Andreas Kohne
Sonja Ringleb
Cengizhan Yücel

Bring your own Device

Einsatz von privaten Endgeräten im beruflichen Umfeld – Chancen, Risiken und Möglichkeiten

Springer Vieweg

Bring your own Device

Andreas Kohne · Sonja Ringleb ·
Cengizhan Yücel

Bring your own Device

Einsatz von privaten Endgeräten im beruflichen Umfeld – Chancen, Risiken und Möglichkeiten

Springer Vieweg

Andreas Kohne
Sonja Ringleb
Cengizhan Yücel
Materna GmbH
Dortmund, Deutschland

ISBN 978-3-658-03716-1 ISBN 978-3-658-03717-8 (eBook)
DOI 10.1007/978-3-658-03717-8

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

Springer Vieweg

Gedruckt auf säurefreiem und chlorfrei gebleichtem Papier.

Springer Fachmedien Wiesbaden GmbH ist Teil der Fachverlagsgruppe Springer Science+Business Media (www.springer.com)

Geleitwort

Die Umwälzungen auf dem Markt der mobilen Endgeräte, die wir seit 2007 beobachten, stellen Unternehmen seitdem vor große Herausforderungen. Konsumenten, speziell die der jüngeren Generationen, sind die eigentlichen Treiber mobiler Innovationen, Unternehmen hingegen agieren verhalten, da hier häufig andere Anforderungen im Fokus stehen.

Private Nutzer gehen häufig viel unkomplizierter, aber auch risikofreudiger mit Daten im Netz um. Öffentliche Verwaltungen und Unternehmen müssen auf Grund von *Compliance-Bedingungen* und gesetzlichen Vorschriften andere Maßstäbe setzen. Dabei stellt sich immer wieder die Frage, ob und wie sich dieser Widerspruch zwischen privater und geschäftlicher Nutzung der mobilen Technologien auflösen lässt.

In einer zunehmend digitalisierten Welt kann man bei der Kommunikation der Beteiligten nur schwer zwischen Beruflichem und Privatem trennen. Durch die immerwährende Erreichbarkeit verschwimmen auch diese Grenzen. Zur Lösung des Problems gibt es keinen Königsweg, sondern jedes Unternehmen muss für sich entscheiden, welche Auswirkungen der Einsatz dieser Technologien auf das ureigene Geschäftsmodell im positiven wie negativen Sinn hat.

Die Gesellschaft als Ganzes, aber auch speziell die jungen Menschen, sollten lernen, ein Verständnis für das Thema Datenschutz bzw. Datensouveränität zu entwickeln – das ist ein Bildungsauftrag. Unternehmen müssen darüber hinaus im Rahmen ihres Risikomanagements bewerten, inwieweit private Kommunikations- und IT-Endgeräte in den Unternehmensalltag Einzug halten. Die damit verbundenen Fragestellungen, die häufig unter dem Schlagwort „*Bring Your Own Device*“ nur oberflächlich angeschnitten werden, bedürfen einer tiefgehenden Analyse und danach Bewertung durch alle betroffenen Verantwortlichen bis hin zur Geschäftsführung eines Unternehmens.

Hier möchte das vorliegende Buch einen Leitfaden an die Hand geben, der alle Aspekte des Betriebs privater Endgeräte im Unternehmensumfeld betrachtet. Es gibt dem Leser vielfältige Hinweise zu technischen, rechtlichen und wirtschaftlichen Aspekten bei der Entscheidungsfindung für seine eigene *BYOD-Strategie*.

Dortmund, April 2015

Dr. Winfried Materna
Gesellschafter und Beirat
Materna GmbH

Vorwort

Seit der Einführung des *Apple iPhones* im Jahre 2007 hat sich der Markt der Mobiltelefone rapide verändert. Immer mehr Hersteller drängen auf den Markt und versuchen mit neuer *Hardware* und anderen mobilen Betriebssystemen Kundensegmente für sich zu gewinnen. Mit der Einführung des *iPad* im Jahr 2010 ist es *Apple* sogar gelungen einen komplett neuen Markt für *Tablet-Geräte* zu schaffen. Auch hier diversifizierte sich der Markt sehr schnell. Im Jahr 2013 haben es die mobilen Endgeräte zum ersten Mal geschafft, höhere Verkaufszahlen aufzuweisen als herkömmliche *PCs* (vgl. [37]).

Die dadurch eingeleiteten Veränderungen sind aber nicht nur technischer Natur. Der Umgang von Anwendern mit mobilen System hat sich grundlegend verändert. Heutzutage ist der Einsatz von *Smartphones* und *Tablets* etwas vollkommen Normales; im persönlichen, aber auch im geschäftlichen Leben. In diesem Zusammenhang von einem Trend zu sprechen, ist sicherlich falsch. Es handelt sich vielmehr um eine grundsätzliche Veränderung, wie mit Daten und Anwendungen gearbeitet wird. IT-Abteilungen, die dies unterschätzen, oder nicht weiter beachten, sehen sich zunehmend in die Ecke gedrängt, da mobile Endgeräte in Unternehmen eingesetzt werden; egal ob die IT-Abteilung dies will oder nicht.

Ein möglicher Ansatz, um den Einsatz von mobilen Endgeräten im geschäftlichen Umfeld zu reglementieren, ist der *BYOD-Ansatz* (*Bring Your Own Device*). Hierbei ist es den Mitarbeitern erlaubt, eigene Geräte für private und geschäftliche Zwecke einzusetzen. In diesem Zusammenhang ergeben sich viele technische, rechtliche und finanzielle Fragestellungen sowie neue Sicherheitsrisiken, mit denen sich die entsprechenden Verantwortlichen im Vorfeld einer *BYOD-Einführung* auseinander setzen müssen.

Deswegen haben wir in diesem Buch allen Geschäftsführern, IT-Entscheidern und -Administratoren, allen anderen Verantwortlichen und Technikinteressierten einen fundierten Überblick über das Thema *BYOD* zusammengestellt. Wir möchten unser Buch dabei als Informationsquelle und Entscheidungshilfe verstehen sehen. Sie können das Buch entweder von vorne bis hinten durchlesen, um sich mit allen Aspekten des Themas vertraut zu machen; Sie können aber auch nur diejenigen Kapitel lesen, die für Ihren Verantwortlichkeitsbereich wichtig sind.

Den Abschnitt der rechtlichen Aspekte haben wir nach bestem Wissen und Gewissen und nach ausgiebigen Recherchen erstellt. Wir können hier aber keine Haftung übernehmen und können nicht als juristische Beratung verstanden werden. Wir bitten Sie die relevanten Punkte jeweils in Ihrem Einzelfall juristisch prüfen und bewerten zu lassen. Die Gesetzgebung ändert sich und ist vor allem bei länderübergreifenden Firmen komplex.

Dieses Buch erhebt weiterhin keinen Anspruch auf technische Vollständigkeit. Die IT-Technik im Allgemeinen und im Bereich der mobilen Endgeräte im Speziellen verändert sich so schnell, dass ein solches Buch nur einen Schnappschuss des jetzigen Ist-Zustandes wiedergeben kann. Die in diesem Buch vorgestellten Fragestellungen, Abläufe und Prozesse sind aber allgemeingültig und können auch auf zukünftige Entwicklungen angewandt werden.

Zum Schluss möchten wir noch darauf hinweisen, dass wir aus Gründen der Lesbarkeit im Folgenden bei Wortendungen stets den männlichen Fall berücksichtigen.

Wir wünschen Ihnen jetzt viel Spaß bei der Lektüre und hoffen, Ihnen ein guter Ratgeber auf dem Weg zu Ihrer eigenen *BYOD-Strategie* zu sein.

Dortmund, April 2015

Andreas Kohne
Sonja Ringleb
Cengizhan Yücel

Buchwerbung – So gewinnen Sie Kunden!

Bücher erfreuen sich einer hohen Wertschätzung bei ihren Lesern – das ist bei Marketingexperten unumstritten.
Die nachhaltige Werbewirkung ist gerade durch die Langlebigkeit des Produktes Buch gewährleistet. Mit unseren Fachbüchern erreichen Sie exakt die anvisierten Personen. Ihre Vorteile der Buchwerbung bei Springer Vieweg:

Ein erstklassiges Umfeld

- durch ein renommiertes Verlagshaus
- und namhafte Autoren

Homogene Zielgruppen

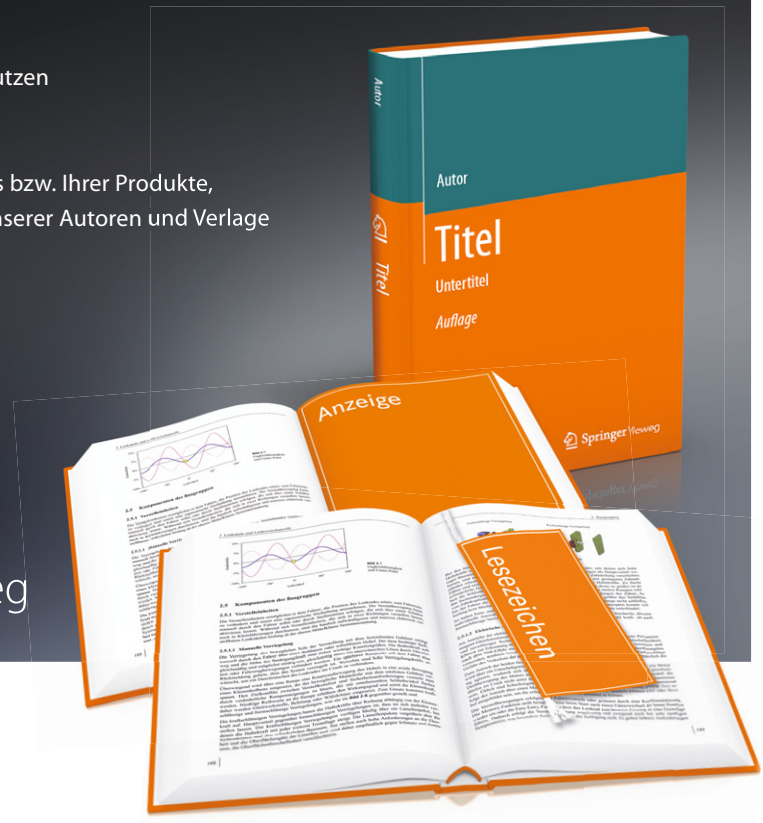
- mit hohem Involvement
- die Ihre Fachbücher regelmäßig nutzen

Positiver Abstrahleffekt

- auf das Image Ihres Unternehmens bzw. Ihrer Produkte, durch den ausgezeichneten Ruf unserer Autoren und Verlage

Werbemöglichkeiten

- Anzeige
- Logo | Sponsoring
- Lesezeichen



Springer Vieweg

Best Ad Media
Springer Fachmedien Wiesbaden GmbH
Abraham-Lincoln-Straße 46
65189 Wiesbaden
tel +49 (0)611 / 78 78 – 555
info@best-ad-media.de

www.best-ad-media.de

Richtig schalten. BEST AD MEDIA

Willkommen in der IT-Fabrik

Ihr Weg zu mehr Agilität, Effizienz und Erfolg

Materna bietet Beratung und Technologie für die Transformation Ihrer IT in eine IT-Fabrik. Hierfür übertragen wir Konzepte und Methoden aus der industriellen Fertigung auf die IT.

Erfahren Sie anhand unserer Best Practices mehr über die effiziente Automatisierung und Standardisierung Ihrer IT-Organisation.

Mehr unter **www.materna.de/it-factory.**

MATERNA
Information & Communications

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

Einleitung

1

Die IT-Welt und die Arbeitswelt verändern sich zur Zeit massiv. Die Grenzen zwischen Arbeitsplatz und Heim, zwischen Arbeitszeit und Freizeit verschwimmen immer mehr. Arbeit wird heute weniger als ein Ort verstanden, an dem gearbeitet wird, sondern mehr als eine Aktivität, die dort durchgeführt werden kann, wo es die Möglichkeit dazu gibt. Früher hat die Technik vorgegeben, wie ein Arbeitsplatz auszusehen hat. Begonnen bei den ersten Schreibtischen mit Terminals, die mit einem Großrechner verbunden waren, bis hin zu den *PCs* und *Laptops*. Heute geben die Anwender mit ihren Anforderungen an eine flexible Arbeitsumgebung den Ton an. Dies stellt eine große Veränderung im Selbstverständnis der Angestellten dar und stellt die klassische IT-Abteilung vor große Probleme. Der Trend geht dahin, dass jeder Mitarbeiter seinen eigenen, individuellen Arbeitsplatz aus verschiedensten Geräten und Anwendungen zusammenstellt. *Ade McCormack* spricht in diesem Zusammenhang von der *DIY* (*Do It Yourself*) IT (vgl. [59]).

Der Trend dahinter heißt *Consumerization*. Der aus dem Amerikanischen stammende Begriff drückt aus, dass die Technologien aus dem *Consumer-Bereich*, also dem Endanwenderbereich, immer größeren Einfluss auf den *Business-Bereich* haben. Früher hat der *Business-Bereich* den privaten Bereich beeinflusst, indem zum Beispiel Taschenrechner in jeden Haushalt Einzug hielten und *PCs* nach und nach ihren Weg vom Büro auf den heimischen Schreibtisch gefunden haben. Heutzutage ist es genau andersherum. *Smartphones* und *Tablets* sind aus dem Alltag nicht mehr wegzudenken. Dies hat enorme Auswirkungen auf die Art und Weise, wie Anwender heutzutage *Services* von der Firmen-IT erwarten. Aus dem privaten Umfeld sind sie es gewohnt permanent über das Internet mit ihren Familien, Freunden und Bekannten verbunden zu sein. Sie sind immer erreichbar, legen Daten, Fotos und Musik bei *Cloud-Dienstleistern* ab und verbinden sich über soziale Netzwerke mit anderen Menschen auf der ganzen Welt. Diese *Always-On-Mentalität* und die daraus resultierenden Anforderungen werden von vielen Arbeitgebern und vielen IT-Abteilungen nicht beachtet oder heruntergespielt. Dies ist aber nicht länger möglich, da die Mitarbeiter bereits angefangen haben, ihre privaten Geräte mit zur Arbeit zu bringen. Dort erwarten sie natürlich, dass sie genauso leicht wie im privaten Bereich auf Firmendaten, *E-Mails*

A. Kohne, S. Ringleb, C. Yücel, *Bring your own Device*, DOI 10.1007/978-3-658-03717-8_1

und Kalender zugreifen können. Dabei werden sie oft enttäuscht, da die IT-Abteilung eine berufliche Nutzung von privaten Geräten in vielen Fällen nicht zulässt. Der Anteil solcher Firmen ist im weltweiten Vergleich in Deutschland immer noch überdurchschnittlich hoch. Laut einer Studie von *Fortinet* ignorieren aber 30 % aller deutschen Angestellten unter 30 Jahren diese Verbote einfach. 55 % der Befragten unter 30 sehen es sogar als ihr Recht an, ihre privaten Geräte geschäftlich einsetzen zu können (vgl. [20]).

Wo ein Wille ist, da ist auch ein Weg. So denken viele, vor allem junge Angestellte heute. Daraus ergeben sich für die IT-Abteilungen große Probleme, denn es entwickelt sich eine *Schatten-IT*. Eine IT, neben der geregelten und abgesicherten, die große Löcher in das Sicherheitskonzept der Administratoren reißt: Mobile Endgeräte werden einfach mit dem *Firmen-WLAN* verbunden, oder es werden private *WLAN-Router* mitgebracht und Zugänge mit Kollegen geteilt, Firmendaten werden in überall verfügbaren *Cloud-Speichern* abgelegt und geheime Daten werden über private *E-Mail-Accounts* verschickt. Dies sind nur einige Beispiele, wie bewusst oder unbewusst die bisher ausreichenden Sicherheitsmechanismen der IT umgangen werden.

Die Augen vor diesen Problemen zu verschließen und zu hoffen, dass dieses Übel schon vorüberziehen wird, ist keine Alternative. Vielmehr müssen sich Firmen jetzt aktiv Gedanken darüber machen, wie sie mit den veränderten Tatsachen zukünftig umgehen wollen. Firmen müssen jetzt eine Antwort auf die offenen Fragen im Bezug auf den Einsatz von mobilen Geräten, wie *Smartphones* und *Tablets*, haben.

BYOD oder *Bring Your Own Device* kann eine Antwort auf diese Fragen sein. Mit *BYOD* wird ein Konzept beschrieben, bei dem Angestellte ihre privaten Endgeräte im geschäftlichen Umfeld einsetzen dürfen. Sie erhalten dabei (limitierten) Zugriff auf Firmenressourcen wie zum Beispiel *E-Mail-Dienste*, Kalender, aber auch Daten und Netzwerke. Üblicherweise bezieht sich *BYOD* vor allem auf die mobilen Endgeräte wie *Smartphones* und *Tablets*. Im weiteren Sinne greifen die dahinterliegenden Konzepte aber auch bei anderen IT-Geräten wie *PCs* oder *Laptops*.

In Amerika ist *BYOD* weitverbreitet. In einer Studie aus dem Jahr 2012 zeigt *Cisco* auf, dass in den USA 95 % aller Unternehmen ihren Mitarbeiten (in der einen oder anderen Art und Weise) den Einsatz privater Endgeräte im beruflichen Umfeld erlauben (vgl. [14]). Den Ursprung hat *BYOD* aber in den asiatischen Ländern. In hochtechnisierten Ländern wie Südkorea, Singapur oder Taiwan gehört *BYOD* schon seit Jahren zum Alltag. Auch Deutschland kann sich nicht länger vor diesen Veränderungen verschließen. Laut der *Cisco*-Studie wurden im Jahr 2014 pro US-Mitarbeiter, welcher sich mit der Verarbeitung von Wissen auseinander setzt, im Durchschnitt 3,3 mobile Endgeräte eingesetzt.

Einer der großen Trends der IT, neben der Virtualisierung, der Automatisierung und dem *Cloud Computing*, ist die Standardisierung. Es werden Hardware, *Software* und *Services* standardisiert. Dies reicht von den eingesetzten *PCs*, *Notebooks* und *Servern*, über die Betriebssysteme und Anwendungen bis hin zu den IT-Diensten wie zum Beispiel *Mail*, *Storage* und Netzwerk. Die Standardisierung ist der nächste Schritt auf dem Weg zur IT-Fabrik. Sie bietet viele Vorteile und hilft der IT schneller und agiler zu werden. *BYOD* läuft diesem Trend auf den ersten Blick entgegen, da jeder Mitarbeiter ein beliebiges Ge-

rät mit einem Betriebssystem seiner Wahl mitbringen kann und beliebige Anwendungen installieren kann. Darum ist *BYOD* für viele IT-Leiter ein großes *No-go*.

Richtig betrachtet ergeben sich aber viele Chancen, die es zu nutzen gilt. Durch den gezielten Einsatz von mobilen Endgeräten lässt sich eine Flexibilisierung der Arbeitszeit erreichen und dadurch eine bessere *Work-Life-Balance*. Weiterhin kann *BYOD* die Motivation der Mitarbeiter steigern und sie länger an das Unternehmen binden. Dies kann in den Zeiten von Fachkräftemangel und *War for Talents* ein echtes Differenzierungsmerkmal sein. Junge Menschen (*Generation Y* genannt), die jetzt auf den Arbeitsmarkt drängen, erwarten heutzutage, dass sie ihre mobilen Endgeräte permanent einsetzen können. Eine strikte Missachtung dieser Anforderungen kann Firmen sehr schnell unattraktiv werden lassen. Oft wird aus Unternehmenssicht auch eine Kostenersparnis durch die Einführung von *BYOD* als Motivation gesehen. Diese Erwartung wird meist nicht erfüllt. Die Kosten, welche durch die private Anschaffung der Endgeräte eingespart werden, werden meist durch die zusätzlichen Kosten für das Management und die zusätzlichen Sicherheitsvorkehrungen aufgefressen. *BYOD* kann sogar höhere Kosten erzeugen. Diese müssen dann mit dem Gewinn an Mitarbeiterzufriedenheit und der Steigerung der Produktivität gegengerechnet werden. Ein finanzieller Vorteil kann es sein, dass es bei dem Einsatz von privaten Endgeräten zu einem Verständniswechsel von “ein Gerät” zu “mein Gerät” kommt und es dadurch weniger oft zu Problemen oder Defekten durch unachtsamen Gebrauch kommt.

Natürlich gibt es auch Risiken. Schnell werden private und geschäftliche Daten vermischt, Geräte werden geklaut oder gehen verloren. Dies kann zu einem Datenverlust oder -diebstahl führen. Weiterhin ist es möglich, dass Zugangsdaten für Firmendienste oder soziale Netzwerke gestohlen werden. Ein Angreifer kann mit den geklauten *Log-In-Daten* in das Firmennetz einbrechen und weiteren Schaden verursachen, oder Nachrichten im Namen eines Angestellten im Netz veröffentlichen. All dies kann schwere finanzielle Schäden aber auch *Image-Schäden* für das Unternehmen bedeuten. Natürlich ist auch Industriespionage ein wichtiges Thema. Die Firma *Watchguard* geht sogar so weit und sagt: *BYOD = Bring Your Own Danger*. All diese Risiken sind nicht von der Hand zu weisen und müssen frühzeitig erkannt und dann gemanagt werden. Dabei können entsprechende *Software-Lösungen* wie zum Beispiel *Mobile Device Management* (*MDM*) Tools unterstützen.

BYOD ist dabei aber nichts, was sich mit der Integration eines Tools einführen oder abwenden lässt. Vielmehr handelt es sich um ein neues Paradigma, welches den Umgang mit privaten Geräten im geschäftlichen Umfeld regelt. *BYOD* ist eine Strategie, die hochgradig individuell an jede Firma, ihre Strategien und ihre Mitarbeiter angepasst werden muss.

Die Erstellung einer solchen Strategie wird dabei oft unterschätzt. Auch wenn es im Grunde genommen um die Integration von IT-Geräten in einen Firmenkontext geht und es sich somit augenscheinlich um ein IT-Projekt handelt, müssen viele unterschiedliche *Stakeholder* berücksichtigt und eingebunden werden. Dazu gehören die Geschäftsleitung, die IT, die HR-, Finanz- und Rechtsabteilung, genauso wie ein Betriebsrat und nicht zu ver-

gessen die Anwender selbst. Die *BYOD-Strategie* stellt dabei das Herzstück eines solchen Projekts dar. Sie legt die unterschiedlichen Aspekte des Umgangs mit den privaten Geräten fest und gibt sozusagen die Leitplanken, innerhalb derer sich die Anwender bewegen dürfen, vor. Dabei sind menschliche, technische, juristische, finanzielle und sicherheitsbezogene Aspekte zu berücksichtigen. Darum sollte die Strategie mit sehr viel Bedacht und Umsicht entwickelt werden.

Die Umsetzung einer *BYOD-Strategie* sollte im Rahmen eines gut geplanten Projekts geschehen. Dabei werden die neuen Regeln allen Mitarbeitern bekannt gemacht und deren Einhaltung zum einen mit Vertragsergänzungen und zum anderen mit entsprechenden Tools und Techniken sichergestellt.

In den folgenden Kapiteln gehen wir Schritt für Schritt auf alle relevanten Aspekte einer *BYOD-Strategie* ein. Die einzelnen Kapitel bauen dabei nicht aufeinander auf. Sie können sich also nur die Aspekte heraussuchen, die für Sie relevant sind, oder sich einen Überblick über die verschiedenen Einflussfaktoren bilden. Sie können das Buch aber natürlich auch von vorne bis hinten durchlesen. Wir beginnen das Buch, indem wir Ihnen im ersten Kapitel *BYOD* ausführlich vorstellen und Ihnen erklären, wie Sie Ihre *BYOD-Strategie* optimal aufbauen. Danach beleuchten wir ausführlich diese weiteren Aspekte:

- Rechtliche Aspekte
- IT Aspekte
- Finanzielle Aspekte
- Soziale Aspekte
- Unternehmenspolitische Aspekte

Des Weiteren gehen wir ganz explizit auf die einzelnen Schritte der Implementierung einer *BYOD-Strategie* ein und runden das Buch mit der Vorstellung einiger *BYOD-Alternativen* ab. In jedem Kapitel erklären wir Ihnen, welche Aspekte wichtig sind und bei der Entscheidungsfindung für oder gegen eine *BYOD-Strategie* beachtet werden müssen, erklären, welche Aspekte von welchen *Stakeholdern* beeinflusst werden und geben Ihnen am Ende jedes Kapitels eine *Checkliste* an die Hand, mit deren Hilfe Sie prüfen können, ob alle wichtigen Aspekte beachtet wurden. Abschließend stellen wir Ihnen noch einen *BYOD-Entscheidungsbaum* zur Verfügung, der Ihnen bei der Entscheidung für oder gegen ein *BYOD-Projekt* helfen kann. Zusätzlich liefern wir Ihnen im Anhang noch fertige *Checklisten* zum Ausfüllen für diverse *BYOD-Aspekte*.

BYOD kann eine sehr gute Ergänzung zu Ihrer bisherigen Standard-IT sein, sollte aber nicht singulär betrachtet werden. *BYOD* sollte als Bestandteil einer ganzheitlichen *Enterprise Mobility Strategie* gesehen werden. Hierbei geht es um die Ausrichtung der gesamten IT in Richtung Zukunft. Machen Sie sich jetzt schon Gedanken über den Arbeitsplatz der Zukunft. Wie sollen Ihre Mitarbeiter in Zukunft arbeiten? Welche Systeme sind dafür notwendig? Wo können die notwendigen Arbeiten erbracht werden? Wie kommunizieren die Mitarbeiter zukünftig? Welche Chancen und Möglichkeiten ergeben sich dadurch? Welche Risiken entstehen? Wie gehe ich mit der Herausforderung um, immer schneller

IT-Services anbieten zu müssen und trotzdem dabei Kosten zu sparen? All dies erfordert ein Umdenken in der IT. Die Rolle des IT-Leiters muss sich dabei vom *CI'No'* zum *Chief Transformation Manager* ändern.

Indem Sie dieses Buch gekauft haben und es lesen, haben Sie den ersten Schritt in Richtung einer für Sie passenden *BYOD-Strategie* getan. Selbst wenn Sie sich nach dem Lesen dieses Buches gegen ein *BYOD-Projekt* entscheiden, so haben Sie zumindest die passenden Argumente, um Ihre Meinung zu begründen. Vielleicht entscheiden Sie sich ja auch für eine der vorgestellten Alternativen. Wenn Sie sich aber für ein *BYOD-Projekt* entscheiden, hoffen wir, dass wir Ihnen auf dem Weg die richtigen Anregungen und Impulse geben und Ihnen helfen, Antworten auf alle nötigen Fragestellungen zu finden. Wir versuchen dabei in diesem Buch das Thema ganzheitlich zu beleuchten, um Ihnen alle Aspekte vorzustellen. Wir würden uns freuen, wenn Ihnen das Buch ein treuer Begleiter und steter Ratgeber ist und wünschen Ihnen viel Erfolg bei Ihrem *BYOD-Projekt*.

Bring Your Own Device

2

BYOD wird von vielen als Heilsbringer bezeichnet, der alle Probleme der modernen Arbeitswelt lösen kann. Außerdem sei *BYOD* ein Traum für die Angestellten und würde dabei noch viel Geld sparen. Für viele IT-Abteilungen ist es aber ein Albtraum. Potentiell sollen sich alle möglichen privaten Geräte mit dem Firmennetz verbinden und Zugriff auf Dienste und Daten erhalten? Undenkbar. Doch was ist dieses *BYOD* genau? Ist es ein Trend, der erst mal abgewartet werden kann? Ist es ein *Hype*, der schnell durch den nächsten ersetzt wird?

Es zeichnet sich immer mehr ab, dass *BYOD* keine kurzfristige Erscheinung oder Laune der IT-Anwender ist, sondern dass sich dahinter ein ernst zu nehmendes Thema verbirgt, mit dem sich jede Firma auseinander setzen sollte. Eine Nichtbeachtung ist grob fahrlässig, da die Mitarbeiter ihre mobilen Geräte mit in das Unternehmen bringen und sie selbstverständlich einsetzen werden. So kann leicht eine sogenannte *Schatten-IT* entstehen, die unbemerkt von der zentralen IT existiert (vgl. Kap. 4). Dies stellt ein echtes Sicherheitsrisiko dar. Im schlimmsten Fall steht die Geschäftsleitung in der Verantwortung, da in letzter Instanz sie für die Datensicherheit Sorge zu tragen hat.

BYOD muss vielmehr als Strategie verstanden werden, die, wenn sich bewusst für eine entsprechende Strategie entschieden wird, zentral von einem Unternehmen festgelegt, eingeführt und gelebt werden muss. Die Entscheidung für oder gegen eine *BYOD-Strategie* ist keine leichte und hängt von vielen Faktoren ab, die in diesem Buch Schritt für Schritt beleuchtet werden. Ein wichtiger Faktor sind sicherlich die Mitarbeiter selbst. Wollen die Angestellten überhaupt eine *BYOD-Strategie*, oder gibt es Alternativen? Falls sich dagegen entschieden wird, muss aber durch vertragliche und technische Regelungen dafür Sorge getragen werden, dass die Mitarbeiter ihre privaten Geräte wirklich nicht geschäftlich einsetzen.

Wird aber beschlossen, eine *BYOD-Strategie* umzusetzen, müssen viele Aspekte besprochen, beschlossen und umgesetzt werden. In diesen Prozess sind viele verschiedene Gruppen der jeweiligen Firma zu involvieren. Dabei wird von den sogenannten *Stakeholdern* gesprochen. Dies sind beteiligte Personen, die ein direktes oder indirektes Interesse

A. Kohne, S. Ringleb, C. Yücel, *Bring your own Device*, DOI 10.1007/978-3-658-03717-8_2

oder Mitspracherecht an oder in dem Projekt haben. Die einzelnen Stakeholder eines *BYOD-Projekts* werden im Laufe dieses Kapitels unter Abschn. 2.2 genau vorgestellt.

Der zentrale Punkt einer *BYOD-Strategie* ist die *Policy* oder Richtlinie. Sie legt die Leitplanken fest, innerhalb derer der Einsatz von privaten Geräten im geschäftlichen Umfeld zugelassen ist. Diese *Policy* muss im Einklang mit den sonstigen Firmenregeln sein, dabei flexibel genug, um den Mitarbeiten die benötigten Freiräume zu gewähren, aber gleichzeitig so konkret, dass eine bestmögliche (Rechts-) Sicherheit gegeben ist. Bei der Erstellung dieser *Policy* sind viele Dinge zu beachten. Dies beginnt bei dem Thema Datenschutz und reicht über rechtliche Aspekte bis hin zum *Support* der Geräte. In Abschn. 2.3 wird der Aufbau und der Inhalt einer *BYOD-Policy* ausführlich beschrieben.

BYOD darf dabei aber nicht singulär betrachtet werden. Vielmehr sollte die Entscheidung für oder gegen eine *BYOD-Strategie* im Rahmen einer zukunftsweisenden Unternehmensstrategie integriert sein. Hierbei wird oft von einer *Mobile-Strategie* gesprochen. Diese Strategie legt fest, wie sich das gesamte Unternehmen zukünftig zu dem Thema mobile Systeme positioniert. Im folgenden Kapitel wird das Thema *Mobile-Strategie* und deren Auswirkungen auf die unterschiedlichsten Bereiche ausführlich besprochen.

2.1 Mobile-Strategie

Mobile Geräte sind aus dem privaten wie auch dem geschäftlichen Alltag nicht mehr weg zu denken. *Smartphone-Nutzer* greifen jederzeit von überall auf Daten und Informationen zu. Was hat das für Auswirkungen auf Unternehmen? Die klassische Art, Informationen an die Kunden heranzutragen (zum Beispiel über *Print-Medien* oder über die offizielle *Homepage*), ist in Teilen überholt und muss angepasst werden. Die *Homepage* muss zum Beispiel darauf vorbereitet sein, dass auch Geräte mit kleinen Bildschirmen darauf zugreifen wollen. Vielleicht kann eine spezielle *App* dem Kunden mehr Informationen zur Verfügung stellen, oder gar einen weiteren Vertriebskanal darstellen. Dies sind Faktoren, die sich nach außen richten. Aber es gibt auch Faktoren, die sich nach innen richten. Wie sollen die Mitarbeiter zukünftig auf interne Daten zugreifen? Von wo ist dies möglich? Welche Vorteile und Nachteile bringt das mit sich? Welche Auswirkungen hat das? All dies muss heutzutage bedacht werden. Grund genug, sich nicht Hals über Kopf in ein Projekt zu begeben, sondern zuerst einen Schritt zurück zu treten und sich dieser Herausforderung strategisch zu nähern. Das Stichwort heißt: *Mobile-Strategie* oder *Mobile-Enterprise*.

Jedes Unternehmen sollte sich grundsätzlich mit dem Thema *Mobile* auseinandersetzen und klar positionieren. Dies sollte bestenfalls im Rahmen einer firmenweiten *Mobile-Strategie* festgehalten werden, die die zukünftige Ausrichtung festlegt. Diese Strategie ist, wie bereits angemerkt, zum einen nach außen gerichtet und zum anderen nach innen. Dies bedeutet, dass die Strategie alle Aspekte der Außen- und Innenwirkung festlegt. Zu den Faktoren mit Außenwirkung zählen alle Aktivitäten rund um das Marketing und den Vertrieb. So muss das komplette Design der *Homepage* überdacht und an die mobilen Gegebenheiten angepasst werden. Wichtige Faktoren sind hier das *Responsive Webdesign*, also

ein *Webdesign*, dass auch *Touch-basierte Geräte* berücksichtigt, und die *User-Experience*, also das Erlebnis des Benutzers auf der Seite. Zusätzlich muss entschieden werden, ob es Sinn macht, eine eigene mobile *App* zu entwickeln, oder entwickeln zu lassen, die hilft, relevantes Wissen an die Kunden heranzutragen, oder sogar eine *App* mit integriertem *Shop* zu gestalten, die einen zusätzlichen Vertriebskanal darstellen kann. Dies alles hat direkte Auswirkungen auf das Kundenverhältnis und sollte daher mit Bedacht geplant und umgesetzt werden. Die hier beschriebenen, nach außen gerichteten Faktoren der *Mobile-Strategie* stellen nur einen Ausschnitt dar. Sie sind sehr wichtig, werden aber in diesem Buch nicht weiter behandelt, da dies den Rahmen des Buches sprengen würde. Zu den angesprochenen Themen existiert aber umfangreiches Material.

Bei den nach innen gerichteten Faktoren der *Mobile-Strategie* geht es um diejenigen, die eine direkte Auswirkung auf die Angestellten oder die interne IT haben. Hierzu zählt zu allererst der Umgang mit mobilen Endgeräten im Unternehmensumfeld. Sollen zukünftig mobile Endgeräte strategisch im Unternehmen eingesetzt werden? Wenn ja: Sind private Endgeräte erlaubt, oder stellt das Unternehmen die Geräte? Diese Frage kommt natürlich sofort auf. Und schon sind wir mitten in einer *BYOD-Diskussion*. Diese Diskussion sollte aber an dieser Stelle erst einmal zurückgestellt werden, da es sehr viele Faktoren zu berücksichtigen gilt und *BYOD* nur einer davon ist.

Eine konsequente *Mobile-Strategie* berücksichtigt nicht nur die mobilen Endgeräte, sondern auch die Applikationen und Daten des Unternehmens. Im Folgenden soll dazu das Beispiel einer klassischen *CRM-* (*Customer Relationsship Management*) *Software* zur Verdeutlichung dienen. Eine *CRM-Anwendung* ist eine der zentralen Anwendungen des Vertriebs. Hier werden alle Kunden-relevanten Daten abgelegt und systematisch verwaltet. Wer gehört zu den Kunden? Wie viel Umsatz macht der Kunde? Wie und wann kommuniziert die Firma mit dem Kunden? Welche Aufträge stehen aus? Welche Verkaufschancen hat der Vertrieb? Usw. Bisher wurde dazu eine klassische *Windows-Anwendung* eingesetzt, die sich mit einer zentralen Datenbank verbindet. Wenn der Vertrieb zukünftig nicht nur mit einem *Laptop* zum Kunden fahren soll, sondern auch mit einem mobilen Endgerät (einem *Tablet* zum Beispiel), dann hat dies enorme Auswirkungen, die vielleicht auf den ersten Blick nicht gleich auffallen. Die bisher eingesetzte *Windows-Anwendung* ist auf einem *Nicht-Windows-Tablet* natürlich nicht lauffähig. Somit muss der Vertriebsmitarbeiter entweder zusätzlich noch den *Laptop* mitnehmen (Aber wofür dann das *Tablet*?), oder die *CRM-Anwendung* erlaubt einen Zugriff über das *Tablet*. Dies kann auf zwei verschiedene Arten geschehen. Zum einen kann eine *Web-basierte Schnittstelle* genutzt werden, die der Hersteller anbietet, oder es muss eine entwickelt werden. Dies hat Vor- und Nachteile. Hier können nämlich hohe Kosten entstehen und außerdem ist eine *Weboberfläche* mit vielen Daten und klassischem *Webdesign* nur sehr schlecht auf einem *Tablet* zu bedienen. Positiv ist, dass eine *Web-basierte Schnittstelle* Endgeräte-unabhängig ist und somit von beliebigen Geräten aus genutzt werden kann. Es bietet sich aber auch eine native *App* für das *Tablet* an. Doch oft existiert keine passende und so müsste auch diese wieder speziell erstellt werden. Selbst wenn das Thema *Web* oder *App* geklärt ist, stellen sich gleich die nächsten Fragen: Wie wird ein sicherer Zugriff über das Internet sichergestellt? Welche

Daten kann der Mitarbeiter auf das Gerät laden? Usw. Vielleicht lässt sich eine mobile Nutzung auch gar nicht darstellen. Dann kommt nur eine Neubeschaffung in Frage. Hier kommen gleich die nächsten Fragen auf: Soll die Lösung überhaupt noch lokal im eigenen Rechenzentrum betrieben werden, oder wird gleich eine *Cloud-basierte Lösung* angeschafft? Aber welche Auswirkungen hat das? Sie sehen, dass allein dieses kleine Beispiel zeigt, wie komplex dieses Thema ist und welche Auswirkungen es haben kann.

Bei all den Möglichkeiten sollte aber eine Frage immer zentral sein: Wo ist der *Business-Mehrwert*? Nur weil etwas technisch möglich ist, von den Angestellten eingefordert oder sogar erwartet wird, ist es nicht immer sinnvoll. Die Begründung für eine *Mobile-Strategie* sollte immer eine *Business-getriebene* sein. Wird das Unternehmen dadurch schneller, agiler, besser? Kann mehr Umsatz generiert werden? Kann die Außenwirkung gesteigert werden? Stehen Kosten und Ertrag in einem günstigen Verhältnis? Nur wenn diese Fragen positiv beantwortet werden können, sollte eine entsprechende Strategie umgesetzt werden.

Eine *Mobile-Strategie* hat auf alle Bereiche eines Unternehmens Auswirkungen. Im Folgenden werden einige aufgezeigt, die im Verlauf des Buches ausführlich beschrieben werden. Zu aller erst fallen natürlich die Auswirkungen auf die IT auf. Eine unternehmensweite *Mobile-Strategie* verlangt auch nach einer neuen (oder zumindest angepassten) IT-Strategie, denn mobile Endgeräte sind nicht mit klassischen IT-Geräten gleichzusetzen. Die Integration von mobilen Endgeräten wirkt sich zum Beispiel auf das lokale Netzwerk aus. *Smartphones* und *Tablets* verbinden sich fast ausschließlich per *WLAN* mit dem Netzwerk. Die vorhandene *WLAN-Infrastruktur* muss somit gegebenenfalls angepasst und erweitert werden, um einen ausreichenden und flächendeckenden Netzwerkzugang zu gewährleisten. Dies zieht eventuell weitere Kosten nach sich. Weiterhin muss im Zweifel über eine neue *VPN-Anbindung* nachgedacht werden, die es erlaubt, dass sich Geräte über das Internet sicher mit der Firmen-internen IT verbinden können. Natürlich müssen dabei die Geräte auch zentral inventarisiert und verwaltet werden. Somit muss auch hierfür eine neue *Software* angeschafft und integriert werden. Wichtiges Stichwort ist hier *Enterprise Mobility Management*. Auch mit den Anwendungen für die mobilen Endgeräte muss sich auseinandergesetzt werden, da sicher nicht jede Anforderung durch eine *App* abgebildet werden kann. All diese Aspekte werden in dem Kap. 4 ausführlich beschrieben.

Darüber hinaus ergeben sich durch eine konsequente *Mobile-Strategie* auch ganz andere und neue Herausforderungen für die Sicherheit. Sicherheitskonzepte müssen neu überdacht und angepasst werden. Datensicherheit und Datenschutz müssen zentral in der Strategie verankert werden. Welche Aspekte hier wichtig sind, wird in Kap. 3 und Abschn. 4.8 beschrieben.

Die *Mobile-Strategie* wirkt sich natürlich auch auf die Mitarbeiter aus. Hier kommen viele unterschiedliche Aspekte zum Tragen. Zum Beispiel: Welche Mitarbeiter (Gruppen) erhalten überhaupt ein mobiles Gerät und warum? Wird es für das Tagesgeschäft benötigt, oder wird es als Anerkennung, Belohnung oder als Statussymbol vergeben? Eine entsprechende Strategie kann aber auch helfen sich in Zeiten des Fachkräftemangels von den Mitbewerbern um Fachkräfte abzuheben. Somit kann eine gute *Mobile-Strategie*