Mobile Security im DB Konzern

Sicher in eine mobile Zukunft

DB Mobility Logistics AG

Dr. Matthias Drodt

ITK-Sicherheitsmanagement DB

Frankfurt am Main, 08.11.2013

Herausforderungen

Die Landschaft der mobilen Endgeräte ist über Jahre gewachsen

- **Smartphones und Tablet-Geräte** sind heute Alleskönner und genießen eine zunehmende Verbreitung.
- Hauptsächlich differenziert in die folgenden Benutzergruppen

I. Für **Manager / Führungskräfte / Wissensarbeiter** im wesentlichen zur klassischen Mail- / Kalender- / Adressenverwaltung (PIM)

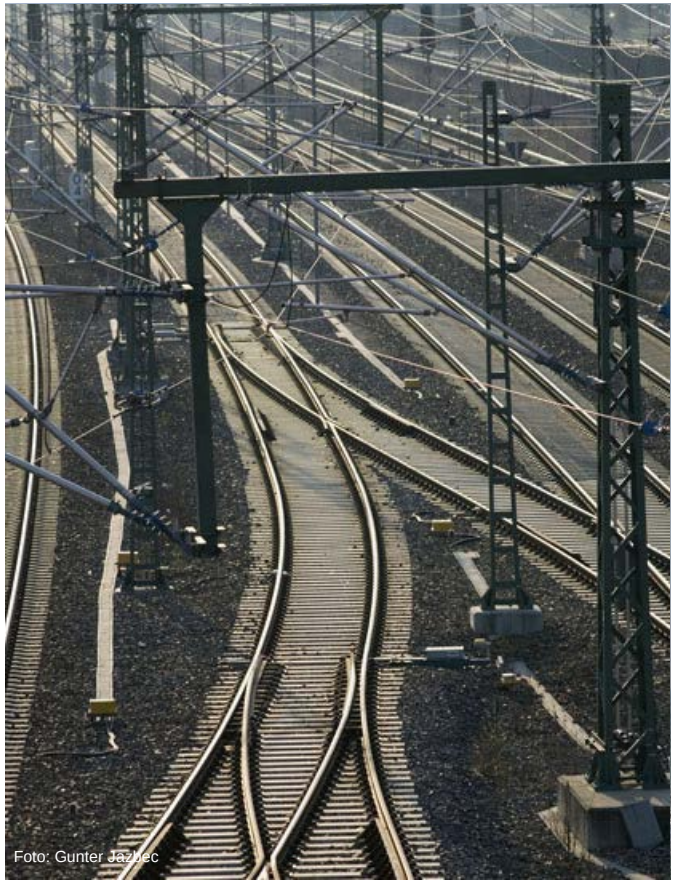
II. **Mobiles Personal** mit sehr unterschiedlichen Einsatzgebieten für den Zugriff auf Anwendungen, z.B.

- Ticketverkauf / Kontrolle **im Zug**
- Arbeitsauftragssteuerung der **Servicemitarbeiter in der Fläche**
- Informationen zum Zuglauf für die **Rangierer**
- Streckeninformationen („Fahrplan“) für **Triebfahrzeugführer**

Mobile Endgeräte müssen den Arbeitsalltag in allen Bereichen der Deutschen Bahn unterstützen.

PIM-Nutzung

Standardisierte und sichere Lösungen sind im Einsatz



- **Mobile Devicemanagement** (MDM) ist seit Jahren eingeführt und kann durch Fachanwendungen genutzt werden.
- Einheitliche **Mobilfunkverantwortung** durch den ITK-Dienstleister
- Liste von **MUSS-Anforderungen** für PIM sind umgesetzt.
  - Betriebssysteme, die diese Anforderungen nicht umsetzen und durch MDM kontrollieren lassen, dürfen für PIM-Szenarien nicht genutzt werden.
  - **Beschränkung auf Blackberry, Android** ab Version 3.0, **iOS** auf aktuellem Stand ab iPhone 4s und iPad 2.
- **Blackberry** als voll **gemanagte Lösung**, Blackberry 10 verfügbar (erste **sichere Lösung** für die Trennung zwischen „geschäftlich“ und „persönlich“ bzw. geschütztem und frei nutzbarem Bereich).
- **Company APP-Store** für eigene und empfohlene APPs.
- Beschlossen ist die Umsetzung einer **Whitelist für APPs**.

Seit Jahren werden für die PIM-Nutzung sichere und standardisierte Lösungen unter Nutzung von MDM-Möglichkeiten eingesetzt

PIM-Nutzung

Die MUSS-Anforderungen umfassen unter anderem

- Verbindlicher **Passwortschutz**, Passwortwechsel, automatischer Bildschirmschutz nach Inaktivität, Gerätesperrung bei Fehleingaben usw.
- **Verschlüsselung** der E-Mail Daten, der Dateianhänge, der Datenübertragung der Mail.
- **Remote Wipe** Möglichkeit
- Betriebssystem Aktualisierung
- Reglementierung von **Cloud Diensten** (Dokumentensynchronisation)
- Schutz vor **Jailbreak**, Manipulation, manuellen Konfigurationsänderungen usw.
- Keine **lokale Synchronisation** zwischen beliebigem PC <> geschäftlichen Daten
- **Virenscanner** auf dem Endgerät (aktuell nur Android)

Mobile Endgeräte müssen ein Mindestmaß an Sicherheitseigenschaften erfüllen, um erlaubt zu werden. Die Sicherheitseigenschaften müssen zentral verwaltet und überwacht werden können (MDM).

Für mobiles Personal und Zugriffen auf Anwendungen
Umfassendes Sicherheitskonzept wurde erstellt

- **Standardarchitektur** „RIM – Rail in Motion“ im Einsatz
- **Ganzheitliches Sicherheitskonzept für mobile Endgeräte** basierend auf dem Schutzbedarf der genutzten Anwendung unter Berücksichtigung von internen und externen **APPs**.
- Einführung **bestellbarer Sicherheitsklassen** beim ITK-Dienstleister, angepasst an die im Konzern vorhandenen Sicherheitsbedarfe.
- **Einheitlicher, verbindlicher Maßnahmenkatalog** für die **Entwicklung** von Anwendungen **sowie** die Sicherheit **mobiler Endgeräte** an sich.
- Wesentliche Ziele
  - Die **Sicherheit** und die **kosteneffiziente Nutzung** für eine wachsende Anzahl an Smartphones / Tablets herstellen.
  - **Mobile Strategien** sicher planen und umsetzen für alle APPs. Hierbei setzt die Sicherheit **„Leitplanken“** in Form von ITK-Sicherheitsmaßnahmen für das Business und die Entwicklung.

Die Deutsche Bahn ist auf dem Weg zu einem standardisierten Vorgehen, angepasst an die Schutzbedarfe der Daten und Anwendungen, im Einklang mit anderen Endgerätetypen.

Ganzheitliches Sicherheitskonzept für mobile Endgeräte

Umsetzung der Risikoeinschätzung und Maßnahmenauswertung

Mobiles Einsatzszenario
(Input)

Parameter:
- Allgemein / System
- App-spezifisch
- Externe Apps (Whitelisting/Abschottung)

Parametrisierung*

Modellierung

- Bedrohungsmatrix
- Maßnahmenmatrix
- Kreuzreferenztabelle
- Klassifizierungsschema für Schutzbedarf

Toolgestützte Automatisierung des Modells

Maßnahmenkatalog, Risikobehandlung und Dokumentation
(Output)

Maßnahmen mit:
- Umsetzungsrelevanz
- Umsetzungsstatus
- Risikoanalyse

**Parameter sind z.B.: Schutzbedarf der verarbeiteten Daten, Betriebssystem, im Auftrag des Unternehmens entwickelte Apps, Whitelisting vs. Abschottung*

Problembereiche – Offene Fragen

Derzeit bleiben einige Fragen offen…

- Das ausgelieferte Image auf den Endgeräten der Anbieter umfasst auch Anwendungen, die aus betrieblicher Sicht nicht geduldet werden können: zum Beispiel **FACEBOOK, Cloud-Speicher** usw.

? Wann gibt es ein **Business-Image**, welches **Social-Media-Konsumer-APPs** ausschließt und sich auf unbedingt notwendige Funktionen und APPs beschränkt?

Drei Möglichkeiten wären denkbar:

- Strikte und sichere Trennung von „geschäftlicher“ und „persönlicher“ Umgebungen für alle Betriebssysteme (auch für die Nutzung von APPs)
- Es gibt ein schlankes Business-Image (ohne Social-Media-Konsumer-APPs)?
- Es können **alle** im Image mitgebrachten APPs durch den ITK-Dienstleister frei konfiguriert werden und damit im Rahmen eines Mobile Devicemanagements beeinflusst werden können.

Das angepasste Image des OS auf den mobilen Endgeräten ist für den Businesseinsatz mit zahlreichen Risiken verbunden. Es wird ein Businessimage benötigt! Ohne Facebook, Cloudanwendungen, …