

Link: <https://www.channelpartner.de/a/mobiles-arbeiten-sicherer-gestalten,3042527>

**Mobility in Unternehmen**

## **Mobiles Arbeiten sicherer gestalten**

Datum: 10.06.2014

Autor(en): Kai Haller

**Sie sind praktisch. Sie sind effektiv. Aber wie ist es um die IT- Sicherheit in Unternehmen bestellt, wenn sich Smartphones, Tablets und Apps zu einem festen Bestandteil der IT-Infrastruktur entwickeln?**

Mobility steht im Fokus der digitalen Kommunikation. Das Thema weckt Bedürfnisse bei Privatanwendern und in Unternehmen. Charmant ist, dass sich digitale Inhalte immer komfortabler über mobile Endgeräte wie Smartphones und Tablets austauschen lassen. Deshalb eignen sich mobile Endgeräte gut für den Einsatz im betrieblichen Umfeld; zudem können die die mobilen Helfer die Produktivität und Motivation der Belegschaft steigern.

Da spielt das Gewicht dieser Geräte im Vergleich zu herkömmlichen Laptops als Optimierung noch die geringste Rolle. Insbesondere haben sich Nutzer an die unkomplizierte Technik von mobilen Endgeräten inklusive der Nutzung von Apps gewöhnt. Das führt zwangsläufig zu einer höheren Erwartungshaltung bei Nutzern, die in ihrem Arbeitsalltag ebenfalls eine bequeme und moderne Kommunikation wünschen.

Private Bedürfnisse sind meistens mit Abschluss eines Mobilfunkvertrags schnell befriedigt, aber was können Unternehmen ihren Mitarbeitern diesbezüglich bieten? Unternehmen stehen vor der großen Herausforderung, ihre IT-Infrastruktur weiterhin sicher, mobilitätstauglich und nachhaltig zu gestalten, um so Arbeitsbedingungen zu schaffen, die zeitgemäß und effektiv sind. An dieser Stelle gilt es die richtigen Entscheidungen zu treffen, denn die Auswirkungen können weitreichend sein.

Ein besonders sensibles Thema ist die Absicherung von Unternehmensdaten gegen unbefugten Zugriff und Verlust durch den sicheren Einsatz von Endgeräten und Anwendungen (Apps). Hinzu kommen weitere Themen wie Effizienz, Verwaltung, Synchronisation, Haftung oder arbeitsrechtliche Fragen, die ebenfalls eine wichtige Rolle spielen. Ziel sind die bestmöglichen Rahmenbedingungen, um die Erreichung der Unternehmensziele sicher zu stellen und realistische Strategien für die zukünftige Modernisierung des Geschäftsbetriebes zu schaffen. Genau an dieser Stelle, vor der Integration von Enterprise Mobility Management (EMM), besteht für Unternehmen die größte Gefahr und es können unnötige Fehler und nachgelagerte Zusatzkosten vermieden werden. Denn den meisten Unternehmen fehlt eine nachhaltige Strategie als Basis für die täglichen Workflows.

[Hinweis auf Bildergalerie: **Sieben Schritte zum MDM** - ] <sup>gal1</sup>

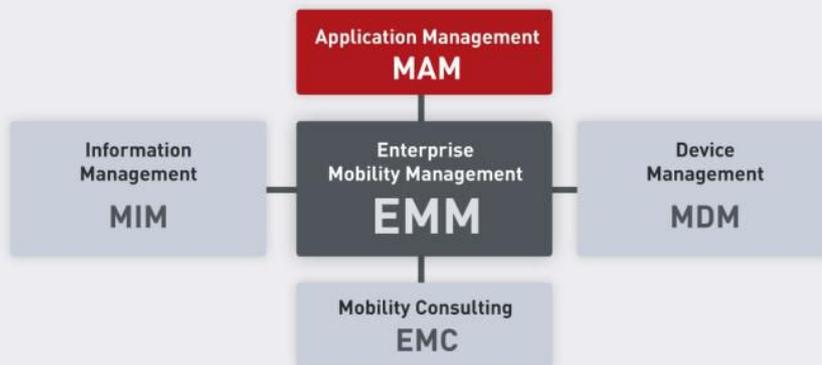
### **Wie gehen Unternehmen heute vor?**

Zu Beginn ist anzumerken, dass Unternehmen nicht per se schwerwiegende Fehler begehen, wenn sie sich mit dem Thema Enterprise Mobility Management beschäftigen. Das Thema ist sehr jung und infolge dessen gibt es auch zahlreiche Ansätze, die zur Verbesserung der IT-Sicherheit führen.

Jeder Ansatz hat bis dato noch seine Daseinsberechtigung, weil die Sensibilität und das Wissen für einen ganzheitlichen Ansatz fehlen. Betrachtet man die Vorgehensweisen von Unternehmen in Bezug auf die Absicherung, Steuerung und Kontrolle ihrer Unternehmensdaten auf mobilen Endgeräten wie Smartphones und Tablets, treten deshalb die unterschiedlichsten Ansätze auf. Vom Ansatz "Mitarbeiter werden vertraglich verpflichtet, Sicherheitsregeln - sofern es sie gibt und diese ausgereift sind - bei der Nutzung von Smartphones einzuhalten" bis zur "Trennung des geschäftlichen und privaten Bereichs auf den Endgeräten" gibt es zahlreiche Möglichkeiten die mobile Infrastruktur aufzubauen und abzusichern.

# Enterprise Mobility Management

mediaTest  
digital



Disziplinen des  
Enterprise Mobility  
Managements: MIM,  
MAM, MDM sowie EMC.  
Foto: mediaTest

Was dabei häufig vergessen wird: es gibt noch so viel mehr Faktoren und Komponenten, die bei dem Thema Enterprise Mobility Management eine gewichtige Rolle spielen. So sind beispielsweise Apps ein wichtiger Bestandteil für Effektivität, Funktionalität und letztendlich auch Spaß bei der Nutzung von mobilen Endgeräten. Außerdem muss Mobility mit der "alten" IT-Infrastruktur funktional sein und reibungslose Abläufe gewährleisten. Hinzu kommen Haftungsfragen, arbeitsrechtliche Rahmenbedingungen, Compliance und die Entscheidung welche Anbieter sich im sicheren Mobility-Setup am besten eignen, um nur einige Themen zu nennen. An dieser Stelle angekommen zeigt sich deutlich, was Unternehmen erwartet und das eine richtige Strategie unabkömmlich ist.

## Strukturierung der Disziplinen von Enterprise Mobility Management

Um das Thema strukturiert und nachhaltig im Unternehmen einzuführen, wird folgend aufgezeigt, welche Disziplinen für eine Strategie berücksichtigt werden müssen.

In der Kürze der Zeit hat sich der Meta-Begriff Enterprise Mobility Management (EMM) durchgesetzt, der momentan drei Disziplinen vereint. EMM ist ein allumfassender Begriff für den richtigen und sicheren Einsatz und die Integration von mobilen Endgeräten in Unternehmen. Die drei Disziplinen lauten **Mobile Information Management (MIM)**, **Mobile Application Management (MAM)** und **Mobile Device Management (MDM)**.

Die Bedeutung der einzelnen Disziplinen können Sie in unserem Beitrag **So behalten Sie Durchblick im EMM-Dschungel**<sup>1</sup>. Weitere Informationen zum Enterprise Mobility Management finden Sie auch im Artikel **So sichern Sie die mobile Infrastruktur ab**<sup>2</sup>. (cvi)

### Links im Artikel:

<sup>1</sup> [https://www.tecchannel.de/netzwerk/management/2059351/so\\_behalten\\_sie\\_durchblick\\_im\\_emm\\_dschungel/](https://www.tecchannel.de/netzwerk/management/2059351/so_behalten_sie_durchblick_im_emm_dschungel/)

<sup>2</sup> [https://www.tecchannel.de/netzwerk/management/2059338/enterprise\\_mobility\\_management\\_so\\_sichern\\_sie\\_die\\_mobile\\_infrastruktur\\_ab/](https://www.tecchannel.de/netzwerk/management/2059338/enterprise_mobility_management_so_sichern_sie_die_mobile_infrastruktur_ab/)

### Bildergalerien im Artikel:

gal1 **Sieben Schritte zum MDM -**



### Sieben Schritte zum MDM

Wie kommt ein Unternehmen zu einem sicheren Mobile-Device-Management?

Foto: buchachon - Fotolia.com



**Mobility-Strategie**  
 Zunächst muss jedes Unternehmen für sich definieren, welche Rolle das Thema Mobilität generell spielen und inwiefern MDM in eine Arbeitsplatzstrategie eingebettet werden soll. Dabei empfiehlt FI-TS, künftige Anforderungen in die Planung einzubeziehen. In der ersten Planungsphase müssen

unternehmensspezifische Bedürfnisse evaluiert, der Status quo beurteilt und die Ziele für den MDM-Einsatz benannt werden.  
 Foto: everythingpossible, Fotolia.com



**ByoD - ja oder nein?**  
 Die zweite wichtige Entscheidung lautet: Darf der Mitarbeiter sein eigenes privates Gerät beruflich verwenden, oder sollen firmeneigene Devices genutzt beziehungsweise angeschafft werden? Und: Welche Mitarbeiter benötigen überhaupt ein Mobilgerät? Für und gegen Bring your own Device (ByoD) gibt es jeweils viele Argumente. FI-TS hat sich für Firmengeräte entschieden - mit der Begründung, dass diese Variante weniger Sicherheitsrisiken berge. Die Festlegung auf ein Betriebssystem erleichtere die Umsetzung.  
 Foto: Robert Lehmann-Fotolia



**Anbieter wählen**  
 Auf dem Markt für MDM-Lösungen tummeln sich zahlreiche Anbieter. Die Unterschiede im Angebot seien oft marginal, so FI-TS. Der Dienstleister plädiert deshalb für einen Anbieter „mit Branchenfokus“, weil dieser mit den spezifischen Anforderungen eines Industriezweigs vertraut sei und die wichtigen Features bereitstelle.  
 Foto: ra2 studio - Fotolia.com



Foto: Scanrail - Fotolia.com

### Technische Lösung

Eine MDM-Lösung umfasst im Wesentlichen folgende Funktionen: die Durchsetzung von Policies zur Absicherung des Endgeräts inklusive Daten und Apps, Richtlinien zur Trennung der beruflichen von der privaten Nutzung und zur Regulierung des Zugriffs auf interne sowie externe Daten, dazu Passwort-Bestimmungen und externe Gerätesteuerung für den Notfall. Ausführliche Beratung und ein sorgfältiger Vergleich der Lösungen sind unerlässlich.



### Betriebsrat & Co.

Rechtlich handelt es sich bei MDM-Einführungen um Vertragsanpassungen oder

Nutzungsvereinbarungen. Darin involviert beziehungsweise damit abgedeckt sind Pflichten und Rechte von Arbeitnehmern und -gebern sowie geldwerte Vorteile, aber auch das Fernmeldegeheimnis. Auf der organisatorischen Seite empfiehlt es sich, Betriebsrat, interne Kommunikation und Personalabteilung frühzeitig in die Planungen einzubeziehen, um Daten- und Mitarbeiterschutz, Personalschulungen, User-Support und begleitende Kommunikationsmaßnahmen abzustimmen.

Foto: baranq - shutterstock.com



**Rollout und Testen**  
Ein Pilotprojekt mit einer begrenzten Zahl von Test-Usern könne bereits im Vorfeld des Rollouts größere Fehler aufdecken und die Benutzerfreundlichkeit der Lösung überprüfen, so FI-TS. Der Rollout selbst sollte von einem Monitoring des technischen Betriebs und der Admin-Prozesse begleitet sein. In dieser Phase lassen sich Nachbesserungen vornehmen sowie das User-Verhalten überwachen und eventuell durch

Kommunikationsmaßnahmen unterstützen.  
Foto: peshkova - Fotolia.com



**User-Support**  
Bei der Einführung eines MDM geht es nicht um die reine Technik. Hier stehen vor allem die Mitarbeiter im Blickpunkt. Die sind unbedingt frühzeitig über die neue Mobility-Strategie des Unternehmens zu informieren. Während und nach dem eigentlichen Rollout müssen sie umfassend geschult und beraten werden. Manche Mitarbeiter brauchen ja vielleicht ein wenig Zeit, um sich an die neuen Geräte und Handhabungen zu gewöhnen. Für ein erfolgreiches MDM ist

zudem wichtig, dass sie nicht nur über die technische Bedienung aufgeklärt werden, sondern auch über ihre Rechte und Möglichkeiten.  
Foto: Realisature 123D/Shutterstock.com