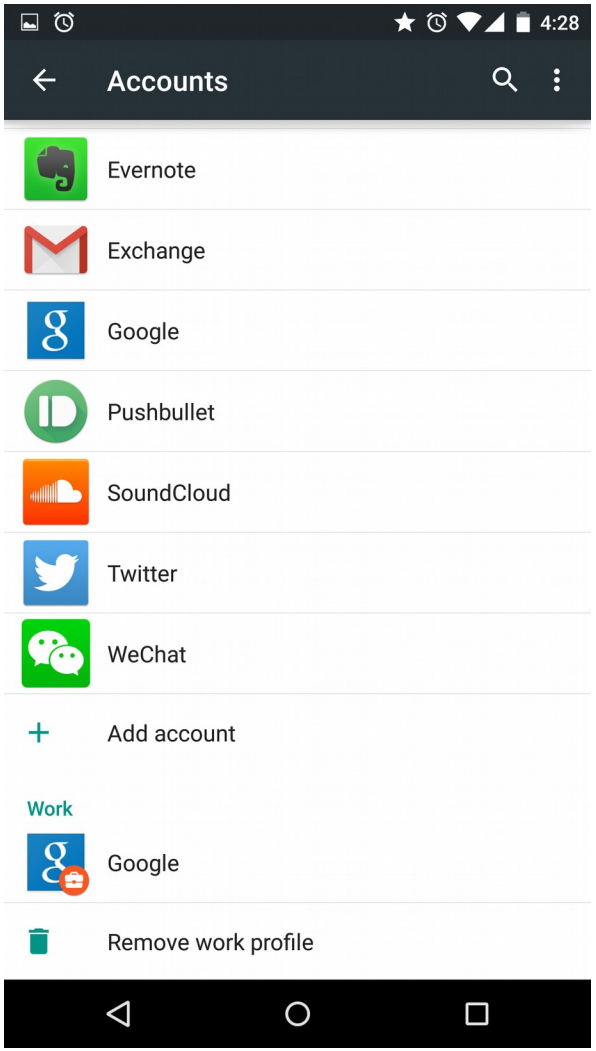
Android for Work

Einführung in Android 5.0

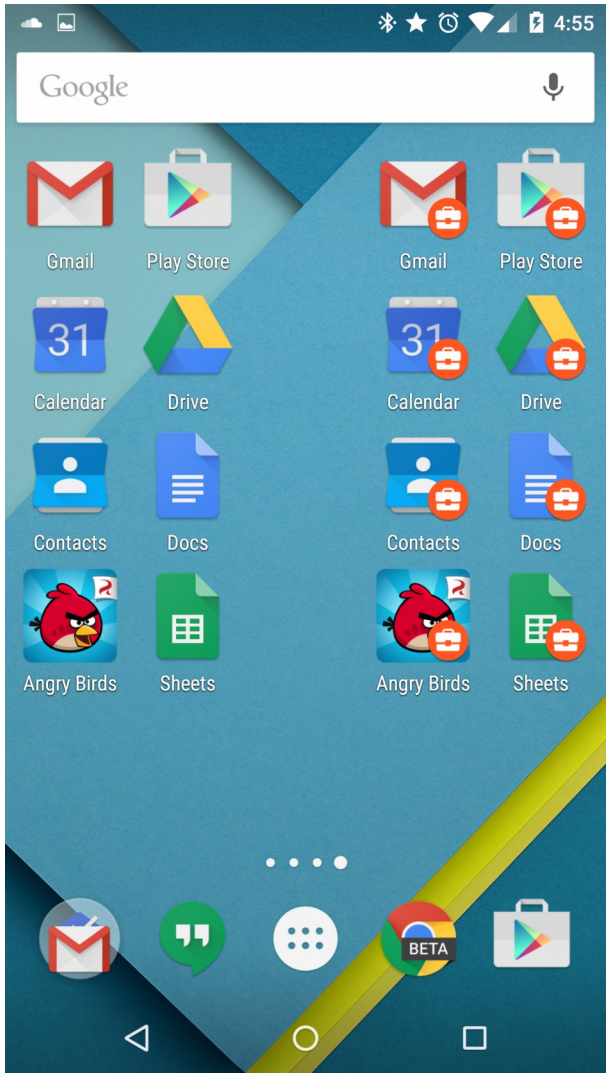
- Durch Android for Work App gibt es auch Support für 4.x Geräte
- Darstellen der Oberfläche mit Android for Work

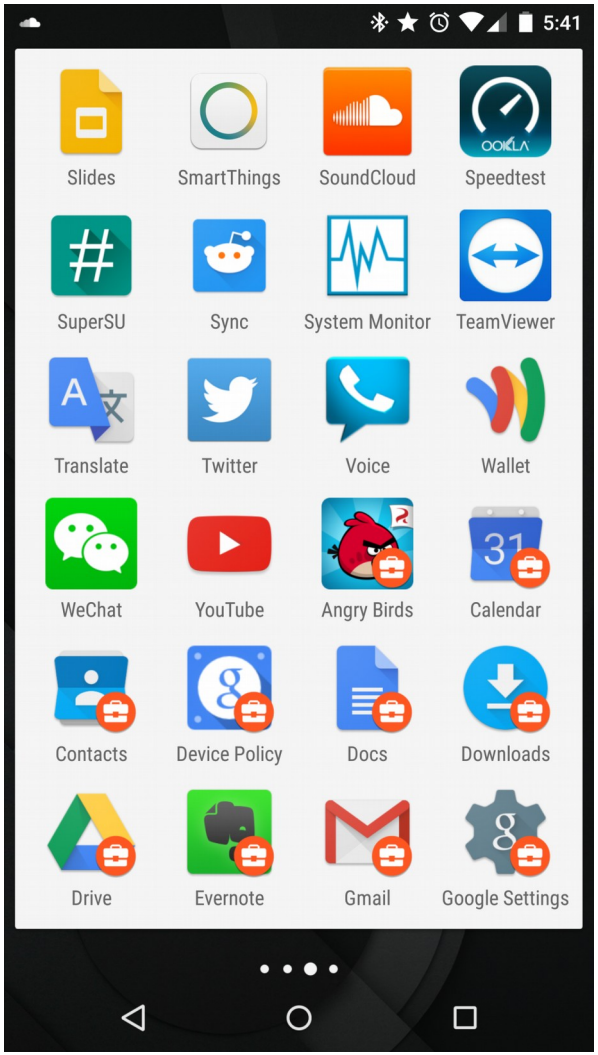
Android for Work



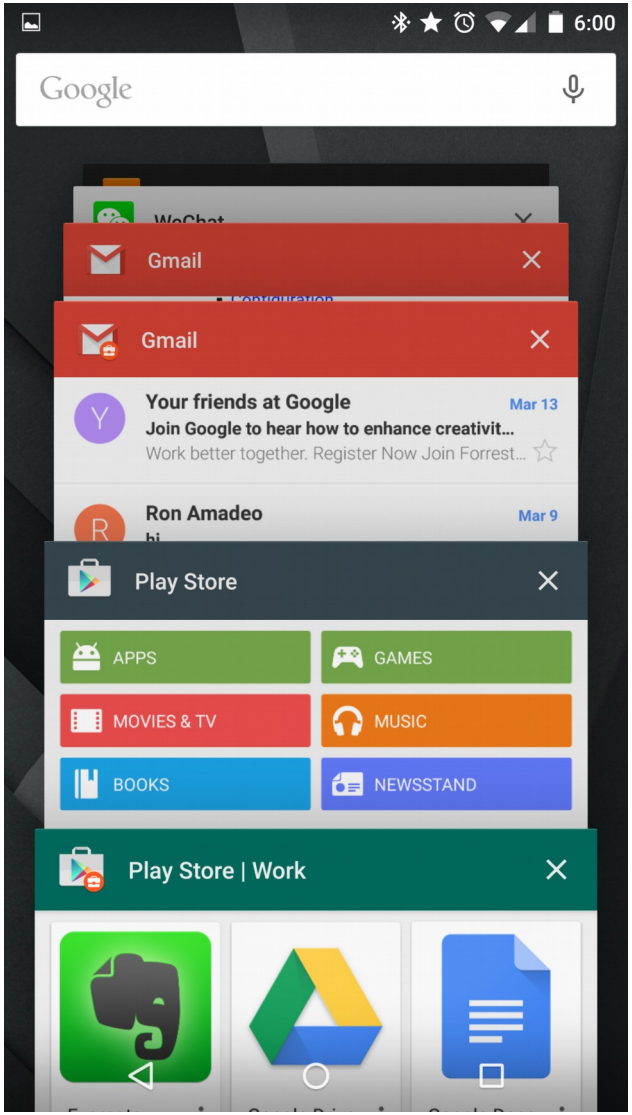


Android for Work





Android for Work



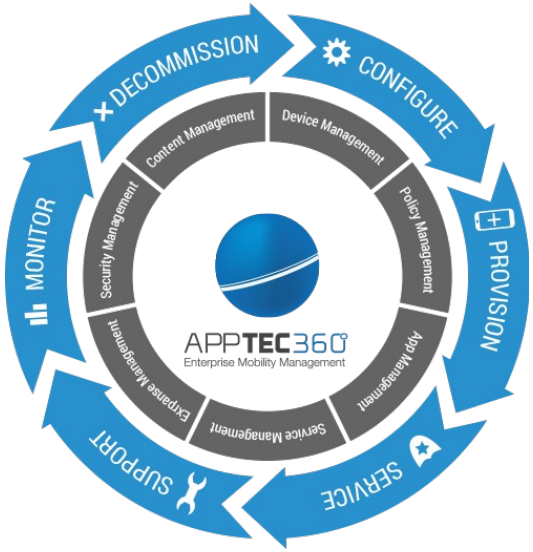
EMM Lösungen

anderScore trust in competence

Ohne Android for Work Support

SOPHOS

WSO2




airwatch
by vmware


BlackBerry


Centrify


CITRIX


Google
Apps for Work


MaaS360
by IBM


ManageEngine


MATRIX42


MobileIron


okta


SAP


SOTI

Showoff Manage Engine MDM

Weitere Informationen

Härten von Android Geräten

https://blog.torproject.org/blog/mission-impossible-hardening-android-security-and-privacy

Teamviewer

https://www.teamviewer.com/de/help/341-wie-kann-ich-mit-teamviewer-mein-android-geraet-steuern

Cyanogenmod

http://www.cyanogenmod.org/

Quellen

http://pretioso.com/consulting/mobile-strategie.html

http://pretioso-blog.com/samsung-knox-der-naechste-spionage-meilenstein-mit-technik-von-nsa-und-centrify/#.Vryf5PnhAb8

https://play.google.com/store/apps/details?id=com.afwsamples.testdpc

https://play.google.com/store/apps/details?id=com.google.android.apps.enterprise.dmagent

https://play.google.com/store/apps/details?id=com.google.android.apps.work.core&hl=de

https://www.google.com/work/android/partners/index.html?activeTab=emm#

http://arstechnica.com/information-technology/2015/03/a-review-of-android-for-work-dual-persona-support-comes-to-android/

https://uit.stanford.edu/service/mobiledevice/management/install_android

http://www.chip.de/artikel/Android-Automatisierung-Handy-Profile-einrichten-Handy-Funktionen-steuern_67714012.html

https://de.wikipedia.org/wiki/USA_PATRIOT_Act

http://www.zeit.de/politik/2015-06/us-senat-patriot-acts/seite-2

http://mobilesecurityares.blogspot.de/2014/10/why-samsung-knox-isnt-really-fort-knox.html

http://woerter.de/android/android-beyond-snowden-guides-and-links/2-hardening-android-os/

https://blog.torproject.org/blog/mission-impossible-hardening-android-security-and-privacy

http://developer.android.com/guide/topics/admin/device-admin.html

http://www.your-android.de/media/2013/05/Google-Datenkrake-660x330.jpg