Gerhard Klett

Heinrich Kersten

Mobile IT-Infrastrukturen

Management, Sicherheit und Compliance

Hinweis des Verlages zum Urheberrecht und Digitalen Rechtemanagement (DRM)

Gerhard Klett, Heinrich Kersten

Mobile IT-Infrastrukturen

Management, Sicherheit und Compliance

Bibliografische Information der Deutschen Nationalbibliothek
Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über <http://dnb.d-nb.de> abrufbar.

ISBN 978-3-8266-9634-3
1. Auflage 2015

www.mitp.de
E-Mail: mitp-verlag@sigloch.de
Telefon: +49 7953 / 7189 - 079
Telefax: +49 7953 / 7189 - 082

Lektorat: Sabine Schulz, Ernst-Heinrich Pröfener
Sprachkorrektorat: Petra Heubach-Erdmann
Coverbild: © marrakeshh
Satz: III-satz, Husby, www.drei-satz.de

Inhaltsverzeichnis

Mobile Infrastrukturen

Einleitung

Smartphones, Tablets/Pads, Netbooks, Laptops und ähnliche Geräte, die auf Reisen weltweit, in Verkehrsmitteln, an »fremden« Arbeitsplätzen, auf Konferenzen oder im Home-Office genutzt werden können, bezeichnet man als *mobile IT-Systeme*.

Sind Sie schon im Besitz eines sogenannten *Wearables*, eines am Körper zu befestigenden, tragbaren Geräts zur Datenverarbeitung? Die Frage wird sicher oft bejaht, denn Headsets gehören zum Beispiel seit vielen Jahren zur Peripherie von Smartphones und werden zum großen Teil als Freisprecheinrichtungen geschäftlich genutzt. Wearables wie Datenbrillen (»Google Glass«), Armbänder und Armbanduhren (»Gear Fit«, »Smartwatch«) sind auf diesem Gebiet die aktuellen Weiterentwicklungen der tragbaren Computer-Peripherie, die am Körper zu befestigen sind.

Viele der oben genannten Systeme sind sehr leistungsfähig und warten auf der Hardware-Seite mit Dual-/Quad-Core-Prozessoren und hohen Grafikauflösungen auf. Auf der Seite der Betriebssysteme sind u.a. iOS, Android, Blackberry OS (mit Unix-basierten Kernels) und proprietäre Systeme wie Windows Phone im Einsatz.

Dass solche Systeme eine immer stärkere Verbreitung in Unternehmen und bei Privatpersonen finden, ist verständlich, wenn man an ihre attraktiven Leistungsmerkmale denkt:

- die Möglichkeit der Einbindung in soziale Netzwerke und Unternehmensnetze
- die Synchronisation von Kalendern, E-Mail, Notizen, Fotos etc. über verschiedene mobile und stationäre Plattformen
- die Nutzung von Cloud-Services als Backup oder zur Synchronisation mit anderen Systemen
- Geo-Dienste (Standortbestimmung/Ortung, Routenplanung und -verfolgung, Verfolgen von Flug- und Schiffsverkehr) u.v.m.

Viele dieser Features werden durch Apps erbracht, die aus App Stores geladen und installiert werden können. Inzwischen sind auch leistungsfähige Software-Pakete wie z. B. Microsoft Office für mobile Systeme verfügbar und machen die Bearbeitung von Dokumenten – synchronisiert über mehrere Plattformen und sogar simultan mit mehreren Nutzern – möglich.

Alle diese Geräte haben zusammen mit drahtlosen Netzen und Clouds das Ziel, komplexe Datenverarbeitung mit hoher Mobilität ortsunabhängig zu gewährleisten. Sie bilden eine *mobile IT-Infrastruktur,* die derzeit mit den traditionellen, stationären IT-Infrastrukturen von Unternehmen und Organisationen koexistiert und immer engmaschiger mit diesen verflochten wird. Oft nicht geplant und organisiert gewachsen, sondern proliferiert, sind mobile Infrastrukturen unverzichtbarer Teil der IT von Mittelstand und Konzernen geworden, über die immer mehr essenzielle, kritische Geschäftsprozesse wegen der hohen Mobilität der Entscheidungsträger abgewickelt werden.

Mobile IT-Systeme haben andererseits differenzierte Sicherheits- und Datenschutzprobleme. Sie sind zunächst nichts anderes als vernetzte IT-Systeme, das heißt, sie unterliegen den bekannten Risiken der Informationsverarbeitung. Gerade aber die hohe Konnektivität und die Vielfalt der Anwendungen machen diese Systeme anfällig für eine Vielzahl von Attacken wie Phishing, Data Leakage, Trojaner, Abhören/Mitschneiden von Kommunikationsinhalten, »Knacken« von Sicherheitseinstellungen usw. Darüber hinaus birgt die Mobilität als solche weitere Risiken: das Verlieren und der Diebstahl von Geräten, das Whaling, die letztlich unbefugte Nutzung durch Fremde, Familienangehörige, Kollegen – mit der Folge, dass in den Geräten gespeicherte sensible Daten (auch Zugangscodes) in unbefugte Hände gelangen oder sogar ein weitergehender Durchgriff auf Unternehmensnetze möglich ist. Je nach Plattform ist auch die Installation von Apps nicht risikofrei, da die jeweiligen App-Entwickler in der Lage sind, verdeckte Funktionen einzubauen, um sensible Daten abzuziehen und Zugriff zu Unternehmensnetzen zu erhalten. Die meist integrierte Nutzung von Cloud-Services trägt ein weiteres Risiko: Wie vielfach berichtet wurde, werden bei den Anbietern der Clouds gespeicherte Daten von den jeweiligen Geheimdiensten abgegriffen.

Bis zu einem gewissen Grad lassen sich mobile IT-Systeme durch geeignete Konfiguration und Aktivierung von eingebauten Sicherheitsfunktionen sicherheitstechnisch »härten«. Für Unternehmen ist es von Vorteil, wenn

hierzu standardisierte Regelsätze (*Security Policies*) erstellt und in die genutzten mobilen Systeme ausgerollt werden können. Ergänzende organisatorische Sicherheitsmaßnahmen findet man häufig in Sicherheitsrichtlinien für mobiles Arbeiten – mit typischen Vorgaben wie, die Systeme verstärkt zu beaufsichtigen, keine öffentlichen Hotspots ungesichert zu nutzen usw.

Der Trend zu BYOD = *Bring Your Own Device* greift um sich: Immer mehr Nutzer wollen ihre eigenen mobilen Geräte auch für dienstliche Zwecke nutzen. Gerade die dienstliche Nutzung privater mobiler Geräte verursacht massive Datenschutzprobleme, da eine präzise Trennung von privaten und geschäftlichen Daten kaum möglich ist, Arbeitgeber andererseits aber eine gewisse Aufsicht und Kontrolle der betrieblichen Nutzung verlangen. Weitere rechtliche Fragen betreffen Nutzungsverträge, finanzielle Kompensationen, Inspektionsrechte und Haftung.

Die sich nicht zuletzt mit BYOD ergebende Vielfalt mobiler Geräte im Unternehmen und ihre technischen Unterschiede machen es schwer, einheitliche Vorgaben und Richtlinien umzusetzen und ihre Einhaltung zu überwachen. Mit spezialisierten *MDM*[1]*-Systemen* lassen sich zentrale Management-Funktionen etablieren, und zwar

- die Inventarisierung aller verwendeten mobilen Geräte
- die Erstellung von Security Policies und ihr automatisiertes Ausrollen in die mobilen Systeme
- Backup und Restore für mobile Systeme
- ein Patch-Management für die verwendeten Betriebssysteme und Apps
- das Management von Zertifikaten und Schlüsseln für den sicheren Zugang zum Unternehmensnetz und für die Datenverschlüsselung
- das Monitoring der Nutzung mobiler Geräte und der Einhaltung von Vorgaben

Alle Prozesse und Einrichtungen eines Unternehmens, die dem Zweck dienen, mobile IT-Systeme in die Geschäftsprozesse einzubinden, fasst man unter dem Begriff *mobile IT-Infrastruktur* zusammen. *Mobile Device Management* (MDM) kümmert sich um die Planung, Einrichtung, den Betrieb und die Überwachung einer solchen mobilen IT-Infrastruktur.

1. MDM = Mobile Device Management

Mobile Device Management ist allein nicht ausreichend – was auch durch einen Blick auf die wichtigsten IT-Prozesse beispielsweise nach COBIT oder ITIL bestätigt wird: Während für die traditionellen IT-Infrastrukturen Standards existieren, organisatorische Prozesse für effiziente Abläufe und Sicherheit sorgen und im Laufe der Jahrzehnte optimiert wurden, fehlt, wie es häufig in der Praxis der Fall ist, die strukturierte Integration von *mobilen* IT-Infrastrukturen in diese Prozesse. Folglich werden wichtige IT-Prozesse nicht oder nur halbherzig gelebt.

Eines der klassischen Themen ist beispielsweise die Business-Continuity-Planung. Was passiert, wenn zwar die darin behandelten kritischen Geschäftsprozesse, die beispielsweise durch SAP-Module unterstützt und von entsprechenden Apps auf Tablets oder Smartphones gesteuert werden, aber nicht die dabei verwendeten Endgeräte, Apps und Kommunikationsmedien Gegenstand der mit der Business-Continuity-Planung einhergehenden Notfallplanung waren? Die Folgen für die Business Continuity können gravierend sein und müssen vorab genau analysiert werden (Business Impact Analysis).

Fazit: Ein Unternehmen muss für den Aufbau und die Nutzung einer mobilen Infrastruktur »größer« denken und vielen Aspekten Rechnung tragen – darunter

- die vertragliche/juristische Ausgestaltung (Zugang durch Geschäftspartner, Nutzung externer Clouds, Geräte-Vorhaltung durch Lieferanten bei Verlust/Ausfall, BYOD oder ähnliche Strategien)
- die Konzeption und Umsetzung von IT-Sicherheit und Datenschutz
- das Mobile Device Management
- das *betriebliche* Management der mobilen Infrastruktur
- die Integration der mobilen Infrastruktur in Unternehmensprozesse, z. B. in die Business Continuity
- Awareness-Programme und Sicherheitstrainings
- die unmittelbaren Kosten und die Folgekosten der mobilen Infrastruktur sowie eine Kosten-Nutzen-Analyse

Die Fachwelt hat für diese Erweiterung des Mobile Device Managements bereits den etwas »schwammigen« Begriff *Enterprise Mobility Management* (EMM) kreiert[2].

2. *http://en.wikipedia.org/wiki/Enterprise_mobility_management*

Mobile IT ist wie die stationäre IT kein Selbstzweck: Sie soll die Geschäftsprozesse des Unternehmens optimal unterstützen und ggf. bestehende Risiken in Einklang mit den Geschäftserfordernissen bringen. Dies umreißt Aufgaben der Leitung und des oberen Managements in Unternehmen, die unter dem Begriff *IT Governance* bekannt sind. Zur Steuerung dieser Aufgabe werden interne Kontrollsysteme eingerichtet, z. B. basierend auf dem sogenannten COBIT-Framework: Ausgehend von den Geschäftserfordernissen werden alle erforderlichen, die IT betreffenden Aktivitäten in eine standardisierte Prozesslandschaft integriert. Vor diesem Hintergrund erkennt man: Eine mobile Infrastruktur hat Auswirkungen bis in die IT Governance hinein und stellt letztlich eine beachtliche Herausforderung für ein Unternehmen dar.

Inhalt

Im ersten Band dieser Reihe [KK2012a] berichteten wir über Mobile Device Management als wichtigen Bestandteil für den geordneten, sicheren Betrieb von mobilen Infrastrukturen. In dem vorliegenden Werk wollen wir weitere wichtige Komponenten vorstellen und ihre Übertragung auf mobile Infrastrukturen – einschließlich der Überprüfung auf Wirksamkeit und Vollständigkeit – behandeln.

Im Einzelnen:

Aktuelle Zahlen und Fakten zu mobilen Systemen, zu Mobile Device Management und Enterprise Mobility Management bilden den Anfang in Kapitel 1.

In Kapitel 2 behandeln wir die relevanten Komponenten und Ebenen von mobilen Infrastrukturen und beschreiben die von ihnen ausgehenden Einflüsse auf die IT-Prozesse in Unternehmen.

Auch wenn die einzelnen mobilen Geräte als solche nicht Gegenstand dieses Buchs sind, ist eine detaillierte Betrachtung der Charakteristika dieser Komponenten erforderlich. Dies ist der Gegenstand von Kapitel 3.

Die teilweise signifikanten Unterschiede zwischen stationären und mobilen Infrastrukturen sowie ihre Auswirkungen auf die Betriebsprozesse stehen in Kapitel 4 im Fokus.

Die Aufgabe, die mobile Infrastruktur mit geeigneten Sicherheitsmaßnahmen auszustatten, um die wesentlichen Schwachstellen und daraus resultierende Risiken abzudecken, beschäftigt uns in Kapitel 5.

Einem zentralen Bestandteil mobiler Infrastrukturen, den Cloud-Services, widmet sich Kapitel 6 und stellt die Architekturen, Anforderungen und die Einbindung in Sicherheitskonzepte dar.

In Kapitel 7 analysieren wir mobile Infrastrukturen daraufhin, welche Einflüsse sie auf existierende Betriebsprozesse der IT haben bzw. was hier zu ergänzen ist.

Die Überwachung mobiler Infrastrukturen durch Monitoring, Kennzahlen, technische und Management-Audits sowie Managementbewertungen ist das Thema von Kapitel 8.

In Fortsetzung eines Beispiels für ein MDM-System aus dem ersten Band *Mobile Device Management* [KK2012a] beschreiben wir in Kapitel 9 weitere marktgängige Produkte aus dieser Kategorie.

Gerhard Klett

Heinrich Kersten

im Oktober 2014

1 Zahlen und Fakten

1.1 Firmware

Mit Firmware wird bei mobilen Endgeräten der Anteil des Betriebssystems bezeichnet, der auf die Hardware in dem Gerät angepasst ist und mit dem Gerät durch Laden in einen Flash-Speicher fest verbunden wird. Die Firmware ist gegen Manipulationen durch Verschlüsselung, elektronische Signaturen und herstellerspezifische Ladeprogramme (»Bootloader«) geschützt. Allerdings gibt es gegen jeden Schutz auch Angriffsmöglichkeiten; in diesem Fall ist es Software für »Jailbreaks« und »Rooting« für iOS- und Android-Geräte, die eine Manipulation der Firmware ermöglichen.

Die Firmware für mobile Endgeräte ist entweder eine Neuentwicklung eines Herstellers oder stammt aus einer bereits existierenden Bibliothek:

- iOS, Android und Blackberry OS 10 sind in ihrem Kern Ableger (»Derivate«) von Unix-Systemen.
- Der Kernel von Windows Phone ist eine Eigenentwicklung von Microsoft.

Android, iOS und Windows Phone dominieren zurzeit den Markt für mobile Firmware, wesentlich kleiner ist der Marktanteil von Blackberry OS10.

Period	Android	iOS	Windows Phone	BlackBerry OS	Others
Q2 2014	84.7%	11.7%	2.5%	0.5%	0.7%
Q2 2013	79.6%	13.0%	3.4%	2.8%	1.2%
Q2 2012	69.3%	16.6%	3.1%	4.9%	6.1%
Q2 2011	36.1%	18.3%	1.2%	13.6%	30.8%

Abbildung 1.1: Marktanteile mobiler Betriebssysteme (1)[1]

1. *http://www.idc.com/prodserv/smartphone-os-market-share.jsp*

Android hat in den letzten Jahren seinen Marktanteil sehr stark vergrößern können und ist heute der absolute Marktführer unter den mobilen Betriebssystemen, während der Marktanteil von Blackberry als ehemaligem Pionier der geschäftlichen Nutzung von mobilen Endgeräten dramatisch gesunken ist.

Eine weitere Grafik zeigt dies sehr deutlich.

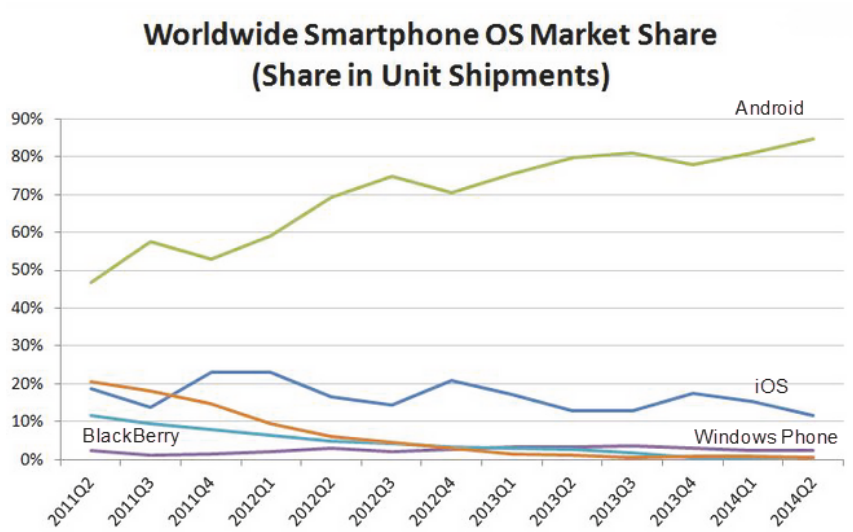

Abbildung 1.2: Marktanteile mobiler Betriebssysteme (2)[2]

Wie später näher erläutert wird, ist die Tatsache, dass es nicht nur *ein* Android, sondern viele in unterschiedlichen Versionen gibt, problematisch für einen möglichst homogenen Aufbau der mobilen Infrastruktur und die einheitliche Administration mit einem Enterprise Mobility Management (EMM).

Die nächste Grafik verdeutlicht die Anteile unterschiedlicher Versionen von Android ohne Berücksichtigung von Branding der Mobilfunk-Anbieter und Hardware-Hersteller, was die Heterogenität natürlich weiter erhöht und gerade bei einer BYOD-Beschaffungsphilosophie sehr problematisch bezüglich der Administrierbarkeit ist.

2. *http://www.idc.com/prodserv/smartphone-os-market-share.jsp*

Version	Codename	API	Distribution
2.2	Froyo	8	0.7%
2.3.3 - 2.3.7	Gingerbread	10	11.4%
4.0.3 - 4.0.4	Ice Cream Sandwich	15	9.6%
4.1.x	Jelly Bean	16	25.1%
4.2.x		17	20.7%
4.3		18	8.0%
4.4	KitKat	19	24.5%

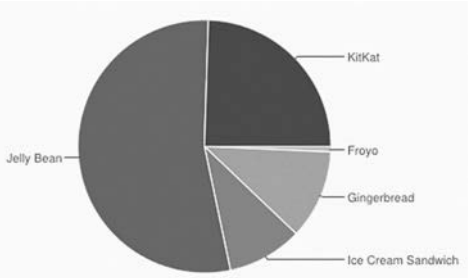

Abbildung 1.3: Verteilung eingesetzter Android-Versionen[3]

1.2 Apps und App Stores

Das von Apple 2008 eingeführte Internet-Verkaufsportal für Programme, die nur auf Apple-Hardware lauffähig sind, ist mittlerweile für fast alle Anbieter in diesem Segment zur Schablone avanciert. Der App Store ist auf der Infrastruktur des iTunes Stores aufgebaut. Apps für Apple-Geräte mit Status »unjailbroken« können nur über diesen App Store oder iTunes gekauft und verwaltet werden.

Der App Store ist riesig, ist aber von Googles Play Store für Android-Apps mittlerweile eingeholt worden.

Im Windows Phone Store sollen sich aktuell mehr als 300.000 Apps[4] befinden; der Appstore von Blackberry, Blackberry World, verzeichnet rund 240.000 Apps, wobei allerdings ca. 20 % davon Android-Apps sein sollen, die in einem Emulator laufen[5].

3. *http://developer.android.com/about/dashboards/index.html*, Stand August 2014
4. *http://www.zdnet.de/88201595/microsoft-meldet-mehr-als-300-000-apps-im-windows-phone-store/*
5. *http://de.wikipedia.org/wiki/Blackberry_World*

Date	Downloads Per Day	Downloads to date	Available Apps[12]
July 30, 2010[13]	1,000,000		10438
September 27, 2010[13]	1,500,000		
February 14, 2011[13]	2,000,000		26179
March 22, 2011[13]	3,000,000		
July 12, 2011[14]	3,000,000	1,000,000,000	36781
February 7, 2012[15]	6,000,000	2,000,000,000	67310
July 8, 2012[16]	6,000,000+	3,000,000,000	77501
March 31, 2013	6,000,000+	4,000,000,000	135,000 [17]
April 23, 2014			234,500 [18]

Abbildung 1.4: Apps in Blackberry World[6]

Year	Month	Applications available	Downloads to date
2009	March	2,300[66]	
	December	16,000[70]	
2010	March	30,000[71]	
	April	38,000[72]	
	August	80,000[73][74]	1 billion
	October	100,000[75]	
2011	May	200,000[67]	3 billion[76]
	July	250,000[77]	6 billion
	October	319,000[78]	
	December	380,297[79]	10 billion[80]
2012	January	400,000[81]	
	February	450,000[82]	
	May	500,000[83]	
	June	600,000	20 billion[84]
	September	675,000	25 billion[85]
	October	700,000[68]	
2013	February	800,000[86]	
	April	850,000	40 billion
	May		48 billion[87]
	July	1,000,000[69]	50 billion[69]
2014	June	1,200,000[88]	
	July	1,300,000[25]	

Abbildung 1.5: Google Play Store[7]

6. *http://en.wikipedia.org/wiki/Blackberry_World*
7. *http://en.wikipedia.org/wiki/Google_Play*

Date	Available apps	Downloads to date	Average downloads per app
July 11, 2008[42]	500	0	0
July 14, 2008[38]	800	10,000,000	12,500
September 9, 2008[43]	3,000	100,000,000	18,334
October 22, 2008[44]	7,500	200,000,000	26,667
January 16, 2009[39]	15,000	500,000,000	33,334
March 17, 2009[45]	25,000	800,000,000	32,000
April 4, 2009[40]	35,000	1,000,000,000	28,571
June 8, 2009[46]	50,000	1,000,000,000+	~20,000
July 11, 2009[*citation needed*]	55,000	1,000,000,000+	~18,182
July 14, 2009[47]	65,000	1,500,000,000	23,077
September 9, 2009	75,000	1,800,000,000	24,000
September 28, 2009[48][49]	85,000	2,000,000,000	23,529
November 4, 2009[50][51]	100,000	2,000,000,000+	~20,000
January 5, 2010[52][53]	120,000	3,000,000,000+	~25,000
March 20, 2010[54]	150,000+	3,000,000,000+	~20,000
April 8, 2010[55]	185,000+	4,000,000,000+	~21,622
April 29, 2010[56]	200,000+	4,500,000,000+	~22,500
June 7, 2010[57]	225,000+	5,000,000,000+	~22,222
September 1, 2010[58]	250,000+	6,500,000,000+	~26,000
October 20, 2010	300,000+[59]	7,000,000,000[60]	~23,334
Jan 22, 2011[61]	350,000+	10,000,000,000+	~28,571
June 6, 2011[4]	425,000+	14,000,000,000+	~32,941
July 7, 2011[7]	425,000+	15,000,000,000+	~35,294
October 4, 2011[62]	500,000+	18,000,000,000+	~36,000
February 28, 2012	500,000+	24,000,000,000+	~40,000
March 3, 2012[63]	500,000+	25,000,000,000+	~50,000
March 5, 2012[64]	550,000+	25,000,000,000+	~45,455
March 7, 2012[*citation needed*]	585,000+	25,000,000,000+	~42,735
June 11, 2012[65]	650,000+	30,000,000,000+	~46,154
September 12, 2012[66]	700,000+[66]	35,000,000,000+[67]	~50,000
January 7, 2013[68]	775,000+[68]	40,000,000,000+[68]	~51,613
January 28, 2013[69]	800,000+[69]	40,000,000,000+[68]	50,000
April 23, 2013	825,000+	45,000,000,000+	50,000
May 16, 2013	850,000+	50,000,000,000+[70]	50,000
June 10, 2013	900,000+	50,000,000,000+	50,000
October 22, 2013	1,000,000+[71]	60,000,000,000+[71]	60,000
June 2, 2014	1,200,000+[1]	75,000,000,000+	62,500

Abbildung 1.6: Apple App Store[8]

8. *http://en.wikipedia.org/wiki/App_Store_(iOS)*

1.3 MDM-Systeme

MDM-Systeme sind in Unternehmen und Organisationen noch nicht flächendeckend verbreitet, ihr Einsatz hängt unmittelbar mit dem Aufbau von mobilen Infrastrukturen und dem anhaltenden Trend zu BYOD zusammen. Gartner schätzt in einer Studie zu diesem Thema, dass bis 2017 zwei Drittel aller Unternehmen und Organisationen MDM-Systeme einsetzen werden.[9]

Viele Prozesse, wie in den folgenden Kapiteln dargestellt, werden technisch von MDM-Systemen unterstützt. Beispielsweise ist der Prozess des Sicherheitsmanagements für mobile Endgeräte und Anwendungen ohne MDM-Systeme nicht realisierbar.

In Bezug auf IT-Sicherheit bedeuten mobile Infrastrukturen eine signifikante Erhöhung des Risikos, denn in beinahe allen Fällen werden nach einer Studie die beruflich eingesetzten Geräte auch privat verwendet.

> *»So setzen nur 1 Prozent der Befragten ihre Smartphones und Tablets ausschließlich beruflich ein. 17 Prozent der Deutschen nutzen mobile Geräte beruflich und privat, 35 Prozent verwenden sie ausschließlich privat und etwa die Hälfte der Deutschen (48 Prozent) besitzt aktuell (2012) kein solches Gerät. Ein weiteres Risiko: 41 Prozent der Befragten, die ihre mobilen Geräte beruflich verwenden, synchronisieren ihre Daten selten oder nie mit einem Server. Bei einem Verlust des Geräts sind viele Daten also nicht an anderer Stelle vorhanden, sondern endgültig verloren. Handlungsbedarf besteht auch bei weiteren Sicherheitsmaßnahmen wie regelmäßigen Updates von Apps und Betriebssystem sowie dem Einsatz von Virenschutz- oder Sicherheitssoftware.«*[10]

Daran dürfte sich auch 2014 nicht sehr viel geändert haben. Das ist gerade im Hinblick auf die weitverbreiteten Android-Apps besorgniserregend, da hier die Zahl der mit Malware verseuchten Apps sehr hoch ist[11]. Die Nachlässigkeit bei der Synchronisation oder dem Backup der Daten auf den mobilen Endgeräten ist in Anbetracht der hohen Verlustraten durch Diebstahl oder Verlieren

9. *http://www.gartner.com/newsroom/id/2213115*
10. *http://www.computacenter-newsroom.de/wp-content/uploads/2012/02/2012-02-23-Studie-Mobile-Ger%C3%A4te-Sicherheitsrisiko-f%C3%BCr-Unternehmen.pdf*
11. *http://www.chip.de/news/Malware-Viele-Android-Apps-sind-verseucht_71277242.html*

der Endgeräte ebenfalls ein sehr ernstes Problem innerhalb des Sicherheitsmanagements.[12]

Wie sieht es nun mit diesem Hintergrund an Risiken mit einer Strategie für MDM in den Unternehmen aus? Hierzu gibt Abbildung 1.7 einen Hinweis.

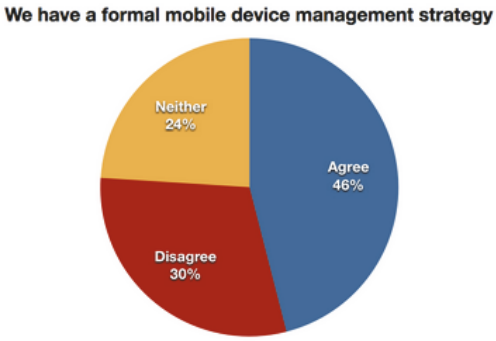

Abbildung 1.7: Befragung von 300 IT-Verantwortlichen im Jahr 2012[13]

Demnach gaben nur 46% der Befragten an, eine formale Strategie für das Mobile Device Management zu haben – was nicht bedeutet, dass ein solches System bereits zu diesem Zeitpunkt in Betrieb war. Die nächste Grafik aus dem Jahr 2013 gibt darüber Aufschluss.

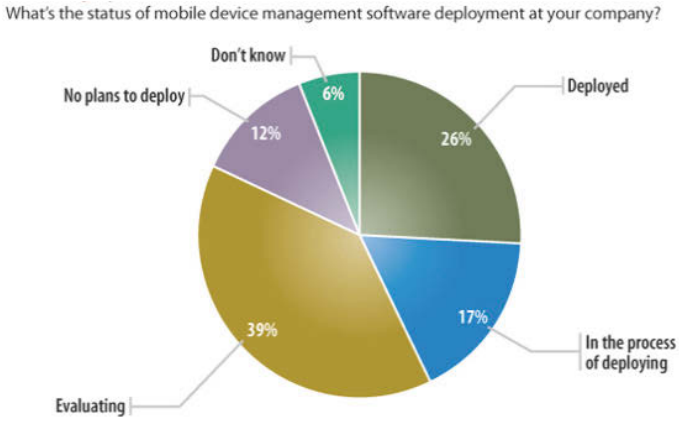

Abbildung 1.8: Bereitstellung von MDM-Software in Unternehmen[14]

12. *http://business.chip.de/news/Handy-Diebstahl-236.500-Geraete-im-Jahr-gestohlen_72428096.html*
13. *http://www.businessinsider.com/how-companies-are-managing-the-explosion-of-mobile-devices*
14. *http://blog.theimf.com/2013/01/your-priority-securing-the-device-or-the-data/*

Nur bei rund 26% der 306 Befragten war eine entsprechende Software im Unternehmen oder der Organisation verteilt und bereitgestellt, der größte Anteil mit 39% war mit der Evaluierung beschäftigt.

Diese Aufteilung findet sich auch in den Reports von Gartner über MDM-Systeme.

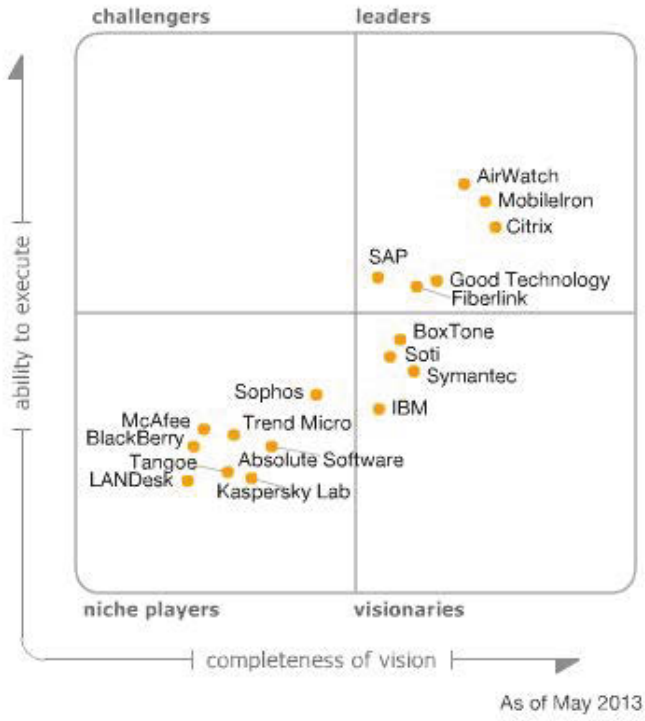

Abbildung 1.9: Gartner Quadrant Mobile Device Management Software[15]

Während im Jahr 2013 Gartner in seiner Quadranten-Darstellung noch zahlreiche Nischen-Anbieter, überwiegend Firmen mit Schwerpunkt auf Sicherheits-Software auflistet, hat sich das Bild 2014 mit dem Eintritt von Enterprise Mobility Management (EMM) sehr geändert: Aus MDM wird EMM.[16]

15. *http://www.cio.de/knowledgecenter/mobile_it/2918587/*
16. *http://blog.mwayconsulting.com/aus-mdm-wird-emm-gartner-magic-quadrant-2014/*

Abbildung 1.10: Magic Quadrant for Enterprise Mobility Management Suites[17]

Basis von EMM sind MDM-Systeme mit erweiterten Funktionen für

- Hardware-Inventarisierung
- Bestandsaufnahme der Anwendungen
- OS-Konfigurationsmanagement
- Mobile-App-Bereitstellung, Aktualisierung und Löschung
- Mobile-App-Konfiguration und Richtlinienverwaltung
- Fernsteuerung des mobilen Endgeräts für die Fehlersuche

17. *http://www.gartner.com/technology/reprints.do?id=1-1UWW5XX&ct=140603&st=sb*

- ferngesteuerte Ausführung und Überwachung von Administrationsvorgängen
- Mobile Content Management

Die Zahl der Anbieter dieser betrachteten Systeme ist überschaubar und erscheint gegenüber dem Quadranten 2013 für MDM sehr ausgedünnt: Die Firmen aus dem Sicherheitssektor mit ihrem Schwerpunkt auf Endpoint Security fehlen hier fast vollständig.

2 Komponenten mobiler Infrastrukturen

In diesem Kapitel beginnen wir mit der Einführung der relevanten Komponenten von mobilen Infrastrukturen und den von ihnen ausgehenden Einflüssen auf IT-Prozesse in Unternehmen und Organisationen. In den nachfolgenden Kapiteln werden die daraus resultierenden Rahmenbedingungen, Aufwendungen und Maßnahmen für die Integration der Komponenten in die Gesamt-IT dargestellt.

Beginnen wir mit einer kurzen allgemeinen Darstellung der Ebenen und Sichten von IT-Infrastrukturen, auf denen IT-Prozesse mit dem vorrangigen Ziel aufbauen, den sicheren Betrieb von Anwendungssoftware unter festgelegten Qualitätskriterien zu ermöglichen.

Für die nachfolgende Aufstellung der wichtigsten IT-Prozesse bedienen wir uns der weitverbreiteten Standard-Prozessmodelle nach COBIT und ITIL.

2.1 Ebenen und Sichten der IT-Infrastruktur

Zwecks einer übersichtlichen Darstellung teilen wir IT-Infrastrukturen in mehrere Ebenen auf, die wir unter zwei Sichtweisen betrachten:

1. Aus technischer Sicht besteht die IT-Infrastruktur aus Hardware, Software sowie aus Gebäuden und dazugehöriger Gebäudetechnik wie etwa Klimatisierung, Energieversorgung, Überwachung etc. – kurz, allen baulichen Einrichtungen, die für den effizienten Betrieb von Anwendungssoftware benötigt werden.

   Zur Hardware gehören die eigentliche Technik für die Datenverarbeitung (Server und Speicher), die Zugangsnetzwerke (Gateways, Router Switches, Verkabelung etc.), Peripheriegeräte (Endgeräte, Drucker, Scanner) sowie weitere Einrichtungen zum Betrieb der Hardware wie zum Beispiel Schaltschränke und unterbrechungsfreie Stromversorgungen.