

Evaluierung und Migration von non Managed Devices in eine EMM Umgebung

IHK – Projektpräsentation von:

Martin Goltschewski

Agenda

BTC





**Ca. 381
Mitarbeiter**

**Standort in
Oldenburg**



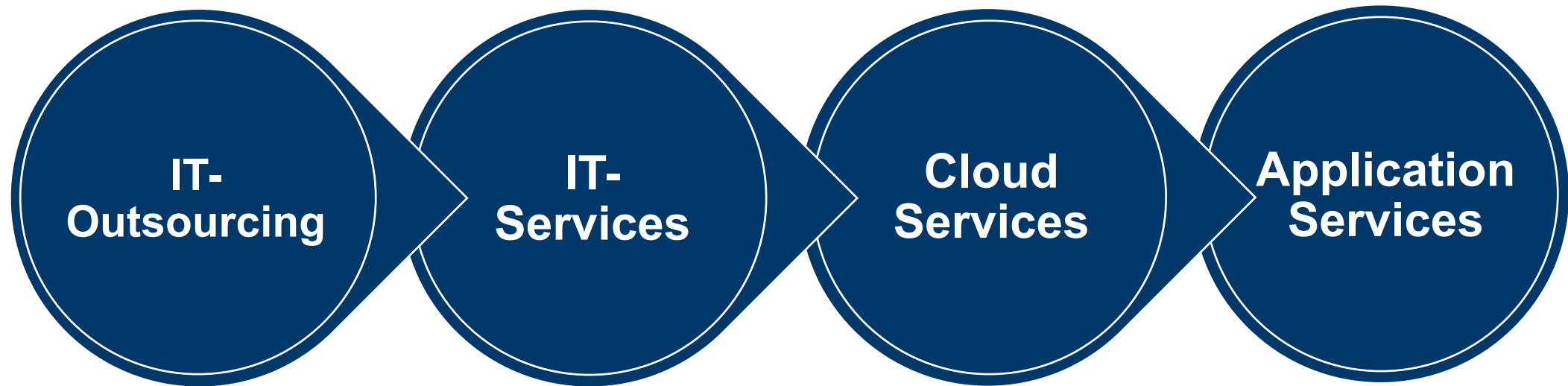
**BTC IT Services
GmbH**



**Tochter
der BTC**

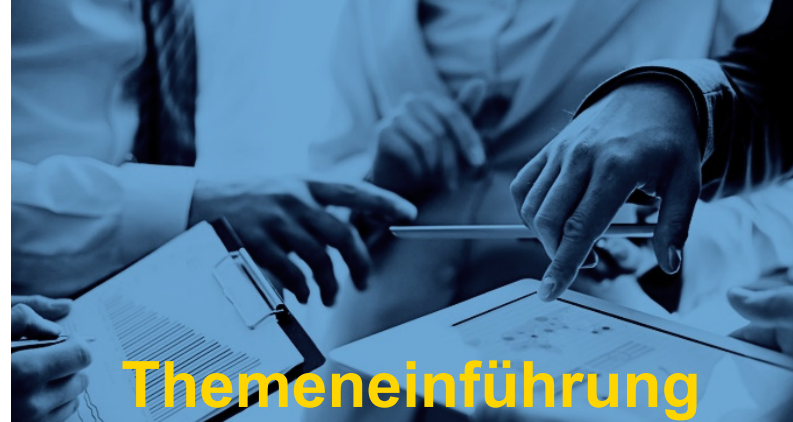
**Ca. 64,2 Mio.
Euro Umsatz**



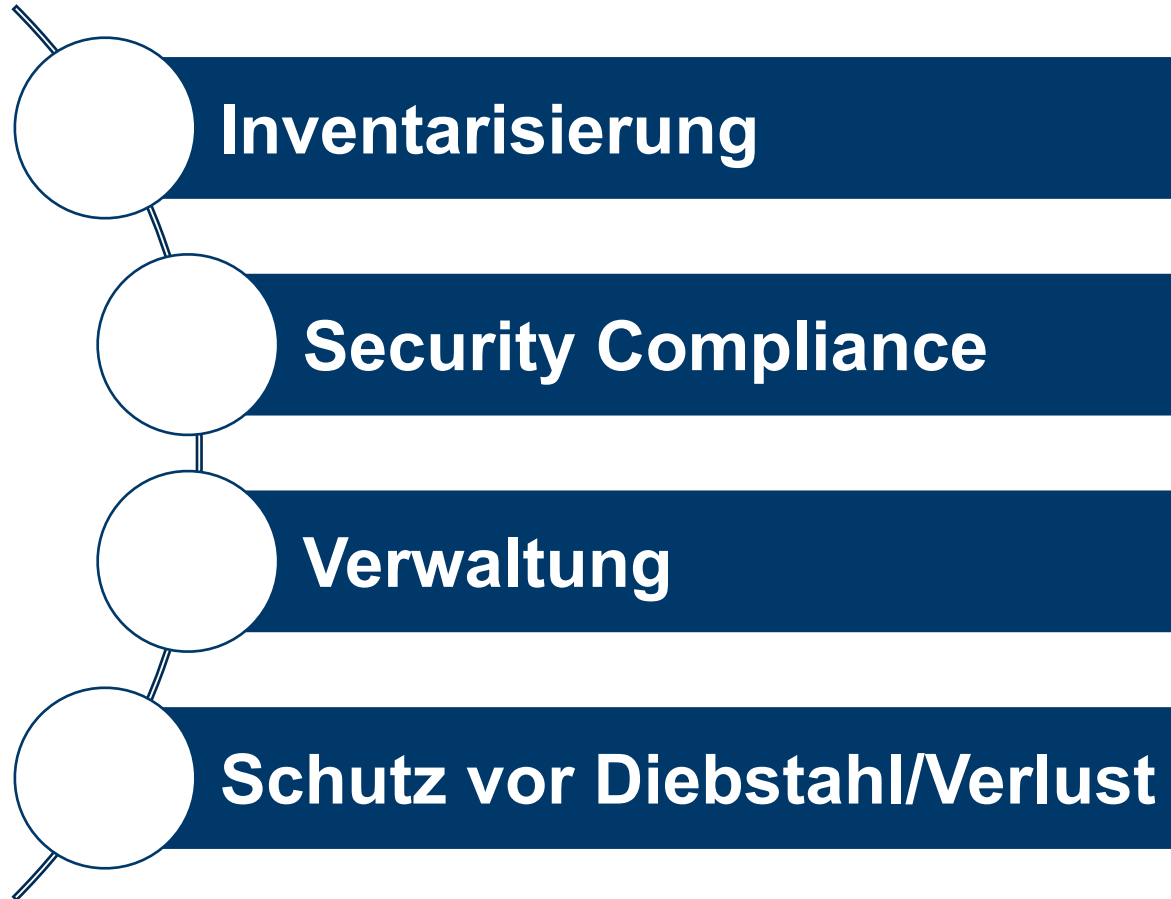


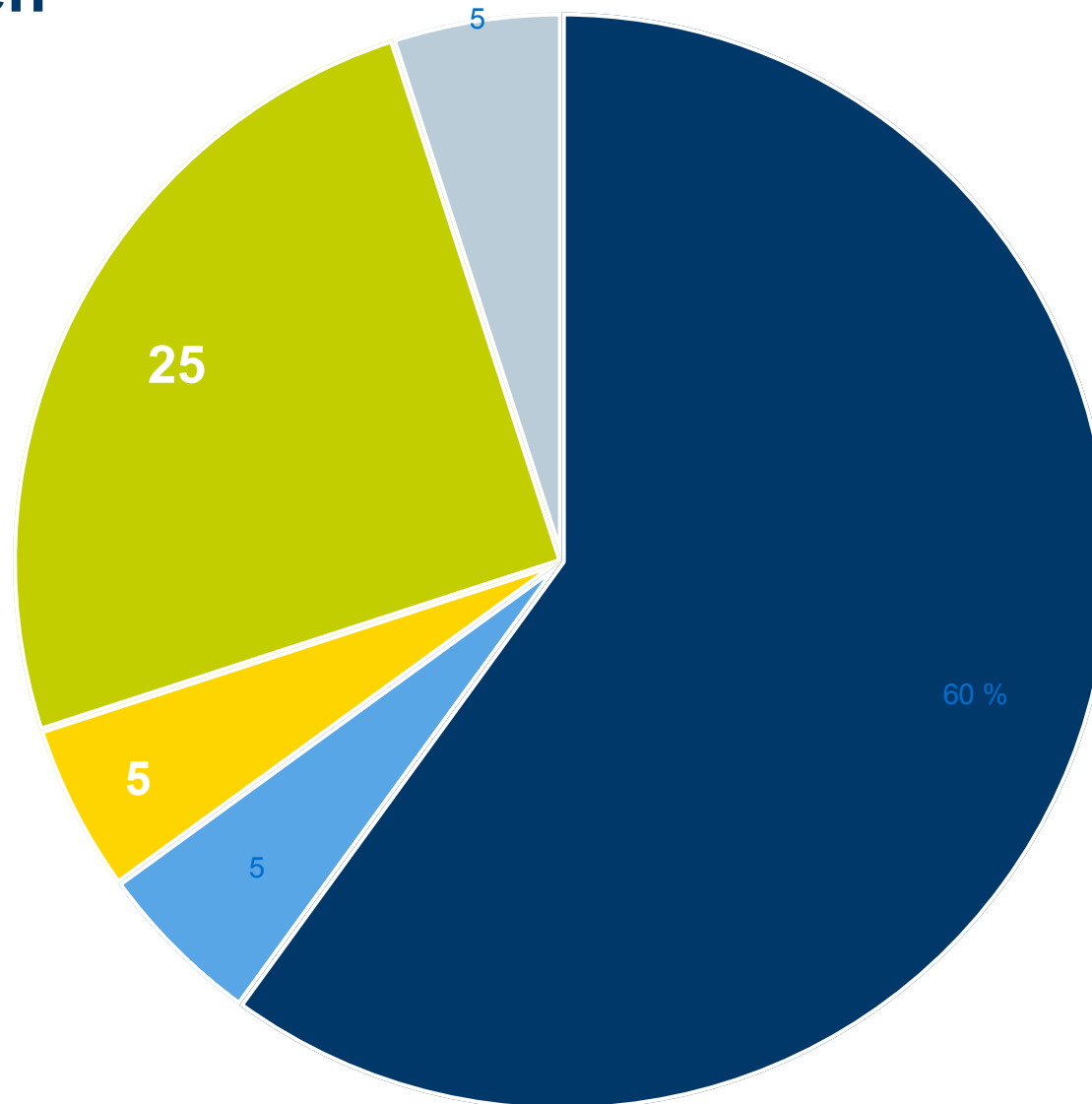
Agenda

BTC



Projektbegründung



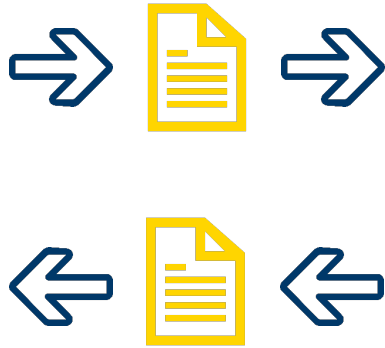


Agenda

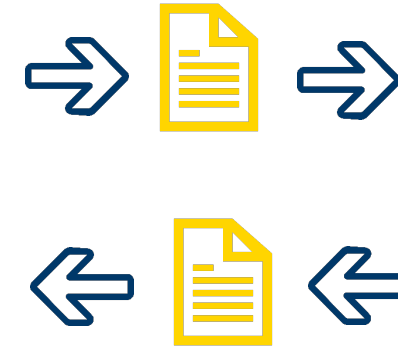
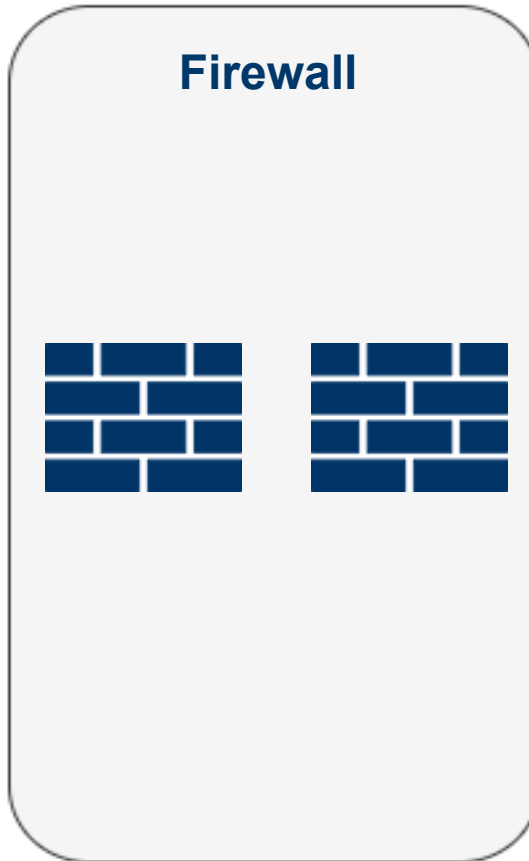
BTC



Mobiles Endgerät



Firewall

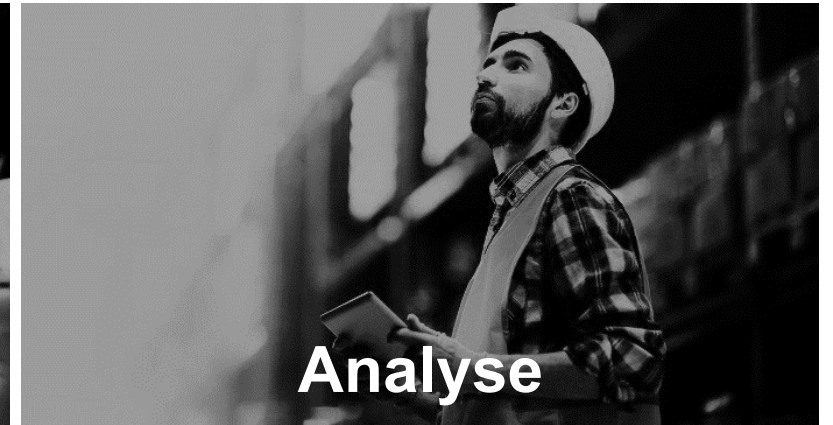


Exchange Server
(On Premise)



Agenda

BTC



Soll-Konzeption

- **Evaluierung von Endgeräten**
- **Evaluierung und Migration einer EMM-Lösung**
- **Security Compliance**

Soll-Konzeption

- **Standardisierte Konfiguration**
- **Bereitstellung von Applikationen**



Anforderungen:

- **Apple Portfolio**
- **Patchzyklus**
- **<= 6,5" Bildschirmdiagonale**
- **Hohe Akkulaufzeit**
- **Im mittleren Preissegment**

Evaluation der mobilen Endgeräte

BTC



iPhone XR



iPhone 11



iPhone 11 Pro



iPhone 11 Pro Max

Endgeräte – Technische Merkmale

BTC



Merkmal	iPhone XR	iPhone 11	iPhone 11 Pro	iPhone 11 Pro Max
Displaydiagonale	6,1“	6,1“	5,8“	6,5“
Prozessor	A12 Bionic Chip 2.Gen	A13 Bionic Chip 3.Gen	A13 Bionic Chip 3.Gen	A13 Bionic Chip 3.Gen
Akku-Kapazität	2.942 mAh	3.110 mAh	3.174 mAh	3.969 mAh
Patchzyklus (vsl.)	4 Jahre	5 Jahre	5 Jahre	5 Jahre
Preis	578,39€	697,14€	949,83€	1032,43€

Nutzwertanalyse – mobile Endgeräte

Kriterium	Gewichtung	Apple iPhone XR		Apple iPhone 11		Apple iPhone 11 Pro		Apple iPhone 11 Pro Max	
		Wertung	Gesamt	Wertung	Gesamt	Wertung	Gesamt	Wertung	Gesamt
Haptik	5%	4	20	4	20	5	25	3	15
Patchzyklus	20%	4	80	5	100	5	100	5	100
Display	5%	4	20	4	20	5	25	5	25
Displaygröße	10%	5	50	5	75	5	50	3	30
Akku Kapazität	10%	3	30	4	60	5	50	5	50
Speicherkapazität	5%	5	25	5	25	5	25	5	25
Performance (Prozessor)	10%	4	40	5	75	5	50	5	50
Erfahrung	10%	4	40	4	60	4	40	4	40
Design	5%	5	25	5	25	5	25	5	25
Wirtschaftlichkeit (P/L)	20%	4	80	5	100	4	80	4	80
Gesamt	100%		410		560		470		440

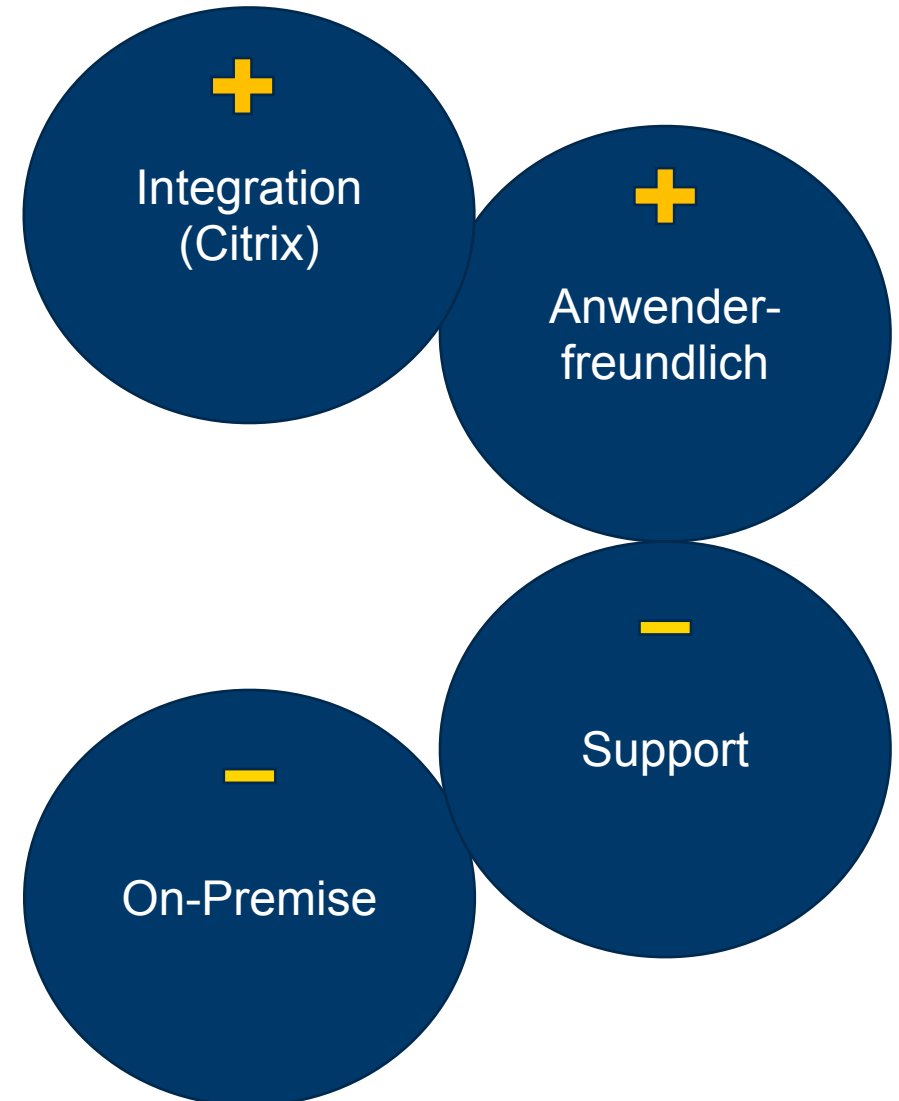
Evaluation einer EMM-Lösung

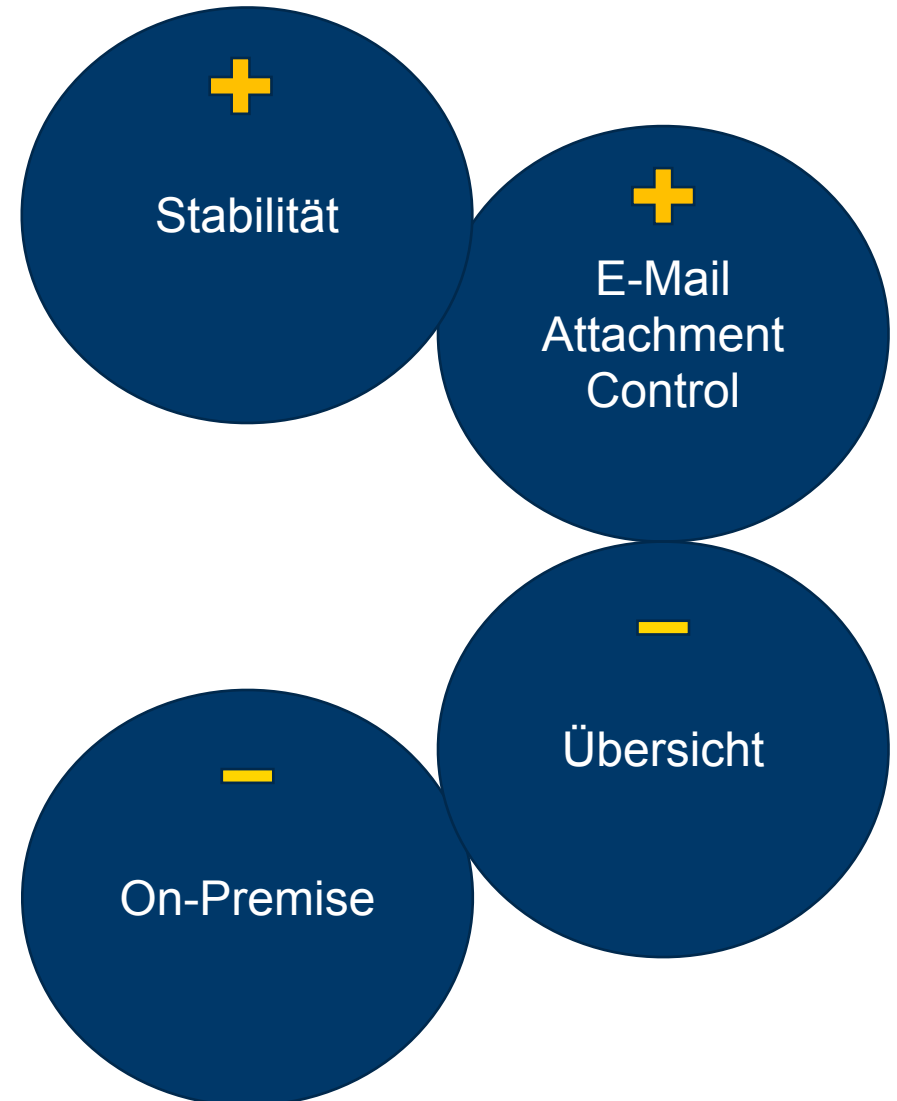


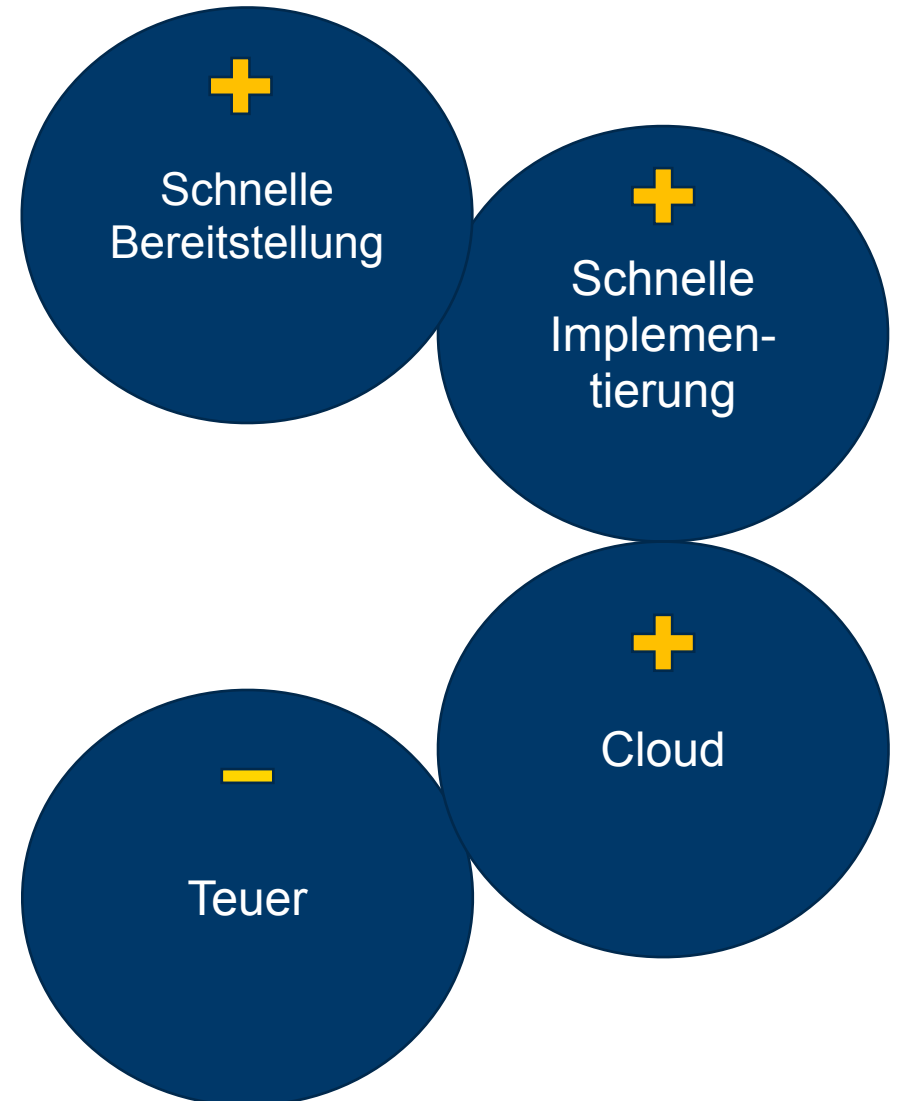
Anforderungen:

- **Security Compliance**
- **Standardkonfiguration**
- **Monitoring**
- **Device Management (Funktionsumfang)**
- **Support**

CITRIX® **XenMobile**





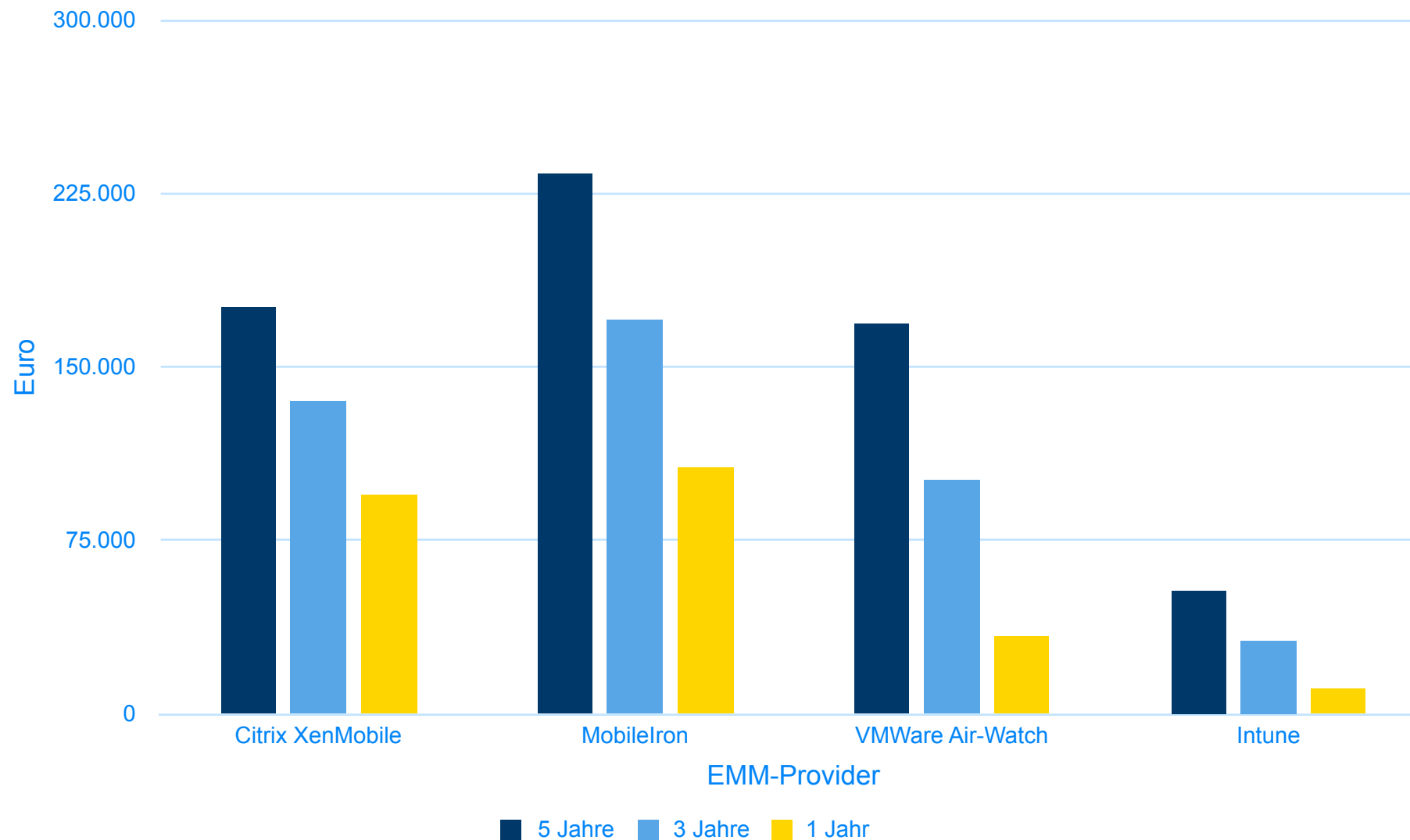




Nutzwertanalyse – EMM-Lösung

		Citrix XenMobile		Mobile Iron		VMWare Air Watch		Microsoft Azure Intune	
Kriterium	Gewichtung	Wertung	Gesamt	Wertung	Gesamt	Wertung	Gesamt	Wertung	Gesamt
Kompatibilität	5%	5	25	5	25	5	25	5	25
Anwenderfreundlichkeit / Bedienbarkeit	10%	5	50	4	40	5	50	5	50
Device Management	25%	4	100	4	100	5	125	4	100
Monitoring	10%	5	50	5	50	5	50	5	50
Support	15%	4	60	4	60	4	60	5	65
Ressourcenbedarf	10%	4	40	4	40	5	50	5	50
Wirtschaftlichkeit (P/L)	25%	3	75	3	75	4	100	5	125
Gesamt	100%		400		390		460		465

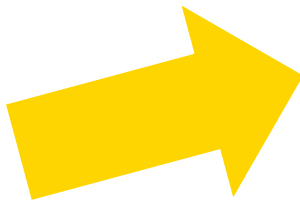
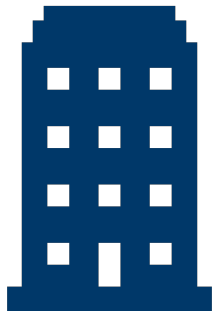
Lizenzkosten - Jahresübersicht



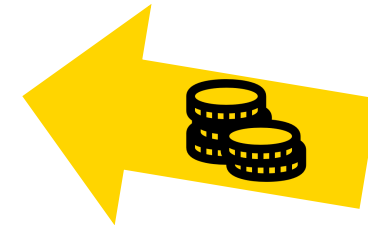


BYOD = Bring-Your-Own-Device

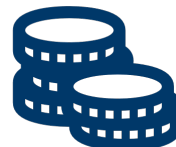
ABC GmbH



EMM-Lösung



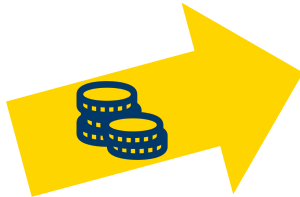
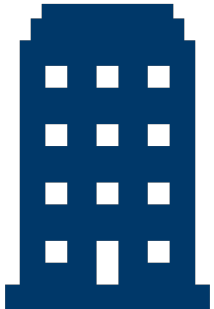
Optional



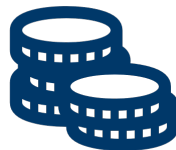


CYOD = Choose-Your-Own-Device

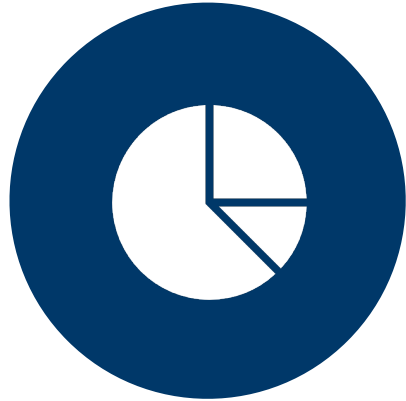
ABC GmbH



EMM-Lösung



Betrachtung der Privatnutzung - Vorteile



**GRÖßERE
NUTZERAKZEPTANZ**



BEQUEM



**KEINE
EINSCHRÄNKUNG DER
PRODUKTIVITÄT**

Betrachtung der Privatnutzung - Nachteile



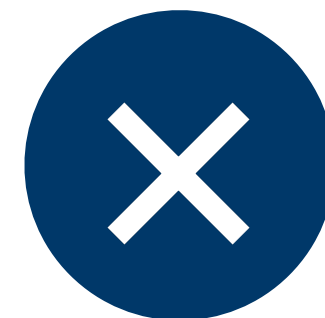
SICHERHEITSRISIKO



**POTENZIELL
ERHÖHTER
SUPPORTAUFWAND**



**KEINE
ORDNUNGSGEMÄßE
FUNKTION**



**HOMOGENITÄT
(APP)**

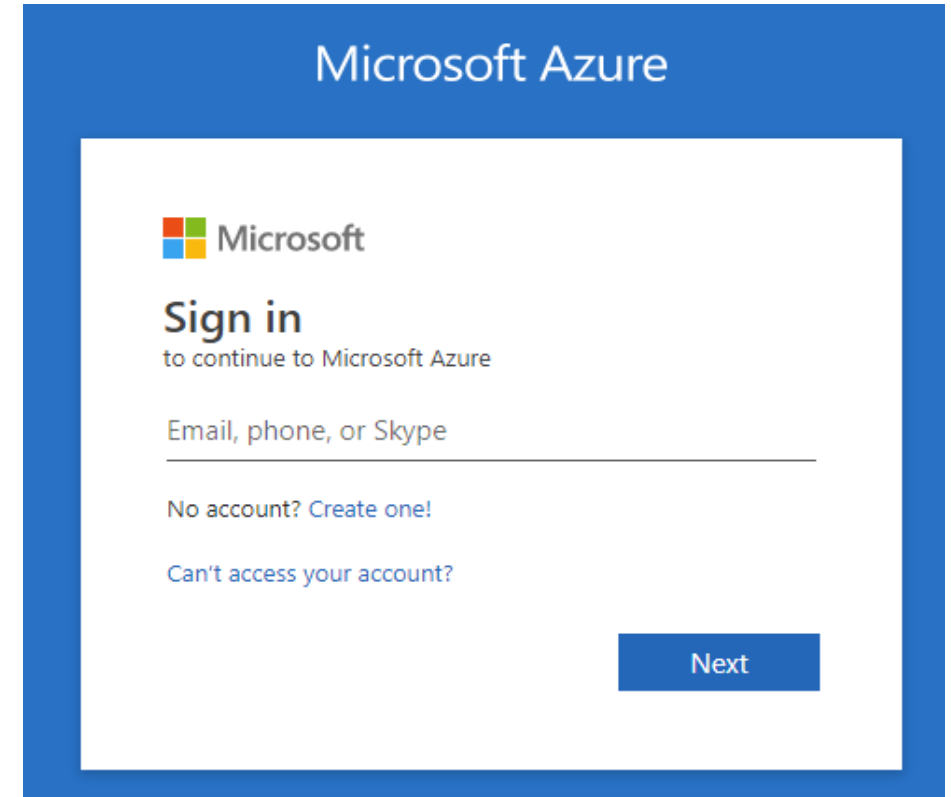
Agenda

BTC

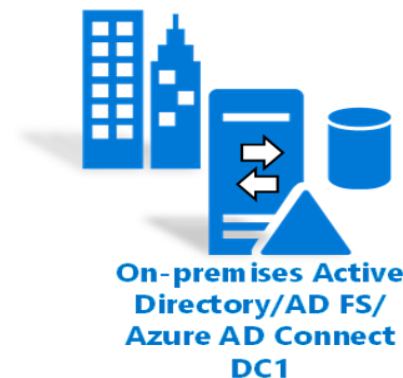


Einrichtung: Microsoft Azure Mandanten

- **Kunde erstellt Azure Mandanten**
- **BITS hat Mitwirkungspflicht**
- **Beschaffung + Zuweisung der E3 Lizenz**



- Synchronisierung zwischen On-Premise AD und dem Azure AD
- Kennworthashsynchronisierung, Azure AD- und Attributfilterung, Kennwortzurückschreiben



Azure AD – Optionale Features

Microsoft Azure Active Directory Connect

Express-Einstellungen
Benutzeranmeldung
Mit Azure AD verbinden
Synchronisierung
Verzeichnisse verbinden
Azure AD-Anmeldung
Domänen-/OE-Filterung
Benutzer werden identifiziert
Filterung
Optionale Features
Azure AD-Apps
Azure AD-Attribute
Konfigurieren

Optionale Features

Wählen Sie erweiterte Funktionen aus, wenn diese von Ihrer Organisation benötigt werden.

- ☐ Exchange-Hybridbereitstellung ?
- ☐ Öffentliche Exchange-E-Mail-Ordner "" ?
- ☒ Azure AD-App- und Attributfilterung ?
- ☒ Kennworthashsynchronisierung ?
- ☒ Kennwortrückschreiben ?
- ☐ Gruppenrückschreiben ?
- ☐ Geräterückschreiben ?
- ☐ Verzeichniserweiterungen-Attributsynchronisierung ?

[Weitere Informationen](#) zu optionalen Funktionen.

Zurück Weiter

Azure AD – APPs

The screenshot shows the 'Microsoft Azure Active Directory Connect' window, specifically the 'Azure AD-Apps' configuration page. The left sidebar contains a list of configuration options: 'Express-Einstellungen', 'Benutzeranmeldung', 'Mit Azure AD verbinden', 'Synchronisierung', 'Verzeichnisse verbinden', 'Azure AD-Anmeldung', 'Domänen-/OE-Filterung', 'Benutzer werden identifiziert', 'Filterung', 'Optionale Features', 'Azure AD-Apps' (which is highlighted in blue), 'Azure AD-Attribute', and 'Konfigurieren'. The main content area is titled 'Azure AD-Apps' and contains the following text: 'Die zur Verwendung der folgenden Apps erforderlichen Informationen werden in Azure AD exportiert. Entfernen Sie eine App nur dann, wenn dies zur Einhaltung strenger Sicherheitsrichtlinien Ihrer Organisation erforderlich ist.' Below this text is a section titled 'AZURE AD-APPS' with a list of applications and their selection status: 'Office 365 ProPlus' (unchecked), 'Exchange Online' (unchecked), 'SharePoint Online' (unchecked), 'Lync Online' (unchecked), 'Azure RMS' (unchecked), 'Intune' (checked), 'Dynamics CRM' (unchecked), and 'Drittanbieteranwendung' (unchecked). At the bottom of this list is a checkbox labeled 'Ich möchte die Liste der Anwendungen einschränken.' which is checked, followed by a blue question mark icon. At the bottom right of the window are two buttons: 'Zurück' (grey) and 'Weiter' (green).

Microsoft Azure Active Directory Connect

Express-Einstellungen
Benutzeranmeldung
Mit Azure AD verbinden
Synchronisierung
Verzeichnisse verbinden
Azure AD-Anmeldung
Domänen-/OE-Filterung
Benutzer werden identifiziert
Filterung
Optionale Features
Azure AD-Apps
Azure AD-Attribute
Konfigurieren

Azure AD-Apps

Die zur Verwendung der folgenden Apps erforderlichen Informationen werden in Azure AD exportiert. Entfernen Sie eine App nur dann, wenn dies zur Einhaltung strenger Sicherheitsrichtlinien Ihrer Organisation erforderlich ist.

AZURE AD-APPS

- ☐ Office 365 ProPlus
- ☐ Exchange Online
- ☐ SharePoint Online
- ☐ Lync Online
- ☐ Azure RMS
- ☒ Intune
- ☐ Dynamics CRM
- ☐ Drittanbieteranwendung

☒ Ich möchte die Liste der Anwendungen einschränken. ?

Zurück Weiter

Azure AD Attribute (Intune)

Microsoft Azure Active Directory Connect

Express-Einstellungen
Benutzeranmeldung
Mit Azure AD verbinden
Synchronisierung
Verzeichnisse verbinden
Azure AD-Anmeldung
Domänen-/OE-Filterung
Benutzer werden identifiziert
Filterung
Optionale Features
Azure AD-Apps
Azure AD-Attribute
Konfigurieren

Azure AD-Attribute

Diese Attribute werden basierend auf der zuvor ausgewählten Anwendung in Azure AD exportiert. Entfernen Sie ein einzelnes Attribut nur, wenn dies für die Erfüllung der Zeichenfolgen-Organisationssicherheitsrichtlinie erforderlich ist.

EXPORTIERTE ATTRIBUTE

- ☒ accountEnabled
- ☒ accountName
- ☒ c
- ☒ cloudUserCertificate
- ☒ cn
- ☒ description
- ☒ deviceId
- ☒ deviceOSType
- ☒ deviceTrustType
- ☒ displayName
- ☒ distinguishedName
- ☒ domainFQDN

☐ Ich möchte die Attribute weiter einschränken, die in Azure AD exportiert werden. ?

[View the list of attribute as comma-separated values](#)

Zurück Weiter

Erstellung und Konfiguration einer Gruppe im Azure Tenant

➤ Anlegen einer Gruppe im Azure Tenant

➤ Festlegen des Gruppentyps

- Sicherheit
- Office 365

➤ Zuweisung der Microsoft E3 Lizenz

Microsoft Azure

Home > Gruppen - Alle Gruppen > Neue Gruppe

Neue Gruppe

Gruppentyp *
Sicherheit

Gruppenname * ⓘ
Geben Sie den Namen der Gruppe ein.

Gruppenbeschreibung ⓘ
Geben Sie eine Beschreibung für die Gruppe ein.

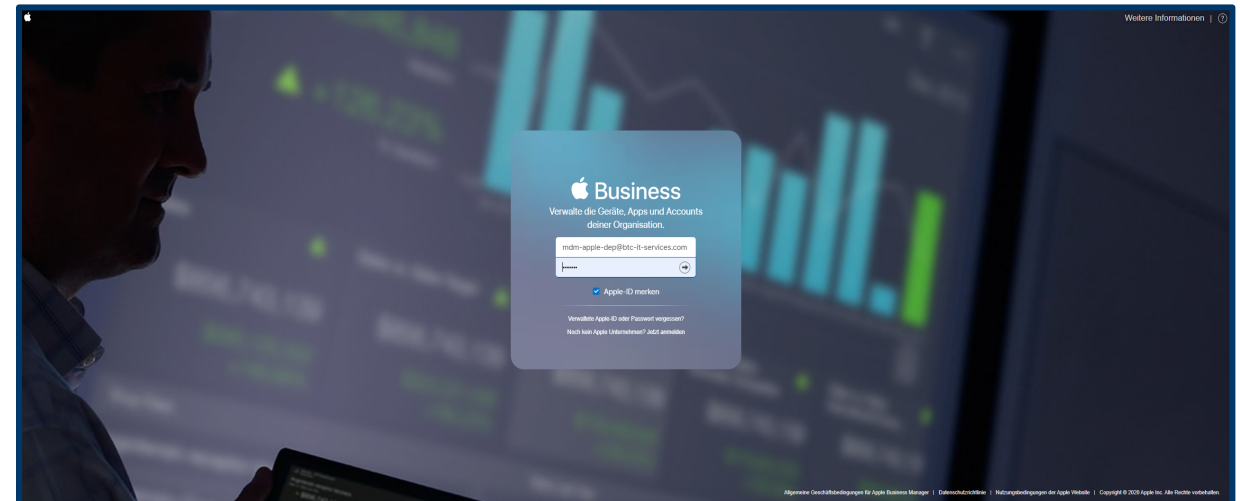
Mitgliedschaftstyp * ⓘ
Zugewiesen

Besitzer
Keine Besitzer ausgewählt.

Mitglieder
Keine Mitglieder ausgewählt.

Apple Business Manager (ABM)

- **Webbasiertes Portal**
- **Dient für die IT-Administration um Apple Endgeräte von einem Ort aus bereitzustellen**
- **Verteilung von Apps und Bücher aus dem APP Store**

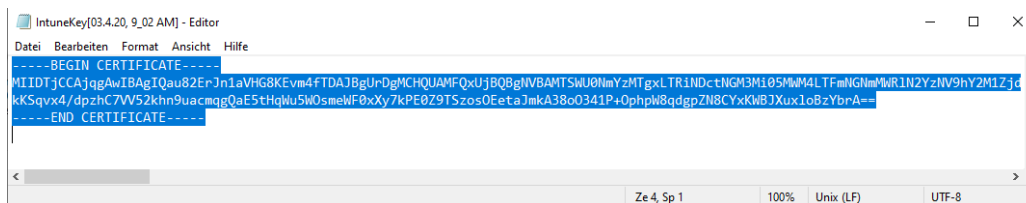


Erstellung eines Apple Business Manager

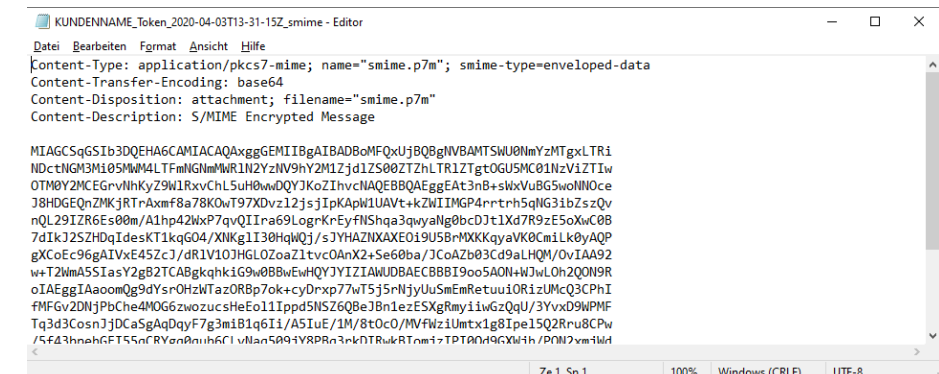
- **Mitwirkungspflicht des Kunden**
- **BITS ist lediglich für die Bereitstellung einer Anleitung verpflichtet**
- **Bestellung der mobile Endgeräte (Organisations-ID)**

Erstellung eines MDM – Server im ABM

- **Zweistufige Authentifizierung**
- **Erstellung eines Token (Registrierungsprogramm) beim MDM Provider**



Intune-Zertifikatsanforderung



MDM-Server Token

Konformitätsrichtlinie:

- Richtlinie die ein Endgerät erfüllen muss, um Unternehmenszugang zu erhalten

Benutzerrichtlinien:

- Richtlinien für die Geräteeinschränkung

- Die Konformitätsrichtlinien sowie die Benutzerrichtlinien wurden mit dem Kunden abgestimmt.

Einrichtung der Konformitätsrichtlinien & Geräterichtlinien



Suchen (STRG+ /)

«

Übersicht

Verwalten

Eigenschaften

Zuweisungen

Monitor

Gerätestatus

Benutzerstatus

Status pro Einstellung

Speichern

Verwerfen

Name *

Beschreibung

Beschreibung eingeben...

Plattform

iOS/iPadOS

Einstellungen Konfigurieren

>

Aktionen bei Inkompatibilität

1 konfiguriert

>

Bereich (Markierungen)

1 Bereich(e) ausgewählt

>

iOS-Konformitätsrichtlinie

iOS/iPadOS

Wählen Sie eine Kategorie aus, um Einstellungen zu konfigurieren.

E-Mail

1 Einstellung verfügbar

>

Geräteintegritätsdienst

1 von 2 Einstellungen konfiguriert

>

Geräteeigenschaften

2 von 4 Einstellungen konfiguriert

>

Systemsicherheit

6 von 10 Einstellungen konfiguriert

>

OK

Geräteintegritätsdienst

iOS/iPadOS

Geräte mit Jailbreak ⓘ

Blockieren

Nicht konfiguriert

Anfordern, dass das Gerät höchstens der angegebenen Gerätebedrohungsstufe entspricht ⓘ

Nicht konfiguriert

▼

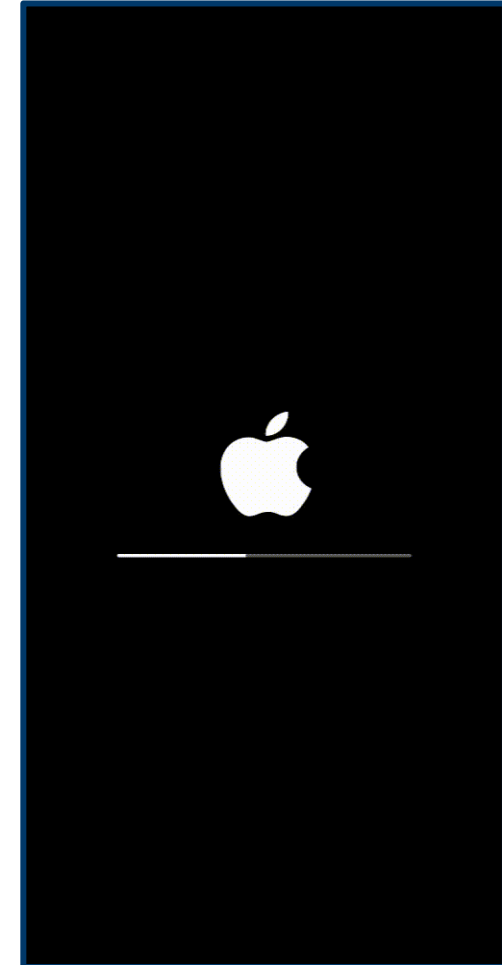
OK

10/07/20 Martin Gotschewski – Evaluierung und Migration von non-managed Devices in eine EMM-Umgebung

40

Erstellung eines DEP-Profil

- **DEP = Device Enrollment Program**
- **iOS Profil**
- **Benutzeraffinität**
- **Einbindung des VPP-Token**



Abstimmung der Unternehmens-App

- Liste der benötigten Apps
- Treffen einer Vorauswahl
- Termin mit dem Kunden zur Abstimmung

Abstimmung der Unternehmens-Apps

Unternehmens-App	Vorauswahl	Abstimmung mit dem Kunden
LikedIn: Business-Netzwerk	x	
Yammer	x	
XING - Ihr berufliches Netzwerk	x	
Lufthansa	x	x
Monal - XMPP chat		
HRS Hotel Suche - Top Hotels		
DB Navigator	x	
Keynote		
Numbers		
Pages		
TimeboxApp		x
Booking.com: Hotel Angebote		x
mehr-tanken		
MeinVodafone	x	x
MeinMagenta		
Microsoft OneNote		



Fazit

- ✓ Inventarisierung
- ✓ Security Compliance
- ✓ Schutz vor Diebstahl/Verlust
- ✓ Homogenität des Endgerätepools



Zeitplan

Projektphase	Dauer (geplant) gesamt in h	Dauer in h	Abweichungen in h
Planungsphase <ul style="list-style-type: none"> Ist-Analyse Evaluierung Rollout-Struktur Private Nutzung 	8	11	+3
Durchführungsphase <ul style="list-style-type: none"> Azure Mandanten AAD Gruppen & Lizenzen APNS & VPP DEP-Profil Richtlinien Unternehmens-Apps 	19	18	-1
Abschluss und Abnahme <ul style="list-style-type: none"> Soll- / Ist-Vergleich Projektkostenanalyse Fazit 	8	6	-2

Kostenart	Person / Abteilung	Aufwand (h)	Einzelkosten €/h	Gesamtkosten (€)
Personelle Kosten	Martin Goltschewski	35	75,00	2.625,00
	Windows Support	1	97,00	97,00
	MDM Betrieb	2	97,00	194,00
	Einkauf	3	97,00	291,00
Materielle Kosten	iPhone 11 (Testgerät)	1.Monat	49,00	49,00
Sonstige Kosten	Kundentermin (Bewirtung)		25,00	25,00
	Gemeinkosten (Strom, Miete etc.)	5 % der Projektkosten 164,05		
Gesamtkosten		3.445,05		



Vielen Dank für Ihre Aufmerksamkeit

Quellenverzeichnis

- www.bsi.bund.de
- www.docs.microsoft.com
- www.microsoft.com
- www.apple.com
- www.mobileiron.com
- www.citrix.com
- www.air-watch.com
- www.portal.azure.com
- www.Contoso.com