Eins–A
Systemhaus GmbH

Eins-A Systemhaus GmbH

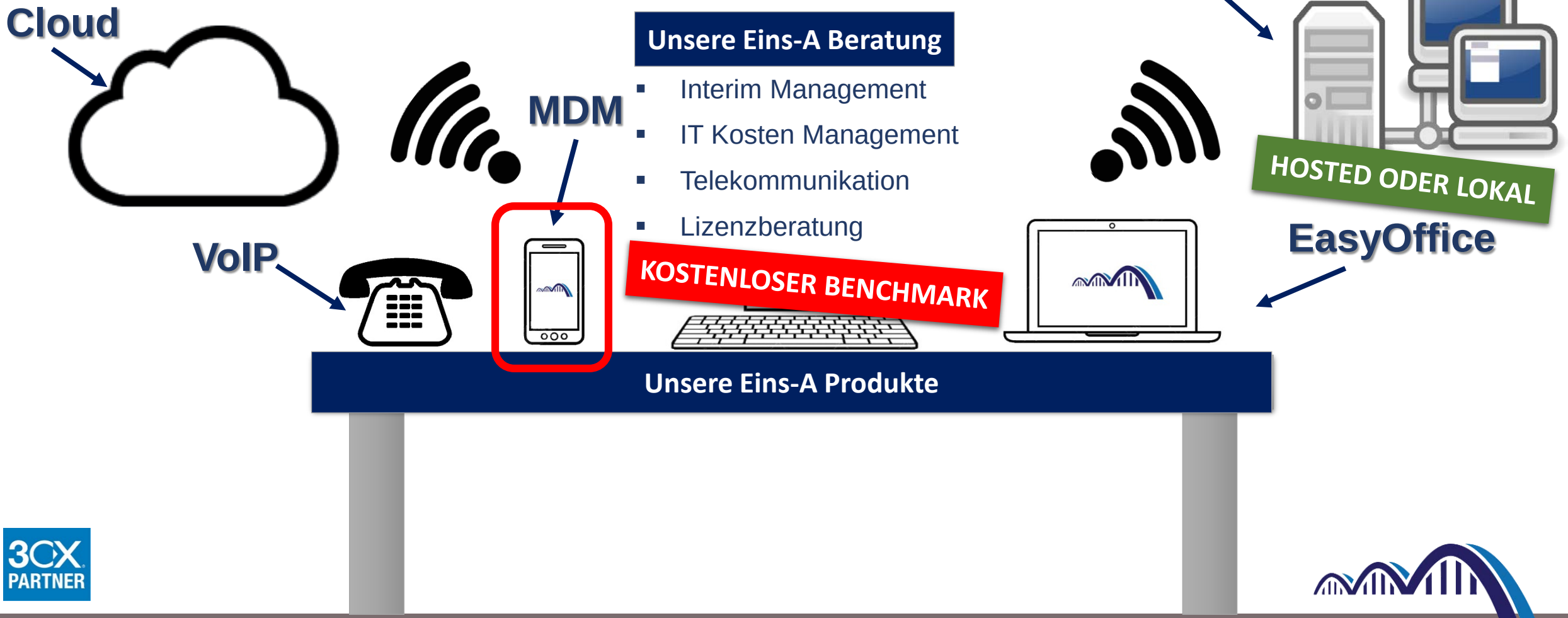
Wien - Hamburg

Ihr IT-Solution Partner

Ing. Walter Espejo

+43 (676) 662 2150

Das **Eins-A** Portfolio



3CX PARTNER

Eins–A
Systemhaus GmbH

MobileIron®

AppSense®

Mobile Device Management

airwatch®

Fixmo

MaaS360®

Eins-A Systemhaus GmbH

Was tut ein MDM?

MDM Mobile-Device-Management steht für die zentralisierte Verwaltung von Mobilgeräten wie Smartphones, Notebooks, PDAs oder Tablets durch Administratoren mit Hilfe einer Software.

Dazu gehören

- Inventarisierung von Hardware
- Software- und Datenverteilung
- Management Profile & Settings
- Schutz der Daten

Zielsetzung ist, möglichst automatisiert viele Endgeräte für unterschiedliche User mit unterschiedlichen Konfigurationen **SICHER** und **EFFIZIENT** zu verwalten.

Auszug von MDM Funktionen und unterstützte Prozesse

SW Rollout	Setting & Profiles	Support	Verlust / Ersatz
Monitoring	Roaming Control	Manage User Groups	Manage System Settings
Passcode & Passcode Policy	Secure Container	Wipe	View Device Settings
Jailbreak Detection	…	…	…

Dazu wird auf den Endgeräten typischer Weise ein Devicemanagement Client installiert, der die Kommunikation mit dem Backend System gewährleistet.

Marktüberblick

Werden international als Marktführer gehandelt.

Am tel ● Apperian ● AppSense ● Aruba Networks ● AT&T (Toggle) ● Bitzer Mobile ● Capricode ● Centrify Cortado ● Dell Kace ● Excitor ● Fixm o ● ForeScout Technologies ● Globo Mobile ● Ibelem ● Juniper Networks ● Kony ● Cicso-Meraki ● Microsoft ● Mobile Active Defense ● MobileFram e ● MobileSpaces ● Mobiquant ● Notify Technology ● Novell ● OpenPeak ● Portsys ● Sam sung SDS ● Seven Principles ● SilverbackMDM ● Sm ith Micro Software ● The Institution ● Vmware ● ...

Am Markt ranken sich mittlerweile zahlreiche Hersteller mit den unterschiedlichsten Historien. Ausgelöst hat den Boom das Wachstum von Smartphones und Tablets und die Vielfalt und Volatilität am Markt. Unternehmen sind damit konfrontiert, diese Vielfalt effizient und sicher zu managen.

Worin bestehen grundsätzlich Unterschiede der Hersteller?

- Funktionsumfang und Abdeckung Betriebssysteme/Endgeräte ist vielfach vergleichbar.
- Unterschiedliche Schwerpunkte je nach Historie (z.B. Motivation Blackberry → Einbindung von ein „paar“ iOS & Android, SAP & Citrix → logische Verlängerung des eigenen System/Cloud Portfolios)
- Geschwindigkeit, mit der neue EG und Betriebssystem Versionen implementiert werden.

Der Markt teilt sich international in

(a) Hersteller (AirWatch, Mobileiron, Citrix,…)

(b) Systemhäuser & Integratoren als nationale MDM Lieferanten und Integratoren. Sind im Gartner Quadranten nicht betrachtet (Eins-A Systemhaus)

Eins–A Systemhaus GmbH

Sicherheit und Kontrolle

***Die DM* Philosophie**: „Ich sehe alle Einstellungen, kann aber Remote nur das konfigurieren, was mir der User erlaubt und was im Rahmen des Betriebssystems (OS) möglich ist“.*

Dadurch lassen sich zahlreiche Settings im Rahmen der OS Möglichkeiten machen (Wipe, Zugangseinstellungen, Passcode, Roaming Settings, WALN Settings, …)

Zusätzliche Sicherheit durch den Einsatz eines **Secure Containers**: Der Secure Container bildet eine „Over-all Sandbox“ für die kritischen Company Daten unabhängig von den privaten Daten am Endgerät.

*) DM – Device Management

Aufbau des DM auf dem Phone

- ***DM Management Komponente (APP)***
  - *Profil #1 (z.B. WLAN)*
  - *Profil #2 (z.B. Exchange)*
  - *Profil #3 (z.B. Passcode)*
  - *Profil #N*

Solange die DM Management Komponente läuft können *):

- Jailbreaks erkannt werden
- Veränderungen in Settings (z.B. Roaming eingeschaltet, etc) können erkannt werden. Eine entsprechende Reaktion seitens Admin ist möglich.
- Admin kann Profile an den User senden. Profile müssen manuell akzeptiert werden, ein Monitoring durch den Admin ist möglich.
- Sollte vom User die Management Komponente gelöscht werden, besteht keine Verbindung zum Backend mehr. Admin kann dann die Zugänge sperren.
- Beim Löschen der Management Komponente werden auch alle Profile gelöscht.

*) je nach Funktionsumfang DM Hersteller

Eins–A Systemhaus GmbH

BYOD Policy

Datenschutzrichtlinie & Policies

Regelung des Zugriffs des U auf das EG und der EG Konfiguration (z.B. welche SW muss installiert sein, Zugriffsrechte U z.B. Devicemanagement , welche SW muss der MA zulassen, Wipe, Gefahr im Verzug, …)

Regelung Service und Supportprozess. Was wird supportet, was nicht.

Private Daten und APPs

Verlust, Reparatur und Ersatz (Prozess, Verantwortung)

Umgang mit privater Usage (z.B. Urlaub): Kosten, APPs, Daten

Regelung „Notfallszenario“ (z.B. bei Verlust), um die Arbeitsfähigkeit des MA aufrecht zu erhalten (z.B. Ersatzgeräte)

Nutzen Sie unseren KOSTENLOSEN Fragenbogen

Welche Geräte und SW sollen zugelassen werden und wie sollen diese beschafft werden.

Kostenbeteiligung MA / U

Betriebsvereinbarung

Organisatorische Maßnahmen (z.B. Schulungen)

Regelung Eigentumsverhältnisse des Geräts und der SW

Regelung Ausstiegsszenario des MA (möchte nach X Monaten aussteigen, Beendigung DV, …)

Entscheidend

- IT Integrations-, Sicherheits- & Supportkonzept
- Vielfalt an unterstützten Endgeräten

Eins-A
Systemhaus GmbH

Eins-A Systemhaus GmbH

@ Wien
MGC Office Center
Modecenterstr. 22
A-1030 Wien
Tel: +43 1 343 9512
Mail: *info@eins-a.at*

@ Hamburg
Repräsentanz Hamburg
Raboisen 38
D-20095 Hamburg
Tel: +49 40 4143115462
Mail: *info@eins-a-hamburg.de*