EuroCloud
TRUSTED DIGITAL COMPETENCE PLATFORM

CLOUD COMPUTING & ENTERPRISE MOBILITY MANAGEMENT



Markt, Produkte und Technische Herangehensweisen sowie Relevante Organisatorische und Juristische Aspekte

PROVIDED BY EUROCLOUD
EuroCloud
CLOUD KNOW HOW
knowhow.eurocloud.org
TRUSTED DIGITAL COMPETENCE PLATFORM

09

EuroCloud Europe a.s.b.l.
L1013 Luxembourg
7, Rue Alcide de Gasperi. Luxembourg

E-Mail: contact@eurocloud.org
Web: https://.eurocloud.org
Copyright: EuroCloud Europe 2016



VORWORT



Liebe Leserinnen und Leser! Vor ziemlich genau drei Jahren präsentierte EuroCloud den ersten Mobility & Cloud Leitfaden. Nur wenige Jahre zuvor – erst im April 2010 – wurde das iPad vorgestellt. Wie immer wusste Steve Jobs früher als alle anderen, welche Funktionalität viele Menschen brauchen können. Und obwohl diese neue Geräteform anfangs noch kritisiert und belächelt wurde und sich viele nicht unmittelbar vorstellen konnten, was man mit solchen Geräten alles tun kann, kaufen Menschen mittlerweile viel mehr dieser kleinen praktischen Endgeräte als PCs oder Laptops. Trotz der verminderten Größe erwarten sie – für Berufs- und Privatleben gleichermaßen – praktisch zu benutzende und bequem zu bedienende Geräte, mit vollem Leistungsumfang.

Die Trennlinie zwischen beruflicher und privater Nutzung der Geräte wird immer fließender, was konsequenterweise heißt, dass die technischen, organisatorischen und rechtlichen Herausforderungen immer umfangreicher werden. Dieser Leitfaden sprich sämtliche relevanten Themen (Technik, Recht, Organisation und Prozesse) an und liefert Checklisten, Vorgangsmodelle und einen Marktüberblick.

Der Leitfaden „Enterprise Mobility Management" wurde von folgenden Autoren erstellt: Reinhard Travniček, Gerald Haidvogl und Christoph Lang-Muhr (Technisches), Árpád Geréd (Juristisches) und Tobias Höllwarth (Organisation und Prozesse).

Das Lektorat wurde wie immer mit höchster Akribie von Michaela Obermeier durchgeführt.

Sollten Sie ein Enterprise-Mobility-Projekt in Ihrem Unternehmen planen, würden wir uns freuen, Sie zu einem einführenden Planungs-Workshop einladen zu dürfen.

Wien, Mai 2016

Dr. Tobias Höllwarth



INHALT

1 EINLEITUNG 5
2 MARKTÜBERSICHT 6
3 BEDARFSERHEBUNG 10
4 MDM UND MAM: PRAKTISCHE UMSETZUNG UND FUNKTIONSWEISEN 11
5 ORGANISATORISCHE MASSNAHMEN 20
6 RECHTLICHE ASPEKTE 24
7 ANBIETERVERZEICHNIS – MANAGEMENTPRODUKTE 29
8 ANBIETERVERZEICHNIS – MIM UND EFSS 32
9 GLOSSAR 34
10 STARAUDIT 37
11 GLOSSAR CLOUD COMPUTING 42
12 RECHTLICHER HINWEIS 48
13 AUTOREN 50



1 EINLEITUNG

In der letzten Auflage des Mobility-Leitfadens wurde angeführt, dass es 2012 sieben Milliarden Menschen auf der Erde gab, denen sechs Milliarden Mobilfunkverträge gegenüberstanden. Zu diesem Zeitpunkt gab es im Vergleich dazu weniger als zwei Milliarden Kreditkarten. Im Jahr 2015 gibt es bereits 7 Milliarden Mobilfunkverträge[1].

Daraus lässt sich ersehen, dass der Markt der mobilen Devices weiterhin ansteigt. Der Mitarbeiter hat oftmals nicht nur ein Mobiltelefon, mit dem er auch seine Emails abrufen kann, sondern er hat ein Smartphone, das ihm den Zugriff auf Firmendaten von unterwegs erlaubt. Oft wird dann für umfangreicheres Arbeiten zusätzlich auch noch ein Tablet verwendet. Diese Devices sind zu 47 Prozent[2] mit mobilen Breitbandinternetzugängen ausgerüstet, was aufzeigt, wie wichtig die mobile Welt geworden ist.

Daher wird heute in den meisten Unternehmen die Notwendigkeit von Managementlösungen für Devices und Daten nicht mehr in Frage gestellt und unter dem Begriff Enterprise Mobility Management (EMM) zusammengefasst.

1 - http://www.itu.int/en/ITUD/Statistics/Documents/facts/ICTFactsFigures2015.pdf
2 - http://www.itu.int/en/ITU-D/Statistics/Documents/facts/ICTFactsFigures2015.pdf

2 MARKTÜBERSICHT

2.1 DIE ANBIETER

Laut Gartner haben sich die wesentlichen Marktteilnehmer in den letzten Jahren nicht verändert. Verändert haben sich nur die Besitzverhältnisse, so wurde z. B. Good Technology von Blackberry übernommen und Airwatch von VMware.



Abbildung 1: © Gartner May 2015

Da sich keiner der im Leader-Quadranten genannten Hersteller mehr als MDM/MAM-Hersteller mit engem Produktfokus sieht, haben viele Hersteller begonnen, durch Entwicklung oder Zukauf die wichtigen Funktionsfelder von EMM wie Filesharing – Synchronisation (EFSS) und Content Management zu besetzen. Auch der Kunde sucht ja nicht mehr nur nach den Funktionen, die unter dem Begriff MDM/MAM zusammengefasst werden. Eine sehr umfangreiche Marktanalyse ist im „Enterprise Mobility Management Smackdown" vom Consultingunternehmen PQR[3] enthalten.

Wer an mehr MxM-Akronymen interessiert ist, der sei an dieser Stelle an das Glossar verwiesen.

Viele Hersteller haben erst jetzt begonnen, durch Entwicklung oder Zukauf die wichtigen Funktionsfelder Filesharing – Synchronisation und Content Management zu besetzen.

3 - http://www.pqr.com/downloadfiles/Whitepaper_EMM_smackdown.pdf



2.2 PRODUKTVARIANTEN

Bis vor nicht allzu langer Zeit stand immer noch die Frage im Mittelpunkt, welche der möglichen mobilen Plattformen eine Mobile-Management-Lösung unterstützt und in welchem Umfang. Heute hat sich die Zahl der für das Business relevanten mobilen Betriebssysteme verringert, laut Unternehmensumfragen sind derzeit fast 90 Prozent aller verwendeten mobilen Endgeräte in Firmen mit Apple iOS oder Android ausgestattet. Dominanter Lösungsansatz ist derzeit im Markt MDM, das eigentlich eine Weiterführung des Laptopbetriebsmodells darstellt, nur für andere Endgeräte und mit anderen Tools. Hauptsächlich geht es darum, die Geräte zu konfigurieren, erwünschte Software zu installieren, unerwünschte Software zu entfernen, ein Inventar zu erstellen, Sicherheitsregeln durchzusetzen und im Fall von Verlust oder Diebstahl entsprechende Maßnahmen zu setzen.

Die für das Business relevanten mobilen Betriebssysteme sind Apple iOS oder Android Derzeit wird vor allem MDM angeboten, das eigentlich eine Weiterführung des Laptopbetriebsmodells ist – nur für andere Endgeräte.

Die Auswahl der MDM-Lösung im Detail richtet sich sehr häufig nach den Sicherheitsanforderungen des Unternehmens. Virtualisierungslösungen mit einer strikten Trennung zwischen privatem und betrieblichem Betriebssystem auf einem Gerät, wie derzeit z. B. von VMware für Android angeboten, sind besonders für Versicherungen, Geldinstitute, Militär etc. interessant.

Die klassischen agentenbasierenden MDM-Systeme machen einen Großteil der derzeit im Markt installierten Lösungen aus und bieten je nach Betriebssystem ausreichende (Android) bis sehr gute (iOS) Sicherheitsfeatures an.



Abbildung 2 – Geräte-Lifecycle im klassischen MDM

Die Herangehensweise im MDM ist gut für COD (Company owned Devices) geeignet, im Bereich BYOD wird der Mitarbeiter aber kaum die totale Kontrolle über sein mobiles Endgerät abgeben wollen.

Hier kommen dann immer häufiger Lösungen ins Spiel, die als MAM (Mobile Application Management) im Markt positioniert werden. MAM-Lösungen, bei denen die Firma Good ein Vorreiter war, sind meist agentenlose Systeme, daher für BYOD (Bring your own Device) gut geeignet, setzen einen Schwerpunkt auf der Applikations- und Datenebene und bieten meist nur sehr eingeschränkte Funktionen im Bereich der Inventarisierung und des Helpdesks.

Welche Fragen, die über den klassischen Device-Management-Ansatz hinausgehen, werden mit MAM beantwortet?

Mitarbeiter wollen nicht die totale Kontrolle über ihr mobiles Endgerät abgeben – hier kommt MAM ins Spiel.

Frage	Lösungsansatz
Haben Sie Bedenken, dass Firmendaten auf einem Mobile Device nicht sicher sind?	Wenn JA: Verteilen Sie Firmendaten nur in sichere Datencontainer.
Wollen Sie E-Mail-Attachments schützen, ohne auf dem Gerät eine eigene Firmen-E-Mail-Applikation zu verwenden?	Wenn JA: Verschlüsseln Sie die Attachments vor dem Versand auf das Mobile Device so, dass diese nur auf diesem Gerät vom authorisierten MDM-Client geöffnet werden können.
Brauchen einige der Appli-kationen einen Netzwerk-zugriff ins Unternehmens-LAN und ist Ihnen das Risiko einer kompletten VPN-Einbindung zu groß?	Wenn JA: Suchen Sie ein Produkt, das appspezifische VPNs unterstützt. Dann wird nur eine Verbindung der Applikation und nicht des ganzen Geräts zum Firmennetzwerk hergestellt.
Wollen Sie private E-Mails, Aufgaben und Kalender von den Firmendaten trennen?	Wenn JA: Verwenden Sie ein Produkt, das eine eigene E-Mail-Applikation mitliefert, die Ihnen diese Managementfunktionen erlaubt.
Müssen Intranet-Webseiten auch extern von mobilen Devices zugreifbar sein?	Wenn JA: Wählen Sie ein Produkt, das einen eigenen Webbrowser mitbringt.
Soll es für die Benutzer ein Applikations-Portal geben, auf dem sie Applikationen zur Nutzung auswählen können?	Wenn JA: Entscheiden Sie sich für ein Produkt mit Portal und Provisionierungsfunktion.

Als weitere Entscheidungshilfe bei der Auswahl des „richtigen" Mobile-Management-Produkts (sowohl MAM- als auch MDM-Produkte) sollte unbedingt beachtet werden, ob eine bereits bestehende Infrastruktur wie z. B. Citrix, Microsoft oder Symantec genutzt werden kann.



2.3 GEFORDERTE FUNKTIONEN

Die vom Produkt einzufordernden Funktionen lassen sich in sechs Gruppen einteilen:

2.3.1 KATEGORISIERUNG IN SECHS FUNKTIONSGRUPPEN.

Mobile Security Management: Passwörter, Sperrschirme, remote löschen, lokale Datenverschlüsselung, Virenscanner

Mobile Software Management: privater Appstore, OS-Updates und Patching, Backup und Restore

Mobile Information Management: Datensynchronisation und Backup, Filesharing, Datendistribution zu Benutzergruppen, Rights Management in Applikationen

Policy Enforcement and Compliance: Erkennung von „rooted" oder „jail-breaked" Geräten, Trennung von persönlichen und Firmendaten, Einhalten von Verschlüsselungen, Passwörter und Sperrschirme, SIM-Wechsel

Analytics: Dashboard-Ansichten, eine Vielzahl an Reports, Analyse der eingesetzten Apps, Dokumentation von Zugriffsrechten etc.

Scalability: betrachtet die Anzahl der verwaltbaren Geräte, die Hochverfügbarkeit und die Art und Weise, wie im Fall eines Desasters der Wiederanlauf geregelt wird

3 BEDARFSERHEBUNG

Mehr denn je ist also für mobile Devices erforderlich, korrekt im Unternehmen eingebunden zu werden. Aufgrund der steigenden Anzahl an Devices wird es immer schwieriger, Devices einzeln korrekt zu konfigurieren und sicherzustellen, dass niemand die Richtlinien umgeht – im Grunde ist es eigentlich unmöglich, selbst bei kleineren Geräteanzahlen.

Im Idealfall muss der Administrator nach der Konfiguration und der Definition der Policies beim einzelnen Endgerät gar nicht mehr Hand anlegen. Der User „enrolled" das Gerät selbst, es wird automatisiert eingebunden und die Policies werden angewendet. Beispiele wären hier z. B. die Konfiguration des E-Mail-Accounts, die Sicherheitsstufen der Verschlüsselung, Black-/Whitelisten für Applikationen. Die Überprüfung des verpflichtenden Virenscanners insbesondere auf Androidgeräten ist ein anderes Beispiel für notwendige Policies.

In der letzten Ausgabe hatten wir erwähnt, dass, je mehr Geräte ein Unternehmen hat, desto früher sich die Investition in ein MDM- bzw. MAM-System rentiert. Diese Feststellung gilt auch weiterhin. Zusätzlich möchten wir aber heute darauf hinweisen, dass mit den gegenwär-tigen MAM-Systemen noch wesentlich höherer Mehrwert für Unternehmen generiert werden kann. Der Mitarbeiter ist wesentlich flexibler und kann somit schneller reagieren. Zum Beispiel kann direkt vom Mobiltelefon aus der in einer Mail enthaltene Link geöffnet werden, da mittels MAM-Lösung ein Tunnel ins Intranet des Unternehmens aufgebaut werden kann. So kann auch von unterwegs schnell eine Aktualisierung an einer Präsentation vorgenommen werden, oder ein Sales-Mitarbeiter kann seine neuesten Statistiken bearbeiten.



4 MDM UND MAM: PRAKTISCHE UMSETZUNG UND FUNKTIONSWEISEN

4.1 REINES MDM, MAM ODER MDM + MAM?

Diese Frage wird sehr oft gestellt, und die Antwort hängt vom Zugang der Administratoren zum Thema Kontrolle, Verwaltung, Support und auch vom Eigentümer des Geräts ab. Generell ist zu bemerken, dass Unternehmen, die mobile Geräte an ihre Mitarbeiter ausgeben, eher die komplette Verantwortung über das Gerät übernehmen wollen oder müssen. Daher wird in diesem Fall immer über eine MDM-Lösung gesprochen werden. Unternehmen, die vom Benutzer verwaltete Geräte (COPE = Company owned – Personal enabled) oder BYOD unterstützen, wollen meist nur Einfluss und Kontrolle über Unternehmensdaten, E-Mail und Zugang zum Unternehmensnetz erlangen, daher liegt hier der Schwerpunkt auf Dataleak Prevention und Applikationsmanagement, das sind Funktionen, die meist in den MAM-Produkten der Hersteller realisiert werden.

Werden COPE oder BYOD unterstützt, dann liegt der Schwerpunkt auf Dataleak Prevention und Applikationsmanagement.

4.2 ON-PREMISE, ALS CLOUD-VARIANTE, INSTALLATION ODER AP-PLIANCE?

Welche Variante ist nun die am besten passende? Das lässt sich nicht so ohne Weiteres sagen, denn es kommt sehr stark darauf an, wie sich der Bedarf darstellt. Ein Unternehmen, das zum Beispiel seine IT on-premise betreibt, wird vermutlich auch hier eine lokal installierte Version bevorzugen. Natürlich entstehen hier neben den Installationskosten auch Kosten des Betriebs (Server, Strom, Klima, Personal etc.). Die Appliance-Variante verringert meist die Basisinstallationskosten und im geringen Maße auch die Betriebs- und Supportkosten. Eine Cloud-Variante bietet oft mehr Flexibilität, speziell bei kleinen Unternehmen, einen raschen und kostengünstigen Einstieg zu ermöglichen. Genannt sind hier auch noch „Hybrid"-Varianten, bei denen z. B. die E-Mail- oder Zugriffsfilterung weiterhin im eigenen Netzwerk erfolgt.

4.3 DER FALLSTRICK ANDROID

Der Vorteil der Android Devices in den Augen vieler Nutzer, nämlich die Vielzahl an Möglichkeiten, ist gleichzeitig das Problem des Administrators. Es gibt eine Vielzahl an Versionen von Androids, und diese unterscheiden sich zum Teil erheblich. Nicht nur, dass es unterschiedliche Android-Versionen gibt, gibt es auch bei den Herstellern gerätespezifische Unterschiede, die wiederum die Möglichkeiten des Administrators einschränken. Einige Hersteller bieten zum Beispiel eigene APIs an, mittels derer die MDM/MAM-Hersteller zusätzliche Möglichkeiten eingeräumt bekommen. So können zum Beispiel auf manchen Android-Versionen nur dann Exchange

Accounts eingerichtet werden, wenn zusätzlich eine Lizenz für spezielle E-Mail-Clients bezogen wird. Ältere Android-Versionen unterstützen hingegen zum Beispiel keine Verschlüsselung. Das ideale Szenario würde hier lauten, die Android-Produkte auf eine bestimmte Version von einem Hersteller zu beschränken. Die Administration würde hier deutlich vereinfacht werden. Das ist in der Praxis allerdings oftmals nicht möglich, daher empfiehlt sich, wenn man Android Devices nutzen möchte, die Auswahl eines Systems, das der Fülle an Möglichkeiten der Android Devices gerecht wird. Hierfür bieten sich beispielsweise Systeme an, die abfragen, welche Version von Android installiert ist, und dann entsprechend entscheiden, welche Einstellungen getroffen werden müssen.

4.4 LIZENZIERUNGSARTEN

Die Hersteller unterscheiden bei den Lizenzen meist zwischen einer Kauf- (Perpetual License) und einer Nutzungsvariante (Subscription License). Es werden entweder die Endgeräte oder die Benutzer lizenziert. Bei Unternehmen, bei denen die Benutzer über mehrere Endgeräte (Smartphone, Tablet) verfügen, ist in der Regel die benutzerbasierende Lizenzierung günstiger. Für Unternehmen mit einer hohen Mitarbeiterfluktuation ist oft die gerätebasierende Lizenz ökonomischer. Natürlich gibt es auch in diesem Produktsegment selbst von den namhaften Herstellern Freeware-Angebote mit eingeschränkter Funktionalität, Nutzer- oder Geräteanzahl.

4.5 NOTWENDIGE INFRASTRUKTUR

Die benötigte Infrastruktur ist davon abhängig, welche Installationsform gewählt wurde. Eine on-premise-Installation besteht in den meisten Fällen aus dem eigentlichen MDM/MAM-Server sowie einer Datenbank. Der MDM/MAM-Server wird meist in der DMZ platziert, um die Kommunikation mit den Endgeräten zu ermöglichen. Der Datenbankserver hingegen sollte stets im Corporate LAN platziert werden, um den Security-Anforderungen gerecht zu werden.

Eine Cloud-Installation hingegen wird mit weniger Komponenten auskommen. Im einfachsten Fall ist gar nichts im firmeneigenen Netzwerk installiert und die Funktionalität wird komplett aus der Cloud gestellt. Dabei empfiehlt es sich, darauf zu achten, dass die Verbindung zu der MDM/MAM-Lösung in der Cloud entsprechend gesichert ist und die Übertragung verschlüsselt erfolgt. Hier bieten die Hersteller verschiedenste Möglichkeiten an, meist wird eine SSL-Verschlüsselung angeboten, seltener VPN-Verbindungen. Speziell bei der Sicherung von Firmen-E-Mails ist oft nicht gewünscht, die Daten in die Cloud zu replizieren, hier bietet sich eine Hybrid-Variante an. Bei dieser wird ein Filtermechanismus als Plug-in in die Systeme der Firma integriert, der sich seine Informationen (welche Devices sind compliant, welche nicht, wer muss gesperrt werden, wer wieder freigeschaltet etc.) vom MDM/MAM-Server aus



der Cloud holt und durchsetzt. Das Device kommuniziert hier also nur mit dem MDM/MAM-Server, wenn es sich Konfigurationsdaten abholt, ansonsten erfolgt die weitere Kommunikation „unternehmensintern".

Der im vorherigen Abschnitt angesprochene Filtermechanismus stellt meist einen Proxy zum E-Mail-System dar und bedingt auch meist ein zusätzliches Server- oder Gateway-System.

Zusätzlich zur benötigten Infrastruktur müssen natürlich auch auf den Firewalls entsprechende Ports freigeschaltet werden, sodass die Systeme ihre Arbeit verrichten können. Auch hier sind die am Markt erhältlichen Systeme sehr unterschiedlich. Manche benötigen lediglich einige wenige Ports, während andere eine Vielzahl an Kommunikationsports brauchen.

4.6 WEITERE VORAUSSETZUNGEN

4.6.1 ZERTIFIKATE UND PKI

Alle MDM-Produkte und die meisten MAM-Produkte müssen in eine Zertifikatsinfrastruktur eingebunden sein, damit entsprechende Zugriffszertifikate auf die mobilen Endgeräte ausgerollt werden können. Um die Zugriffspunkte von außen abzusichern, sind meist einige öffentliche Webserverzertifikate notwendig.

4.6.2 APPLE DEVELOPER ENTERPRISE

MAM-Produkte umgeben die Applikationen meist mit einer vom MAM verwalteten Hülle, dadurch wird verhindert, dass Applikationen für jede MAM-Lösung neu programmiert werden müssen. Das Einbetten der Applikation in die Hülle nennt man „wrappen". Zum „Wrappen" bedarf es meist eines Apple-Betriebssystems (MAC-OS) und eines Apple Developer Enterprise Accounts. Auch die Android-Apps werden mit diesem System gewrapped.

4.6.3 APPLE ID

Ab IOS 5 lässt sich ein IOS-Device ohne Apple ID aktivieren. Da der User aber für viele MDM/MAM-Systeme einen entsprechenden Client installieren muss, der meist aus dem Appstore zu beziehen ist, kommt man um die persönliche ID momentan trotzdem nicht herum. Lässt sich das Gerät ohne Client einbinden, kann der Administrator Apps, die er lokal auf dem MDM/MAM-Server hat, auf das Device pushen. Soll aber eine App über den Appstore installiert werden (per Link kann installiert werden oder der Link als „Vorschlag" auf das Device aufgebracht werden), benötigt der User eine ID, um die App abrufen zu können.

Gleiches gilt für den Administrator. Die meisten MDM/MAM-Systeme nutzen APNS (Apple Push

Notification Services), um das Device zur schnellen Kommunikation mit dem MDM/MAM-Server aufzufordern. Um diesen Service nutzen zu können, benötigt der MDM/MAM-Server ein APNS-Zertifikat, das nur mittels gültiger Apple ID bezogen werden kann. Es empfiehlt sich hier dringend, eine eigene Apple ID für den Server anzulegen und keine personalisierte ID zu nutzen, damit im Falle des Ausscheidens des Mitarbeiters nichts geändert werden muss.

Die VPP-(Volume Purchase Program)-Lizenzen, die Firmen die Möglichkeit geben, Lizenzen von Apps zu kaufen und dann ihren Usern zur Verfügung zu stellen, würden das Problem der eigenen IDs für User lösen. Leider ist dieser Service noch nicht überall in Europa verfügbar, und Apple gibt keine Informationen preis, wann er überall verfügbar sein wird.

4.6.4 GOOGLE ID

Um ein Android Device zu aktivieren, benötigt der User bei Google ebenso keine ID wie bei Apple. Will er aber den Play Store nutzen, steht er wiederum vor dem Problem, eine ID zu benötigen. Auch hier gilt: Der Administrator kann zwar Applikationen vom MDM/MAM-Server aus installieren, wird aber ein Link in den Google Play Store genutzt, braucht der User eine ID, um die App abrufen zu können.

4.7 MOBILE INFORMATION MANAGEMENT (MIM)

Dateien werden neben E-Mail, Kontakten und Terminen die von den Benutzern am meisten benötigten Daten sein. Zugriff auf Daten ist aus Unternehmenssicht heute leicht zu lösen, es gibt eine Vielzahl von Produkten, und die meisten decken die Anforderungen gut ab. Schwieriger wird es, wenn die Notwendigkeit zu Digitial Rights Management und/oder Dataleak Prevention besteht. Ein gutes Enterprise-File-Sharing-Produkt muss eng mit der MDM-Lösung kooperieren, um ein zentrales Management zu ermöglichen. Wesentlich ist es, an dieser Stelle daran zu erinnern, dass Dateien nicht die einzigen Datenbestände auf mobilen Geräten sind, die schützenswert sind. Viele Apps wie Facebook, Evernote usw. speichern auch Daten, aber nicht im klassischen Dateiformat.

Ein gutes MIM-Produkt muss eng mit der MDM-Lösung kooperieren, um ein zentrales Management zu ermöglichen.

Wenn ein solches Produkt in BYOD-Umgebungen eingesetzt wird, sind Funktionen wie „Löschen“ und „Blockieren“ innerhalb des Produktes unumgänglich, es wird in BYOD-Umgebungen nicht möglich sein, das gesamte Gerät zu löschen. Je nach Dateninhalt und Compliance-Anforderungen kann es notwendig sein, dass die Dateien nur auf On-Premise-Speicher kommen. Unkritische Daten (siehe Datenklassifizierung) können unbedenklich in jedem Cloud-Produkt abgelegt werden.



Werden den Benutzern keine Möglichkeiten zum Filesharing bereitgestellt, weichen diese Nutzer unweigerlich auf Produkte aus, die sie selbst installieren können, die aber die Unternehmens-IT dann nicht mehr kontrollieren kann.

Ein Minimum-Set an Funktionen eines MIM-Produktes umfasst:

Funktion	Enthalten	Fehlt
Speicherort entspricht Compliance-Vorschriften		
Service-Provider hält Compliance-Vorschriften für gewisse Bereiche ein, z. B. U.S. Securities and Exchange Commission, Independent Securities Regulator FINRA oder HIPAA Business Associate Agreement		
Zugriffssteuerung		
Active Directory Integration		
Benutzergruppen und Ordner-Mapping		
Granulare Administration		
Abgrenzung zwischen Zugriff von Mitarbeitern und externem Zugriff		
Möglichkeit der On-Premise-Datenhaltung		
Schutz vor Datenverlust durch Synchronisati-onsfehler		
Kontrolle über die Daten auf Mobile Devices (Wipe, Lock) für Administratoren		
Datensicherung und Restore auf Item-Level		
Einfordern von Richtlinien am Mobile Device		
Verschlüsselung der Daten am Mobile Device		
Integritätstest am Mobile Device (rooted, jail-breaked)		
Umfangreiches (revisionssicheres) Reporting		
Dokumentation des Zugriffs (Art, Dauer etc.) auf Daten		
Report der Zugriffsrechte einzelner Personen		

Folgende Funktionen sind optional und wünschenswert:

Funktion	Enthalten	Fehlt
View-only-Dokumentenzugriff		
Automatische zeitgesteuerte Löschung		
Versionierung von Dokumenten		
Papierkorbfunktion		
Single Sign On		
Zweifaktor-Authentifizierung		
Digital Rights Management (DRM)		
Dataleak Prevention		
Zugriff auf SharePoint		
Zugriff auf allgemeine CIFS Shares		



4.8 MOBILE DEVICE SECURITY

Durch die vermehrte Verwendung von mobilen Geräten im Unternehmensumfeld rückt natürlich auch die Sicherheit der Geräte und der darauf gespeicherten Daten in den Mittelpunkt. Es gelten auch in dieser Geräteklasse die bereits bekannten Schutzziele für Daten und Services, nämlich Vertraulichkeit, Integrität und Verfügbarkeit.

Um diese Ziele erfüllen zu können, muss man sich zu allererst über das geänderte Gefährdungspotenzial im Klaren werden. Die Gefahren für die mobilen Geräte unterscheiden sich deutlich von den Threat-Vektoren eines PCs mit Windows-Betriebssystem.

Die Bedrohung durch herkömmliche Angriffe (wie z. B. Malware) sind durch die Sicherheitsmechanismen der führenden mobilen Betriebssysteme oder der MAM-Lösung, wie Sandboxing der Apps usw., wesentlich geringer. Bei mobilen Geräten gibt es andere Gefahren.

4.8.1 VERLUST DER GERÄTE

Verlust oder Diebstahl der Geräte und somit auch der darauf gespeicherten sensiblen Daten (von Kontakten und Mails bis hin zu gespeicherten Passwörtern und Files) ist eine der größten Gefahren von mobilen Geräten.

Um den Schutz der Daten zu gewährleisten, ist eine Zugangssperre/Screenlock mittels PIN oder Passwort unerlässlich. Des Weiteren müssen die Daten am Gerät sicher, sprich verschlüsselt gespeichert sein, um die Extraktion durch forensische Tools bzw. Hacker zu vereiteln. Diese beiden Maßnahmen schützen die Daten direkt nach dem Verlust oder Diebstahl. Um die Zeitspanne der eventuellen Angriffe auf das Gerät möglichst kurz zu halten, sollte es schnellstmöglich mittels eines „Remote Wipes" gelöscht und somit für den Angreifer unbrauchbar gemacht werden.

Bei den meisten EMM-Lösungen lassen sich zwei Varianten des Remote Wipes unterscheiden:

1. Enterprise Wipe – nur die sensiblen Unternehmensdaten werden gelöscht.

Diese Variante des Remote Wipes ist z. B. bei Bring-Your-Own-Device-Szenarien sinnvoll, da keine privaten Daten des Mitarbeiters oder Exmitarbeiters gelöscht werden.

2. Device Wipe – es werden alle Daten am Gerät gelöscht, und es kann auch für jede weitere Benutzung unbrauchbar gemacht werden (betriebssystemabhängig).

4.8.2 DATA LEAKAGE

Data Leakage meint Datenverlust durch die Benutzung von Cloud-Services wie DropBox, Google Drive, Apple iCloud, Microsoft One Drive usw.

Durch die teilweise tiefe Integration in die Betriebssysteme ist es sehr schwierig, den Datenfluss zu diesen Services zu kontrollieren. Die Speicherung der Daten der populären Cloud-Dienste ist fest in der Hand von US-Unternehmen, weshalb sich europäische Datenschutzgesetze nur eingeschränkt anwenden lassen. Mittels eines EMM-Systems können diese Apps deaktiviert oder deren Einsatz beschränkt werden. Neuere EFSS Systeme unterstützen Digital Rights Management und DLP Systeme.

4.8.3 MANIPULATION DER GERÄTE

Durch Manipulation der Geräte wie „Rooten" oder „Jailbreaken" (Administratorrechte erlangen) werden die implementierten Sicherheitsmechanismen ausgehebelt und im schlimmsten Fall für Malware Tür und Tor geöffnet.

Mit diesen manipulierten Geräten können außerdem keine Policies des EMM mehr verlässlich ausgerollt werden. Daher haben die EMM-Systeme eine Jailbreak- oder Root-Erkennung an Bord, um diese Geräte aus dem Unternehmensnetz ausschließen zu können und somit das Risiko zu minimieren.

4.8.4 BÖSARTIGE APPS

Eine weitere Gefahr ist die Installation von Apps aus nicht autorisierten Quellen anstelle der Hersteller-App-Stores. In diesen offiziellen Stores werden die Programme auf Schadcodes von den Betriebssystemher-stellern wie Apple, Google, Amazon oder Microsoft überprüft. Diese Überprüfung erfolgt jedoch nicht für App Stores von Drittherstellern (wie bei Android – Galaxy Apps, F-Droid oder Slide ME). Bei diesen muss man sich auf deren Sicherheitschecks, wenn vorhanden, verlassen.

Bösartige Apps können auch als kostenlose Apps wie Bildschirmschoner, Spiele usw. auftreten und im Hintergrund sensible Daten des Gerätes abgreifen und an den App-Hersteller schicken. Diese Apps erkennt man an den Rechten, die sie bei der Installation in Anspruch nehmen wollen, wie z. B. Zugriff auf das Adressbuch, Position usw. Man sollte sich daher immer in Erinnerung rufen, dass kostenlose Apps meist nicht kostenlos sind, sondern der User sie meist mit seinen Daten bezahlt.



4.8.5 ALWAYS-ON CONNECTIVITY

Mobile Geräte sind permanent online und tauschen Daten teilweise über ungeschützte Verbindungen wie WLAN-Hotspots ohne Verschlüsselung aus. Bei diesen Datenübertragungen können bekannte Attacken wie Man-In-The-Middle-Angriffe ausgeführt und die übertragenen Daten mitgeschnitten und/oder verändert werden. Daher sollte man in ungeschützten Verbindungen bzw. Netzen auf eine weitere Sicherheitsschicht wie VPN (Virtual Private Network) oder zumindest SSL-Verschlüsselung setzen.

4.8.6 PHISHING

Diese Angriffsart erlebt eine Renaissance auf mobilen Geräten, da durch die kleinen Displays und mobilen Web Browser und Mailclients die Unterscheidung zwischen der echten Webseite/ Mail und der gefälschten wesentlich schwerer fällt als auf einem PC.

4.8.7 FEHLENDE UPDATES

Je nach Hersteller der Geräte werden Updates und Security Fixes zu unterschiedlichen Zeitpunkten, oder bei älteren Geräten gar nicht mehr, ausgerollt. Dies stellt das EMM vor die Aufgabe, alte oder ungepatchte Geräte aus dem Unternehmensnetz zu isolieren und sie erst wieder zu integrieren, wenn die Compliance-Richtlinien erfüllt werden.

5 ORGANISATORISCHE MASSNAHMEN

Neben der zweifelsfrei unumgänglichen Klärung der technisch optimalen Lösung dürfen bei der Implementation einer Enterprise-Mobility-Lösung keinesfalls die rechtlichen (siehe nächstes Kapitel) und organisatorischen Maßnahmen übersehen werden. Wenn Enterprise Mobility reibungslos und mit wenigen manuellen „Eingriffen" funktionieren soll, sollten jedenfalls die folgenden Fragen rechtzeitig und verbindlich mit allen Betroffenen geklärt werden.

5.1 VERTEILUNG UND WARTUNG DER GERÄTE

Der Nutzer mobiler Devices war bisher gewohnt, dass er selbst Einkauf, Einrichtung, Wartung, Reparatur, Wechsel und Sicherung seiner Geräte verantworten und durchführen muss. Bei COD (Company owned Devices) lag diese Verantwortung im Regelfall bei der Unternehmens-IT, und der Benutzer musste sich lediglich an die vereinbarten Nutzungsbedingungen halten. Mit den komplexeren Nutzungsformen BYOD oder COD mit privater Nutzung müssen ebenso klare und für alle Seiten nachvollziehbare und verständliche Abläufe eingeführt werden.

Klare Abläufe für Geräteanforderung, Genehmigung, Ausgabe, Defekt, Änderungen, Rückgabe sowie Verlust.

Dies gilt insbesondere für Fragen der Sicherung privater Daten und der Abläufe rund um Updates, die eventuell auch Auswirkungen auf ausschließlich privat genutzte Applikationen haben könnten.

Klare Abläufe rund um Anforderung, Genehmigung und Ablauf der Geräteausgabe, für Prozesse bei Gerätedefekt (inkl. Datenübernahme und Ersatzgerät), Änderungen am Gerät, Rückgabe des Geräts bei Veränderung des Arbeitsverhältnisses, erforderliches Gerätezubehör und Geräteverlust (insbesondere im Ausland) müssen erstellt, mit allen Stakeholdern besprochen und verbindlich vereinbart werden.

5.2 LEISTUNGEN DES HELPDESKS

Ebenfalls unumgänglich ist die klare Abgrenzung der Leistungen, die durch einen internen oder ausgelagerten Helpdesk im Rahmen eines Enterprise-Mobility-Konzepts zu erbringen sind. Diese Leistungen sind insbesondere hinsichtlich der Benutzeranfragen zu Geräte- und Bedienungsproblemen keinesfalls zu unterschätzen und können zu beachtlichen Kosten führen. Besonders beim Ansatz BYOD muss geklärt sein, welche Helpdesk-Leistung der Benutzer erwarten kann, der ja ansonsten (bei einem Unternehmens-PC) gewohnt war, die Services eines zentralen Ansprechpartners beanspruchen zu dürfen. Ebenso muss die Frage beantwortet



werden, ob man dem Benutzer eines Mobile Devices den gleichen Helpdesk-Komfort anbieten möchte wie einem Laptopbenutzer (z. B. Remote Control).

Besonders bei BYOD muss geklärt sein, welche Helpdesk-Leistung der Benutzer erwarten kann.

5.3 PASSWORD RESET UND GERÄTELÖSCHUNG

Wie auch im klassischen PC-Umfeld ist es unumgänglich, einen einfachen, aber sicheren Prozess für die Passwort-Rücksetzung zu etablieren. Passwörter werden von Benutzern vergessen, müssen regelmäßig geändert werden oder bei Missbrauchsverdacht sofort rücksetzbar sein. Idealerweise kann der Benutzer dies selbst über ein Portal durchführen und damit Kosten für einen Helpdesk einsparen.

Im Falle eines Geräteverlustes muss eine rasche Folge von Prozessen zwischen Benutzer und IT-Abteilung vereinbart sein, die sicherstellt, dass ein unbefugter Zugriff auf die Daten am Gerät möglichst ausgeschlossen wird. Die technische Infrastruktur bzw. das Gerät muss diesen Prozess unterstützen, jedoch liegt es insbesondere an den Schritten, die vom Benutzer rechtzeitig gesetzt werden müssen, ob der Schutz der Daten rasch und erfolgreich verläuft.

Im Falle eines Geräteverlustes muss eine rasche Folge von Prozessen zwischen Benutzer und IT vereinbart sein.

Idealerweise sind die Sicherungen der Gerätedaten so vollständig und zeitnah, dass der Benutzer auch keine Bedenken haben muss, das Gerät fernzulöschen, selbst wenn nur der Verdacht eines Verlustes besteht (z. B. Benutzer findet Gerät nicht). Dazu muss die Rücksicherung auf das wiedergefundene Gerät oder ein Ersatzgerät rasch und unkompliziert möglich sein.

5.4 FLEXIBILISIERUNG DER ARBEITSZEIT

Die permanente Erreichbarkeit, der ständig mögliche Zugriff auf Daten und E-Mails werden ungeachtet aller Vorteile zunehmend auch zu einer Last und Bürde für alle Menschen. Dies gilt insbesondere dann, wenn die Flexibilisierung der Arbeitszeit übertrieben wird und Wochenenden und Familienurlaube unter den permanenten Erinnerungen an die Arbeit leiden. Hier können sowohl organisatorische als auch technische Maßnahmen ergriffen werden, die in manchen Unternehmen durchaus einschneidend sein können (Mailsperre am Wochenende, Maillöschung während des Urlaubs). Klarerweise ist eine Balance zwischen Aufgabe, Verantwortungsbereich, Dringlichkeit und Branche zu finden. Dies kann nur in enger Abstimmung mit allen Stakeholdern erfolgversprechend umgesetzt werden.

Mobility als Last und Bürde.

5.5 DATENKLASSIFIZIERUNG

Eine der technisch und organisatorisch komplexesten Herausforderungen liegt in der Klassifikation der Daten und den damit verbundenen Sicherheitsanforderungen. Es ist für jeden einsichtig, dass allgemeine und öffentlich verfügbare Produktdaten und Preisblätter einem anderen Schutz (auch am mobilen Endgerät) unterliegen müssen als technische, vertrauliche Produktinformationen, Kundendaten oder kaufmännische Kalkulationen. Nur wenn eine einfach nachvollziehbare Datenklassifikation und eine damit verbundene Kennzeichnung erfolgt sind, können technische Systeme und die Benutzer eine Systematik einhalten, die je nach Datenklasse unterschiedliche Vorgangsweisen und Speicherräume vorsieht. Zu beachten ist dabei, dass diese Klassifikation ein durchaus aufwendiger und langfristiger Prozess ist, der bei zu hoher Komplexität weder technisch noch von den betroffenen Personen eingehalten werden kann. Ein Zwiebelschalenmodell (außen geringste Schutzwürdigkeit und innen höchste Sicherheitsstufe) kann helfen, die Differenzierung der Daten nachvollziehbar darzustellen.

Ein Zwiebelschalenmodell kann die Datenklassifizierung nachvollziehbar darstellen.

5.6 SCHULUNGEN

„Jeder muss lernen, sich zu schützen", das ist zwar richtig, sollte aber idealerweise lauten: „Jedem muss geholfen werden, zu lernen, sich zu schützen". Es ist unerlässlich, ein initiales und in weiterer Folge wiederholendes und ergänzendes Schulungskonzept für alle Benutzer zu erstellen und durchzuführen. Durch einen Ausbildungsplan, eine Schulungsreihe, Informationsblätter und Unterweisungen muss sichergestellt werden, dass bei den Mitarbeitern eine selbstverständliche „Awareness" hinsichtlich des erlaubten und möglichen Einsatzes der Geräte und Applikationen entsteht. Ziel soll eine Balance zwischen den möglichen Risiken und sämtlichen Vorteilen und Potenzialen eines Enterprise-Mobility-Konzepts sein.

Jedem muss geholfen werden, zu lernen, sich zu schützen.

5.7 EINKLANG ZWISCHEN UNTERSCHIEDLICHEN INTERESSEN HERSTELLEN

Wenn man sicherstellen möchte, dass ein Enterprise-Mobility-Konzept langfristig erfolgreich umgesetzt wird, muss bereits bei der konzeptiven Arbeit dafür gesorgt werden, dass es zu einer von allen Stakeholdern akzeptierten und unterstützten Balance zwischen den unterschiedlichen Interessen kommt. Dies gilt insbesondere für die Aspekte einer notwendigen und berechtigterweise geforderten Sicherheit von Unternehmens- und Personendaten versus einer bequemen Nutzbarkeit der Geräte durch die Benutzer im Alltag. Beispielsweise:



Wenn die Verschlüsselung des gesamten Geräts gefordert wird, dann wird meist auch ein komplexes Passwort am Sperrbildschirm gefordert, was wiederum gewöhnliches Telefonieren unangenehm erschwert.

5.8 REVIEW DER ORGANISATORISCHEN REGELUNGEN UND PROZESSE

Eine Überprüfung und eventuelle Anpassung der organisatorischen Konzepte und Prozesse sollte laufend erfolgen. Es wird jedoch empfohlen, nach drei und nach zwölf Monaten einen verbindlichen Review mit allen beteiligten Stakeholdern einzuplanen.

Verbindlichen Review mit allen Stakeholdern einplanen.

6 RECHTLICHE ASPEKTE

6.1 AUSGANGSSITUATION

Auch wenn das Thema MDM rechtlich nicht neu ist, so schafft insbesondere BYOD neue Herausforderungen. Als erstes rechtliches Thema wird im allgemeinen „Datenschutz" genannt. Das Datenschutzrecht ist im Bereich Enterprise Mobility jedoch von nachrangiger Bedeutung. Viel wesentlicher ist nämlich das Arbeitsrecht.

Das Arbeitsrecht kennt bislang noch keine speziellen Regelungen zu diesen Themen, allerdings kennt es Grundprinzipien, an denen man sich zur Lösung orientieren kann.

Die wichtigsten sind einerseits die gesetzlich vorgesehene Fürsorgepflicht des Arbeitgebers und andererseits die Treuepflicht des Arbeitnehmers. Verkürzt gesagt verlangen diese einen fairen, rücksichtsvollen Umgang von Dienstgeber und Dienstnehmer miteinander und die Wahrung der Interessen des jeweils anderen, wobei der Schwerpunkt bei der Fürsorgepflicht auf den Persönlichkeitsrechten des Arbeitnehmers liegt, bei der Treuepflicht hingegen auf den wirtschaftlichen Interessen des Arbeitgebers.

Gesetzliche Regeln verlangen einen fairen, rücksichtsvollen Umgang von Dienstgeber und Dienstnehmer miteinander und die Wahrung der Interessen des jeweils anderen.

Auf diesen Grundsätzen beruhend existieren bereits Regelungen und Gerichtsentscheidungen zur Nutzung von durch den Dienstgeber bereitgestellten Geräten und insbesondere Kommunikationseinrichtungen, beispielsweise Telefon oder Internet. Insgesamt darf der Arbeitgeber nicht jeglichen Privatgebrauch der von ihm selbst bereitgestellten Infrastruktur verbieten, beispielsweise das Führen privater Telefonate oder die Überprüfung privater E-Mails während der Dienstzeit. Der Dienstnehmer hingegen muss die private Nutzung auf ein Minimum beschränken, damit er nicht mitunter sogar seine Anstellung riskiert.

Hinsichtlich COD wandeln Unternehmen daher auch mit mobilen Geräten auf recht begangenen Pfaden. Wesentlich ist aber, dass den Arbeitnehmern ihre Rechte und Pflichten klar, vorzugsweise schriftlich, kommuniziert werden und diese mit den geltenden gesetzlichen Regelungen und der Rechtsprechung, auf die hier nicht im Detail eingegangen werden kann, im Einklang stehen.



6.1.1 BESONDERHEITEN BEI BYOD

Bei privaten Endgeräten muss der Arbeitgeber Sorge tragen, dass solche Geräte, jedenfalls außerhalb der Dienstzeit, auch zu privaten Zwecken genutzt werden können.

Bei Privatgeräten, die der Arbeitnehmer zur beruflichen Nutzung in das Unternehmen einbringt, gelten hingegen andere Voraussetzungen. Während nämlich vom Arbeitgeber bereitgestellte Geräte in erster Linie für berufliche Zwecke zu nutzen sind und der Arbeitgeber daher die Rechte des Arbeitnehmers rechtlich oder technisch stark beschränken darf, sind Privatgeräte in erster Linie zum persönlichen, nicht-beruflichen Gebrauch bestimmt.

Der Arbeitgeber muss daher Sorge tragen, dass solche Geräte, jedenfalls außerhalb der Dienstzeit, auch zu privaten Zwecken genutzt werden können. Wie weit diese Rechte gehen müssen bzw. ob Einschränkungen erhalten bleiben können, etwa bezüglich der Möglichkeit, eigene Applikationen zu installieren, ist zurzeit ungeklärt. Hier hilft aktuell am ehesten die genaue Abklärung der Bedürfnisse von Arbeitgeber und Arbeitnehmer, die von Unternehmen zu Unternehmen unterschiedlich sein können, um späteren Diskussionen oder gar Konflikten vorzubeugen.

Wesentlich ist es auch, zu beachten, dass ein Unternehmen bei BYOD immer auch mit persönlichen Daten zu tun hat. Ob diese auch „personenbezogen" im Sinne des Datenschutzgesetzes sind, sich somit diese Daten einer bestimmten Person zuordnen lassen, spielt dabei keine Rolle. Es ist daher besonderer Wert darauf zu legen, dass diese Daten ordnungsgemäß gesichert werden und vor allem auch wiederhergestellt werden können. Hier empfiehlt es sich, Sicherung und Wiederherstellung so zu gestalten, dass die einzelnen Daten (z. B. Fotos oder Texte) dabei nicht eingesehen werden können.

Das Datenschutzgesetz kann in dieser Konstellation aber durchaus relevant werden, nämlich insbesondere im Zusammenhang mit der Pflege der persönlichen Daten, sofern es sich bei diesen um personenbezogene Daten handelt und sie somit dem Datenschutzgesetz unterliegen. Letzteres regelt nämlich nicht nur die Modalitäten der legalen Erlangung und Verwendung personenbezogener Daten, sondern schreibt auch vor, dass diese auf Wunsch der Person, auf welche sie sich beziehen, richtigzustellen oder zu löschen sind.

Wenn daher die private Nutzung mobiler Geräte erlaubt ist und das Unternehmen die Sicherung sämtlicher mobiler Daten durchführt, kann die Situation entstehen, dass das Unternehmen über Sicherungen privater Daten und Dateien verfügt, die andernorts bereits gelöscht sind oder die ehemaligen Mitarbeitern gehören. Um dies und damit verbundene Komplikationen zu

vermeiden, empfiehlt es sich, technisch oder organisatorisch vorzusehen. Technisch ließen sich etwa unternehmensbezogene Daten separat sichern, um private Daten regelmäßig löschen zu können. Organisatorisch müsste sichergestellt werden, dass alle Mitarbeiter unternehmensbezogene Daten und Informationen regelmäßig vom mobilen Gerät in die dafür vorgesehenen Systeme übertragen, damit die Sicherungen sodann bedenkenlos als Ganzes gelöscht werden können.

6.1.2 BESONDERHEITEN BEI CLOUD-DIENSTEN

Bei Nutzung von Cloud-Diensten ist darauf zu achten, dass auch der verwendete Dienst sowie der herangezogene Dienstleister die unternehmensinternen Vorgaben einhalten. Dies gilt insbesondere bei der Sicherung privater Daten in die Cloud.

Bei der ursprünglichen Einführung von MDM/MAM als Cloud-Variante sind daher die technischen und rechtlichen Rahmenbedingungen zunächt mit dem Cloud-Dienstleister zu klären. Bei der Migration einer bestehenden MDM/MAM-Lösung in die Cloud ist die technische und rechtliche Kompatibilität und ein allfälliger Anpassungsbedarf der bestehenden unternehmensinternen Vorgaben zu prüfen.

Bei der Migration einer bestehenden MDM/MAM-Lösung in die Cloud besteht möglicherweise ein Anpassungsbedarf der bestehenden unternehmensinternen Vorgaben.

Zwischen Arbeitgeber und Cloud-Dienstleister müssten nicht nur die Einhaltung dieser unternehmensinternen Vorgaben, sondern auch die ergänzenden Pflichten des Cloud-Dienstleisters und seine Beschränkungen im Hinblick auf private Daten (abhängig vom Umfang der Dienstleistung und der erforderlichen Zugriffsmöglichkeiten) vertraglich abgesichert werden.

Darüber hinaus ist bei Cloud-Diensten die Einhaltung der datenschutzrechtlichen Vorgaben zu beachten, da in einer solchen Konstellation regelmäßig personenbezogene Daten an einen Dritten, nämlich den Cloud-Dienstleister, weitergegeben werden. Dies macht unter anderem den Abschluss einer entsprechenden Datenschutzvereinbarung erforderlich. Dafür stellt die Datenschutzbehörde aber ein Muster zur Verfügung, sodass sich der Mehraufwand in Grenzen hält.



6.2 DATENLÖSCHUNG

Sollte ein Gerät abhanden kommen oder der Nutzer das Unternehmen verlassen, ist es für den Dienstgeber essenziell, die auf dem Gerät gespeicherten Daten möglichst vollständig löschen zu können.

Bei COD stellen sich hier keine neuen Herausforderungen. Sofern vereinbart wurde, dass auf diesen keine privaten Daten gespeichert werden dürfen, ist die vollständige Löschung rechtlich möglich, ebenso wie die Abnahme, falls das Gerät vorhanden ist.

Bei Privatgeräten, die in die Unternehmensinfrastruktur eingebracht wurden, ist hingegen die Abnahme grundsätzlich nicht möglich. Für die Löschung ist ausschlaggebend, welche Kontrollmöglichkeiten dem Unternehmen eingeräumt bzw. dem Arbeitnehmer belassen wurden. Sind letztere entsprechend weitgehend, kann dem Arbeitnehmer auch eine Pflicht zur Sicherung privater Daten auferlegt werden, sofern dies klar kommuniziert wird und technisch zumutbar ist. Ansonsten müsste der Arbeitgeber für die regelmäßige und zeitnahe Sicherung auch der privaten Daten Sorge tragen.

Dem Arbeitnehmer kann unter Umständen die Pflicht zur Sicherung privater Daten auferlegt werden.

Die Beschränkung auf die Nutzung von Mobilgeräten, die die Verwaltung mehrerer Nutzerkonten erlauben (z. B. Blackberry 10 oder Android ab Version 4.2), ist hier von großem Vorteil.

6.3 VERGÜTUNG MOBILER ARBEIT AUSSERHALB DER KERNARBEITSZEIT

Grundsätzlich gilt zwar, dass Mehr- und Überstunden vom Arbeitgeber vorab zu genehmigen sind, jedoch stellt die praktische Umsetzung dieser Regel in einem mobilen Arbeitsumfeld eine Herausforderung dar.

Lösungsansätze gibt es einige: flexible Arbeitszeiten, vorab genehmigte Mehr- und Überstundenkontingente, das grundsätzliche Verbot der mobilen Arbeit insbesondere an Wochenenden oder Feiertagen und andere mehr. Eine einzige Lösung, die für jedes Unternehmen gleich passend ist, gibt es jedoch nicht.

Wesentlich ist daher, dass der Arbeitgeber die für ihn beste Lösung analysiert und diese schon bei Einführung von MDM/MAM mit den Arbeitnehmern rechtsverbindlich vereinbart.

Wesentlich ist eine rechtsverbindliche Vereinbarung bezüglich der mobilen Arbeit außerhalb der Kernarbeitszeit.

6.4 EINBINDUNG DES BETRIEBSRATS

Abgesehen von der gesetzlich verpflichtenden Zustimmung des Betriebsrats bei der Einführung bestimmter technischer Systeme (z. B. zu Kontrollmaßnahmen im Sinne des § 96 Abs 1 Z 3 Arbeitsverfassungsgesetz) kann die Befassung des Betriebsrats (sofern einer vorhanden ist) auch außerhalb einer gesetzlichen Pflicht sowohl bei COD als auch bei BYOD von Vorteil sein.

So können beispielsweise in einem kleinen Kreis die technischen Freiräume und Einschränkungen bei der Nutzung mobiler Endgeräte, aber auch Vorschriften für deren berufliche Nutzung außerhalb der Arbeitszeit festgelegt werden. Empfehlenswert ist es dennoch, den Betriebsrat erst nach Erstellung eines Konzepts als Diskussionsgrundlage zu konsultieren.

Selbst wenn die abgestimmten Vorgaben nicht in Form einer Betriebsvereinbarung fixiert werden können, ist die Unterstützung des Betriebsrats bei deren Einführung und Durchsetzung von unschätzbarem Vorteil.

6.5 CHECKLIST

- COD, BYOD oder beides?
- Soll BYOD auf bestimmte Geräte beschränkt sein?
- Soll die Nutzung mobiler Geräte auf bestimmte Personen/Personengruppen beschränkt werden?
- Welche Nutzungsmöglichkeiten/Einschränkungen soll es geben?
- Wie soll die Sicherung erfolgen, und wer soll sie durchführen?
- Ist sichergestellt, dass zumindest die Sicherungen privater Daten regelmäßig gelöscht werden?
- Wie soll die Löschung erfolgen?
- Sollten externe Anbieter (z. B. Cloud-Dienstleister) herangezogen werden?
- Falls ja: Sind deren Pflichten rechtskonform vertraglich geregelt?
- Wurde der Betriebsrat konsultiert?
- Wurden die Nutzungsbedingungen mit den Arbeitnehmern schriftlich detailliert und rechtskonform geregelt?
- Wurde die Nutzung außerhalb der Kernarbeitszeiten mit den Arbeitnehmern schriftlich detailliert und rechtskonform geregelt?



7 ANBIETERVERZEICHNIS – MANAGEMENTPRODUKTE

Hersteller	Produkt	Website
7P	7P MDM	www.7p-group.com/enterprise-mobility/seven-principles/
Absolut Software	Absolut Management	http://www.absolutemanage.com/en/manage/mdm
AirWatch	AirWatch	www.air-watch.com/de
Alcatel	Motive Device Management	www.alcatel-lucent.com/solutions/device-management
Amtel	Mobile Device Security	www.amtelnet.com
Apperian	Mobile Application Management	www.apperian.com/mobile-application-management-platform/mobile-application-management/
Baramundi	Mobile Device Management	www.baramundi.de/loesungen/mobile-device-management
Capricode	SyncShield	www.capricode.com/
CA Technologies	XenMobile MDM	www.citrix.de/products/xenmobile-mdm/overview.html
Cortado	Workplace	corporateserver.cortado.com/de-de/
Dell	Mobility Software	www.dell.com/us/business/p/enterprise-mobility-management?~ck=anav

Hersteller	Produkt	Website
equinux	Tarmac Mobile Device Management	www.tower-one.net/de/
Excitor	EMM	www.excitor.com/enterprise-mobility-management
FancyFon Software	Famoc	www.fancyfon.com/
Good Technologie	Mobile Device Management	www.good.com
Kaseya	Mobile Device Management	www.kaseya.com/products/enterprise-mobility-management
LANDesk	Management Suite	www.landesk.com/products/mobility-manager.aspx
Matrix42	Mobile Device Management	www.matrix42.com/de/produkte/matrix42-mobile-apps/
Microsoft	Enterprise Mobility	www.microsoft.com/en-us/server-cloud/enterprise-mobility/overview.aspx
Microsoft	Intune	www.microsoft.com/en-us/windows/windowsintune/explore.aspx
Microsoft	Office 365	Mobile Device Management for Office 365
Mobile Active Defense	Mobile Enterprise/ Security Server	www.mobileactivedefense.com/
MobileIron	Mobile Device Management	www.mobileiron.com/en/solutions
OpenPeak		www.openpeak.com/mdm.php



Hersteller	Produkt	Website
Relution	Enterprise Mobility Platform	www.relution.io/de/
RIM	Blackberry	de.blackberry.com/enterprise/solutions/emm.html
SAP		go.sap.com/germany/solution/platform-technology/enterprise-mobility-management.html
Sophos	Mobile Control	www.sophos.com/de-de/products/mobile.aspx
SOTI	MobiControl	www.soti.net/solutions/enterprise-mobility-management/
Symantec	Mobile Management	www.symantec.com/mobile-device-management
Tangoe	Matrix	www.tangoe.com/products-services/managed-mobility-services-matrixmobile/enterprise-mobility-management/
Trend Micro	Mobile Security	www.trendmicro.de/produkte/mobile-security/index.html
universit		universitplatform.com/
Wavelink	Avalanche	www.wavelink.com/products/avalanche/

8 ANBIETERVERZEICHNIS – MIM UND EFSS

Hersteller	Produkt	Website
Accellion		www.accellion.com/solutions/online-file-sharing/file-sync
AirWatch		www.air-watch.com/solutions/mobile-content-management
Amazon	Amazon Cloud Drive	www.amazon.de/clouddrive/home
Apple	iCloud	www.icloud.com
Appsense	DATANOW	www.appsense.com/products/datanow
box		www.box.com
Carbonite		www.carbonite.com
Citrix	Sharefile Enterprise	www.sharefile.com/enterprise/
Cloudme		www.crashplan.com/enterprise/mobile.html
Cortado	Workplace	corporateserver.cortado.com/de-de/
CTERA		www.ctera.com/solutions/by-business-need/enterprise-file-sync-share-efss
Cubby (LogMeIn)		www.cubby.com
DROPBOX	Dropbox for Business	www.dropbox.com/business
EGNYTE		www.egnyte.com
EMC	Syncplicity	www.syncplicity.com



Hersteller	Produkt	Website
Excitor	Excitor DME™ File Browser	www.excitor.com
Google	Google Drive	drive.google.com
Hightail	Yousendit	www.hightail.com
Huddle		www.huddle.com
Insync	Google Drive AddOn	www.insynchq.com
JustCloud		www.livedrive.com
Microsoft	OneDrive	onedrive.live.com/about/de-at/
Microsoft	Office 365	Mobile Device Management for Office 365
Mozy	Mobil	mozy.com/mobile
OpenDrive		www.opendrive.com
OwnCloud		owncloud.com/products/enterprise
PowerFolder		www.powerfolder.com
Primadesk	Unifyle	www.unifyle.co
SpiderOak		spideroak.com
SOONR (Autotask)		www.soonr.com
SugarSync		www.sugarsync.com
TeamDrive		www.teamdrive.com
TeamPlace		www.teamplace.net/de-de/
Trend Micro	SafeSync	www.trendmicro.com/us/home/products/storage-backup/safesync
Unwired Revolution	DocLink	www.unwiredrevolution.com/products/

9 GLOSSAR

Abkürzung	Langform	Erklärung
Agent	Agent	Software-Komponente, die auf einem Mobile Device installiert werden muss, um ein Management zu ermöglichen
Android	Android	Smartphone-Betriebssystem von Google
BYOA	Bring Your Own Application	Mitarbeitern wird es gestattet, unter Einhaltung der Lizenz-, Sicherheits- und Datenkompatibilitätsvorgaben Applikationen zu verwenden, die sie selbst auf ihrem Mobile Device ins Unternehmen mitbringen.
BYOD	Bring Your Own Device	Mitarbeitern wird es gestattet, private Geräte für Firmenzwecke zu nutzen. Manchmal wird diese Betriebsvariante vom Unternehmen auch gefördert und forciert.
Cloud		Synonym für viele Daten- oder Programmdienste, die von Benutzern über das Internet bezogen werden. Exaktere Definitionen siehe „Cloud Migration“, ISBN 978-3-8266-9261-1
COD	Company-owned Device	Geräte, die sich im Besitz des Unternehmens befinden. Auf diesen Geräten ist eine Durchsetzung von Richtlinien und Policies meist leichter möglich als bei BYOD-Geräten.
COPE	Company-owned – Personally Enabled	Das Gerät wird vom Unternehmen gestellt, aber komplett vom Benutzer betrieben. BYOD mit dem Vorteil, dass die Gerätetypen begrenzt sind.
DLP	Data Loss Prevention	DLP gehört zu den Schutzmaßnahmen, die direkt den Schutz der Vertraulichkeit von Daten unterstützen. „Data Loss Prevention“ und „Data Leakage Prevention“ werden meist synonym ge-braucht.
EFSS	Enterprise File Sharing and Sync	Siehe auch MFM



Abkürzung	Langform	Erklärung
EM	Executive Mobility	Beschreibt den steigenden Mobilitätsanspruch von Führungskräften in Unternehmen
EMM	Enterprise Mobility Management	Ist ein umfassender Ansatz, um die Nutzung von Smartphones und Tablets durch Mitarbeiter zu ermöglichen und zu sichern. Eine starke EMM-Strategie befasst sich nicht nur mit Sicherheitsfragen, sondern unterstützt die Beschäftigten auch dabei, ihre Produktivität zu steigern. Dazu werden ihnen die Tools zur Verfügung gestellt, die sie brauchen, um arbeitsbezogene Aufgaben auf Mobilgeräten durchführen zu können.
IOS	IOS	Betriebssystem des Apple Smartphones iPhone und der Apple Tablets iPad
MAM	Mobile Application Management	Beschäftigt sich mit Software auf mobilen Endgeräten, dabei unterstützt MAM Administratoren bei der Bereitstellung, Lizenzierung, Konfiguration, dem Application Lifecycle Management (ALM) und der Nutzungsverfolgung mobiler Anwendungen. Viele Mobile Application Manager können auch die Einhaltung definierter Unternehmensrichtlinien abgleichen und den Austausch betrieblicher Daten zwischen mobilen Apps kontrollieren und einschränken. Eine wichtige Voraussetzung für den Einsatz von MAM-Software ist, dass sie Administratoren die Möglichkeit gibt, mobile Unternehmens-Apps und/oder Daten vom Gerät eines Endanwenders aus der Ferne zu löschen.
MDM	Mobile Device Management	Steht für die zentralisierte Verwaltung von Mobilgeräten wie Smartphones, Sub-Notebooks, PDAs oder Tablet-Computer durch einen oder mehrere Administratoren mit Hilfe spezieller Software. Die Verwaltung bezieht sich auf die Inventarisierung von Hardware in Organisationen, die Software- und Datenverteilung sowie den Schutz der Daten auf diesen Geräten.

Abkürzung	Langform	Erklärung
MFM	Mobile File Management	Zu diesen Produkten gehören alle jene, die es erlauben, Dateien auf mobilen Devices sicher mitzunehmen, mit anderen Geräten zu synchronisieren und/oder Dateien in der Cloud abzulegen. Nicht zu verwechseln mit MIM, bei MIM geht es um den Dateninhalt von Diensten wie Facebook, Evernote usw.
MIM	Mobile Information Management	Ist die nächste Stufe des Managements und geht so weit, dass Applikationen verstehen, wie sie mit gewissen Daten (Type, Quellen und/oder Inhalten) umgehen dürfen oder müssen. Heute gibt es bereits Anwendungen, die Rights Management unterstützen oder auch Mail-Software (iOS), die zwischen privaten und beruflichen Einstellungen unterscheidet.
MMP	Mobile Management Product	Produkte zum Management von mobilen Devices und den auf ihnen gespeicherten Daten
Mobile Device	Mobile Management Product	Smartphone, Tablet, Handheld Device
Off-Premise	Off-Premise	Als off-Premise werden IT-Services bezeichnet, die nicht von einem Standort des Unternehmens aus erbracht werden.
On-Premise		Als on-Premise werden IT-Services bezeichnet, die vom Unternehmen selbst von Standorten des Unternehmens aus erbracht werden.



10 STARAUDIT

Die Organisation EuroCloud bietet eine Cloud-Zertifizierung unter dem Namen „StarAudit" an. Die Zertifizierung ist spezifisch auf die Bereiche IaaS, PaaS und SaaS ausgelegt und hat definierte Aussagen zu Kontrollelementen, die abgestuft zu erfüllen sind, um als vertrauenswürdiger Cloud-Anbieter zertifiziert zu werden.

Zur qualitativen Prüfung der Leistungserbringung hinsichtlich der Datensicherheit, des technischen Betriebes und der organisatorischen Abläufe bedarf es einer weitreichenden Expertise, um die jeweiligen Anforderungen, die sich aus den Servicegarantien ergeben, zu prüfen. Aus diesem Grund werden zumeist Zertifikate herangezogen, die eine kompakte Aussage zu den Sicherheitsaspekten und der Zuverlässigkeit des Serviceanbieters geben.

Für die vorgenannten vertraglichen, technischen und organisatorischen Anforderungen hat EuroCloud ein spezielles Gütesiegel entworfen, dessen Nutzung voraussetzt, dass die für die Bereitstellung von Cloud-Services grundlegenden Anforderungen durch geschulte Auditoren geprüft und durch ein Zertifikat bestätigt werden. Für die Prüfanforderungen wurde in enger Abstimmung mit öffentlichen Institutionen, Forschungseinrichtungen, Cloud-Anbietern, Rechtsexperten und Wirtschaftsprüfungsgesellschaften ein Kriterienkatalog erstellt.

Konkret werden im StarAudit folgende Kategorien erfasst:

- Anbieterprofil
- Vertrag und Compliance
- Sicherheit
- Betrieb der Infrastruktur
- Betriebsprozesse
- Anwendung
- Implementierung

Durch ein Punktesystem und die Vorgabe von Mindestkriterien kann ein Anbieter verschiedene Gütestufen (ein Stern bis fünf Sterne) erreichen.

Im Kern geht es um rechtliche Aspekte, zuverlässige Bereitstellung von technischen Dienstleistungen sowie Datenschutz, Datensicherheit und Einhaltung grundlegender Qualitätsstandards für Betriebsprozesse und Anwendungsgestaltung. Für seine Angaben im Audit muss der Anbieter konkrete Nachweise vorlegen; zudem verpflichtet er sich, signifikante

Änderungen der Rahmenbedingungen (zum Beispiel Ort der Leistungserbringung, Änderung der Subunternehmervereinbarungen) und kritische Vorfälle unverzüglich zu melden.

Im Ergebnis werden je nach Umsetzungsgrad die drei folgenden Gütestufen vergeben:

- Trusted Cloud-Service – drei Sterne
- Trusted Cloud-Service Advanced – vier Sterne
- Trusted Cloud-Service Advanced HA (High Availability) – fünf Sterne

10.1 EIN-STERN-ZERTIFIZIERUNG

Der Anbieter hat folgende Pflichtkriterien erfüllt:

- Es handelt sich um ein im EU-Handelsregister eingetragenes Unternehmen.
- Der technische Betrieb der Anwendung erfolgt in einer für die Bereitstellung von webbasierten Diensten geeigneten Infrastruktur.
- Hierzu gehört:
  - ein abgeschlossener Bereich für die verwendeten Hardwarekomponenten
  - redundante Stromversorgung mit USV-Betrieb für mindestens 20 Minuten
  - redundante Internetanbindung
  - Zutrittskontrolle
  - grundlegende Arealsicherheit
- Die vertraglichen Vereinbarungen sind konform mit den Datenschutzanforderungen im Sinne des Bundesdatenschutzgesetzes.
- Es bestehen nachvollziehbare Kündigungsvereinbarungen.
- Es bestehen eindeutige Vereinbarungen bezüglich der Kundendaten ohne Zurückbehaltungsrecht durch den Auftragnehmer.
- Es bestehen vertraglich vereinbarte Regelungen mit dokumentierten Datenexportschnittstellen zur Rückgabe und Löschung von Kundendaten bei Beendigung des Vertragsverhältnisses.

10.2 ZWEI-STERNE-ZERTIFIZIERUNG

Ergänzend zu den vorgenannten Anforderungen sind folgende Pflichtkriterien erfüllt:



- Der Anbieter macht nachvollziehbare Angaben zu den zugesicherten Serviceleistungen in Bezug auf Verfügbarkeit und Geschwindigkeit der Anwendung. Diesbezüglich stehen auch Berichtsfunktionen zum Nachweis der Servicezusagen zur Verfügung.
- Der technische Betrieb entspricht den Minimalanforderungen eines Rechenzentrums hinsichtlich der redundanten Auslegung der technischen Grundversorgung. Arealrisiken und Gebäudesicherheit sind durch Dokumentation des Anbieters ausgewiesen.
- Die Exportformate der Kundendaten sind durchgängig dokumentiert und für die Migration in andere Umgebungen verfügbar.

10.3 DREI-STERNE-ZERTIFIZIERUNG

Ergänzend zu den vorgenannten Anforderungen sind folgende Pflichtkriterien erfüllt:

- Der Anbieter ermöglicht die Wahl des nationalen Gerichtsstandes durch den Anwender oder bietet direkt den Vertrag nach Recht des Anwenders an.
- Der Anbieter bietet eine umfangreiche Dokumentation sowie Schulungsmaterial zur Einführung in die Nutzung des Services an. Eine Hotline steht zu üblichen Arbeitszeiten des Anwenders zur Verfügung. Probleme können durch ein elektronisches Ticketsystem übermittelt werden. Der Anbieter hat Prozesse mit garantierten Bearbeitungsabläufen und den dazu notwendigen internen Anwendungen auch mit möglichen Vorlieferanten etabliert.
- Die jeweiligen Zusagen im Service-Management und bezüglich der technischen Bereitstellung wurden durch geschulte Auditoren vor Ort geprüft.

10.4 VIER-STERNE-ZERTIFIZIERUNG

Ergänzend zu den vorgenannten Anforderungen sind folgende Pflichtkriterien erfüllt:

- Die technische Bereitstellung entspricht den Anforderungen an einen professionellen Rechenzentrumsanbieter. Die Kommunikationsanbindung erfolgt über einen direkten und redundant ausgelegten Internet-Exchange-Knoten (IX).
- Die Serviceprozesse entsprechen den Anforderungen gemäß ITIL und ISO 27001 im Sinne eines ISMS (Information Security Management System).
- Die Sicherheitsfunktionen und Anwendungen von Verschlüsselungstechniken sind nachvollziehbar dokumentiert und entsprechen den normalen IT-Sicherheitsanforderungen. Schutzmaßnahmen gegen externe Angriffe sind vorhanden und entsprechen zum Zeitpunkt der Auditierung den Anforderungen der ISO 27001.
- Die direkten Zugriffe durch Administratoren sind eingeschränkt, und für Einzelzugriffe

erfolgt eine Anonymisierung von Transaktionsdaten gegenüber den Benutzerprofilen. Hierzu bestehen auch entsprechende Verfahrensdokumentationen, die dem Kunden bei Bedarf zur Verfügung gestellt werden.

- Sofern nicht durch andere Maßnahmen die Langzeitarchivierung von Kundendaten im Sinne der Grundsätze zum Datenzugriff und der Prüfbarkeit digitaler Unterlagen umgesetzt wird, werden durch den Anbieter die Archivierungs- und Bereitstellungsfunktionen von Kundendaten im Umfang der gesetzlichen Anforderungen erfüllt.

10.5 FÜNF-STERNE-ZERTIFIZIERUNG

Ergänzend zu den vorgenannten Anforderungen sind folgende Pflichtkriterien erfüllt:

- Der Anbieter verfügt über eine redundante Bereitstellung des Serviceangebotes über mindestens zwei Rechenzentren mit einer Verfügbarkeit von 99,99 Prozent und einer hochausfallsicheren Infrastruktur.
- Es werden regelmäßig (mindestens einmal pro Jahr) Notfallübungen durchgeführt und dokumentiert gemäß BS 25999.
- Es werden regelmäßig (mindestens einmal pro Jahr) Penetrationstests zum Nachweis der Sicherheitsfunktionen durchgeführt und dokumentiert.
- Der Anbieter verfügt über ein variables Preismodell und erlaubt auch im laufenden Vertrag den Wechsel in ein allgemein angebotenes, günstigeres Vertragsmodell zu den jeweiligen Laufzeitkonditionen (Best-Price-Option).

10.6 STARAUDIT

Die StarAudit Zertifizierung ist ein Best-Practice-Ansatz, um die wichtigen Managementfragen bei der Auswahl eines geeigneten Cloud-Anbieters zu beantworten. In Abgrenzung zu reinen Sicherheits- oder Datenschutzzertifizierungen wird hier der gesamte Bereich berücksichtigt und in einer verständlichen Aussage attestiert. Es werden sich klassische Zertifizierungssysteme weiter in Richtung Cloud-Prüfung entwickeln; dies kann aber zum Teil mehrere Jahre dauern. In den Kernfragen und besonders für den Mittelstand sind jetzt Hilfestellungen notwendig.



Anbieter mit dem folgenden Siegel haben die Kriterienerfüllung durch EuroCloud bestätigt bekommen:



10.7 STARAUDIT.ORG

Alle Details, die genauen Inhalte des StarAudit-Kataloges und die Assessment Tools, auch für ein Self Assessment, sind online unter staraudit.org kostenfrei erhältlich.



11 GLOSSAR CLOUD COMPUTING

11.1 WAS IST UNTER CLOUD COMPUTING ZU VERSTEHEN?

„Cloud Computing ist ein Modell, das es erlaubt, bei Bedarf jederzeit und überall bequem über ein Netz auf einen geteilten Pool von konfigurierbaren Rechnerressourcen (z. B. Netze, Server, Speichersysteme, Anwendungen und Dienste) zuzugreifen, die schnell und mit minimalem Managementaufwand oder geringer Serviceprovider-Interaktion zur Verfügung gestellt werden können."[4]

Folgende fünf Eigenschaften charakterisieren gemäß der NIST-Definition[5] einen Cloud-Service:

- On-demand Self Service: Die Provisionierung der Ressourcen (z. B. Rechenleistung, Storage) läuft automatisch ohne Interaktion mit dem Service-Provider ab.
- Broad Network Access: Die Services sind mit Standard-Mechanismen über das Netz verfügbar und nicht an einen bestimmten Client gebunden.
- Resource Pooling: Die Ressourcen des Anbieters liegen in einem Pool vor, aus dem sich viele Anwender bedienen können (Multi-Tenant-Modell). Dabei wissen die Anwender nicht, wo die Ressourcen sich befinden, sie können aber vertraglich den Speicherort, also z. B. Region, Land oder Rechenzentrum, festlegen.
- Rapid Elasticity: Die Services können schnell und elastisch zur Verfügung gestellt werden, in manchen Fällen auch automatisch. Aus Anwendersicht scheinen die Ressourcen daher unendlich zu sein.
- Measured Services: Die Ressourcennutzung kann gemessen und überwacht werden und entsprechend bemessen auch den Cloud-Anwendern zur Verfügung gestellt werden.

11.2 BEREITSTELLUNGS- UND BEZUGSFUNKTIONEN VON CLOUD-SERVICES

Es existieren vielfältige Möglichkeiten der Bereitstellung und des Bezugs von Cloud-Computing-Leistungen. Daher ist zwischen den folgenden Rollen zu differenzieren:

(A) BEREITSTELLUNG

- Cloud-Serviceanbieter – Unternehmen, das die Cloud-Leistungen gegenüber dem Kunden als Vertragsgeber anbietet.
- Cloud-Service-Subunternehmer – Vorlieferanten von Cloud-Services, die vom Cloud-Serviceanbieter als Teilfunktion integriert werden.

4 - https://www.bsi.bund.de/DE/Themen/CloudComputing/Grundlagen/Grundlagen_node.html
5 - http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf



- Cloud (Managed) Hosting Provider – Cloud-Services-Subunternehmer, der technische IT-Leistungen, die dem klassischen IT-Outsourcing entsprechen (Rechner, Speicher, Netzwerk), erbringt, die nicht als vollwertige Cloud-Serviceleistung bezogen werden.
- Co-Location Provider – Vorlieferant von Infrastrukturkomponenten, der Gebäude, Strom, Klima, Kommunikation etc. als Grundversorgung bereitstellt.
- Cloud-Servicevermittler – Unternehmen, das für den Cloud-Serviceanbieter Kunden wirbt (und rechtlich die Stellung eines Handelsvertreters einnimmt).
- Cloud Service Reseller – Wiederverkäufer von Cloud-Services, der selbst keine Anpassung des Cloud-Services erbringt, sondern sämtliche Leistungen der Serviceerbringung vom Cloud-Serviceanbieter bezieht (und rechtlich als Vertragshändler zu qualifizieren ist).
- Cloud-Lösungsanbieter – Cloud Service Reseller, der mehrere Cloud-Services bündelt und als integriertes Paket weiterverkauft.

Der Begriff „Broker" wird hier bewusst nicht verwendet, da dieser im Markt in unterschiedlichen Bedeutungen verwendet wird, d. h. sowohl im Sinne von Vermittler als auch im Sinne von Lösungsanbieter.

Auch der Begriff „Marktplatz" wird im Markt in unterschiedlichen Bedeutungen verwendet, d. h. im Sinne von „Vermittler" oder „Reseller".

(B) BEZUG

- Cloud-Serviceabnehmer – Vertragspartner des Cloud-Serviceanbieters, der als Unternehmen den Service nutzen will.
- Cloud-Servicenutzer – einzelner Benutzer eines Cloud-Services, in der Regel ein Arbeitnehmer des Cloud-Serviceabnehmers.
- Cloud-Serviceadministrator – Fachbereich des Cloud-Serviceabnehmers, der mit der Verwaltung von Identitäten und Nutzungsoptionen des Cloud-Services betraut ist.

Im Markt wird teilweise der Begriff „Broker" auch als Bezeichnung einer internen Funktion im IT-Bereich des Cloud-Serviceabnehmers verwendet, die den Cloud-Servicenutzern cloudbasierte Lösungen bereitstellt.

11.3 CLOUD-SERVICES UND DEREN EIGENSCHAFTEN

Als typische Eigenschaften für einen Cloud-Service treten häufig die folgenden Merkmale auf:

- Selbstverwaltung des Services und der damit verbundenen Leistungen durch den Anwender.
- Technisch uneingeschränkter Netzwerkzugriff mit Standardanwendungen (z. B. Web-Browser) des Anwendergeräts (z. B. Notebook, Smartphone).
- Multimandantennutzung der technischen Ressourcen, zumeist über ganze Rechenzentrumsbereiche oder mehrere verteilte Rechenzentren als Ressourcenpool.
- Unmittelbare Elastizität, das heißt die automatische Bereitstellung von technischen Ressourcen aus dem Ressourcenpool bei Spitzenanforderungen oder Erweiterung der Zahl der Benutzer.
- Kontinuierliche Messung der tatsächlichen Nutzung pro Mandant und leistungsgerechte Abrechnung.

11.4 CLOUD-SERVICES UND BETRIEBSMODELLE

Bei der Bereitstellung von Cloud-Services gibt es zwei Unterscheidungsebenen: die Art der Cloud-Services und die verschiedenen Betriebsmodelle, die in freier Kombination verwendet werden können.

(C) CLOUD-SERVICES

Bei der Bereitstellung von Cloud-Services unterscheidet man in erster Linie drei Ebenen:

- SaaS – Software as a Service

Sämtliche Angebote von Anwendungssoftware, die den Kriterien des Cloud Computings entsprechen, fallen in diese Kategorie. Dem Angebotsspektrum sind hierbei keine Grenzen gesetzt. Als Beispiele seien Kontaktdatenmanagement, Finanzbuchhaltung, Textverarbeitung oder Kollaborationsanwendungen genannt.

- PaaS – Platform as a Service

Ein PaaS-Anbieter stellt eine komplette Infrastruktur bereit und bietet dem Kunden auf der Plattform standardisierte Schnittstellen an, die von Diensten des Kunden genutzt werden. So kann die Plattform z. B. Mandantenfähigkeit, Skalierbarkeit, Zugriffskontrolle, Datenbankzugriffe etc. als Service zur Verfügung stellen. Der Kunde hat keinen Zugriff auf die darunterliegenden Schichten (Betriebssystem, Hardware), er kann aber auf der Plattform eigene Anwendungen laufen lassen, für deren Entwicklung der PaaS-Anbieter in der Regel eigene Werkzeuge anbietet. Als Beispiel kann force.com der Firma Salesforce oder Azure der Firma Microsoft genannt werden.



- IaaS – Infrastructure as a Service

Bei IaaS werden IT-Ressourcen wie z. B. Rechenleistung, Datenspeicher oder Netze als Service angeboten. Ein Cloud-Serviceabnehmer kauft diese virtualisierten und in hohem Maß standardisierten Services und baut darauf eigene Services zum internen oder externen Gebrauch auf. So kann ein Cloud-Serviceabnehmer z. B. Rechenleistung, Arbeitsspeicher und Datenspeicher anmieten und darauf ein Betriebssystem mit Anwendungen seiner Wahl laufen lassen.

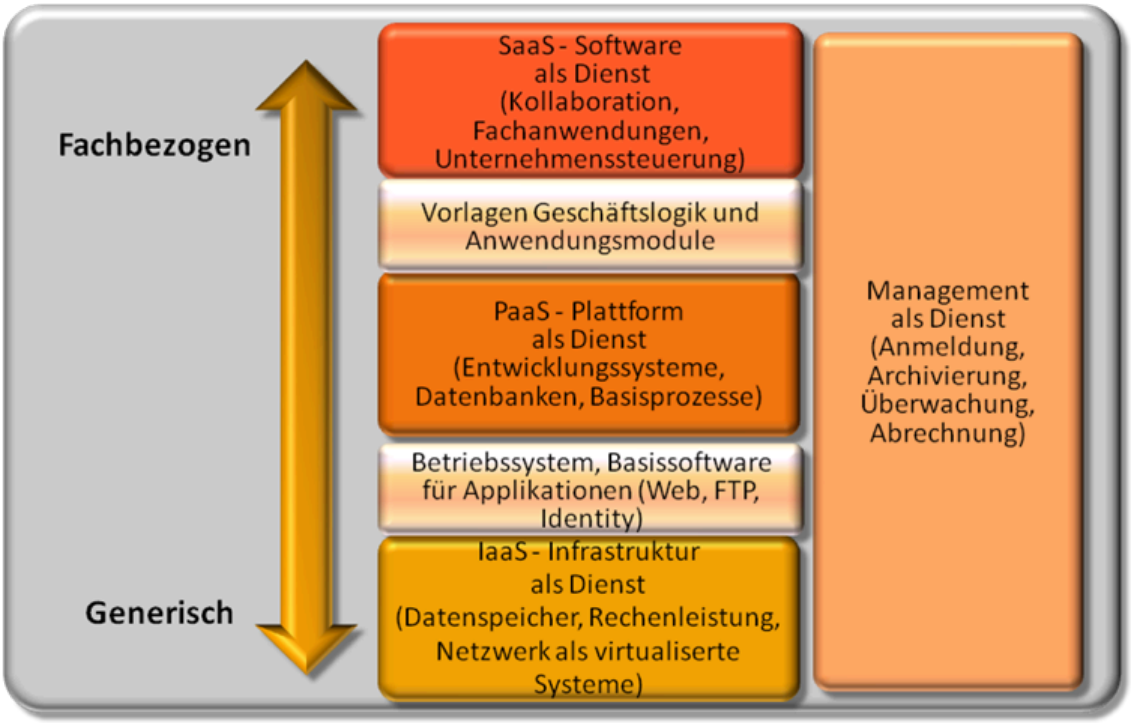


Abbildung 3: Quelle EuroCloud

Daneben gibt es weitere Ausprägungen als Sonderform, wie zum Beispiel Security, Business Process, Storage, Monitoring oder Communication as a Service, die zusammenfassend oftmals auch als XaaS benannt werden.

(D) CLOUD-BETRIEBSMODELLE

Bei den Betriebsmodellen ist zu unterscheiden, wer der Betreiber ist und wer generell Zugriff auf die Services hat:

Private Cloud: Dedizierte Bereitstellung der Services für einen definierten Kunden unter Verwendung von abgrenzbaren Hardware-Ressourcen (also in der Regel Rechenzentren,

abgeschlossene Bereiche innerhalb des Rechenzentrums) und Netzwerkbereiche, die nicht von Dritten genutzt werden.

Virtual Private Cloud: Im Gegensatz zur Private Cloud erfolgt die Mandantenabgrenzung lediglich auf der logischen Netzwerkebene, bei gleichzeitiger Nutzung der Hardware durch mehrere Kunden.



Abbildung 4: Quelle EuroCloud

Public (öffentliche) Cloud: Generelle Bereitstellung der Services für einen unbeschränkten Kundenkreis, der Hardware-Ressourcen gemeinschaftlich nutzt. Die von den Kunden in Anspruch genommenen Cloudleistungen werden mittels logischer Mandantenzuordnung separiert.



Abbildung 5: Quelle EuroCloud

(E) DANEBEN EXISTIEREN NOCH SONDERFORMEN WIE

- Community Cloud:

Kombination mehrerer Cloud-Services für bestimmte Anwendergruppen. Dies kann zum Beispiel im Bereich Logistik, Fertigung, Forschung oder Branchenvereinigungen definiert werden. Der Zugang ist nicht öffentlich, sondern erfordert zusätzliche Authorisierung durch die Betreiber der Community Cloud. Die an einer Community Cloud teilnehmenden Unternehmen haben meist ähnliche Anforderungen an Verfügbarkeit, Compliance und Sicherheit der bereitgestellten Ressourcen. Als Beispiel seien hier Banken oder Regierungsstellen genannt.

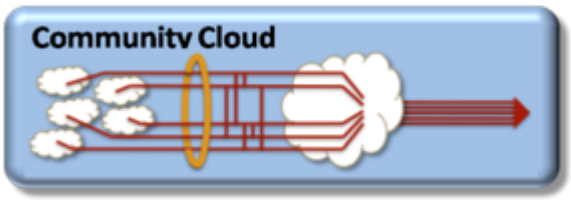


Abbildung 6: Quelle EuroCloud

- Hybrid Cloud:

Kombination von Private und Public Cloud. Hierbei erfolgt ein kombinierter Betrieb von Cloud-Services, bei denen ein Teil in einer privaten Umgebung (zum Beispiel ein ERP-System) und ein Teil aus einem öffentlichen Bereich (z. B. CRM) technisch und logisch zusammengeführt wird. Ein Beispiel für die Entstehung einer Hybrid Cloud ist die Verlagerung einer öffentlichen Firmenwebseite aus der Private Cloud in die Public Cloud. Da die Firmenwebseite ohnehin aus dem Internet erreichbar sein muss, kann einer Verlagerung in die Public Cloud unter Umständen sogar für höhere Sicherheit sorgen.

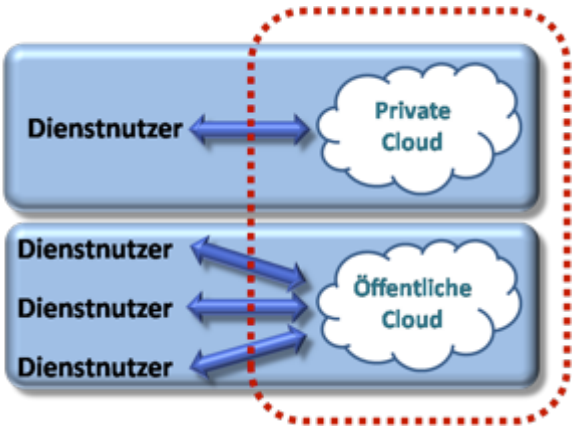


Abbildung 7: Quelle EuroCloud

11.5 CLOUD-SERVICE-MARKTPLATZ

Unterschiedliche Institutionen bieten ihre Leistungen über einen gemeinsamen Marktplatz und gegebenenfalls auch über eine gemeinsame Ausführungsplattform in der Cloud an. Diese Dienste können wiederum zur Unterstützung von Geschäftsprozessen zu komplexeren Mehrwert-Dienstleistungen gebündelt werden. Neben den Anbietern und Abnehmern dieser Dienste sowie den Entwicklern der Dienste und den Prozessdesignern, die die Mehrwert-Dienstleistungen zusammenstellen, kommt dem Betreiber des Marktplatzes als Lösungsanbieter oder Reseller eine zentrale Rolle zu.

12 RECHTLICHER HINWEIS

12.1 ALLGEMEINES

Die in diesem Leitfaden zur Verfügung gestellten Informationen dienen der allgemeinen Darstellung spezieller rechtlicher Aspekte im Zusammenhang mit Cloud Computing, stellen keine Rechtsberatung dar und können auch keine Rechtsberatung ersetzen, da eine solche immer die Kenntnis aller Einzelumstände, insbesondere des konkreten Einzelfalls, voraussetzt.

12.2 INHALT DES LEITFADENS

Der Herausgeber/die Autoren übernehmen keine Gewähr für die Vollständigkeit, Richtigkeit oder Aktualität der bereitgestellten Informationen. Dies gilt insbesondere im Hinblick auf neueste Entwicklungen in der Rechtsprechung oder der Gesetzeslage. Haftungsansprüche gegen den Herausgeber/die Autoren, die sich auf Schäden materieller oder ideeller Art beziehen, die durch die Nutzung oder Nichtnutzung der dargebotenen Informationen beziehungsweise durch die Nutzung fehlerhafter und unvollständiger Informationen verursacht wurden, sind grundsätzlich ausgeschlossen.

12.3 VERWEISE UND LINKS

Bei direkten oder indirekten Verweisen auf fremde Inhalte (z. B. „Links"), die außerhalb des Verantwortungsbereichs des Herausgebers/der Autoren liegen, würde eine Haftungsverpflichtung ausschließlich in dem Fall in Kraft treten, in dem der Herausgeber/die Autoren von den Inhalten Kenntnis hatten und es ihnen technisch möglich und zumutbar wäre, die Nutzung im Falle rechtswidriger Inhalte zu verhindern. Der Herausgeber/die Autoren erklären hiermit ausdrücklich, dass zum Zeitpunkt der Linksetzung keine illegalen Inhalte auf den zu verlinkenden Seiten erkennbar waren. Auf die aktuelle und zukünftige Gestaltung, die Inhalte oder die Urheberschaft der verlinkten Seiten haben der Herausgeber/die Autoren keinen Einfluss. Sie distanzieren sich ausdrücklich von allen Inhalten aller verlinkten Seiten, die nach der Linksetzung verändert wurden. Für illegale, fehlerhafte oder unvollständige Inhalte und insbesondere für Schäden, die aus der Nutzung oder Nichtnutzung solcherart dargebotenen Informationen entstehen, haftet allein der Anbieter der Seite, auf welche verwiesen wurde, nicht derjenige, der über Links auf die jeweilige Veröffentlichung lediglich verweist.

12.4 URHEBERRECHT

Die in diesem Leitfaden dargestellten Inhalte wie Texte, Graphiken oder Bilder sind nach dem österreichischen Urhebergesetz urheberrechtlich geschützt. Jede urheberrechtlich nicht



gestattete Verwertung bedarf der vorherigen schriftlichen Zustimmung des Herausgebers. Beiträge Dritter sind als solche gekennzeichnet. Dies gilt insbesondere für Vervielfältigung, Bearbeitung, Verarbeitung bzw. Wiedergabe von Inhalten in Datenbanken oder anderen elektronischen Medien. Die unerlaubte Vervielfältigung oder Weitergabe einzelner Teile oder des gesamten Leitfadens ist ausdrücklich nicht gestattet. Ausgenommen ist dabei der individuelle bzw. private Gebrauch, wobei die private Nutzung kein Recht zur Weitergabe an Dritte beinhaltet. Gleiches gilt für Veröffentlichungen oder sonstige Arbeiten.

12.5 VERGÜTUNG

Dieser Leitfaden wird den Adressaten/Empfängern kostenlos zur Verfügung gestellt.

13 AUTOREN

Reinhard Travniček
X-tech Handelsges.m.b.H.
Hauptstraße 157
2231 Strasshof, Österreich

E-Mail: reinhard.travnicek@x-tech.at
Web: www.x-tech.at



Dr. Tobias Höllwarth
Höllwarth Consulting
Gluckgasse 2
1010 Wien, Österreich

E-Mail: office@hoellwarth.at
Web: www.hoellwarth.at



Mag. Árpád Geréd
Maybach Görg Lenneis Geréd Zacherl
Rechtsanwälte GmbH
Museumstraße 5
1070 Wien, Österreich

E-Mail: a.gered@mglp.eu
Web: www.mglp.eu





Gerald Haidvogl
Fujitsu Technology Solutions
Guglgasse 15
1110 Wien, Österreich

E-Mail: gerald.haidvogl@ts.fujitsu.com
Web: http://www.fujitsu.com/at/



Dipl. Ing. Christoph Lang-Muhr
Fachhochschule St. Pölten GmbH
Institut für IT Sicherheitsforschung
Matthias-Corvinus-Straße 15
3100 St. Pölten, Österreich

E-Mail: clangmuhr@fhstp.ac.at
Web: www.fhstp.ac.at/de/studium-weiterbildung/informatik-security





EuroCloud Europe a.s.b.l.
L1013 Luxembourg
7, Rue Alcide de Gasperi. Luxembourg

E-Mail: contact@eurocloud.org
Web: https://.eurocloud.org
Copyright: EuroCloud Europe 2016