Mobile Device Management

Basics und Tipps zur Regelung der mobilen Kommunikation

Heinz-Peter Höller,
Achim Thannheiser

Unternehmen und Behörden begrüßen die neue Flexibilität durch Smartphone und Tablet. Zentral verwaltet und überwacht werden die mobilen Geräte durch das Mobile Device Management. Das Gute: Diese Systeme unterliegen der vollen Mitbestimmung. Zeichnen sie doch alles lückenlos auf. Aber neue betriebliche Vereinbarungen müssen her – die alten scheitern an der Auswertungsvielfalt.

Darum geht es:

- Arbeitgeber verwalten mobile Endgeräte mit einer speziellen Software – dem Mobile Device Management.
- Diese Administrationsprogramme bieten sehr weitreichende Zugriffsmöglichkeiten auf Inhaltsdaten.
- Betriebs- und Personalräte können der totalen Kontrolle von mobil arbeitenden Beschäftigten einen Riegel vorschieben.

Mobile Arbeit nimmt zu. Digitalisierung und Miniaturisierung haben dazu geführt, dass nicht nur die klassischen Außendienstberufe sondern auch viele andere Arbeitsplätze betroffen sind. Man kann Mails unterwegs empfangen und bearbeiten, Dokumente sichten und auf Websites zugreifen. Man kann den dienstlichen Kalender pflegen und Terminanfragen bearbeiten. Die dafür notwendigen Geräte, die Smartphones und die Tablets, werden den Beschäftigten vom Unternehmen zur Verfügung gestellt oder sie nutzen gleich die eigenen.

Für beide Seiten sind mit der zunehmend mobilen Arbeit Vor- und Nachteile verbunden. Viele Beschäftigte begrüßen die Flexibilität und Modernität, sehen aber auch die damit verbundenen Gefahren der Entgrenzung und für die eigene Privatsphäre.[1]

Die Unternehmen freuen sich über die ständige Erreichbarkeit und die kleine Hilfe »mal eben« in der Freizeit. Aber Tablets und Smartphones sind kleine, handliche Geräte. Man nimmt sie überall mit hin, man kann sie verlieren, verlegen und sie können gestohlen werden. Auf den Geräten liegen neben privaten Daten auch dienstliche Mails,

1 Wedde, »Mobile Work« – immer und überall arbeiten können, in: CuA 9/2015 4 ff. (6); Backaitis, What If Your Boss Could See Everything on Your Phone?, 2015, www.cmswire.com/mobile-enterprise/what-if-your-boss-could-see-everything-on-your-phone/

Kalendereinträge und Dokumente. Die Verwaltung mobiler Geräte geht über das hinaus, was bisher hinsichtlich der innerbetrieblichen IT-Systeme notwendig und üblich war. Es geht darum, den Datenfluss auf die und von den Geräten zu kontrollieren und zu überwachen, was auf dem Gerät genau geschieht und was zu tun ist, wenn das Gerät abhandenkommt.

Dazu kommt, dass die Geräte nicht immer im Eigentum der Unternehmen sind. Viele Beschäftigte lehnen es ab, mit zwei Geräten gleichzeitig umzugehen und fordern geradezu, ihre privaten Geräte auch dienstlich nutzen zu können – Bring Your Own Device oder kurz BYOD genannt (siehe dazu den Kasten auf Seite 7). Dann soll aber Privates von Dienstlichem getrennt und dennoch Datenschutz und -sicherheit gewährleistet sein.

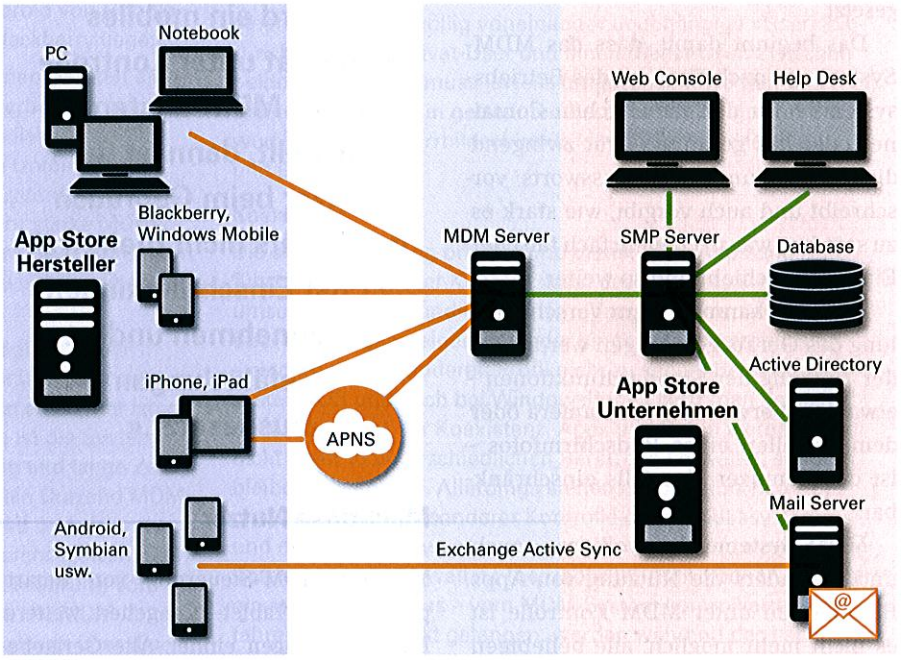
Architektur und Funktion von MDM-Systemen

Für diese konfligierenden Kontroll- und Verwaltungsaufgaben werden zunehmend MDM-Systeme eingesetzt.[2] Im Rahmen der Geräteverwaltung ermöglichen diese Systeme beispielsweise die Bestandsverwaltung der Geräte, das Lizenzmanagement oder die Gerätekonfiguration und sie bieten stets eine komfortable Verwaltungskonsole.

MDM-Systeme sind insbesondere zur Gewährleistung eines hohen Maßes an Sicherheit entwickelt worden. Sie setzen meist Passwort- und Verschlüsselungsrichtlinien durch, erlauben das Fernlöschen von Daten und untersuchen die Geräte auf Malware. Sie achten darauf, welche Apps auf das Gerät geladen werden und verhindern das Zuladen unerwünschter Apps. Und diese Systeme achten streng darauf, auf welche Unternehmensdaten die Nutzer mit welchen Apps zugreifen und welche Daten auf das Gerät übertragen werden dürfen. Wegen dieser weit über die eigentliche Geräteverwaltung hinausgehenden Funktionen, wird zunehmend umfassender von Enterprise Mobility Management gesprochen.

Das, was ein MDM-System kann, wird in der Zusammenarbeit mehrerer IT-Systeme erbracht (siehe dazu die Abbildung oben).

Da ist zunächst der MDM-Server.[3] Er steht grundsätzlich mit allen anderen Systemen in Verbindung. Hierüber steuern die Administratoren die mobilen Geräte, konfigurieren sie und rufen von Ihnen Informationen ab. Sie kontrollieren die Art und Weise, wie die Geräte betriebliche Apps laden und wie sie auf betriebliche Ressourcen (Directory-Service, Mail-Server, Dokumentenmanagement) zugreifen.



Mobile Management Architecture

Als »Vertreter« des MDM-Systems wird ein Software-Client auf das mobile Gerät geladen. Er erhält Aufträge vom MDM-Server und erledigt diese auf dem Gerät. Je nachdem, wie gut die MDM-Unterstützung des jeweiligen Betriebssystems ist, kann der MDM-Client umfangreich und gezielt in die Funktionsweise des Gerätes eingreifen, kann Aktivitäten erzwingen, einschränken oder verbieten und kann – wie es im Jargon heißt – »policies« durchsetzen.

Aus den App-Stores beziehen die Geräte unter MDM-Kontrolle ihre Apps. Die App-Stores können von den Geräteherstellern betrieben werden oder auch eigene Server des Unternehmens sein. Das MDM-System nimmt Einfluss darauf, welche Apps von wem geladen werden können. Auf die anderen Unternehmensserver können die mobilen Geräte über den MDM-Server zugreifen. Unter Verwendung von ActiveSync und Exchange-Server findet auch eine direkte Kommunikation statt, da Exchange in der Lage ist, den Zugriff auf die dort verwalteten Daten selbst gut abzusichern.

Im laufenden Betrieb tauschen der MDM-Server und die mobilen Endgeräte immer wieder Daten miteinander aus. Aus technischen Gründen kann sich der MDM-Server nicht direkt an sie wenden.[4]

Stattdessen muss er Kontakt zu einem Server des Geräteherstellers aufnehmen, da nur der weiß, wie das Gerät angesprochen werden kann. Dieser Server des Herstellers wendet sich dann an das Gerät und fordert es auf, mit dem MDM-Server Kontakt aufzunehmen. Das alles nennt sich »Push-Service« und führt dazu, dass jede Kommunikation zwischen dem MDM-Server des Unternehmens und seinen

2 Als Beispiel für eine umfangreichere Funktionsbeschreibung siehe MobileIron, Betriebssystemübergreifende Verwaltung (MDM), 2015, www.mobileiron.com/de/losungen/betriebssystem-ubergreifende-verwaltung

3 Das können auch mehrere kooperierende Server mit leicht unterschiedlichen Aufgaben sein.

4 Die Geräte haben keine festen IP-Adressen, sie werden ihnen von Mal zu Mal zugeordnet. Nur der Hersteller kennt die aktuelle IP-Adresse, weil sich jedes Gerät immer bei dem Push-Server des Herstellers meldet.

Beschäftigten über einen Server des Geräteherstellers läuft.

Eingeschränkter Gebrauch

Wird ein mobiles Endgerät unter Kontrolle eines MDM-Systems gestellt, dann ist der Nutzer beim Gebrauch des Geräts nicht mehr frei. Er hat Einschränkungen hinzunehmen und ist Gefährdungen ausgesetzt.

Das beginnt damit, dass das MDM-System – je nach Konzept des Betriebssystems – für den dienstlichen Container oder das gesamte Gerät zwingend die Verwendung eines Passworts vorschreibt und auch vorgibt, wie stark es zu sein hat, was nach mehrfach falscher Eingabe geschieht und so weiter.

Der User kann auch zur Verschlüsselung des Geräts gezwungen werden. In der Nutzung der Standardfunktionen – etwa dem Verwenden der Kamera oder dem Erstellen eines Bildschirmfotos – ist der Benutzer ebenfalls einschränkbar.

MDM-Systeme kontrollieren auch und besonders die Nutzung von Apps. Bei Geräten unter MDM-Kontrolle ist es nicht mehr möglich, alle beliebigen Apps auf das Gerät zu laden. Im einfachsten Falle verhindern das Black- oder auch Whitelists, die vom MDM-Client durchgesetzt werden.

Bei den fortgeschrittenen BYOD-Ansätzen wird das Zuladen von betrieblichen Apps genau kontrolliert und die Nutzer werden insofern eingeschränkt, als sie nicht mit beliebigen Apps etwa auf Unternehmensdaten zugreifen können, auch »Copy and Paste« zwischen privaten und dienstlichen Apps wird unterbunden. Teilweise verhält sich eine dienstlich genutzte App auch anders als die gleiche private App, nur weil sie vom MDM-System verwaltet wird. Und teilweise kann der konkrete Funktionsumfang einer App auch noch auf dem Gerät im laufenden Betrieb geändert werden.[5]

Geht ein mobiles Gerät verloren, wird es gestohlen oder nur verlegt, dann sind davon auch die Unternehmensdaten betroffen. Es liegt dann ganz in der Entscheidung des MDM-Administrators, ein solches Gerät von Ferne für jeglichen weiteren Gebrauch zu sperren. Es können aber auch alle Daten oder – und das ist bei BYOD regelmäßig der Fall – nur die dienstlichen Apps und Daten gezielt gelöscht werden. Der Administrator kann auch das ganze Gerät löschen und in den Fabrikzustand versetzen, ohne dass es – zumindest technisch – der Zustimmung des Nutzers bedürfte.

»Wird ein mobiles Endgerät unter Kontrolle eines MDM-Systems gestellt, dann ist der Nutzer beim Gebrauch des Geräts nicht mehr frei. Er hat Einschränkungen hinzunehmen und ist Gefährdungen ausgesetzt.«

Machtlose Nutzer

Mit der MDM-Steuerung von Smartphones und Tablet-PCs gehen weitere Einschränkungen einher. Alle Gerätebetriebssysteme stellen den MDM-Systemen einen umfangreichen Satz an Geräteinformationen wie die Gerätenummer, die Telefonnummer, den Netzbetreiber und auch eine Liste aller installierten Apps zur Verfügung. Diese Daten können vom MDM-Server unmittelbar abgerufen werden.

Besonderes Augenmerk ist darauf zu richten, ob die Systeme auch auf private Mails, Kontakte und Kalender oder auch die Telefonverbindungsdaten zugreifen können, ob sie Zugang zu Sensordaten haben oder das Mikrofon, die Kamera oder sogar die Telefonfunktion nutzen können.[6]

Das alles regelt sich über die Rechte, die dem MDM-System vom Nutzer beziehungsweise dem Betriebssystem eingeräumt werden. Und das ist ein sehr schnelllebiges Gebiet, auf dem sich die Betriebssystemeigenschaften ständig ändern.

Grundsätzlich gilt: Jede App verwaltet ihre eigenen Daten (»Sandbox«) und andere Apps haben darauf keinen Zugriff. Soll eine App dennoch auf die Daten einer anderen App, also zum Beispiel auf die Positionsdaten oder Kalendereinträge zugreifen, dann muss ihr dieses Recht zugestanden werden. Da gibt es Ansätze in den Betriebssystemen, bei denen diese Rechte zum Zeitpunkt der App-Installation angefordert werden und dann – unwiderruflich – gelten. Der Nutzer kann sie meistens nicht zurücknehmen.[7]

Welche Rechte diesen Apps zugewiesen werden und welchen Einfluss der Nutzer darauf hat, ist im Einzelfall zu betrachten. Man muss allerdings davon ausgehen, dass in bestimmten Situationen – insbesondere beim »lautlosen Konfigurieren«[8] oder auch beim Update – Apps auf die Geräte geraten, auf deren Berechtigungen die Nutzer keinen Einfluss haben. Dann ist unklar, auf welche eventuell auch privaten Daten oder Systemfunktionen die MDM- und Unternehmens-Apps Zugriff haben.

Permanente Kontrolle

Positionsdaten, die zur Ortung und für Bewegungsprofile genutzt werden können, sind natürlich besonders sensibel. Auch darauf haben MDM-Systeme Zugriff. Denn das Orten der Geräte und die Darstellung des Aufenthaltsorts in Karten gehört regelmäßig zu deren Funktionsumfang.

Mit mobilen Geräten greifen Beschäftigte auf interne Datenbestände zu und empfangen Mails und Telefonate. Diese Vorgänge können – den internen vergleichbar – registriert und aufgezeichnet werden. Es ist wie gesagt möglich, festzustellen, wer sich wann

5 MobileIron, Was Android for Work für Unternehmen bedeutet, 2015, 11, www.nomasis.ch/fileadmin/user_upload/flyer/produkte/mobileiron/WP_Android_for_Work_DE.pdf

6 In modernen Smartphones sind unter anderem verbaut: Barometer, Beschleunigungs-, Fingerabdruck-, Helligkeits- und elektromagnetischer Sensor.

7 Es sei denn, man deinstalliert die App komplett.

8 Vgl. Microsoft, Windows Phone 8.1 Enterprise Device Management Protocol, 2015, 131, http://go.microsoft.com/fwlink/p/?LinkId=279003; Samsung, In-Depth Look at Capabilities:Samsung KNOX and Android for Work, 2015, 2, www.samsungknox.com/de/system/files/whitepaper/files/Samsung%20KNOX%20and%20Android%20for%20Work_2.pdf; Im Englischen wird »silent« verwendet.

MDM-Geräteverwaltung

Betriebssystem spielt zentrale Rolle

Die Art und Weise, wie ein MDM-System ein Gerät tatsächlich verwalten kann, wie stark es in die Nutzung eingreifen, sie beschränken oder in Teilen verbieten kann, das hängt ganz wesentlich von der MDM-Fähigkeit des Geräts und damit des jeweiligen Betriebssystems ab.

Bei der betrieblichen Nutzung von mobilen Geräten spielen zurzeit noch vier Betriebssysteme eine Rolle, wobei die zwei bedeutendsten wohl IOS von Apple und Android von Google sind, die deutlich vor WindowsPhone und Blackberry liegen.

Apple, das sein Betriebssystem nur auf eigenen Geräten einsetzt, ist mit seinen Produkten im Verbraucherbereich sehr erfolgreich und die Geräte »drücken« durch diese weite Verbreitung über die Beschäftigten selbst in die Unternehmen. Apple setzt – vielleicht als Hebel, um in die Unternehmen zu gelangen – seit geraumer Zeit auf eine sehr starke MDM-Unterstützung und bietet den MDM-Systemen über einhundert MDM-Befehle an, mit denen IOS-Geräte verwaltet und beeinflusst werden können.

Android ist ein Betriebssystem, das von Google als Open Source entwickelt wurde, aber auf vielen Geräten ganz unterschiedlicher Hersteller eingesetzt wird, denen es erlaubt ist, das Betriebssystem weiterzuentwickeln. Deshalb ist die Systemlandschaft bei Android-Geräten sehr vielfältig und lange Zeit gab es im Android lediglich etwas mehr als ein Dutzend MDM-Befehle, also sehr wenig Möglichkeiten, starke und sichere Unternehmensrichtlinien auf den Geräten durchzusetzen. Das hat sich erst vor wenigen Monaten mit der Einführung von »Android for Work« geändert. Android weitet die MDM-Unterstützung stark aus und geht in manchen Bereichen über die bisherigen Ansätze hinaus. Das Betriebssystem soll das Image unsicher und für Unternehmenszwecke nicht geeignet zu sein, verlieren. Man will in die Unternehmen.

BYOD-Konzepte

Vieles spricht dafür, dass der Erfolg von Geräten und Betriebssystemen im betrieblichen Einsatz letztlich davon abhängen wird, wie es den Herstellern gelingt, das Betreibermodell BYOD umzusetzen.* Darunter versteht man den Ansatz, ein mobiles Gerät sowohl dienstlich als auch privat zu nutzen. Die Frage, ob das Unternehmen oder der Beschäftigte selbst Eigentümer ist, ist für die technische Problemstellung nachrangig. Wichtig für beide Seiten ist, dass das Dienstliche und das Private so gut wie möglich getrennt und ein hohes Maß an Sicherheit für die Unternehmens-Apps und -Daten gewährleistet ist.

Die derzeitigen Trends gehen in zwei Richtungen: Einerseits die strikte Trennung des Dienstlichen vom Privaten mit dem »Container-Prinzip« und andererseits die kontrollierte Koexistenz.

Container

Darunter versteht man einen abgeschotteten Bereich auf dem Gerät, in dem sich die betrieblichen Apps und deren Daten befinden. Zwischen dem betrieblichen Bereich, dem Container, und dem privaten Bereich soll es nur in ganz bestimmten Fällen zum gegenseitigen Zugriff kommen. Die älteste, zumeist auf Android realisierte Form des Containers, ist eine einzige App. Öffnet man diese App, dann verbergen sich hinter ihr eine Vielzahl von Funktionen wie etwa ein Mail-Client, ein Adressbuch für die Kontakte oder ein Kalender. Neuere Container-Lösungen nutzen das dem Betriebssystem Android nachträglich hinzugefügte Dual-User-Konzept. Damit ist es möglich, auf einem Gerät zwei völlig voneinander unabhängige »User« einzurichten, einen Privat-User und einen Dienst-User. Zwischen beiden »Sphären« muss jeweils umgeschaltet werden und man befindet sich dann in getrennten Bereichen mit eigenem Passwort, eigenem Sperrbildschirm und natürlich eigenen Apps und Daten.

Koexistenz

Die strikte Trennung privater und dienstlicher Apps und Daten führt beim Container-Konzept dazu, dass man stets explizit umschalten muss und Benachrichtigungen – beispielsweise über den Eingang einer Mail oder eines Kalendereignisses – sind im jeweils anderen Profil nicht zu sehen. Beim Betriebssystem IOS und auch bei WindowsPhone setzt man deshalb auf ein Konzept der Koexistenz. Apps und Daten werden dabei nicht mehr in unterschiedlichen Bereichen verwaltet, sondern bleiben zusammen. Allerdings stehen die betrieblichen Apps und Daten unter besonderer Kontrolle des Betriebssystems und des MDM, sie werden »verwaltete« Apps und »verwaltete« Daten genannt. Verwaltete (betriebliche) Apps können nur über ein streng geregeltes – vom MDM-System kontrolliertes – Verfahren auf das Gerät gelangen, werden während des Lebenszyklus auf dem Gerät gegenüber Fremdzugriffen geschützt und können – getrennt von den privaten Apps – vom MDM-System gezielt verändert (etwa durch ein Update) und gelöscht werden.

Android for Work

Die jüngste Entwicklung stellt »Android for Work« dar. Damit wird Android hinsichtlich der grundsätzlichen MDM-Fähigkeit umfassend erweitert. Zur Umsetzung von BYOD setzt Android for Work ebenfalls auf den Dual User-Container. Um aber das ständige Umschalten zu vermeiden, wird von beiden Bereichen (privat, dienstlich) der Bildschirm gemeinsam genutzt. Obwohl also die privaten und die dienstlichen Apps auf dem Bildschirm gemeinsam erscheinen – die dienstlichen sind besonders gekennzeichnet – und sowohl Benachrichtigungen zu dienstlichen und privaten Apps auf dem gemeinsamen Bildschirm erscheinen, bleiben Apps und Daten über den Dual-User-Betrieb getrennt.

* Dazu grundlegend der CuA-Schwerpunkt: Trend BYOD – Arbeiten mit privaten Geräten, in: CuA 10/2011, 4 ff.

wo aufgehalten hat. Aber auch, wer wie oft sein Smartphone verlegt oder verloren hat oder wer wie oft und mit welcher Findigkeit gegen die Regeln auf dem Gerät verstoßen hat, wird aufgezeichnet. Insbesondere der Echtzeit-Remote-Zugriff (auch Remote-Control genannt) bedeutet:

Die Firma, die MDM zur Verfügung stellt oder nutzt, kann sich – je nach Freigabe durch das MDM-System – auf die Mobiltelefone aufschalten und diese auch – je nach Vereinbarung – fernbedienen.

Hierdurch wird sichergestellt, dass im Falle von Verlust oder Diebstahl des Handys Dokumente des Unternehmens nicht in die Hände Unberechtigter ge-

Zeitschriftenblick

■ Die **geltenden Gesetze** zu kennen gehört zum A und O der Betriebsratsarbeit. Der CuA-Autor Jochen Brandt erklärt in der Oktober-Ausgabe der Zeitschrift für Betriebsräte **»Arbeitsrecht im Betrieb«**, wo genau was zu finden ist. Außerdem werden wichtige Gerichtsentscheidungen etwa zum Initiativrecht der Interessenvertretung aus § 87 Abs. 1 Nr. 6 BetrVG besprochen. Titelthema ist: Mitarbeitergespräche. Auch hier haben Belegschaftsvertretungen ein gewichtiges Wörtchen mitzureden.

■ Die **Gefährdungsbeurteilung psychischer Belastung** ist ein wichtiges Handlungsfeld von betrieblichen Interessenvertretungen. Schließlich steigt der Stresspegel in der Arbeitswelt stetig an. Die Beschäftigten sind dringend auf wirksame Prävention angewiesen – und zwar auf Grundlage der Ergebnisse aktueller Gefährdungsbeurteilungen. Sandra Wolf und Ina Zwingmann erläutern in der Zeitschrift für Gesundheitsschutz und Arbeitsgestaltung **»gute Arbeit«** (10/2015) die wesentlichen theoretischen und rechtlichen Grundlagen zur Pflicht der ganzheitlichen Gefährdungsbeurteilung. Die Beiden zeigen den Weg auf von der Betriebsratsinitiative über die Mitbestimmung und Einigungsstelle bis hin zur betrieblichen Vereinbarung. Weitere Themen sind **»Industrie 4.0«** und **Schlaganfall-Risiko durch Überstunden.**

■ Wie **Personalversammlungen** von Personalvertretungen gut vorbereitet und spannend gestaltet werden können, zeigt die Zeitschrift **»Personalrat«** ausführlich im Oktober-Heft. Denn Personalversammlungen sind nicht nur Pflichtprogramm, sondern bieten vielmehr Chancen, sich und seine Erfolge – aber auch Misserfolge und deren Gründe – den Beschäftigten zu präsentieren.

Bestellhinweis

Einzelexemplare der hier genannten Zeitschriften können bestellt werden bei:

Bund-Verlag, Leserservice, 60424 Frankfurt/M., fon 069 795010-96

» abodienste@bund-verlag.de

raten und es wird ferner sichergestellt, dass nicht einmal Datenspuren auf dem Gerät verbleiben. Denn: Per Remote-Zugriff können die Daten des Telefons bei Verlust oder Diebstahl sofort gelöscht und der Datenschutz und die Sicherheit vor Zugriffen Unberechtigter auf interne Informationen gewährleistet werden.

Wurden private Apps nach der Installation von MDM aufgespielt, sind diese und die dazugehörigen Daten bei einer Fernlöschung auch nicht mehr vorhanden. Andererseits sind mit regelmäßigen Bildschirmfotos Kontrollen über die Inhalte der Nutzung des Geräts im Verlauf des Tages möglich.

Schutzlose Daten

Mit einem MDM-System ist es möglich, auf die persönlichen Daten der Beschäftigten zuzugreifen. Der Schutz der personenbezogenen Daten ist ein Grundrecht, Art. 2 und Art. 1 Grundgesetz (GG) und damit ein hohes Gut. Dieses Recht wird durch die Datenschutzgesetze konkretisiert. Das Bundesdatenschutzgesetz (BDSG) ist als Verbot mit einem sogenannten Erlaubnisvorbehalt konzipiert (§ 4 BDSG).

Das Erheben, Verarbeiten oder Nutzen von personenbezogenen Daten ist danach nur erlaubt, wenn es durch dieses Gesetz oder eine andere Rechtsvorschrift zugelassen wurde oder der Betroffene eingewilligt hat.

Auch für das Beschäftigungsverhältnis gilt, dass nicht einfach alle anfallenden personenbezogenen Daten vom Arbeitgeber genutzt werden dürfen. Dies ist grundsätzlich nur im Rahmen des § 32 BDSG zulässig, soweit das für das Arbeitsverhältnis nötig ist. Das Unternehmen benötigt entweder die Zustimmung der Beschäftigten (§ 4a BDSG) oder eine betriebliche Vereinbarung, die eine Erlaubnis darstellen könnte.[9]

Wenn dazu noch Daten aus der Privatsphäre der Beschäftigten, ihr Aufenthaltsort, E-Mail-Inhalte und privaten Adressen betroffen sind, handelt es sich um besonders sensible Daten im Sinne von § 3 Abs. 9 BDSG, für die erhöhte Anforderungen an das Erheben und Speichern zu stellen sind.[10] Daher wird für diesen Fall immer eine ausdrückliche – auf die konkreten Daten bezogene – Einwilligung der Beschäftigten erforderlich sein.[11]

Tür zur Mitbestimmung weit geöffnet

Diese komplexen Kontrollsysteme für mobile Geräte und ihre Daten kontrollieren zugleich die Beschäftigten. Ihr Nutzungsverhalten, ihr Aufenthaltsort und der Umfang privater Nutzung während der Arbeitszeit werden erkennbar. Die Möglichkeit von Kontrollen reicht aus, auf eine Absicht des Unternehmens kommt es nicht an.

Daher bestimmt der Betriebsrat über § 87 Abs. 1 Nr. 6 BetrVG bei »der Einführung und Anwendung von technischen Einrichtungen, die dazu bestimmt (das heißt in der Lage sind), das Verhalten oder die Leistung der Beschäftigten zu überwachen«, mit.[12] Die Kontrollmöglichkeit ist bei der Nutzung von MDM-Software vorhanden.[13] Die Interessenvertretung muss also beteiligt werden und zwar mindestens hinsichtlich der Fragen:

- Welche Daten der Beschäftigten dürfen überhaupt erfasst und gespeichert werden?
- Wo werden sie wie lange gespeichert?
- Wer ist Empfänger der Daten?
- Wie und wofür (Zweck) dürfen diese Daten verwendet werden?
- Wie dürfen sie verknüpft und ausgewertet werden?
- Wie werden die Beschäftigten vor Nachteilen geschützt?

Aufklärung tut not

Welche Beschäftigten kennen aber all die dargestellten technischen Zusammenhänge? Woher sollten sie es auch wissen. Daher: Aufklärung tut not. Nur wer weiß, was alles erfasst wird, kann sich schützen. Nur wer um die Gefahren bei der Nutzung

9 BAG vom 14.12.2004, Az.: 1 ABR 34/03

10 BAG vom 23.8.2012, Az.: 8 AZR 804/11

11 Däubler, in: Däubler/Klebe/Wedde/Weichert, BDSG, 5. Auflage, 2015, § 32 Rn. 10

12 Ausführlich dazu Thannheiser, Mobile Kommunikation, in: CuA 2/2014, 4 ff. (5)

13 Siehe auch Flake, Smartphone-Kontrollen, in: CuA 10/2014, 11 ff.; MDM-Checkliste für Interessenvertretungen bei Steinwender, Flöhe hüten 2.0 – Mobile Geräte im Sinne der Beschäftigten verwalten, in: CuA 9/2013, 4 ff. (6)

mobiler Geräte weiß, kann sein Handeln danach ausrichten.

Die Mitbestimmungsgremien haben umfangreiche Rechte hinsichtlich Qualifizierungsinhalten und Auswahl der Teilnehmer.

Daher bietet es sich an, initiativ zu werden hinsichtlich

- der Einführung entsprechender betrieblicher Berufsbildungsmaßnahmen nach § 97 Abs.2 BetrVG,
- der Ermittlung des Berufsbildungsbedarfs (§ 96 BetrVG) und
- damit der Bestimmung, wer welche Qualifizierung brauchen könnte.
- Dazu kann der Betriebsrat Vorschläge zu der Teilnahme für Beschäftigte oder auch Gruppen von Beschäftigten machen.

Auch Gerätehersteller mischen mit

Über MDM-Systeme greift der Arbeitgeber auf mobile Endgeräte zu. Aber auch die Geräte- oder Betriebssystemhersteller nehmen auf die Funktionsweise der Geräte Einfluss und greifen so auf Daten zu.

Selbst wenn ein MDM-System ein mobiles Endgerät übernommen hat, ist es auf den Push-Dienst des Herstellers wie beschrieben angewiesen, um überhaupt Kontakt zum Gerät aufnehmen zu können. Damit wird beim Hersteller (beispielsweise Apple oder Google) jeweils erfasst, wann das Unternehmen Kontakt zum Beschäftigten aufgenommen hat.

Aber auch ganz unabhängig von solchen Systemen mischen die Hersteller mit. Selbst wenn man ein Gerät mit minimaler – datenschutzfreundlicher – Konfiguration in Betrieb nimmt, bauen diese innerhalb von wenigen Stunden mit mehreren Dutzend anderen Endsystemen/Servern selbstständig Verbindungen auf, es werden zwischen zehn und siebzig Megabyte Daten übertragen und nur in ganz wenigen Fällen kann gesagt werden, welche Daten da ausgetauscht werden.[14]

Die genauere Untersuchung der Kommunikationsvorgänge macht allerdings einiges deutlich. IOS-Geräte beispielsweise bauen sofort die Verbindung zum Push-Server auf und die bleibt bestehen, bis das Gerät abgeschaltet wird.

Manche Geräte bauen Verbindungen zu Servern auf, die die Daten für die Ortung verfeinern. Bei Android zum Beispiel werden Verbindungen zu Werbeservern und auch – obwohl kein Google-Konto eingerichtet wurde – zu einem Google-Server aufgebaut. WindowsPhone wiederum gleicht die Kontaktdaten des Microsoft-Kontos mit den Kontaktdaten auf dem mobilen Gerät ab und alle mobilen Geräte senden Spracheingaben zur Analyse und Beantwortung an die entsprechenden Hersteller.

Daten außer Haus

Auch beim Verarbeiten, Nutzen oder Speichern von personenbezogenen Daten der Beschäftigten bei Dritten hat die Belegschaftsvertretung zumindest ein Informationsrecht (§ 80 BetrVG). Ihr ist vorzulegen, wo, welche Daten ausgetauscht, genutzt oder verarbeitet werden. Damit ist es möglich, auch die Vorlage der Dokumente einzufordern, die die Rechtmäßigkeit der Datenverarbeitung belegen. Das Unternehmen ist verpflichtet – durch eine entsprechende Vereinbarung nach § 11 BDSG – sicherzustellen, dass der Betriebsrat die Möglichkeit erhält, den Datenschutz auch beim Auftragsdatenverarbeiter zu prüfen.[15]

Auskunftsrecht der Beschäftigten

Bei der Frage, ob personenbezogene Daten der Beschäftigten auf – unbekannten – Servern, an allen möglichen Standorten gespeichert werden, hat die betriebliche Interessenvertretung kein direktes Mitbestimmungsrecht. Aber die Beschäftigten haben den Anspruch, dass ihnen auf Wunsch vom Arbeitgeber Auskunft erteilt wird (§ 34 BDSG) über:

- die zu ihrer Person gespeicherten Daten,
- die Art der Daten,
- die Empfänger dieser Daten und
- den Zweck der Speicherung.

Wenn sie dabei feststellen, dass Fehler vorliegen, haben sie den Anspruch, dass fehlerhafte Daten berichtigt werden (§ 35 BDSG). Darüber hinaus sind unzulässig erhobene oder gespeicherte Daten

14 Vgl. zum Nachfolgenden DIVSI, Wissenswertes über den Umgang mit Smartphones, 2014, 28 ff., www.divsi.de/wp-content/uploads/2014/10/DIVSI-Studie_WissenswertesSmartphones-WEB.pdf

15 Weller, Arbeitgeber, Betriebsrat und Datenschützer: Trio infernale?, in: AuA 9/2014, 504 ff.

MDM-Vereinbarungen

Mobile Device Management – Mobile Endgeräte verwalten und mehr

Die Hans-Böckler-Stiftung hat 21 betriebliche Vereinbarungen zum Mobile Device Management durch den CuA-Autor Achim Thannheiser auswerten lassen und die Ergebnisse für Regelungen in der Praxis zusammengestellt.

» **www.boeckler.de**

zu löschen. Bei starken Verstößen kann von der Möglichkeit Gebrauch gemacht werden, den Datenschutzbeauftragten im Unternehmen oder auch des Bundeslandes zu informieren. Die Aufsichtsbehörde für den Datenschutz kann Prüfungen in den Unternehmen vornehmen und gegebenenfalls Bußgelder verhängen (§ 38 BDSG).

Im Betrieb steht den Beschäftigten das Beschwerderecht über den Betriebsrat (§ 85 BetrVG) zu. Dieser kann auf Abhilfe drängen und im Streitfall sogar die Einigungsstelle (§ 85 Abs.2 in Verbindung mit § 76 BetrVG) anrufen.

Ergonomie und Psyche

Es stellt sich schließlich die Frage, welche Auswirkungen diese Systeme und die Arbeit mit mobilen Geräten auf die Gesundheit der Beschäftigten haben. Der Interessenvertretung steht dabei ein Mitbestimmungsrecht zur Ausfüllung der Regelungen über den Gesundheitsschutz im Rahmen der gesetzlichen Vorschriften zu.

Solche ausfüllungsbedürftigen Rahmenvorschriften sind beispielsweise die §§ 3 ff. des Arbeitsschutzgesetzes (ArbSchG). So besteht nach der Generalklausel in § 3 unter anderem die Pflicht des Arbeitgebers, auf die Gesundheit der Beschäftigten zu achten und Verbesserungen des Gesundheitsschutzes anzustreben.

Dabei hat er sich nach § 4 Nr.1 davon leiten zu lassen, dass Gefährdungen der Gesundheit – auch psychische – möglichst vermieden oder zumindest kleingehalten werden. Dazu gehören ebenfalls entsprechende Gefährdungsanalysen. Die konkreten arbeitsplatz- oder aufgabenbezogenen Unterweisungen sind an den Erkenntnissen der Gefährdungsanalyse im Sinne von § 5 auszurichten.

Gesundheit umfasst die körperliche und psychische Unversehrtheit. Gefährdungen können durch die Geräte selbst oder die Software entstehen. Die ergonomischen Mindestanforderungen an die Geräte und die Software sind gemäß § 87 Abs.1 Nr.7 und § 91 BetrVG mitbestimmungspflichtige Themen.

Hinsichtlich möglicher psychischer Belastungen und dem Ausdehnen der beruflichen Belange in die Freizeit durch eine ständige Erreichbarkeit oder Sichtbarkeit von beruflichen Anforderungen (zum Beispiel E-Mails) und deren belastenden Folgen, wie psychische oder psychosomatische Erkrankungen, wären ebenfalls Regelungen sinnvoll.

Allgemein gilt, dass der Betriebsrat nach § 87 Abs.1 Nr.7 BetrVG bei betrieblichen Regelungen über den Gesundheitsschutz mitzubestimmen hat. Hierzu gehört auch die durch § 12 ArbSchG dem Arbeitgeber auferlegte Pflicht, die Beschäftigten über Sicherheit und Gesundheitsschutz bei der Arbeit zu unterweisen. Einigen sich die Betriebsparteien nicht über Art und Inhalt der Unterweisung, ist gemäß § 87 Abs.2 und § 76 BetrVG eine Einigungsstelle zu bilden, um den Streit beizulegen.

Fazit

Der Einzug kleiner mobiler Geräte in Unternehmen und Behörden zieht deren Verwaltung mit Hilfe von Mobile Device Management-Systemen nach sich. Sie übernehmen die Kontrolle der Geräte, schränken die Nutzer im Gebrauch ein und erlauben dem Arbeitgeber Einblicke in die Gerätenutzung.

Unter bestimmten Umständen können diese Systeme auch auf sensible Daten der Beschäftigten zugreifen. Das alles zusammen macht den Einsatz mobiler Geräte und von Administrationssystemen zu einem Prozess, der der Mitbestimmung unterliegt und genau zu regeln ist.[16]

Aber, die Gefährdungen für die Mitarbeiter liegen eben nicht nur in der betrieblichen Nutzung, auch der Gebrauch an sich ist mit erheblichen Herausforderungen verbunden. Es empfiehlt sich, den Schutz der Persönlichkeitsrechte von Beschäftigten durch klare betriebliche Vereinbarungen zu sichern.

Autoren

Heinz-Peter Höller ist seit 1993 Professor für Rechnernetze und Telekommunikation an der Hochschule Schmalkalden, Blechhammer 8, 98574 Schmalkalden, fon: 0160-5878800
» **h.hoeller@hs-sm.de**
» **www.hs-schmalkalden.de**

Achim Thannheiser ist selbstständiger Rechtsanwalt und Betriebswirt in Hannover; Rechtsanwaltskanzlei Thannheiser & Koll., Hannover, Rühmkorffstraße 18, 30163 Hannover, fon 0511 990 490
» **thannheiser@thannheiser.de**
» **www.thannheiser.de**

16 Vereinbarungen zu MDM-Systemen sind bereits in vielen Unternehmen abgeschlossen worden, siehe Thannheiser, Mobile Device Management – Mobile Endgeräte verwalten und mehr, Hans-Böckler-Stiftung (Hrsg.), 2015, www.boeckler.de/pdf/mbf_bvd_mobile_device_management.pdf; Übersicht über die wesentlichen Inhalte einer Betriebsvereinbarung zu MDM bei Thannheiser, Alles ist möglich – MDM-Software in AiB 6/2015, 22 ff.