Mobile-Device-Management im Zeitalter von IT Consumerization

Fabian Schomm und Gottfried Vossen, Universität Münster

Ob Smartphone oder Tablet, mobile Endgeräte sind auf dem Vormarsch und halten immer mehr Einzug ins geschäftliche Umfeld. In diesem Artikel werden die Trends „IT Consumerization" und „Bring Your Own Device" (BYOD) erklärt sowie deren Möglichkeiten und Risiken aufgezeigt.

Sofern Mitarbeiter sowohl private als auch Firmen-Daten auf ihren Geräten unterhalten, ist eine angemessene Verwaltung der Geräte erforderlich. Der Artikel stellt Mobile-Device-Management-Software sowie deren wichtigste Anbieter vor und ist damit insbesondere für IT-Entscheider in Unternehmen interessant, die einen Einstieg in diese Thematik suchen.

Während eines Meetings die gerade relevanten Unternehmenskennzahlen vom Smartphone abrufen, auf dem Weg nach Hause im Zug noch schnell eine Präsentation fertigstellen, in der Mittagspause Urlaubsfotos von Verwandten ansehen oder einfach nur den Film vom letzten Abend zu Ende gucken: Was vor einigen Jahren in Mitteleuropa – anders als etwa in Japan – noch undenkbar schien und eher nach Science-Fiction klang, ist inzwischen für viele Arbeitnehmer zur Realität geworden. Dafür sind vor allem zwei Trends verantwortlich: zum einen der anhaltende Smartphone-Boom, der sich mittlerweile in Form von Tablets und demnächst als deren Kombination „Phablets" fortsetzt, zum anderen das immer mehr genutzte Angebot von Personal-Cloud-Diensten, die eine nahtlose Integration beliebig vieler Endgeräte erlauben. Dabei ist insbesondere interessant, dass diese Entwicklungen meist nicht aus einem Unternehmenskontext stammen, sondern primär vom Endverbrauchermarkt getrieben werden. Beispielsweise ist BlackBerry nicht mehr das De-facto-Businesshandy. Arbeitnehmer wollen immer häufiger lieber iPhones oder Android-Geräte für ihre Arbeit einsetzen. Dieses Phänomen, dass Endverbraucher ihre IT selbst auswählen (wollen), wird als „IT Consumerization" bezeichnet und gewinnt seit etwa Mitte des Jahres 2010 an Bedeutung. Begleitet wird dieser Trend von Bring Your Own Device (BYOD), einem Modell, bei dem der Arbeitgeber seinen Mitarbeitern erlaubt, private Geräte für die berufliche Tätigkeit einzusetzen. Das fängt bei E-Mails an, reicht aber nicht selten über die Freigabe von Unternehmensdateien bis hin zur Verwendung von Geschäftsanwendungen. Sehr komfortabel ist dabei, dass man nur noch ein einziges Gerät für Privates und Geschäftliches braucht. Das zusätzliche Arbeitshandy kann man sich also sparen.

BYOD wird fälschlicherweise oft mit IT Consumerization gleichgesetzt. Während BYOD lediglich aussagt, dass das verwendete Gerät im Privatbesitz des Mitarbeiters ist, geht es bei IT Consumerization darum, dass der Mitarbeiter die Auswahl über das Gerät trifft. Das kann zusammenfallen, muss es aber nicht. Es gibt auch Modelle, bei denen der Mitarbeiter sich ein Gerät aussuchen darf, das dann vom Unternehmen gekauft und zur Verfügung gestellt wird. Bezeichnet wird das als „Corporate Owned, Personally Enabled" (COPE). IT Consumerization beschränkt sich aber nicht nur auf die Hardware, sondern es gibt auch Software, die im Unternehmenskontext genutzt wird, obwohl sie nicht primär dafür entwickelt wurde, wie etwa Dropbox, Doodle oder auch Twitter.

Dem datenschutzbewussten Leser wird es jetzt vielleicht kalt den Rücken herunterlaufen. Die Vorstellung, dass unternehmensinterne Daten auf mobilen Endgeräten quer durch die Welt getragen oder gleich direkt bei einem Cloud-Dienstleister im Ausland mehrfach repliziert werden, ist in der Tat nicht angenehm. Fakt ist jedoch, dass IT Consumerization und BYOD bereits heute Realität in vielen Unternehmen sind. Selbst wenn der Arbeitgeber explizit verbietet, Derartiges zu praktizieren, wird es immer wieder vorkommen, dass sich jemand nicht dran hält. Es ist halt sehr bequem, sich seine Arbeit mal eben nach Hause zu mailen, um diese dann in Ruhe fertigzustellen.

Vor- und Nachteile von BYOD und IT Consumerization

Die Frage für Arbeitgeber sollte also nicht lauten, wie man diesem Trend entgegenwirken kann, sondern eher, wie man ihn sinnvoll lenken kann, denn es gibt eine ganze Reihe von Vorteilen [1] für beide Seiten. Ein Mitarbeiter, der selbst entscheiden kann, wie und womit er seine Arbeit erledigt, erfährt einen höheren Grad an Autonomie. Außerdem kann BYOD dazu beitragen, dass er kompetenter ist, weil er den Umgang mit der IT bereits privat erlernt hat. All das wirkt sich im Allgemeinen positiv auf die Mitarbeiterzufriedenheit aus, wovon letzten Endes auch der Arbeitgeber profitiert. Darüber hinaus ist ein Mitarbeiter, der nur ein Smartphone für Arbeit und Privates einsetzt, für den Arbeitgeber jederzeit erreichbar, was zu einer schnelleren Reaktionszeit in kritischen Situationen führen kann.

Demgegenüber stehen aber natürlich auch Nachteile. Ein Mitarbeiter, der in seiner Freizeit des Öfteren mit Geschäftlichem konfrontiert wird, empfindet eine höhere Arbeitsbelastung und ist tendenziell früher überlastet. Grund für Bedenken sind jedoch eher Sicherheitsaspekte. Wenn ein Unternehmen seinen Mitarbeitern erlaubt, von beliebigen Geräten auf interne Daten zuzugreifen, erfordert das ein umfassendes Sicherheitskonzept. Für die IT-Abteilungen ergibt sich ein erheblicher Mehraufwand durch die steigende Support-Komplexität,

weil plötzlich eine Vielzahl von Geräten anstatt nur ausgewählter Diensthandys unterstützt werden muss.

Mobile-Device-Management-Software als Lösung

Zu dieser neuartigen Problemstellung gibt es auch bereits Lösungsansätze: „Software für Mobile Device Management" (MDM) bietet die Möglichkeit, eine zentralisierte Verwaltung aller im Unternehmen eingesetzten mobilen Endgeräte einzurichten. Im Folgenden werden die grundlegenden Funktionen von MDM-Software aufgelistet:

- Softwareverteilung
- Zentrale Bereitstellung von Software (In-House App Store), automatische Übertragung, Installation und Wartung (Push Apps)
- Remote-Konfiguration
- Remote-Zugriff zum Auslesen und Einstellen sämtlicher Konfigurationen, Netzwerkinstallation, Push-Benachrichtigungen, gegebenenfalls Abschaltung
- Inventarisierung
- Übersichten über Hardware, Software und Lizenzen
- Möglichkeit für Backup und Restore
- Verschlüsselung
- Endgerätesicherheit
- Konfiguration von Sicherheitsrichtlinien, Fernsperrung/-löschung (Remote Lock & Wipe), Patch-Management
- Containerisierung
- Strikte Trennung zwischen privaten und geschäftlichen Daten und Anwendungen
- Infrastruktur-Kontrolle
- Schutz vor unbefugtem Zugriff auf Unternehmensdienste, Jailbreak-/Root-Erkennung

Damit das alles funktioniert, wird eine Client-App als „Enforcement Agent" auf dem jeweiligen mobilen Endgerät installiert. Neuere Betriebssysteme bieten als Alternative hierzu mittlerweile ein spezielles MDM-API an. Das Mobilgerät kommuniziert mit einem MDM-Server, der entweder on Premise oder als SaaS betrieben wird. Dieser speichert nicht nur sämtliche Daten und Konfigurationen, sondern überwacht auch Zugriffe und Richtlinien.

Obwohl dieser Software-Bereich relativ neu ist, gibt es bereits eine Vielzahl unterschiedlicher Anbieter am Markt. Forbes schätzt, dass derzeit etwa 80 Unternehmen in diesem Bereich tätig sind, während Gartner 20 Hauptanbieter von MDM-Software identifiziert hat [2].

Im Folgenden wird ein kurzer Überblick über die größten und wichtigsten Anbieter von MDM-Software sowie deren Features gegeben. Dieser Überblick ist als Einstieg in die Thematik gedacht. Um eine fundierte Auswahl eines konkreten Anbieters treffen zu können, wird in jedem Fall geraten, sich tiefergehend mit der Marktsituation zu beschäftigen. Die fünf wichtigsten MDM-Anbieter sind:

- MobileIron ist ein Unternehmen aus Kalifornien, das sich vollständig auf Mobility Management spezialisiert hat. Obwohl erst 2007 gegründet, hat es sich mit seiner gleichnamigen Software-Suite schon 2009 als einer der ersten reinen MDM-Anbieter am Markt platziert.
- AirWatch ist ebenfalls ein US-Unternehmen und bietet seine MDM-Software in erster Linie als SaaS an, wobei auch eine On-Premise-Installation möglich ist. Insbesondere angepriesen wird hier die Skalierbarkeit, wodurch es möglich ist, eine sehr große Anzahl von Geräten zu verwalten. Es wird von Fällen berichtet, in denen mehr als 40.000 Geräte eingebunden sind.
- Good Technology aus Kalifornien ist etwas breiter aufgestellt und bietet neben einer dedizierten MDM-Lösung auch Software in den Bereichen „Mobile Collaboration" und „Enterprise Communication". Dadurch wird versucht, nicht nur eine einzige Nische zu auszufüllen, sondern ganzheitlich den Workflow in einem Unternehmen zu unterstützen.
- Fiberlink bietet einen MDM-Service unter dem Namen „MaaS360" an, der rein Cloud-basiert ist. Angefangen in den USA, hat Fiberlink mittlerweile ein großes Partner-Netzwerk, über das eine globale Reichweite angestrebt wird. Bei Kunden aufgefallen sind dabei immer wieder der gute Support sowie die reibungslose Installation.
- Zenprise ist 2003 in Kalifornien gegründet worden und hat sich von Beginn an auf Mobility fokussiert. Als Alleinstellungsmerkmal wird insbesondere der Schutz vor Datenverlust hervorgehoben. Im Januar 2013 wurde Zenprise von Citrix aufgekauft.

Tabelle 1 stellt die wichtigsten Funktionalitäten dieser Anbieter einander gegenüber (mit der Bedeutung „grün" für „vorhanden" beziehungsweise „wird unterstützt" und „rot" für das Gegenteil).

Wie man sieht, unterscheiden sich die Anbieter nicht allzu sehr in ihrem Funktionsumfang. Das liegt unter anderem daran, dass die erreichbare Funktionalität maßgeblich durch die Vorgaben der Betriebssystem-Hersteller limitiert wird. Nichtsdestotrotz versuchen die Anbieter, Alleinstellungsmerkmale herauszustellen, um sich von der Konkurrenz abzuheben. So bietet MobileIron bewusst keine Containerisierung an, um die native Benutzeroberfläche nicht zu beeinträchtigen. Fiberlink hingegen setzt auf eine rein Cloud-basierte Lösung, bei der Nutzer nur wenig konfigurieren müssen, um einen Einstieg so leicht wie möglich zu gestalten.

Ausblick

Es ist zu erwarten, dass sich der Markt in der nächsten Zeit konsolidieren wird. Wie so oft bei neuen technologischen Trends gibt es zuerst eine Fülle an Angeboten, bis sich einige wenige große Anbieter herauskristallisieren, die dann die kleineren aufkaufen oder vom Markt verdrängen. Dabei ist MDM-Software immer abhängig von den Herstellern der mobilen Betriebssysteme. Diese sind bereits dabei, die Containerisierung zur sauberen Trennung von privaten und geschäftlichen Daten selbst zu implementieren. Allen voran ist BlackBerry, das mit der neuen Version 10 und dem integrierten Balance versucht, seine ehemalige Vormachtstellung im geschäftlichen Umfeld wiederzuerlangen. Balance agiert als Trennbarriere für die Daten auf einem Gerät und soll so für maximale Sicherheit sorgen, ohne die Benutzerfreundlichkeit einzuschränken. Samsung entwickelt für seine Galaxy-Geräte ein ähnliches System unter dem Namen „KNOX". Es wird im zweiten Quartal dieses Jahres erwartet.

Denkbar sind auch Hardware-Lösungen im Stile der bei Gebäuden oder Fahrzeugen verbreiteten Keyless-Entry-Systeme. Die Idee ist hier, den Zugang zu Unternehmens-Anwendungen beziehungsweise -Daten auf dem privaten Gerät so zu verschlüsseln,

dass er nur in Gegenwart eines Hardware-Schlüssels erfolgen kann, den der zugangsberechtigte Mitarbeiter bei sich trägt. Eine solche Lösung würde das Problem der Trennung von Privatem und Beruflichem in dem Fall vereinfachen, dass, wenn der betreffende Mitarbeiter das Unternehmen verlässt, lediglich der Schlüssel abgegeben werden müsste.

Quellen

[01] http://www.ercis.org/publication/401
[02] http://www.gartner.com/technology/reprints.do?id=1-1AKKJNN&ct=120518

Fabian Schomm
fabian.schomm@uni-muenster.de

Gottfried Vossen
g.v@wwu.de

	MobileIron	AirWatch	Good	Fiberlink	Zenprise
In-House App Store					
Push Apps					
Remote-Konfiguration					
Push-Benachrichtigungen					
Inventarisierung					
Backup/Restore					
Remote Lock & Wipe					
Containerisierung					
Zugriffskontrolle					
SaaS-Angebot					
On-Premise-Deployment					
Android					
BlackBerry					
iOS					
Symbian					
Windows Phone					

Tabelle 1: grün = vorhanden, rot = nicht vorhanden

Qualitätssicherung in Integrationsprojekten

Dr. Michael Gebhart, Gebhart Quality Analysis (QA) 82

Die Automatisierung von Geschäftsprozessen im Rahmen des Business Process Management erfordert meist die Integration bestehender Anwendungen. Neben der rein technischen Umsetzung wird von Integrationsprojekten dabei zunehmend gefordert, eine flexible und wartbare Lösung zu erstellen, wobei die Realisierung gleichzeitig kosteneffizient zu erfolgen hat. Um die qualitativen Eigenschaften sicherzustellen, ist eine Abstimmung zwischen allen Beteiligten erforderlich, die wiederum mit hohem Aufwand einhergeht. Der vorliegende Artikel zeigt daher auf, wie die Erstellung eines Qualitätsmodells dabei helfen kann, die Qualitätssicherung in Integrationsprojekten zu strukturieren und gleichzeitig die Effizienz zu steigern.

Unternehmen streben zunehmend eine Automatisierung von Geschäftsprozessen im Rahmen eines ganzheitlichen Business Process Management (BPM) an. Ziel ist es dabei, die Geschäftsprozesse zu optimieren und gleichzeitig die Kosten für die Durchführung zu reduzieren. Aufgrund der steigenden Zahl betriebener Anwendungen, die in den Geschäftsprozessen genutzt werden sollen, resultieren derartige Vorhaben verstärkt in Integrationsprojekten. Neben der rein technischen Umsetzung, also der technischen Integration von Anwendungen in neu umzusetzende Geschäftsprozesse, sind mit derartigen Projekten jedoch auch strategische Ziele verknüpft: So geht damit häufig auch eine Restrukturierung der IT einher, wie es insbesondere beim Wechsel hin zu serviceorientierten Architekturen der Fall ist. Unabhängig von dem Paradigma wird von der resultierenden IT-Architektur ein hohes Maß an Nachhaltigkeit erwartet, sodass diese auf der einen Seite kostengünstig gewartet werden kann, sich aber auch flexibel an neue geschäftliche Anforderungen anpassen lässt.

Gleichzeitig hat sich in der Vergangenheit der Druck auf die Softwarebranche weiter erhöht. So wird verlangt, dass derartige Lösungen in noch kürzerer Zeit mit noch geringeren Kosten umgesetzt werden können. Bei Projekten dieser Größe sind eine regelmäßige Abstimmung zwischen allen Beteiligten sowie eine Qualitätssicherung