Apps & Mobile Services – Tipps für Unternehmen

Zweite, erweiterte Auflage

BITKOM

Impressum

Herausgeber:	BITKOM Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e. V. Albrechtstraße 10 A 10117 Berlin-Mitte Tel.: 030.27576-0 Fax: 030.27576-400 bitkom@bitkom.org www.bitkom.org
Ansprechpartner:	Tobias Arns (BITKOM e.V.) Tel.: 030.27576-115 t.arns@bitkom.org
Copyright:	BITKOM 2014
Redaktion:	Tobias Arns (BITKOM), Elisa Häusle (BITKOM)
Grafik/Layout:	Design Bureau kokliko / Matthias Winter (BITKOM)
Titelbild:	© istockphoto.com – tumpikuja

Apps & Mobile Services – Tipps für Unternehmen, Zweite, erweiterte Auflage

Apps & Mobile Services – Tipps für Unternehmen

Zweite, erweiterte Auflage

BITKOM

Inhaltsverzeichnis

Autoren

Dieser Leitfaden wurde von einer Projektgruppe des BITKOM-Arbeitskreises Apps & Mobile Services erstellt:

- Tobias Arns | Bereichsleiter Social Media & Mobile, BITKOM
- Stefan Bessing | Director Mobile Strategy, T-Systems Multimedia Solutions
- Christian Buggisch | Leiter Corporate Publishing, Datev
- Marco Gracklauer | Mobile Manager, Datev
- Steffen Hess | Leiter Research Area GoMobile und Teamleiter User Experience, Fraunhofer-Institut für Experimentelles Software Engineering (IESE)
- Christian Klöppel | Head of Mobile Business Center of Excellence, CSC Deutschland
- Sven Portmann | Director Product Management Mobile Solutions, Lufthansa Systems
- Klaus Rodewig | Senior IT Security Analyst, TÜV Trust IT GmbH
- Jürgen Röhricht | Center of Excellence D/A/CH, Mobile Business Solutions, SAP
- Raphael Schulna | Leiter Consulting, adesso mobile solutions
- Dr. Stephan Steglich | Leiter des Kompenzzentrums Future Applications and Media, Fraunhofer Fokus

1 Einleitung

Gerade einmal ein Jahr ist vergangen, seitdem der BITKOM-Arbeitskreis Apps & Mobile Services die erste Auflage dieses Leitfadens veröffentlicht hat. Und dennoch sind nach dieser vermeintlich kurzen Zeit bereits etliche Zahlen, Fakten und Aussagen unserer ersten Publikation überholt. Grund genug, eine Neuauflage anzugehen und Ihnen mit der zweiten Auflage eine aktualisierte und erweiterte Entscheidungshilfe zum Thema Apps & Mobile Services in Unternehmen an die Hand zu geben. Die neue Auflage haben wir außerdem um ein Kapitel über Datenschutz und Datensicherheit ergänzt: In Anbetracht der Diskussionen rund um Prism oder die EU-Datenschutzgrundverordnung eine Pflichtlektüre!

Die Erfolgsmeldungen im mobilen Umfeld sprechen für sich: 90 Prozent aller Deutschen über vierzehn Jahre haben ein Mobiltelefon, mehr als 40 Prozent ein Smartphone. Bei den Neuverkäufen sind rund 80 Prozent der Geräte Mobiltelefone mit Touchscreen und Internetfähigkeit.[1] Auch immer mehr Ältere greifen zum Smartphone. So hat sich der Anteil an Smartphone-Besitzern in der Altersklasse der 50- bis 64-Jährigen innerhalb von sechs Monaten von 26 auf 39 Prozent gesteigert.[2] Jeder zehnte Bundesbürger besitzt zudem einen Tablet Computer, Tendenz steigend. Für das Jahr 2013 ist ein neuer Absatzrekord zu erwarten. Gleichzeitig steigt auch die Zahlungsbereitschaft für Apps und mobile Lösungen.[3]

Zusätzliche Anwendungen (sogenannte Apps), die Nutzer auf ihrem Gerät installieren, sind besonders beliebt: Rund 1,7 Milliarden Apps wurden 2012 in Deutschland heruntergeladen. Eine Steigerung von 80 Prozent gegenüber dem Vorjahr und ein erzielter Gesamtumsatz von 430 Millionen Euro. Nicht wenige Nutzer installieren mehr als vierzig mobile Anwendungen auf ihr Gerät.[4]

Grund genug, den Trend »Mobile« ernst zu nehmen und der Erwartungshaltung der gesamten Gesellschaft gerecht zu werden. Information und Interaktion zu jeder Zeit, an jedem Ort – auch mit Ihrem Unternehmen – ist heute alles andere als ein Hype und steht deshalb zwingend auch auf der Agenda Ihres Unternehmens.

Mobile Business und Enterprise Mobility sind begriffliche Klammern für eine Vielzahl von Konzepten und Angeboten für Unternehmen. Dabei wird unter Mobile Business eher die Nutzung mobiler Anwendungen und -services zur Unterstützung der Unternehmensziele und zur Förderung des Geschäftserfolgs verstanden, während Enterprise Mobility eher das Management der mobilen Geräte, Anwendungen und Inhalte innerhalb von Unternehmen meint. Von Bring your own Device (BYOD) über die Mobilisierung der eigenen Website bis hin zur Entwicklung eigener Apps gibt es in diesem Umfeld viele Herausforderungen für Unternehmen, die dieser Entwicklung Rechnung tragen und den wachsenden Anforderungen, z. B. in puncto Sicherheit und User Experience entsprechen wollen. Dieser Leitfaden will Ihnen daher einen ersten Überblick über das komplexe Thema vermitteln und Ihren Entscheidungen eine solide Wissensgrundlage geben.

Smartphones und Tablets integrieren und kombinieren Eigenschaften ursprünglich ganz verschiedener Geräte. Dadurch eröffnen sie nicht nur privaten Nutzern, sondern auch Unternehmen völlig neue Möglichkeiten. So wird beispielsweise bei Augmented-Reality-Anwendungen ein Bild der Smartphone-Kamera in Kombination mit dem ermittelten Standort sowie einem Lagesensor mit Inhalten aus einer Internet-Datenbank angereichert – das Smartphone »weiß«, wo Sie sind, was Sie gerade sehen,

1 BITKOM-Presseinformation: 63 Millionen Handy-Besitzer in Deutschland (www.bitkom.org/de/presse/8477_77178.aspx)
2 BITKOM-Presseinformation: Auch Ältere steigen auf Smartphones um (www.bitkom.org/de/presse/8477_76387.aspx)
3 BITKOM-Presseinformation: Tablet Computer werden zu Allround-Geräten (www.bitkom.org/de/presse/8477_76932.aspx)
4 BITKOM-Presseinformation: Umsatz mit Apps hat sich 2012 mehr als verdoppelt (www.bitkom.org/de/presse/8477_76094.aspx)

und sagt Ihnen, was Sie in dieser Situation vielleicht noch wissen wollen. Diese enormen technischen Möglichkeiten, genauer: deren Ausschöpfung als Ergebnis komplexer Mobile-Projekte, sind beeindruckend, sollten aber im unternehmerischen Kontext immer konkreten Zielen und Anwendungsszenarien unterliegen, um Mehrwert zu erzeugen und um mehr zu sein als eine elegante Spielerei.

Dieser Leitfaden beantwortet daher jene Fragen, die Sie sich zum Thema Mobile in Ihrem Unternehmen stellen sollten, und zeigt Ihnen, warum es nur dann sinnvoll ist, »eine App zu machen«, wenn diese einem klar benennbaren Unternehmensziel dient, einer abgestimmten Strategie folgt und die Anwender über einen konkreten Nutzen mit Ihrem Unternehmen verbindet, ihn als Kunden oder Mitarbeiter folglich nie aus dem Blick verliert.

Nach einer kurzen Einführung vermitteln Ihnen zahlreiche Beispiele einen Überblick über die unternehmerische Bedeutung von Mobile und darüber, welche Anwendungsszenarien auch für Ihr Unternehmen entstehen. Die anschließenden Kapitel unterstützen Sie dabei, Mobile-Projekte sinnvoll vorzubereiten und erfolgreich durchzuführen, zahlreiche Checklisten helfen Ihnen, den Überblick zu behalten. Im Glossar am Ende des Leitfadens finden Sie schließlich Erläuterungen zu den wichtigsten Fachbegriffen aus dem Mobile Umfeld.

2 Was bedeutet Mobility für Unternehmen? Mögliche Anwendungsgebiete von Enterprise Mobility?

Die zunehmende Verbreitung von mobilen Endgeräten markiert nicht nur den Beginn der Post-PC-Ära, sie zwingt auch Unternehmen zum Umdenken. Mittlerweile werden Geschäftsprozesse vermehrt auf Basis von mobilen Plattformen realisiert und damit nicht nur Mitarbeitern, sondern auch Kunden zugänglich gemacht. »Mobile« ist längst viel mehr als der Zugriff auf E-Mails, Kalender und Kontakte.

Apps für Smartphones und Tablets, die sich an Konsumenten richten, prägen hierbei die Nutzererwartungen und werden so auch zum Maßstab für mobile Unternehmensanwendungen. Diese »Consumerization of IT« ist längst ein zentraler Faktor der mobilen Revolution. Dies betrifft sowohl die Qualität und User Experience der mobilen Lösungen, als auch die Geschwindigkeit, mit der sie im Unternehmen eingeführt werden. Intuitive Bedienbarkeit und eine als innovativ wahrgenommene Benutzeroberfläche sind bei mobilen Anwendungen das A und O des Erfolges. Denn die Ansprüche an die User Experience sind mit dem Erfolg moderner Smartphones und Tablets stark gestiegen.

Soll ein Mobile-Projekt also Erfolg haben und von den Nutzern gut angenommen werden, so ist eine enge Zusammenarbeit zwischen IT-Abteilung und der Fachabteilung, in der die Anwender arbeiten, bereits in der Konzeptphase notwendig. Die IT-Abteilungen, die in den letzten Jahren nicht überall eine Vorreiterrolle in Sachen Enterprise Mobility übernommen haben, müssen sich daher erneut als »Enabler« profilieren.

Aufgrund der Vielzahl von Geräten und Plattformen steigt dabei sowohl für Entwickler als auch für Anwender die Zahl der Entscheidungsmöglichkeiten; damit wachsen gleichzeitig die Ansprüche an die Integrationsfähigkeit der mobilen Dienste und an die Einheitlichkeit bei der Bedienbarkeit der Lösungen. Die Anpassung von Applikationen und Services an die Erwartungen der Nutzer führt die Unternehmen dabei im Idealfall zu ganz neuen Ansätzen.

Wichtige Sicherheitserfordernisse oder die Bereitstellung notwendiger Schnittstellen zu Backend-Systemen dürfen natürlich auch bei mobilen Anwendungen nicht vernachlässigt werden. Häufig hapert es jedoch gerade hier: Oft sind weder die bestehenden IT-Sicherheitskonzepte auf den Zugriff durch mobile Geräte zugeschnitten noch sind die bestehenden IT-Systeme ohne weiteres von mobilen Geräten aus erreichbar. So wurde beispielsweise in der Vergangenheit verstärkt auf Thin Clients und Server Based Computing gesetzt. Für den Einsatz mobiler Anwendungen sind aber intelligente Konzepte zur Online- und Offline-Nutzung notwendig. Dies erfordert wiederum neue Herangehensweisen bei der Datenhaltung und damit verbunden auch neue Sicherheitskonzepte. Für IT-Abteilungen und -Dienstleister verlagert sich der Schwerpunkt durch diese Veränderungen weg von der Entwicklung spezialisierter, komplexer, in sich geschlossener Systeme und Thin Clients hin zu interagierenden Plattformen und intelligenten Clients, die über standardisierte und moderne Schnittstellen miteinander kommunizieren.

Anwendungsgebiete von Mobile Business

Schaut man sich die Alternativen bei mobilen Lösungen für Unternehmen genauer an, so können einige Anwendungscluster identifiziert werden:

- Für das produzierende Gewerbe etwa werden mobile Anwendungen im Service und Support (z. B. Bearbeitung von Reparatur- und Supportanfragen) immer wichtiger. Hier eröffnen mobile Lösungen – insbesondere in Kombination mit Social-Media-Ansätzen – einen zusätzlichen Kommunikationskanal zum Kunden.

- Zahlreiche Unternehmen setzen bereits auf Tablet-Anwendungen zur Unterstützung der eigenen Vertriebs- und Servicemitarbeiter. Dabei werden CRM-Systeme, Informationen zum Bestellvorgang sowie Produkt- und Ersatzteilkataloge mobil verfügbar gemacht und mit verbesserten, interaktiven Darstellungen angereichert. Dies zielt auf eine Verbesserung der Beratungs- und Servicequalität beim Kunden.

- Für einige Unternehmen werden mobile Kanäle auch zum integrierten Produktbestandteil. Zu denken wäre hier beispielsweise an die Steuerbarkeit einer Heizung oder eines TV-Gerätes via Smartphone – als Ersatz für die Fernbedienung. Der Trend, das Smartphone in dem beschriebenen Sinne zur Steuerung von Geräten einzusetzen, wird sich in Zukunft in Verbindung mit Connected Home Technologien mit Sicherheit noch verstärken.

- Für das dienstleistende Gewerbe treffen die obigen Punkte in abgewandelter Form ebenfalls zu. Vor allem bieten mobile Anwendungen hier Möglichkeiten zu einer Aufwertung der bisherigen Service- und Vertriebskanäle.

- Für alle Branchen rücken im internen Einsatz vor allem Reporting- und Genehmigungsprozesse in den Vordergrund. Entscheider, die viel unterwegs arbeiten, können Pausen und Wartezeiten nutzen, um aus der Ferne Geschäftsvorgänge voranzutreiben, deren weiterer Fortgang sonst auf ihre Rückkehr ins Unternehmen hätte warten müssen.

- Auch im Marketing und Branding werden mobil optimierte Websites und Apps natürlich immer wichtiger.

Smartphones und Tablets – dies lehrt die rasante Entwicklung – werden zum primären Zugangskanal der Unternehmen zu ihren Kunden und Mitarbeitern und gleichzeitig zu einem zentralen Instrument im Service und Vertrieb. Durch die Consumerization of IT steigen zusätzlich die Erwartungen von Kunden und Mitarbeitern an die entsprechenden Lösungen und die Geschwindigkeit bei der Einführung. Diese Tatsachen sollten sowohl bei strategischen Entscheidungen wie auch bei der Planung neuer Projekte berücksichtigt werden.

3 Auf dem Weg zur idealen mobilen Anwendung: Strategie und Vorüberlegungen

Die Entscheidung, mobile Anwendungen und Services zu entwickeln, sollte keinem »spontanen« Impuls folgen, sondern eine bewusste und strategische Entscheidung für die Nutzung des mobilen Kanals sein. Daher sollte vor der Entwicklung von mobilen Anwendungen und Diensten eine Reihe von Vorüberlegungen stehen.

Zielgruppe und Ziele

Zu Beginn müssen zunächst die Zielgruppe und Ziele definiert werden. Mögliche Zielgruppen für mobile Anwendungen und Services sind Neu- und/oder Bestandskunden, eigene Mitarbeiter im Service oder Vertrieb oder Geschäftspartner im B2B-Umfeld.

Ausgehend von der Zielgruppe kann das Unternehmen dann die Ziele bestimmen, die mit der mobilen Lösung erreicht werden sollen. Diese Zieldefinition ermöglicht die Ausrichtung der geplanten Anwendungen auf die Zielgruppe. Eine App als Marketingmaßnahme zur Steigerung der Markenbekanntheit und Steuerung des Images verfolgt andere Ziele als eine Anwendung zur Vertriebsunterstützung und Optimierung interner Geschäftsprozesse. Die Definition der Zielgruppe und Ziele ist daher entscheidend für Art und Umfang der Mehrwerte, die den künftigen Nutzern sowie dem Unternehmen durch einen mobilen Service geboten werden können.

Ein Beispiel: »Umsatzsteigerung durch mehr Kundenbesuche pro Vertriebsmitarbeiter pro Tag« ist ein konkretes Ziel für die Optimierung des eigenen Vertriebs. Damit der Vertrieb mehr Zeit für Kundenbesuche hat, soll mittels einer mobilen Applikation der Prozess der Besuchsvor- und -nachbereitung verbessert werden. Ziele und Zielgruppe sind also definiert. Eine mobile Applikation, mit der die Vertriebsmitarbeiter immer und überall Zugriff auf Kundendaten und relevante Vertriebsdokumente haben und mit der sie ihre Besuchsberichte elektronisch erfassen und übermitteln können, würde einen hohen Mehrwert bieten. Ist die Anwendung darüber hinaus in der Lage, sich mit dem CRM-System zu synchronisieren, so dass die Mitarbeiter unterwegs noch zusätzliche Termine auf ihrer Route wahrnehmen können, ist es sehr wahrscheinlich, dass das übergeordnete Ziel erreicht wird.

Vom Konzept zur Feinspezifikation

Entschließt sich ein Unternehmen zur Umsetzung eines mobilen Projektes, so muss zunächst ein Konzept hierfür entwickelt werden. Dieses Konzept stellt die Grundlage für die Feinspezifikation dar und ist deshalb von hoher Wichtigkeit für den Projekterfolg. Im Konzept werden die Ziele und Zielgruppen definiert sowie die Vorteile der mobilen Anwendung gegenüber den bisherigen Lösungen beschrieben. Das Konzept dient der internen Abstimmung und Entscheidungsfindung über Inhalte und Funktionen des künftigen mobilen Services. Daher sollten bereits in dieser Phase alle relevanten Projektbeteiligten im Unternehmen (Fachabteilungen, IT-Abteilung, Datenschutzbeauftragter, ggf. Betriebsrat etc.) einbezogen werden.

Oft entstehen Konzepte ohne die Beteiligung der definierten Zielgruppe, die später mit der Anwendung arbeiten bzw. von ihr profitieren soll. Da eine breite Akzeptanz bei der Zielgruppe aber für den Erfolg mobiler Anwendungen entscheidend ist, können Vertreter der Nutzer bereits in der Konzeptphase wichtigen Input liefern (vgl. Kap. 4). Bezogen auf das oben skizzierte Beispiel könnten z. B. die Vertriebsmitarbeiter beschreiben, welche Kundeninformationen und Dokumente benötigt werden und bei welchen Tätigkeiten eine mobile Unterstützung im Tagesgeschäft tatsächlich sinnvoll ist.

Nach der Konzepterstellung erfolgt die Feinspezifikation der mobilen Anwendung, in der diese detailliert beschrieben wird. Hier wird unter anderem bestimmt, ob eine browserbasierte Anwendung oder eine plattformspezifische App entwickelt werden soll (vgl. Kap. 5). Inhalte und Funktionen der Anwendung werden innerhalb des Feinkonzeptes ebenso beschrieben, wie das Navigationskonzept und das Design der Benutzeroberfläche.

Sofern relevant, sollte die Definition der Datenübertragung, -haltung und -sicherheit einen Schwerpunkt der Feinspezifikation bilden. In der Regel werden die Daten nicht statisch auf dem mobilen Gerät gespeichert, sondern dynamisch von einem Server an das mobile Endgerät übertragen. Hier muss also definiert werden, wie die Daten von den Servern zu den Geräten gelangen und ob es sich um Daten handelt, die durch Verschlüsselung vor unbefugtem Zugriff geschützt werden müssen (vgl. Kap. 6).

Da bei mobiler Nutzung (noch) nicht von einer vollständig unterbrechungs- und störungsfreien Internetverbindung ausgegangen werden kann, muss die eingeschränkte Konnektivität des Gerätes bei der Anwendungskonzeption immer bedacht werden. Eine Möglichkeit zum Offline-Arbeiten und zur späteren Synchronisierung der Daten mit dem Server sollte daher implementiert werden.

Agile Entwicklungs- und Projektmanagementmethoden

Bei der Entwicklung mobiler Anwendungen werden zunehmend agile Methoden anstelle des klassischen Modelles der Anwendungsentwicklung (Anforderungsanalyse → Spezifikation → Entwicklung → Test) bevorzugt. Durch den iterativen Prozess der agilen Entwicklung, mit dem die Lösung nicht als Ganzes, sondern Schritt für Schritt entwickelt wird, können auch während der Umsetzungsphase neue oder geänderte Anforderungen berücksichtigt werden, die bei klassischen Entwicklungsmethoden zu erheblichen Verzögerungen oder Verteuerungen des Projekts geführt hätten.

Agile Entwicklungs- und Projektmanagementmethoden eignen sich besonders dann, wenn der endgültige Funktionsumfang der mobilen Lösung zu Beginn der Entwicklungsphase noch nicht genau definiert werden kann oder wenn unterschiedliche Lösungsszenarien getestet werden sollen (z. B. native Anwendung vs. hybride Lösung).

Für die Kalkulation gilt es jedoch zu bedenken, dass agile Projekte in der Regel nicht als Festpreis- sondern als T&M-Projekte (Time and Material, Abrechnung nach Aufwand) durchgeführt werden müssen.

4 Vom Nutzungskontext zum Interaktionskonzept

Wie bereits in Kapitel 3 erläutert: Voraussetzung für die erfolgreiche Implementierung von Mobile-Business-Projekten ist eine systematische und zielgerichtete Herangehensweise. Die spontane Äußerung »Wir brauchen eine App« ist keinesfalls ausreichend. Die Weichen für den Erfolg werden bereits in der Konzeptphase einer mobilen Lösung gestellt, in der die Zielgruppe und die zu erreichenden Ziele in Form von Anforderungen definiert werden müssen.

Bereits in der Konzeptphase sollte insbesondere der Nutzungskontext der Anwendung beschrieben werden, der u.a. die Aspekte Einsatzzweck, Einsatzort, Nutzer, Nutzungssituation (psychische Situation des Nutzers und Umgebungseinflüsse) und das Endgerät beinhaltet. Mobile Anwendungen sollen ja zunächst dem Nutzer einen konkreten Mehrwert bieten und nicht zuletzt auch Spaß machen. Eine gute mobile Anwendung bietet für den jeweiligen Nutzungskontext die optimale Unterstützung und ist schnell sowie intuitiv bedienbar. Hierfür ist das Interaktionsdesign der Anwendung von hoher Bedeutung: Es gilt, aus dem zur Verfügung stehenden Spektrum an Interaktionsmöglichkeiten, die am besten geeigneten für die entsprechende Anwendung auszuwählen und diese dann so zu gestalten, dass eine optimale User Experience erreicht wird. Zielführend für mobile Business-Anwendungen ist also eine klare Fokussierung auf den Interaktionsablauf zwischen Nutzer und Anwendung in Kombination mit der übergeordneten Arbeitsaufgabe des Nutzers.

Um bei mobilen Anwendungen – egal ob native Apps oder webbasierte Anwendungen – exzellente Usability und User Experience zu erreichen, ist neben der systematischen Vorgehensweise auch Agilität im Projektmanagement gefragt. Sowohl das User Interface als auch das Interaktionsdesign müssen bereits bei der Erstellung eng mit anderen Entwicklungsaufgaben wie z. B. dem Design der Software-Architektur verwoben sein. Abbildung 1 zeigt, wie das Interaktionskonzept in einen ganzheitlichen Erstellungsprozess einer mobilen Anwendung eingebunden werden kann.

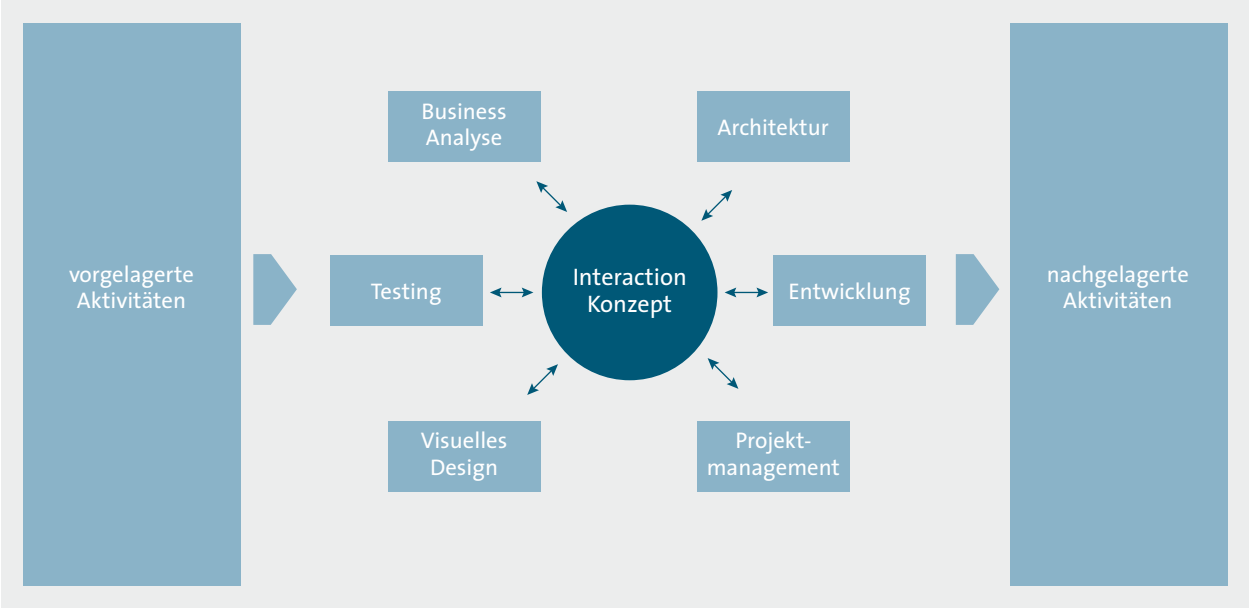

Abbildung 1: Das Interaktionskonzept in Relation zu anderen Aspekten einer mobilen Anwendung

Entwicklung des Interaktionskonzepts als iterativer Prozess

Die ganzheitliche Entwicklung eines Interaktionskonzepts sollte als iterativer Prozess verstanden werden:

- Nach der Erhebung aller relevanten Informationen für das Interaktionsdesign wird dieses von einem Projektverantwortlichen als Entwurf spezifiziert, an die Nutzer und den Fachbereich zurückgespielt und anschließend validiert. Hierbei sollte auf interne Experten oder externe Dienstleister zurückgegriffen werden, die das Nutzungsverhalten der Zielgruppe, einschlägige Best Practices sowie die Besonderheiten der gewählten mobilen Plattform kennen. Je nach Umfang des Projekts ist darauf zu achten, ausreichend Zeit und Ressourcen hierfür vorzusehen. Verschiedenste Rollen (z. B. User Interface Designer, Usability-Ingenieure, Produktmanager oder Software-Entwickler) können das Interaktionsdesign entwickeln, bei der Auswahl der Verantwortlichen sollte aber darauf geachtet werden, dass deren Wissen über User Experience, Usability und User Centered Design auf dem neuesten Stand ist.

- Die Praxis zeigt, dass zwei bis drei Iterationen der Entwürfe mit den Nutzern sowie dem Fachbereich ausreichend sind. Die Erstellung des Interaktionsdesigns besteht im Wesentlichen aus der Gestaltung von Prototypen (sog. Screenflows und / oder Prototypen auf Papier), die dazu dienen, den Projektverantwortlichen, Nutzern und Entscheidern einen ersten Eindruck der Applikation zu vermitteln. Durch den iterativen Prozess werden die Darstellung der Informationen auf dem Screen und die Bedienung derart an den Bedürfnissen der Nutzer ausgerichtet, dass schließlich eine Anwendung mit optimaler User Experience entsteht. Wichtig hierbei ist, dass technische und organisatorische Einschränkungen diesen Prozess nicht dominieren, damit bei der Umsetzung innovative Wege beschritten werden können.
  Das Motto »Das haben wir schon immer so gemacht« ist hier fehl am Platz.

Um die notwendige Informationsbasis für die Erstellung des Interaktionskonzepts zu erhalten, sollten folgende Informationen von den Projektverantwortlichen zusammengestellt werden:

- Nutzungskontext der Anwendung
- Zielgruppe und Ziele (inkl. Ziele für die User Experience)
- Beschreibung von Personas (eine Persona stellt einen für eine Gruppe von Nutzern typischen User dar, der zu Konzeptionszwecken mit konkreten Eigenschaften und einem entsprechendem Nutzungsverhalten ausgestattet wird)
- Beschreibung des aktuellen Prozesses, der durch die mobile Lösung verbessert werden soll
- Probleme des aktuellen Prozesses
- Zielvorstellung des Sollprozesses
- Mehrwert und Hauptfunktionen der Lösung
- Technische und organisatorische Einschränkungen, z. B. Verfügbarkeit von Geräten, Sicherheitsbestimmungen

Auf Basis dieser Daten kann dann zunächst die Auswahl einer für die Anwendung geeigneten Geräteklasse (Smartphone vs. Tablet) erfolgen. Maßgebliche Rahmenbedingungen hierfür sind die Hauptfunktionen der Anwendung und der Nutzungskontext. Dabei ist auch zu beachten, welche und wie viele Informationen dem Nutzer zugänglich gemacht werden müssen. Benutzt er die Anwendung dauerhaft als sogenannte primäre Aufgabe oder führt er nur eine sekundäre Aufgabe durch, während er primär an etwas anderem arbeitet?

Von den Anwendungsfällen zum Interaktionsdesign

Um den Mehrwert der mobilen Anwendung weiter zu spezifizieren, sollten als nächstes die einzelnen Anwendungsfälle, die mit ihr abgedeckt werden sollen, so detailliert wie nötig beschrieben werden. Alle Anwendungsfälle werden dazu in einem Ablaufdiagramm miteinander in Verbindung gebracht, um ihre Abfolge und Abhängigkeiten zueinander zu dokumentieren.

Anschließend kann ein erster Design-Prototyp in Form eines schematischen, funktionalen Modells erstellt werden – mithilfe eines sogenannten Wireframes. Zunächst reicht es hier, einfache Skizzen anzufertigen, z. B. mit einem Zeichenprogramm oder auf Papier. Wichtig ist es aber, bereits in dieser Phase ausgewählte künftige Anwender einzubinden und deren Feedback einzuholen.

Ein erweiterter Test durch Anwender sollte allerdings frühestens nach der ersten Iteration der dargestellten Vorgehensweise stattfinden. Dieser kann mit einem sogenannten Clickdummy durchgeführt werden. Ein Clickdummy ist ein nicht funktionaler Prototyp, der auf Wireframes basiert und der sich in der Interaktion mit dem Nutzer ähnlich verhält wie eine echte Anwendung. Für die Erstellung von Clickdummys gibt es eine Reihe von kostenpflichtigen und kostenfreien Tools. Neben Vorlagen für Präsentations-Software wie Microsoft PowerPoint, gibt es webbasierte Tools[5] , Desktop-Anwendungen sowie Apps für Smartphones und Tablets.

Die Wireframes und der Clickdummy ermöglichen jetzt mit den zugeordneten Anwendungsfällen einen ganzheitlichen Blick auf die Navigation der späteren App und dienen als Grundlage für die Entwickler sowie die User Interface Designer, die die mobile Anwendung schließlich nach den erarbeiteten Anforderungen umsetzen. Zusätzlich kann man die Benutzer testen lassen, inwiefern sie bestimmte Interaktionsabläufe mit der Anwendung reibungslos durchführen können. Durch solche Nutzertests oder Nutzerstudien erhält man wertvolles Feedback zur Optimierung des Interaktionskonzeptes und verhindert, dass die Anwendung von den künftigen Nutzern abgelehnt wird.

5 z. B. www.clickdummy.com

5 Die Plattformfrage: Vor- und Nachteile von nativen und browserbasierten mobilen Anwendungen

Nachdem sich die vorigen Kapitel vor allem mit der Konzeption und Planung eines Mobile-Projekts beschäftigten, erfahren Sie nun, welche technischen Ansätze zur Entwicklung mobiler Angebote existieren. Im Allgemeinen wird zwischen nativ und web- bzw. browserbasiert entwickelten Apps unterschieden. Die gewählte Strategie hat unmittelbaren Einfluss auf zahlreiche Faktoren, an die wir Sie nun heranführen möchten.

5.1 Wie können mobile Anwendungen entwickelt werden?

Bei der Entwicklung von Apps ist es wichtig, die unterschiedlichen Ansätze der Plattformbetreiber und die jeweiligen Besonderheiten zu kennen. Die aktuell relevanten mobilen Plattformen unterscheiden sich nämlich im Detail deutlich:

- Eingesetzte Programmiersprache
- Zugriff auf Geräteressourcen (z. B.: Kamera, GPS-Sensor, Telefonie, SMS) und die dafür eingesetzten Software Development Kits (SDKs)
- Sicherheitskonzepte, die den Zugriff auf diese Ressourcen in unterschiedlichen Ausprägungen erlauben
- Generelle »Spielregeln« im Ökosystem (Marktplätze, Entwicklungs- und Veröffentlichungsrichtlinien, Update-Zyklen, Umsatzbeteiligungen)
- Nicht zu vergessen: Die Verbreitung der Plattform bei der Zielgruppe und deren durchschnittliche Zahlungsbereitschaft.[6]

Native Apps

Als native App werden Programme bezeichnet, die speziell mit den Software Development Kits und der Programmiersprache der jeweiligen Plattform entwickelt wurden und die als »echte« Programme direkt vom Betriebssystem ausgeführt werden. Sie zeichnen sich in der Regel durch eine hohe Performance und eine gute Anpassung an die Plattform aus. Native Apps werden über die Marktplätze der Plattformbetreiber vertrieben. Nativ entwickelte Anwendungen laufen immer nur auf der Plattform, für die sie entwickelt wurden.

Web Apps

Webbasierte Anwendungen oder Web Apps werden anders als native Apps in einem Browser ausgeführt. Die Fähigkeiten einer Webanwendung sind daher immer begrenzt durch den Funktionsumfang, den der Browser bereitstellt.

Neue Standards wie HTML5 und CSS3 ermöglichen die Programmierung technisch und optisch hochwertiger Lösungen, die oft mit nativen Apps mithalten können. Allerdings ist der Zugriff auf Hardwarefunktionen, z. B. Kamera, bei Webanwendungen oft nur eingeschränkt möglich. Ein Vorteil von Web Apps ist die plattformübergreifende Unterstützung in modernen Browsern: So können diese meist ohne Anpassung auf allen mobilen Plattformen ausgeführt werden. Auch sind webbasierte

6 Laut Mobile Zeitgeist ist der bei Apple/iOs erwirtschaftete Umsatz durch App-Verkäufe für Entwickler im Durchschnitt 4 bis 8 mal so hoch wie bei Android / Google Apps (www.mobilbranche.de/2013/10/neuer-investor-board/39654)

Anwendungen, verglichen mit nativen Anwendungen, meist einfacher und kostengünstiger zu erstellen.

Eine Webanwendung kann nicht über die Marktplätze der Plattformen vertrieben werden, muss daher aber auch keinen Genehmigungsprozess zur Bereitstellung durchlaufen. Die Anwendung wird auf einem Web-Server betrieben und kann von einem Administrator unabhängig vom Plattformbetreiber verwaltet und aktualisiert werden.

Webbasierte Anwendungen sind in der Regel etwas langsamer als native Anwendungen, das typische »App-Gefühl« der schnell laufenden nativen Anwendungen stellt sich bei Web Apps häufig nicht ein. Ob besonders zeitkritische Anwendungen oder Apps mit starkem Fokus auf die User Experience als reine Web App umgesetzt werden, sollte kritisch geprüft werden, denn die Ansprüche der Anwender an die Geschwindigkeit mobiler Anwendungen sind mitunter sehr hoch.

Neue mobile Plattformen wie z. B. FirefoxOS oder Tizen setzen verstärkt auf Web-Technologien, es wird abzuwarten sein, inwiefern sich diese am Markt durchsetzen.

Hybride Apps

Hybride Anwendungen versuchen die Vorteile von webbasierten Anwendungen mit denen der nativen Apps zu kombinieren. Eine hybride Anwendung unterstützt mit einem meist vertretbaren Mehraufwand auch andere Plattformen. Mit hybriden Anwendungen ist außerdem der Zugriff auf nahezu alle Systemfunktionen möglich. Für hybride Apps gibt es zwei unterschiedliche Entwicklungsansätze:

Beim ersten Ansatz wird eine Anwendung entwickelt, die einen integrierten Webbrowser enthält, der die webbasierte Anwendung darstellt. Der native Rahmen der App stellt zusätzliche Funktionen (z. B. Kamera) bereit, auf die eine reine Web App nicht zugreifen könnte.

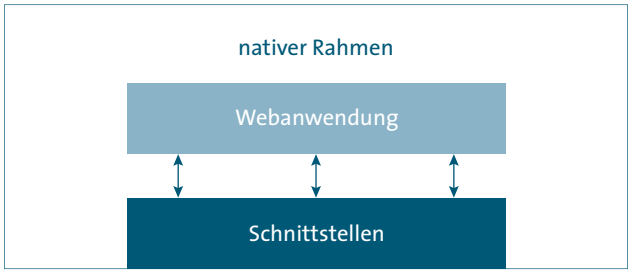

Abbildung 2: Nativer Container mit integrierter Webanwendung

Der zweite Ansatz basiert auf dem Konzept des Cross Platform Development, das zum Ziel hat, möglichst viel Programmcode plattformübergreifend zu programmieren. Dieser wird dann mittels eines Frameworks in plattformspezifischen Code konvertiert.

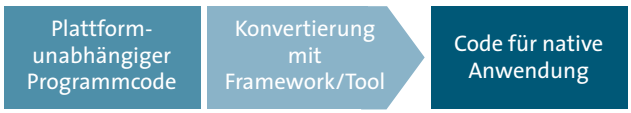

Abbildung 3: Umwandlung von plattformunabhängigem Anwendungscode in Code der nativen Anwendung

Der Vorteil hybrider Apps ist vor allem ein wirtschaftlicher, da Teile des Programmcodes für mehrere Plattformen verwendet werden können. Das reduziert den Entwicklungsaufwand und damit die Kosten. Außerdem können hybride Apps wie native Apps direkt über die Marktplätze der Plattformbetreiber vertrieben werden.

Mobil optimierte Websites

Die optimierte Darstellung einer klassischen Website für mobile Endgeräte muss von echten Apps, egal ob nativ, hybrid oder webbasiert abgegrenzt werden. Eine mobil optimierte Website, auch als Mobilportal bezeichnet, ermöglicht es Nutzern, die Webseite auch mit einem kleinen Smartphone-Display optimal zu benutzen. Das gilt im Prinzip auch für komplexe Websites wie z. B. Online-Shops.

Oft ist es für Unternehmen ausreichend, eine mobil optimierte Variante der eigenen Website anzubieten. Insbesondere zur Darstellung statischer Inhalte (z. B. Kontaktinformationen, Unternehmensvorstellung, Anfahrtsbeschreibung) ist keine App in den Marktplätzen notwendig.

Eine besondere Herausforderung mobiler Websites ist es, die oft komplexe Navigationsstruktur einer Website zu übertragen. Die Nutzer müssen auch mit einem Smartphone die für sie relevanten Informationen und Funktionen schnell finden können und die Struktur der Website im Überblick haben. Außerdem sollte die zu übertragende Datenmenge der Website möglichst gering sein, dies wird u.a. durch Komprimierung erreicht.

Die verschiedenen Betriebssysteme, Browser, Bildschirmgrößen und -auflösungen machen mobile Website-Projekte oft komplex. Der Testaufwand sollte in keinem Fall unterschätzt werden und ist durchaus mit dem von Apps zu vergleichen. Um den Test- und Entwicklungsaufwand zu begrenzen, existieren am Markt einige Anbieter, die mit Hilfe von Middleware bestehende Websites als Datenquelle nutzen und automatisch optimierte mobile Varianten ausliefern. Mit Hilfe dieser Software lassen sich auch komplexe Websites und Online-Shops auf mobilen Geräten darstellen.

Responsive Webdesign

Responsive Webdesign ist ein noch recht junges Entwicklungs- und Designkonzept, bei dem Websites so angelegt werden, dass sie sich beim Laden an das jeweils anfragende Gerät anpassen und im Idealfall immer optimal dargestellt werden. Technisch gesehen wird dabei immer die gleiche Website ausgeliefert, jedoch werden je nach zur Verfügung stehender Bildschirmgröße vorher definierte Elemente (z. B. Textabsätze, Navigationselemente, Bilder) anders angeordnet oder verkleinert. Oft wird die Webseite dazu bei der Konzeption in mehrere Spalten unterteilt. Ein Smartphone stellt dann etwa die einspaltige Variante dar, ein Tablet die zweispaltige und ein Laptop die maximale, dreispaltige Ansicht. Einige Entwickler berichten, dass es die Programmierung und Optimierung einer responsiven Website vereinfacht, wenn die mittlere Variante für Tablet als Standard-Website behandelt wird und die kleinere Smartphone- sowie die größere Desktop-Varianten als Ableitungen von diesem Standard definiert werden. Eine besondere Herausforderung ist auch beim Responsive Design die Organisation der Navigation. Auch der technische Aufwand zur Programmierung und zum Test einer gut funktionierenden responsiven Website darf nicht unterschätzt werden.

5.2 Welcher mobile Anwendungsansatz ist der Richtige für mein Unternehmen?

Der für Ihr Unternehmen und Ihr Mobil-Projekt richtige Ansatz ist von einer Reihe an technischen und wirtschaftlichen Faktoren abhängig:

- Möchten Sie mit Ihrer Anwendung auf Hardwarekomponenten (z. B. Kamera) zugreifen, oder Inhalte auch offline zur Verfügung stellen, ist eine native oder zumindest hybride App zurzeit die bessere Wahl. Mit Webtechnologie können Sie derzeit hier noch nicht das Potenzial der Plattformen und Geräte ausschöpfen.

- Auch lassen sich besonders sensible Unternehmensdaten mit nativer Technologie z. B. bei der Kommunikation zwischen App und Server besser absichern und verschlüsseln.

- Die Entwicklungsaufwände und -kosten unterscheiden sich zwischen den verschiedenen Ansätzen deutlich. Sollten Sie für Ihr Projekt mit mehreren Zielplattformen planen, so ist es meist günstiger einen hybriden oder webbasierten App-Ansatz zu wählen, da dann zumindest Teile des Programmcodes wiederverwendet werden.

- Der Vertrieb über die Marktplätze der Plattformanbieter ist nur für native und hybride Apps möglich. Marktplätze für Web Apps haben derzeit nur eine geringe Verbreitung und Sichtbarkeit.

Welche Folgen hat eine Entscheidung für einen der Ansätze?

Es gibt eine Reihe von Konsequenzen die sich aus der Entscheidung für eine native, webbasierte oder hybride Lösung ergeben:

- Generell gilt, dass Wartungs- und Update-Kosten bei mobilen Anwendungen nicht unterschätzt werden dürfen. Auch bei diesen Kosten sind hybride und webbasierte Anwendungen gegenüber nativen Apps im Vorteil.

- Webbasierte Apps, insbesondere wenn sie auf dem eigenen Server gehostet werden, können jederzeit und unabhängig von Genehmigungsprozessen der Plattformbetreiber aktualisiert und gewartet werden.

- Die übliche Umsatzbeteiligung der Plattformbetreiber, meist 30 Prozent des Verkaufspreises, entfällt bei einer Distribution außerhalb der Marktplätze. Allerdings müssen Sie sich dann selbst um ein geeignetes Vertriebs- und Abrechnungssystem kümmern, wenn mit einer App Umsatz generiert werden soll.

Wer wird in Zukunft das Rennen machen – native oder webbasierte Anwendungen?

Aktuelle Entwicklungen zeigen, dass Webtechnologien zunehmend wichtiger werden. Neue Betriebssysteme (z. B. FirefoxOS, Chrome OS oder Tizen) setzen auf Webtechnologien. Auch bei anderen proprietären Technologien lässt sich ein Trend hin zu offenen Webstandards beobachten. HTML5 und CSS3 lösen im Web zunehmend andere Technologien wie Adobe Flash oder Microsoft Silverlight ab. Dennoch sollte diese Entwicklung zumindest mittelfristig nicht überinterpretiert werden. So ist beispielsweise fraglich, ob alle Plattform- und Browseranbieter die HTML5-Unterstützung in ihren Browsern derart ausbauen, dass auch komplexe Webanwendungen realisiert und von den Nutzern ausgeführt werden können. Außerdem ist zu erwarten, dass bestimmte Gruppen von Anwendungen, z. B. grafikintensive Spiele oder rechenintensive Apps, auch weiterhin unmittelbaren, nativen Zugriff auf Hardware-Ressourcen benötigen, um zufriedenstellend zu funktionieren. Nicht zu vernachlässigen sind auch subjektive Faktoren, wie persönliche Vorlieben der Entwickler und Nutzer für die eine oder andere Plattform.

6 IT-Sicherheit, Datenschutz und Compliance im Umfeld mobiler Anwendungen

Die funktionalen Anforderungen und Kosten wurden behandelt, doch zwei wichtige und grundlegende Bausteine für die erfolgreiche Einführung mobiler Anwendungen und Services wurden bisher noch vernachlässigt: Datenschutz und Datensicherheit. Unternehmen, die mobile Dienste in ihre Infrastruktur und Geschäftsprozesse integrieren möchten, unterliegen neben gesetzlichen Bestimmungen wie dem Bundesdatenschutzgesetz (BDSG) oft noch eigenen Sicherheitsrichtlinien oder branchenspezifischen Regelwerken und Normen wie z. B. MaRisk, ISO 27001, TKG.

Mit den Funktionen aktueller Smartphones und Tablets ergeben sich für Unternehmen auch neue Bedrohungen, die durch entsprechende Regelungen und Maßnahmen adressiert werden müssen. Die Grundlage dafür ist eine detaillierte Risikoanalyse, die alle spezifischen Risiken für das betreffende Unternehmen modelliert, welche durch die Einführung mobiler Anwendungen und Services entstehen. Das Ergebnis der Risikoanalyse muss dann mit den bestehenden Vorgaben abgeglichen werden, um notwendige technische und organisatorische Maßnahmen ableiten zu können.

Gerade beim Einsatz von Smartphones im Unternehmen lassen sich nicht alle Sicherheitsmaßnahmen mit technischen Mitteln allein umsetzen. Während manche Smartphone-Plattformen mittlerweile eine sehr ausgereifte Management-Schnittstelle für die technische Verwaltung bereitstellen, sind andere Plattformen diesbezüglich erst am Anfang und stellen nur einige rudimentäre Möglichkeiten bereit, die Endgeräte über ein zentrales Management-System zu verwalten (vgl. Kap. 7). Solch ein Management-System oder Mobile Device Management (MDM), ist beim Einsatz der gängigen Smartphone-Plattformen Apple iOS, Google Android oder Windows 8 Phone optional. Der Betrieb der Endgeräte und die Integration in die Infrastruktur sind daher technisch möglich, ohne dass ein MDM-System vorhanden ist.

Wird dieser Weg gewählt, ergeben sich jedoch eine Reihe tiefgreifender Probleme bezüglich des Datenschutzes und gegebenenfalls der Compliance.

Ein einleuchtendes Beispiel sind böswillige Apps aus den App Stores, die z. B. das Adressbuch eines Endgerätes auslesen und die Daten an Dritte schicken, häufig an Firmen außerhalb der EU. Apps dieser Art gibt es leider nach wie vor in den Marktplätzen der gängigen Smartphone-Plattformen. Installiert ein Mitarbeiter eine solche App und überträgt damit (unbemerkt) sein Adressbuch, womöglich sogar mit Kundenadressen, an Dritte, so liegt ein veritabler Verstoß gegen das BDSG vor.

Abhilfe dagegen schafft ein MDM-System in Verbindung mit einem Verfahren, das die Benutzer darüber informiert, welche Apps unbedenklich sind und welche im Unternehmen nicht verwendet werden dürfen. Dieses Verfahren nennt sich White- und Blacklisting und wird später in diesem Kapitel erläutert. Gleichzeitig wird so das Bewusstsein der Mitarbeiter (»Awareness«) für Risiken bei der Nutzung von Apps gesteigert.

Allerdings kann ein MDM-System auch Probleme beim Datenschutz bereiten, wenn es dem Arbeitgeber zu viele Daten von den Geräten der Mitarbeiter liefert. Neben Systeminformationen kann ein MDM-System auch Informationen über genutzte Apps, Erreichbarkeit und mitunter sogar den Aufenthaltsort eines Mitarbeiters liefern. Dabei ist zu beachten, dass bei Einführung und Anwendung eines solchen Systems mindestens der Betriebsrat eingebunden werden muss. In jedem Fall aber sollte der Datenschutzbeauftragte des Unternehmens involviert werden, der über notwendige Maßnahmen und Anpassungen informieren kann.

Gängige Anforderungen aus Standards wie ISO27001 lassen sich ausschließlich mit einem MDM-System wirksam umsetzen:

- Passwortverwendung: Verwendung starker Passwörter, Durchsetzen von unternehmensweiten Passwortrichtlinien
- Überwachung der Systemparameter: Protokollierung, Monitoring
- Schutz vor Schadsoftware: Black- und Whitelisting
- Kontroller technischer Schwachstellen: Patch-Management, Kontroller von Updates

Darüber hinaus gibt es viele Aspekte, die sich nicht rein technisch regeln lassen. Hier hilft nur ein unternehmensweites Regelwerk, dass sich an die Mitarbeiter richtet, eine sogenannte Mobile Device Policy.

Relevante Vorgaben für App-Entwickler

Das BDSG und andere sicherheitsrelevante Vorgaben sind nicht nur für die Betreiber und Nutzer mobiler Anwendungen und Services relevant, sondern auch für App-Entwickler. Eine App, die personenbezogene Daten verarbeitet, muss diese angemessen schützen.
Neben dem rein rechtlichen Aspekt gibt es hier noch einen weiteren wichtigen Faktor: die Wahrnehmung der Anwender und der Öffentlichkeit. Gerät eine App aufgrund von Sicherheitslücken in Verruf, ist das für die Reputation des betroffenen Unternehmens schlecht. Eine Bank z. B., die eine unsichere Online Banking App veröffentlicht, wird von Kunden als wenig vertrauenswürdig gesehen. Hier müssen also neben gesetzlichen Vorgaben insbesondere Best-Practice-Beispiele zur Entwicklung sicherer Apps beachtet werden.

Black- und Whitelisting – aber wie?

Nachdem Browser die Sandbox-Technologie zum Schutz des Rechners vor Angreifern aus dem Internet populär gemacht haben, setzen sich Sandbox-Lösungen auch für den Smartphone-Einsatz im Unternehmen zunehmend durch. Es gibt kaum noch MDM-Hersteller, die keine Container-Apps für ihre Kunden anbieten. Einige Hersteller, wie z. B. Blackberry setzen mittlerweile gar auf eine ins Betriebssystem implementierte Trennung dienstlicher und privater Daten.

Das Problem dieser technischen Lösungen ist, dass sie immer nur einen kleinen Teil aller Sicherheitsbedrohungen adressieren, die eine böswillige App auf einem Smartphone ausüben kann bzw. denen eine App auf einem Smartphone unterliegt. Überdies führt eine strikte technische Trennung des dienstlichen vom privaten Bereich häufig dazu, dass Mitarbeiter den dienstlichen Teil ihres Smartphones als zu eingeschränkt und unpraktisch empfinden und daher nur für die notwendigsten Tätigkeiten nutzen. Den Großteil ihrer Tätigkeiten erledigen sie dann im uneingeschränkten, privaten Teil. Das Ergebnis ist eine ungewollte Vergrößerung der Angriffsfläche für Sicherheitsbedrohungen.

Eine sinnvolle Ergänzung besteht daher darin, die Fähigkeit moderner MDM-Systeme zu nutzen und unternehmensweite Black- und/oder Whitelists von Apps zu pflegen, die Mitarbeiter dienstlich (und privat) nutzen können. Zur Bewertung von Apps sollte ein objektives Risikoprofil auf Basis einer Bedrohungsanalyse mit Threat Models herangezogen und die Überprüfung der Apps dann an einen unabhängigen Dienstleister abgegeben werden. So kann eine große Anzahl von Apps überprüft und in die Whitelist/Blacklist aufgenommen werden, um die Nachfrage der Nutzer zu befriedigen.

Die Blacklist definiert dann solche Apps, die Mitarbeiter nicht verwenden dürfen, da sie eine Gefahr für das Unternehmen darstellen. Die Whitelist definiert hingegen die Apps, die Mitarbeiter unbedenklich verwenden dürfen, also solche, die weder ungefragt Daten übertragen und die Daten des Nutzers und damit des Unternehmens angemessen gegen unbefugten Zugriff schützen.

Mobile Device Policy und Awareness

Die fehlende Möglichkeit, alle relevanten Sicherheitsaspekte von Smartphones auf rein technische Weise zu regulieren, führt zu der Notwendigkeit einer organisatorischen Richtlinie zum Umgang mit Smartphones, einer so genannten Mobile Device Policy. Diese Richtlinie sollte im Stil bereits vorhandener Unternehmensrichtlinien Handlungsempfehlungen und Anweisungen für Mitarbeiter enthalten. Neben rein sicherheitstechnischen Aspekten sind die folgenden Themen üblicherweise in einer Mobile Device Policy zu finden:

- Verhalten beim Verlust eines Smartphones
- Verbot von Jailbreaking oder Rooting
- Allgemeine Verhaltensanweisungen (z. B. das Smartphone nicht unbeaufsichtigt liegen lassen)
- Umgang mit und in öffentlichen Netzen (Hot Spots etc.)
- Vorgaben zum Daten-Roaming
- Verweis auf Black- und Whitelists

Generell hat es sich als erfolgversprechende Strategie erwiesen, die Mitarbeiter in diesen Prozess einzubinden. Smartphones sind für viele Menschen ein ständiger Begleiter im Alltag geworden, da ist es selbstverständlich, dass Mitarbeiter ihr vom Arbeitgeber zur Verfügung gestelltes Gerät auch privat nutzen. Diesen Umstand kann man sich als Unternehmen durch entsprechend gestaltete Awareness-Maßnahmen zu Nutze machen. Risiken, denen die Mitarbeiter auch auf ihren privaten Smartphones unterworfen sind, lassen sich viel plakativer und eingängiger vermitteln als rein dienstliche Risiken, denen Mitarbeiter häufig mit größerem emotionalem Abstand gegenüberstehen.

Entwicklung sicherer Apps mit dem Threat Model

Apps für den Einsatz in Unternehmen unterliegen in der Regel einem höheren Schutzbedarf als Consumer Apps. Dienstliche Daten, die mit diesen Apps verarbeitet werden, dürfen beispielsweise nicht in die Hände Unbefugter gelangen. Ebenso wenig dürfen Kommunikationswege zwischen Endgeräten und der unternehmenseigenen IT-Infrastruktur kompromittierbar sein.

Nun sind Unternehmen häufig bei der Entwicklung mobiler Anwendungen mit kleinen Budgets und aufgrund der noch vergleichsweise neuen Plattformen mitunter mit Entwicklern konfrontiert, die wenig Erfahrung in der Programmierung sicherer Apps haben. Die Vielfalt und Komplexität der Plattformen tut ihr übriges - für die sichere App-Entwicklung ist dies ein schwieriges Umfeld.

Vorgehensmodelle aus der klassischen Softwareentwicklung, wie z. B. ein ausformulierter Secure Development Lifecycle (SDL) scheiden damit aus Kostengründen in den meisten Fällen von vornherein aus, da sie die App-Entwicklung unrentabel machen würden.

Genau wie bei der Einführung mobiler Services gilt auch hier: eine fundierte Risikoanalyse ist das Fundament für die Entwicklung sicherer Apps. Das dafür aus dem SDL entliehene Vorgehensmodell ist das Threat Model, die methodische Bedrohungsanalyse.

Im Threat Model tragen Entwickler, Software-Architekten und Sicherheitsexperten die spezifischen Bedrohungen einer App zusamen, die ja häufig Dreh- und Angelpunkt einer Client-Server-Architektur ist und somit ein hohes Gefährdungspotenzial aufweist. Zu jeder Bedrohung wird dann eine Maßnahme definiert, die bei der Implementierung zu berücksichtigen ist.

Für die Implementierung sollten dann wiederum Sicherheitsvorgaben existieren, die den Entwicklern möglichst genaue Richtlinien für die sicherheitskritischen Funktionalitäten der App geben. Je weniger konkret die

Anforderungen und Vorgaben sind, desto weniger wirksam werden natürlich die implementierten Sicherheitsmaßnahmen sein.

Das Threat Model dient auch nach der Implementierungsphase als roter Faden für Entwickler und bietet eine ideale Grundlage für einen sicherheitstechnischen Abnahmetest. Dieser sollte aus einem konventionellen Penetrationstest gegen App und Server bestehen und, sofern es das Budget zulässt, aus einer Prüfung der Teile des Programmcodes, die die sicherheitskritischen Funktionalitäten steuern. Der Teufel steckt hier im Detail. Insbesondere der richtige Umgang mit Kryptographie ist für viele Entwickler noch Neuland, hier stoßen selbst erfahrene Programmierer an ihre Grenzen.

Vertragliche Aspekte für Entwickler und Auftraggeber

Das größte Problem bei der Beauftragung eines App-Projekts ist oft die fehlende Anforderungsdefinition für sicherheitsrelevante Funktionalitäten. Mitunter sind Auftraggeber der Apps in Unternehmen Abteilungen, die wenig oder kein Fachwissen in IT, geschweige denn IT-Sicherheit haben. Dementsprechend fehlt es in den Anforderungsspezifikationen regelmäßig an hinreichend klar definierten Forderungen nach Sicherheitsfunktionalitäten.

Die im Threat Model erarbeiteten Maßnahmen haben daher auch bei der Vergabe von Aufträgen hohe Relevanz als Anhang zu den Anforderungsspezifikationen. Gut ausformulierte Sicherheitsforderungen und -maßnahmen lassen keinen Spielraum für Interpretationen. Gegenseitige Schuldzuweisungen zwischen Auftraggeber und Entwickler nach Bekanntwerden einer Schwachstelle gehören der Vergangenheit an, wenn die Spezifikationen im Vorhinein sauber festgehalten wurden.

Aber auch die Entwickler von Apps sollten sich nicht mit seitenlangen, allgemeinen Sicherheitsrichtlinien oder der abstrakten Forderung nach einer »sicheren« App begnügen. Im Normalfall sind App-Entwickler nicht gleichzeitig auch Experten für IT-Sicherheit, sie sind daher verständlicherweise nicht in der Lage, anhand ungenauer Vorgaben eine App mit hinreichenden Sicherheitsfunktionalitäten zu programmieren. Bestehen Sie daher als Auftragnehmer auf konkreten und umsetzbaren Anforderungen, und engagieren Sie, wenn der Auftraggeber diese nicht liefern kann, einen Sicherheitsexperten, der Ihnen dabei hilft, diese Anforderungen zu erarbeiten.

Checkliste

In dieser Checkliste finden Sie die wichtigsten Elemente, die Sie vor und während der Einführung mobiler Anwendungen und Services in Ihrem Unternehmen betrachten sollten, um Datenschutz und Datensicherheit angemessen zu berücksichtigen:

- Erstellen Sie ein objektives Risikoprofil auf Basis einer methodischen Bedrohungsanalyse mit einem Threat Model
- Gleichen Sie die gewünschten Funktionalitäten der Anwendung gegen das BDSG und relevante Compliance-Vorgaben Ihres Unternehmens ab
- Administrieren Sie die mobilen Geräte und Anwendungen in Ihrem Unternehmen mit einem MDM-Konzept
- Setzen Sie bei der Verwaltung von Apps Black- und Whitelisting ein
- Erarbeiten Sie eine Mobile Device Policy und achten Sie auf deren Umsetzung
- Binden Sie hierbei alle notwendigen Akteure aus Ihrem Unternehmen ein, mindestens den Betriebsrat und den Datenschutzbeauftragten
- Unterstützen Sie die Umsetzung der Policy mit einer Awareness-Kampagne für Ihre Mitarbeiter
- Erarbeiten Sie für Ihre eigenen Programmierer und für Auftragnehmer klare Entwicklungsvorgaben für Apps

7 Distribution und Vermarktung mobiler Anwendungen

Distribution von Enterprise Apps

Nach der erfolgreichen Umsetzung einer mobilen Anwendung schließt sich die Frage der Distribution und ggf. der Vermarktung an.

Bei Enterprise Apps, die Mitarbeitern zur Verfügung gestellt werden sollen, werden für die Distribution in der Regel bestehende Mobile Device Management (MDM) oder Mobile Application Management Systeme (MAM) eingesetzt. So können z. B. durch das Enterprise Agreement von Apple, den Google Play Private Channel oder die Company App Distribution für Windows Phone Anwendungen von einem Administrator direkt auf unternehmenseigenen mobilen Geräten installiert werden. Diese Apps müssen also nicht den Weg über den öffentlichen App Store nehmen und sind daher auch vom Zertifizierungs- oder Genehmigungsprozess ausgenommen. Dennoch können sie von Nutzern auch selbstständig über einen Enterprise App Store installiert werden, sofern ein solcher im Unternehmen zur Verfügung steht.

Derzeit starten eine Reihe von anderen Anbietern ebenfalls Enterprise bzw. B2B App Stores. Einige davon dienen ausschließlich der Distribution eigener Anwendungen, wie z. B. der SAP Store, andere sind wie herkömmliche App Stores als Marktplatz für Anwendungen von Drittanbietern konzipiert, z. B. das Volume Purchase Program für Unternehmen von Apple. Ein weiterer Ansatz, der immer mehr an Attraktivität gewinnt, ist die Implementierung eines unternehmenseigenen App Stores. Mittlerweile gibt es am Markt eine Vielzahl solcher Lösungen. Diese Enterprise App Stores sind oft mit einem Mobile Device Management und / oder einem Mobile Application Management verknüpft. Auf diese Weise wird eine umfassende Administration von Anwendungen und Geräten ermöglicht (vgl. Kap. 8).

Zusätzliches internes Marketing ist für die Verbreitung und Akzeptanz von Enterprise Apps natürlich auch wichtig und sollte über die etablierten Kanäle wie Mitarbeiterzeitschrift, Intranet, Newsletter oder ein internes Social Network stattfinden.

Auch darf bei internen Mobile-Projekten eine externe Kommunikation der innovativen Anwendung nicht fehlen. Wenn ein Unternehmen mit mobilen Anwendungen neue Wege im Business beschreitet und dadurch etwa die Produktivität von Mitarbeitern gesteigert werden kann, so kann dies im Rahmen des Marketings oder der Öffentlichkeitsarbeit aufgegriffen werden. Hierzu bietet sich eine Kommunikation in Social Media an. Mehr Informationen zu den Möglichkeiten für Unternehmen finden Sie im BITKOM-Leitfaden Social Media.[7]

Distribution über öffentliche App Stores

Die Verbreitung über öffentliche App Stores, wie den Apple App Store, Google Play Store, Blackberry World oder den Windows Store, unterliegt immer dem Genehmigungsprozess des jeweiligen Anbieters. Um unangenehme Überraschungen oder Verzögerungen zu vermeiden, sollten die für die Veröffentlichung notwendigen Informationen daher sorgfältig recherchiert und zusammengestellt werden. Insbesondere sind folgende Aspekte für die Veröffentlichung in einem App Store wichtig:

7 BITKOM: Leitfaden Social Media, zweite Auflage (www.bitkom.org/de/publikationen/38337_73802.aspx)

- Ein »sprechender« Name für die Anwendung, der ein leichtes Auffinden der App ermöglicht
- Sinnvolle Schlüsselwörter zur Unterstützung der Suchfunktion
- Eine treffende App-Beschreibung
- Ein ansprechendes Icon
- Aussagekräftige Screenshots
- Die Auswahl der richtigen Kategorie

Eine der Veröffentlichung vorangestellte Recherche sollte auch eine Analyse des Wettbewerbs umfassen: Wie stellen andere Unternehmen ihre Anwendungen im App Store dar? Hierbei zeigen die entsprechenden Schlüsselwörter schnell die relevanten Apps der Wettbewerber. Auch die Kategorie der Anwendung sollte mit Bedacht ausgewählt werden: Zwar hat die Kategorie »Soziale Netze« z. B. deutlich mehr Zugriffe als die Kategorie »Lifestyle«. Jedoch ist es nur mit großer Anstrengung möglich, im Bereich »Soziale Netze« unter den Top-Apps zu landen, denn in dieser Kategorie konkurriert man mit Apps von Facebook, Twitter, Linkedin oder Xing. Der Bereich »Lifestyle« hingegen ist nicht von internationalen Playern dominiert – man konkurriert hier eher mit Koch- oder Horoskop-Apps um die Top-Plätze.

Begleitende Marketingmaßnahmen für mobile Anwendungen

Nach der Veröffentlichung einer Anwendung auf einem Online-Marktplatz können verschiedene Aktivitäten dazu beitragen, deren Verbreitung zu erhöhen:

- Versuchen Sie, die Anwendung auf Review-Portalen zu platzieren
- Fordern Sie Anwender dazu auf, die App zu bewerten und sie im App Store zu kommentieren, eine solche Aufforderung kann auch innerhalb der App platziert werden
- Setzen Sie Mobile App Tracking ein, das gibt Ihnen Aufschluss darüber, welche Ihrer Marketingmaßnahmen zu einem Anstieg der Downloadzahlen führen
- Ermöglichen Sie es Anwendern, App-Inhalte in Social Networks und anderen Apps zu teilen
- Setzen Sie Mobile Advertising in Apps oder auf mobilen Websites ein
- Veröffentlichen Sie Beiträge über die mobile Anwendung auf der eigenen Website, im Unternehmens-Blog oder in Social Media

Da mobil optimierte Websites und Web Apps nicht über App Stores distribuiert werden können, müssen diese aus der Marketing-Perspektive wie normale Web-Angebote oder Anwendungen behandelt und beworben werden. Dabei sollte die Marketingmaßnahme immer auf den mobilen Kanal ausgerichtet sein, d.h. eine Print-Anzeige zur Bewerbung einer mobilen Anwendung ist nur dann sinnvoll, wenn auch ein QR-Code angeboten wird, mit dem Smartphone-Nutzer direkt zur Anwendung gelangen können.

Neben den beschriebenen Marketingmaßnahmen darf natürlich die Kommunikation mit den App-Nutzern nicht vernachlässigt werden. In der Regel erhält man nach dem Launch einer mobilen Anwendung sehr schnell Feedback über die Qualität und Beliebtheit via Social Media oder Kommentar im App Store. Hier ist es wichtig, eventuelle Kritik der Nutzer ernst zu nehmen. Keine Anwendung ist bereits in der ersten Version perfekt – es gilt daher, das Feedback der Nutzer genau zu analysieren und sinnvolle Verbesserungsvorschläge beim nächsten Update auch umzusetzen. Es versteht sich von selbst, dass Bugs zeitnah nach dem Auffinden behoben werden sollten.

8 Mobile Geräte, Anwendungen und Services im Unternehmen implementieren und verwalten

Strategien für die Implementierung mobiler Lösungen

Um Apps und mobile Services effektiv und sicher im Unternehmen zu nutzen, braucht es eine umfassende mobile Strategie, die belastbare Leitlinien für Entwickler, Administratoren und andere Projektverantwortliche enthält und die bei allen Implementierungsprojekten herangezogen werden kann. Verfügt die Strategie über einheitliche Entwicklungs- und Integrationsstandards, so sorgt sie für hohe Effizienz bei der Realisierung mobiler Lösungen. Sie sollte daher auf die folgenden Kernfragen eingehen:

- Welche mobilen Plattformen sollen im Unternehmen unterstützt werden (Google Android, Apple iOS, Windows 8 Phone, Blackberry OS etc.)
- Welche Geräte sollen genutzt werden (Feature Phones, Smartphones, Tablets, Convertibles / Hybrids)?
- Wie sollen diese Plattformen und Geräte integriert und verwaltet werden?
- Welche Nutzergruppen im Unternehmen (z. B. mobile Vertriebler, mobile Wissensarbeiter, Führungskräfte etc.) sollen welche Arten von Geräten zur Unterstützung ihrer Arbeit erhalten?
- Welche technischen Grundlagen müssen für die Umsetzung der Strategie geschaffen werden (Infrastruktur, Architektur etc.)
- Wie soll das Unternehmen die Einhaltung von Sicherheitsstandards und anderen maßgeblichen Unternehmensrichtlinien gewährleisten (vgl. Kap. 6)?
- Wie soll das Unternehmen mit Bring your own device (BYOD) umgehen?

Es empfiehlt sich, wie immer bei IT-Integrationsprojekten, die technische Integration einheitlich an zentraler Stelle vorzunehmen, um einen Wildwuchs an Schnittstellen, Plattformen, Management-Tools und Entwicklungstechnologien zu vermeiden. Idealerweise erfolgt die technische Integration mobiler Anwendungen über eine entsprechende Mobile Enterprise Application Plattform (MEAP) auf Basis einer serviceorientierten Schnittstellenlandschaft. Die Verwaltung der Geräte, Applikationen und Daten sollte durch eine Enterprise-Mobility-Management-Lösung (EMM) erfolgen.

Unabhängig davon, für welche Vorgehensweise Sie sich in Ihrem Unternehmen entscheiden, muss die Datensicherheit gewährleistet werden. Auf vielen mobilen Geräten sind mittlerweile mehr sensible Daten gespeichert als auf Laptops oder stationären PCs, daraus können sich Sicherheitsrisiken ergeben. Unternehmen müssen daher die wachsende Zahl von Mitarbeitern, die ihre Arbeit außerhalb des Büros mit mobilen Geräten erledigen, im Blick behalten. Bei der Entwicklung einer mobilen Strategie sollten Sie daher die mobile Sicherheitsstrategie, die Sie idealerweise von Ihrer IT-Sicherheitsstrategie ableiten, nicht vernachlässigen.

8.1 Mobile Device Management als Ausgangspunkt

Basis für die sichere Nutzung mobiler Geräte im Unternehmen ist eine Mobile-Device-Management Lösung (MDM), die für die Verwaltung, Konfiguration und Kontrolle der Endgeräte genutzt wird. Am Markt gibt es eine Vielzahl von MDM-Lösungen sowohl großer Softwarehäuser wie beispielsweise SAP (Afaria) als auch spezialisierter Anbieter wie Good Technology, Cortado oder Amagu.

Per MDM werden die mobilen Endgeräte in einem Unternehmen zentral verwaltet und gesteuert, unabhängig von der Anzahl der Geräte, dem Gerätetyp oder dem Betriebssystem. MDM ermöglicht es zudem, private und geschäftliche Anwendungen und Daten technisch voneinander zu trennen. Mittels Fernzugriff lässt sich der Status aller eingebundenen Geräte jederzeit abrufen und viele Gerätefunktionen (z. B. Kamera oder Daten-Roaming) können konfiguriert oder gesperrt werden. IT-Verantwortliche können Updates aufspielen, Anwendungen installieren oder löschen und prüfen, ob die Nutzer die Sicherheitsrichtlinien (»Policies«) einhalten. Im Fall eines Verlusts können Geräte inklusive aller darauf gespeicherten Informationen lokalisiert und aus der Ferne gelöscht bzw. gesperrt werden (Remote Wipe bzw. Kill).

Wichtig ist, dass Unternehmen beim Management ihrer mobilen Geräte den gesamten Lebenszyklus betrachten (vgl. Abbildung 4 und Tabelle 1 auf der nächsten Seite), der aus den Phasen Provisioning (Inbetriebnahme), Production (Nutzung) und Decommission (Außerbetriebnahme) besteht:

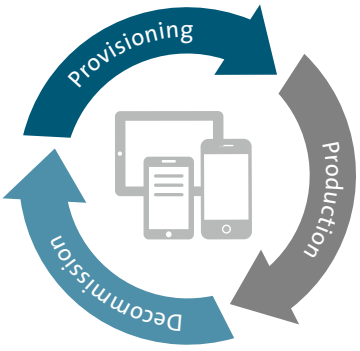

Abbildung 4: Lebenszyklus mobiler Endgeräte im Unternehmen

8.2 Vom Gerätemanagement zu einem umfassenden Enterprise Mobility Management

Das bis hierher beschriebene Management mobiler Geräte im Unternehmen ist zwar eine wichtige Basis, es reicht aber nicht aus, das Sicherheitsmanagement nur auf die mobilen Geräte zu beschränken. Bei IT-Sicherheitsexperten reift die Einsicht, dass Geräte nicht 100-prozentig sicher gemacht werden können. Eine strategisch geplante Integration und zentrale Verwaltung nicht nur der mobilen Geräte, sondern auch der Anwendungen (selbst entwickelte und gekaufte), Informationen und Dateien (z. B. Dokumente, Präsentationen, Preislisten, Verträge, Strategiepapiere) sowie in der Zukunft darüber hinaus weitere »Dinge« im Rahmen des Internet of Things ist die Grundlage für eine erfolgreiche und sichere Nutzung mobiler Geräte und Lösungen im Unternehmen.

- Mobile Geräte = Mobile Device Management
- Mobile Apps = Mobile Application Management
- Mobile Inhalte = Mobile Content Management
- Internet of Things

Abbildung 5: Dimensionen des Managements mobiler Geräte, Anwendungen und Inhalte

Enterprise Mobility Management (EMM) umfasst dabei sowohl die Verwaltung der Geräte (Mobile Device Management, MDM), die Verwaltung des Mobile Application Lifecycles (Mobile Application Management, MAM) und oft auch die Sicherung des Zugangs zu zentralen Unternehmensdokumenten im Intranet bzw. dem zentralen Content Management Systems des Unternehmens, durch sogenannte Mobile Content Management (MCM) Lösungen.

	Provisioning	Production	Decommission
Management	■ Gruppenzugehörigkeiten und Policies zuordnen ■ Endgeräte konfigurieren ■ Over-the-Air-Client-Verteilung (OTA, z. B. Installation von Apps via WLAN oder LTE) ■ Applikationen bereitstellen	■ Geräte dokumentieren und verfolgen ■ Softwareinstallationen updaten und ggf. reparieren ■ Konfigurationen warten und ändern ■ Daten verteilen und aktualisieren ■ Softwarelizenzen managen ■ Aktivitäten planen und automatisieren	■ Endgeräte ersetzen ■ Endgerätekonfiguration wiederherstellen ■ Softwareinstallationen erneuern ■ Daten wiederherstellen (nach Remote Kill)
Security	■ Sicherheits-Policys durchsetzen ■ Einschalt und Unlock-Passwort erzwingen ■ Daten verschlüsseln	■ Datensicherung managen ■ Patches und Security-Updates erzwingen ■ Sicherheits-Policys durchsetzen ■ Sicherheitslücken und Angriffe überwachen und nachverfolgen ■ Protokollieren von Administrator- Aktivitäten (Compliance)	■ Verlorene/gestohlene Geräte aus der Ferne löschen bzw. sperren (Remote Wipe bzw. Kill) ■ Geräte sperren bei Verletzung der Sicherheits-Policys ■ Apps deaktivieren bzw. löschen

Tabelle 1: Aktivitäten des Geräte-Lebenszyklus im Detail

Mobile Application Management

Die Bereitstellung mobiler Applikationen innerhalb eines Unternehmens erfordert neben dem Management der Geräte auch ein Management der Apps. Entsprechende Lösungen sollten dabei folgende Anforderungen abdecken:

- Sichere Trennung von privaten und geschäftlichen Daten, z. B. durch »Containerlösungen«
- Verschlüsselung der Daten, sowohl bei der Übertragung als auch bei lokaler Speicherung auf dem Gerät
- Authentifizierung und Autorisierung von Nutzern
- Verwaltung des Application Lifecycles (z. B. Installation von Updates)
- Distribution der Apps über entsprechende Enterprise App Stores
- Fernwartung der installierten Apps, z. B. Sperren oder Löschen

Warum benötigen Unternehmen eine Mobile-Application-Management-Lösung, wenn sie bereits über eine MDM-Lösung verfügen? Dies kann in folgenden Szenarien der Fall sein:

- Das Management mobiler Anwendungen hat zusätzliche funktionale Anforderungen, die von vielen MDM-Lösungen nicht abgedeckt werden, z. B. ein Enterprise App Store.
- Im Fall der Implementierung von BYOD im Unternehmen, kann es in bestimmten Fällen sein, dass ein Management dieser BYOD-Geräte mittels MDM nicht die beste Lösung ist.
- In stark regulierten Branchen (z. B. Öffentiche Institutionen, Finanzbranche), in denen es zusätzliche Sicherheitsrichtlinien gibt, kann ein MAM dabei helfen, diese Richtlinien zu erfüllen
- In Fällen, in denen das Unternehmen nicht die Kontrolle über das Endgerät hat (vor allem im B2C-Umfeld, also bei Consumer Apps, oder im B2B-Bereich bei Apps für Geschäftspartner), und deshalb Funktionalitäten »In app« also in bzw. durch die App sicherstellen muss, z. B. »In-app VPN, In-app-Verschlüsselung, Location Masking etc.

Ziel der o.g. Funktionen und Maßnahmen ist es, dass das Unternehmen möglichst zu jedem Zeitpunkt die Kontrolle über die mobil zur Verfügung gestellten geschäftlichen Daten behält. Hierfür bieten sich z. B. sogenannte Container- oder Sandbox-Konzepte oder ein »App Wrapping«, eine bestimmte Form der Containerisierung an, ggf. unterstützt durch MDM-Lösungen, um die personalisierte Bereitstellung von Sicherheitszertifikaten oder Konfigurationsprofilen für die Nutzer zu steuern. Durch diese Vorgehensweise erreichen Sie, dass sämtliche Daten des Unternehmens (E-Mails, Kontaktdaten, Dokumente, Anwendungen) ausschließlich in einem gesicherten, abgeschlossenen Bereich auf dem mobilen Gerät zur Verfügung gestellt werden. Alle Daten innerhalb eines solchen Containers können verschlüsselt werden, d.h. sie sind erst nach Eingabe eines Passworts zugänglich und können von den übrigen (privaten) Daten und Anwendungen auf dem Gerät getrennt werden. So behält das Unternehmen die Kontrolle über die eigenen Daten im geschäftlich genutzten Bereich des Smartphones, wohingegen der private Bereich von dieser Kontrolle unberührt und damit dem Nutzer vorbehalten bleibt. Dies ist ein großer Gewinn für die Nutzerfreundlichkeit und trägt daher zum sicheren Umgang mit Unternehmensdaten auf mobilen Geräten bei. Eine Containerlösung kann durch sogenanntes App Wrapping auch auf eine oder wenige Apps dediziert übertragen bzw. beschränkt werden, d. h. eine einzelnen App kann einen eigenen Container haben.

Mobile Content Management

Neben Geräten und Applikationen sollten auch die mobil zur Verfügung gestellten Daten des Unternehmens stets sicher verwaltet werden.

Das Spektrum reicht dabei vom einfachen Zugriff und Austausch von Dateien über die Anbindung an Dokumenten-Management-Systeme (DMS) bis hin zum verschlüsselten Intranet-Zugang. Entsprechende Lösungen gehören mittlerweile zum Portfolio von EMM-Anbietern und beinhalten oft eine Anbindung an weit verbreitete Plattformen wie Microsoft Sharepoint, sichere Intranet-Browser oder sichere Dokumentenaustauschplattformen wie z. B. SAP Mobile Documents.

Ziel des Mobile Content Management ist es, dem Nutzer unternehmenseigene, sichere Alternativen zu öffentlichen Angeboten wie Dropbox, Google Drive, Microsoft Skydrive oder ähnlichen Public Cloud Services anzubieten. Diese sind in der Lage, den Datenaustausch für die Nutzer möglichst komfortabel zu gestalten und sorgen gleichzeitig dafür, dass Unternehmen jederzeit die Kontrolle über ihre Daten behalten, weil diese zu keinem Zeitpunkt auf den Servern nicht autorisierter Dritter lagern. Die Daten sollten dabei sowohl auf dem Transportweg als auch bei lokaler Speicherung auf dem mobilen Gerät verschlüsselt werden. Der Nutzer sollte sich daher vor einem Zugriff autorisieren müssen und im Bedarfsfall sollten die Daten aus der Ferne von einem Administrator gelöscht werden können.

Werden z. B. Dokumente im Unternehmen ausschließlich über derartige Plattformen ausgetauscht, so kann eine solche Lösung die unkontrollierte Verbreitung z. B. durch Weiterleitung von E-Mails oder durch Öffnen in privaten, unkontrollierten Apps unterbunden werden.

8.3 Bring-your-own-Device und Consumerization

Neben dem strategisch durchdachten und sicheren Management der unternehmenseigenen Geräte, Anwendungen und Daten gibt es für Unternehmen eine Reihe weiterer Herausforderungen im Zusammenhang mit Mobility. Eine davon betrifft den Umgang mit privaten Endgeräten der Mitarbeiter, die mit dem Unternehmensnetzwerk verbunden werden (Bring your own Device, BYOD).

Im Zentrum von BYOD steht die Frage, ob der Zugriff auf Unternehmensdaten und -anwendungen über privaten Geräte, z. B. Smartphones, Tablets oder Laptops, gestattet werden soll.[8] Zugrunde liegt hier ein »Consumerization« genannter Trend, der die zunehmende Verschiebung der Technologieführerschaft weg vom Unternehmen hin zum (privaten) Konsumenten bzw. Mitarbeiter beschreibt. Dieser Trend führt zu einer steigenden Erwartungshaltung seitens der Mitarbeiter, bevorzugte Privatgeräte auch geschäftlich oder als frei gewählte Alternative zu Unternehmensgeräten zu nutzen.

Insbesondere die starke Verbreitung von Smartphones und Tablets hat in jüngster Vergangenheit dazu geführt, dass Angestellte im privaten Umfeld »moderner« und technisch fortschrittlicher ausgestattet sind als im geschäftlichen Umfeld. Außerdem haben Unternehmen heute mitunter große Mühe, in puncto Hard- und Softwarewareausstattung ihrer Mitarbeiter mit den im Consumer-Umfeld üblichen Innovationszyklen mitzuhalten.

Dies führt vielerorts zu einem Szenario, das für Unternehmen neue Herausforderungen und Risiken beinhaltet: Mitarbeiter nutzen private Endgeräte – vorwiegend Smartphones und Tablets, aber auch

8 Detaillierte Handlungsempfehlungen zu Bring-your-own-Device aus datenschutzrechtlicher Perspektive finden Sie im entsprechenden BITKOM-Leitaden (www.bitkom.org/de/themen/50792_75275.aspx)

Notebooks und Desktop-PCs – um damit auf geschäftliche Ressourcen und Daten zuzugreifen, auch wenn dies von der IT-Abteilung oder Unternehmensleitung nicht gestattet oder entsprechend geregelt ist. Aktuell erlauben 43 Prozent der ITK-Unternehmen in Deutschland ihren Mitarbeitern, eigene Geräte mit dem Firmennetzwerk zu verbinden. 40 Prozent dieser Unternehmen haben hierfür allerdings keine Richtlinien aufgestellt.[9]

Diese unkontrollierte Nutzung von privaten Endgeräten im Unternehmen nennt man »Shadow-IT«.

Typische Beispiele hierfür sind:

- Weiterleitung von geschäftlichen E-Mails an private E-Mail-Konten, mitunter sogar automatisch mithilfe von Weiterleitungsregeln
- Ablage von Unternehmensdaten in sogenannten Public Clouds wie Dropbox, Google Drive oder Microsoft SkyDrive
- Umgehen von Sicherheitsbarrieren, um mit einem privaten Endgerät auf geschäftliche Anwendungen und Daten zuzugreifen

Bei all diesen Beispielen verliert das Unternehmen die Kontrolle über die jeweiligen Daten. IT-Verantwortlichen ist die Brisanz dieser Vorgehensweise oft nicht bewusst – sie sind aber verpflichtet, derartige Szenarien zu unterbinden und die Sicherheit geschäftlicher Daten zu gewährleisten. Dabei geht es zum einen um den Verlust von Kontrolle, wenn Daten das sichere Umfeld eines Unternehmens verlassen, zum anderen aber auch um rechtliche Aspekte, wie z. B. den Speicherort der Daten. Die meisten Public-Cloud-Dienste etwa betreiben ihre Rechenzentren nicht in Europa, sondern in den USA. Die Nutzung dieser Dienste für Unternehmensdaten ist daher, je nach Art der Daten, oft nicht mit deutschem Datenschutzrecht vereinbar.

Bring-your-own-Device sicher implementieren

Vor diesem Hintergrund scheint das Konzept BYOD zunächst negativ besetzt zu sein. Begegnet man dem Phänomen allerdings nicht mit Verboten, sondern mit Aufklärung und durchdachten, sicheren Angeboten für die Mitarbeiter, so können diese mobilen Zugriff auf Unternehmensdaten und -anwendungen erhalten, ohne dass neue Sicherheitsrisiken entstehen:

- Der Zugriff auf geschäftliche E-Mails sollte nur unter Verwendung sicherer Lösungen gestattet werden, mit der die E-Mails verschlüsselt übertragen werden
- Das Unternehmen sollte eigene Angebote zum einfachen und sicheren Austausch von Dateien anbieten, um zu verhindern, dass Mitarbeiter zum Speichern und Teilen von Unternehmensdaten auf Public Cloud Services zurückgreifen
- Um als Unternehmen Kontrolle über die eigenen Daten zu behalten, sollten geschäftliche und private Daten auf mobilen Endgeräten mittels entsprechender Softwarelösungen strikt voneinander getrennt werden

Folgende Handlungsempfehlungen können Unternehmen dabei helfen, sich auf die zunehmende Verbreitung von privat genutzten Smartphones und Tablets im Unternehmen einzustellen:

- Mit der Nutzung privater Geräte am Arbeitsplatz durch Mitarbeiter sollten sich Arbeitgeber konstruktiv auseinandersetzen. Vor allem jüngere Mitarbeiter erwarten häufig, ihre eigenen Smartphones und Tablets auch im Unternehmen einsetzen zu können. Dieser Trend lässt sich nicht ignorieren und erfordert daher ein Umdenken bei IT-Verantwortlichen

9 BITKOM-Presseinformation: Private Smartphones werden für den Job genutzt (www.bitkom.org/de/themen/54633_73615.aspx)

- Unternehmen sollten prüfen, in welchem Umfang ihre Mitarbeiter private Geräte und Services für geschäftliche Zwecke nutzen und danach entscheiden, welche Regeln sie aufstellen und welche sicheren Alternativen sie anbieten wollen

- IT-Experten sollten sich strategisch auf eine künftig äußert heterogene Plattformlandschaft vorbereiten – aber dennoch anhand der individuellen Situation entscheiden, welche Plattformen das Unternehmen unterstützen möchte

- Die hier beschriebenen Veränderungen erfordern oftmals auch organisatorische und regulatorische Anpassungen im Unternehmen, u.a. den Aufbau von Support-Strukturen für Mitarbeiter, Anpassungen bei den IT-Beschaffungsprozessen oder bei Rahmenverträgen mit Mobilfunkanbietern. Darüber hinaus sind umfassende Nutzungsvereinbarungen zwischen dem Unternehmen und seinen Mitarbeitern eine wichtige Rahmenbedingung für BYOD-Konzepte.

Die neuen Anforderungen, die Unternehmen durch diese Veränderungen entstehen, werden weitestgehend durch die in diesem Kapitel beschriebenen Lösungen abgedeckt, die unter dem Begriff Enterprise Mobility Management eine Vielzahl von Funktionalitäten zur strategischen Begleitung und Steuerung entsprechender Szenarien anbieten.

9 Die Autoren

Tobias Arns, Bereichsleiter Social Media & Mobile, BITKOM
t.arns@bitkom.org, Twitter: @bitkom_somedia

»Die Art und Weise, wie Menschen konsumieren, kommunizieren und arbeiten, ändert sich derzeit rapide durch die massenhafte Verbreitung mobiler Geräte und Internetzugänge. Innovative und konsequent umgesetzte mobile Lösungen sind mittlerweile in der Lage, viele Kunden, Partner oder Mitarbeiter zu erreichen, und Unternehmen besser und wettbewerbsfähiger zu machen. Mitunter lohnt sich hier ein Blick auf Start-ups, von denen viele mit einer erfolgreichen ›Mobile first, Web second‹ Strategie zeigen, wie man es richtig macht.«

Stefan Bessing, Director Mobile Strategy, T-Systems Multimedia Solutions
stefan.bessing@t-systems.com

»Viele App-Projekte werden zu Change-Projekten. Dessen sollten sich Unternehmen frühzeitig bewusst sein. Denn es geht nicht nur um die Entwicklung von Lösungen: Um mit Enterprise Mobility nachhaltig erfolgreich zu sein, muss die Unternehmensorganisation darauf vorbereitet werden.«

Christian Buggisch, Leiter Corporate Publishing, Datev
christian.buggisch@datev.de, Twitter: @chris_buggisch

»In der mobilen Welt stehen alle Zeichen auf Wachstum: mehr Smartphones, mehr Tablets, mehr heruntergeladene Apps in den App-Stores. Umso wichtiger ist es für Unternehmen, Ihren Kunden und Interessenten mobile Angebote zu machen, die einen echten Mehrwert bieten. Denn mit der zunehmenden mobilen Durchdringung steigen auch die Ansprüche der Nutzer. Hier liegen Chancen und Risiken für Unternehmen gleichermaßen: Eine enttäuschende App ist schnell wieder gelöscht und ein (potenzieller) Kunde verloren. Zugleich entstehen neue Geschäftsmodelle und es tun sich völlig neue Möglichkeiten auf, enger denn je mit den Kunden in Kontakt zu bleiben.«

Marco Gracklauer, Mobile Manager, Datev
marco.gracklauer@datev.de

»Die wohl größte Herausforderung für Unternehmen ist die hohe Dynamik am Markt. Neue Betriebssystem-Versionen kommen in der Regel jährlich, die damit entstehenden Anwendungsszenarien sind immens. Klassische Entwicklungsmodelle stoßen dann schnell an ihre Grenzen. Erfolgreiche Apps fordern daher auch immer ein Umdenken im eigenen Unternehmen. Unternehmen sollten frühzeitig dafür sorgen, dass schnell und flexibel auf neue äußere Einflüsse reagiert werden kann. Das erfordert Pragmatismus bei Entscheidungen und den Mut, auch neue Wege zu gehen.«

Steffen Hess, Leiter Research Area GoMobile und Teamleiter User Experience, Fraunhofer-Institut für Experimentelles Software Engineering (IESE)
steffen.hess@iese.fraunhofer.de

»Apps und Mobile Services erhalten eine immer größere Bedeutung bei der Unterstützung und Optimierung von Geschäftsprozessen. Eine herausragende User Experience steigert dabei nachweislich zusätzlich die Produktivität und Zufriedenheit der Mitarbeiter. Der Einsatz von bewährten Methoden aus dem User Experience Engineering spart nicht nur Entwicklungskosten sondern sichert nachhaltig den Unternehmenserfolg.«

Christian Klöppel, Head of Global Mobility Consulting, CSC
christian.kloeppel@csc.com, Twitter: @herrkloeppel

»Die Anforderungen and das Management von mobilen Geräten und Applikationen sind gestiegen und gehen über die einfache Vergabe von Passwörtern oder das sperren des AppStores mittlerweile weit hinaus. Unternehmen sollten verstehen, das Mobility wesentlich gesamtheitlicher gesehen werden muß und sollten im Rahmen einer Mobility-Strategie bereits frühzeitig ein umfassendes Konzept für das Management von Devices, Apps, Services und Content entwickeln.«

Sven Portmann, Director Product Management Mobile Solutions,
Lufthansa Systems
sven.portmann@lhsystems.com

»Das explosive Wachstum im Bereich Mobility birgt enorme Chancen für Unternehmen, stellt sie aber auch vor große Herausforderungen. So sollte z. B. der Implementierungs- und auch der Vermarktungsaufwand einer App weder im B2B- noch im B2C-Umfeld unterschätzt werden. Es bedarf eines strategischen Ansatzes der koordiniert, kohärent und nachhaltig sein muss. Der richtige Mix von Marketinginstrumenten, gepaart mit innovativen Ideen und einer professionellen Umsetzung ist dabei der Schlüssel zum Erfolg.«

Klaus M. Rodewig, Senior IT Security Analyst, TÜV Trust IT GmbH
klaus.rodewig@it-tuv.com, Twitter: @cocoanehead

»Mobility und Sicherheit sind keine Gegensätze; ganz im Gegenteil. Mit der richtigen Strategie und Methodik lassen sich Smartphones und Tablets sicherer betreiben als so manch althergebrachte Plattform. Und auch die vielgescholtenen Themen Consumerization und BYOD müssen kein rotes Tuch für Unternehmen sein. Egal ob Einsatz mobiler Endgeräte, die Verwendung von Apps aus offiziellen App Stores oder die Entwicklung eigener Apps; sind die psychologischen Hemmschwellen einmal überwunden, steht einer sicheren Implementierung und Verwendung heutzutage nichts mehr im Weg.«

Jürgen Röhricht, Center of Excellence D/A/CH, Mobile Business Solutions, SAP
juergen.roehricht@sap.com

»Mobile Technologien und Geschäftslösungen sind heute allgegenwärtig und in fast jedem Unternehmen präsent. Durch die Mobilisierung von Mitarbeitern (B2E), Partnern/Geschäftskunden (B2B) oder Konsumenten (B2C) ergeben sich riesige Nutzenpotenziale hinsichtlich Prozesseffizienz, besseren Entscheidungen, einfacherer Zusammenarbeit, Kundenbindung und auch völlig neuer Geschäftsfelder. Unternehmen müssen sich jedoch auch den damit verbundenen Herausforderungen stellen. Sicherheit von Unternehmensdaten und Compliance zu gewährleisten sowie die Total Cost Of Ownership und Total Cost of Development der gesamten Mobilen Architektur und Apps zu managen. Deswegen ist eine Verankerung von Mobile und eine holistische Mobile Strategie in der IT und im Business sehr wichtig.«

Raphael Schulna, Leiter Consulting, adesso mobile solutions
schulna@adesso-mobile.de

»Mobile ist längst kein Trend mehr, sondern mittlerweile Mainstream geworden. Unternehmen benötigen daher dringend eine mehrwertige Mobile-Strategie, statt aktionistisch mobile Features ohne roten Faden zu entwickeln und/oder einzukaufen. Stellen sie sich dieser Aufgabe nicht, so verlieren sie wertvolle Zeit und damit in der Zukunft auch Marktanteile und Kunden. Es gilt, jetzt die Auswirkungen der neuen technologischen Möglichkeiten auf die eigenen Prozesse/Produkte/Lösungen/etc. zu evaluieren und dann an die neuen Herausforderungen anzupassen.«

Dr. Stephan Steglich, Leiter des Kompenzzentrums Future Applications and Media, Fraunhofer Fokus
stephan.steglich@fokus.fraunhofer.de

»Das World Wide Web hat in den letzten Jahren eine unglaubliche Entwicklung erlebt. Es wächst rasant und ist aus dem täglichen Leben aber vor allem auch aus dem kommerziellen Umfeld nicht mehr wegzudenken. Von dem ursprünglichen Zweck, vernetzte Inhalte darzustellen, hat es sich zu einer vollwertigen Plattform auch für Anwendungen und Dienste weiterentwickelt. Mit der stetigen Weiterentwicklung der dahinter steckenden Technologien wirkt sich dies auch zunehmend auf mobile Anwendungen und Geräte aus. Das Mobile Web – vielleicht derzeit noch in den Kinderschuhen – wird ähnlich rasant und dominant die Welt der Mobile Economy beeinflussen.«

10 Glossar

- **App**
  Apps im mobilen Bereich sind kleine Software-Programme, die speziell für Smartphones und Tablets entwickelt werden. Sie umfassen die verschiedensten Anwendungsgebiete, darunter Nachrichten- und Informationsdienste, Zugang zu sozialen Netzwerken, Navigationsdienste oder Spiele. → Native Apps repräsentieren das klassische Entwicklungsmodell, bei dem Applikationen speziell für eine jeweilige Plattform unter Benutzung der dafür vorgesehenen Programmiersprache entwickelt werden. Verbreitet und installiert werden Apps über den Marktplatz der jeweiligen Plattform (z. B. Apple App Store, Google Play Store oder Windows Store). Neben nativen Apps gibt es auch → Web Apps und → Hybrid Apps

- **App Store (App-Marktplatz)**
  Ein App Store oder App-Marktplatz ist eine Distributions- und Verkaufsplattform für mobile und Desktop-Applikationen. Jeder mobile Plattformanbieter unterhält einen solchen Store, über den sowohl der Plattformbetreiber als auch Drittanbieter Apps zum Download zur Verfügung stellen können (z. B. Apple App Store, Google Play Store oder Windows Store). App Stores beinhalten üblicherweise einen durchsuchbaren, in Kategorien unterteilten App-Katalog sowie ein Verkaufs- und Abrechnungssystem für kostenpflichtige Apps und andere Inhalte. Mittlerweile gibt es auch App Stores für Desktop-Anwendungen.

- **Bring your own Device (BYOD)**
  Das aus den USA stammende Schlagwort Bring your own Device (BYOD) beschreibt dort häufig das Vorgehen, Mitarbeiter beim Kauf privater Geräte finanziell zu unterstützen, sofern diese auch für geschäftliche Zwecke genutzt werden. In Deutschland wird mit BYOD hingegen die Frage diskutiert, wie der Zugriff auf Unternehmensdaten und -anwendungen mit privaten Geräten, z. B. Smartphones, Tablets oder Laptops, geregelt werden soll und welche Vorkehrungen getroffen werden müssen, damit dies wirtschaftlich, sicher und unter Beachtung geltenden Rechts geschehen kann.

- **Consumerization**
  Der Ausdruck Consumerization beschreibt die zunehmende Verschiebung der Technologieführerschaft weg vom Unternehmen hin zum privaten Konsumenten. Früher waren es zunächst Unternehmen, die neue und häufig teure Informationstechnologie anschaffen und implementieren konnten. Insbesondere die starke Verbreitung von Smartphones und Tablets hat in jüngster Vergangenheit dazu geführt, dass Angestellte im privaten Umfeld »moderner« und technologisch fortschrittlicher ausgestattet sind als im geschäftlichen Umfeld.

- **Container Apps**
  Eine Container App kapselt Daten innerhalb der App gegen unbefugte Zugriffe und bietet, je nach Hersteller, die Möglichkeit, Dritt-Apps in einer → Sandbox abzulegen.

- **Clickdummy**
  Ein Clickdummy ist ein nicht funktionaler Designprototyp, der auf → Wireframes basiert. Er verdeutlicht insbesondere die Struktur der künftigen Anwendung oder Website und demonstriert ihr Verhalten in der Interaktion mit dem Nutzer. Für die Erstellung von Clickdummys gibt es eine Reihe von kostenpflichtigen und kostenfreien Tools.[10] Neben Vorlagen für Präsentations-Software wie Microsoft PowerPoint, gibt es webbasierte Tools , Desktop-Anwendungen sowie Apps für Smartphones und Tablets.

- **Enterprise Mobility**
  Enterprise Mobility beschreibt all diejenigen Endgeräte, Services, Anwendungen und Prozesse, die in Unternehmen eingesetzt werden, um Mitarbeiter in die Lage zu versetzen, ihre Aufgaben auch unterwegs zu erledigen.

10 z. B. www.clickdummy.com

- **Enterprise Mobility Management (EMM)**
  Enterprise Mobility Management beschreibt die ganzheitliche Verwaltung von mobilen Geräten, Nutzern, Applikationen und Daten. In der Regel handelt es sich bei entsprechenden Lösungen um Weiterentwicklungen bzw. Kombinationen von Mobile Device Management, Mobile Application Management, Mobile Security oder Mobile Content Management. Viele Hersteller haben umfassende Suiten und Produktpakete für EMM entwickelt und zusammengestellt, um alle notwendigen Management-Funktionen aus einer einheitlichen Plattform heraus bedienen zu können.

- **HTML 5**
  HTML5 ist die Weiterentwicklung des HTML4-Standards und enthält Verbesserungen von bewährten Methoden der Webentwicklung sowie vollständig neue Ansätze. HTML5 ist zwar noch ein »Candidate Recommendation«, also kein vom World Wide Web Consortium (W3C) verabschiedeter Standard, aber bereits ein marktrelevanter Defacto-Standard. Viele Browser integrieren die neuen Spezifikationen von HTML5 (z. B. zum Abspielen von Videos direkt im Browser ohne Plugin) bereits heute, wobei die Anzahl der implementierten HTML5-Funktionen von Browser zu Browser stark variiert.[11]

- **Hybrid Apps**
  Hybride Anwendungen versuchen die Vorteile von Web Apps mit denen von nativen Applikationen zu kombinieren.
  Sie bestehen aus nativem Programm-Code, bedienen sich jedoch zusätzlich Webtechnologien wie HTML5, CSS3 und JavaScript. Hybride Apps lassen sich meist leichter auf andere Plattformen portieren als vollständig nativ entwickelte Anwendungen. Bei der Entwicklung wird der Umstand ausgenutzt, dass innerhalb von Apps Browserfenster geöffnet werden können (sog. Web Views), welche Webinhalte darstellen können. Da Adressleiste und Steuerelemente des Browsers ausgeblendet werden, merkt der Nutzer in der Regel nicht, dass es sich um Web Views handelt. Hybrid Apps können wie Native Apps über die jeweiligen Marktplätze vertrieben werden. Bei einigen Plattformen ist zu beachten, dass Apps, die nur aus Web-Views bestehen, vom Betreiber des Online-Marktplatzes zurückgewiesen werden können.

- **Jailbreaking**
  Jailbreaking nennt man das Entfernen von Sicherheitsvoreinstellungen bei iPhone und iPad. Dieses Verfahren senkt das Sicherheitsniveau eines Gerätes signifikant und sollte daher, auf Unternehmensgeräten nicht erlaubt sein.

- **Mobile Application Management (MAM)**
  Unter Mobile Application Management (MAM) werden Anwendungen und Services verstanden, die die zentrale Administration von mobilen Anwendungen in einem Unternehmen ermöglichen. Mit einer MAM-Lösung können Unternehmen ihren Mitarbeitern fremd- und eigenentwickelte mobile Anwendungen zur Verfügung stellen und darüber hinaus managen, wie diese Anwendungen genutzt und aktualisiert werden. MAM funktioniert dabei sowohl auf unternehmenseigenen als auch auf privaten Geräten der Mitarbeiter, wenn das Unternehmen dies unterstützt und zulässt. → BYOD

- **Mobile Device Management (MDM)**
  Unter Mobile Device Management (MDM) werden Anwendungen und Services verstanden, die die zentrale Administration von mobilen Endgeräten in einem Unternehmen ermöglichen. Mit MDM kann z. B. die Installation von Anwendungen und die Verteilung von Daten sowie die Einhaltung von Sicherheitsrichtlinien gemanagt werden. Auch ist es möglich, verlorengegangene Geräte aus der Entfernung zu sperren oder deren Speicher zu löschen, um zu verhindern, dass Unbefugte Zugriff auf Unternehmensdaten erhalten.

10 Siehe HTML5 & CSS3 Readiness (http://html5readiness.com/)

- **Mobile Enterprise Application Platform (MEAP)**
  Eine Mobile Enterprise Application Platform ist eine zentrale, strategische Komponente in der Systemarchitektur eines Unternehmens, welche oft die Basis für sämtliche mobilen Applikationen darstellt. Sie bündelt Schnittstellen zu Backend-Systemen und bietet oft eine einfache Realisierung von typischen Mobility-Anforderungen wie Datensynchronisation, Authentifizierung und Authorisierung, Personalisierung oder Verschlüsselung aufgrund vorgefertigter Programmierschnittstellen (API). Der Schwerpunkt einer MEAP liegt auf der Integration von Apps in eine bestehende IT-Architektur.

- **Mobil optimierte Website**
  Im Unterschied zu Web Apps, die versuchen, dem Nutzer das »Look and Feel« einer nativen App zu bieten, sind mobil optimierte Websites für die Nutzung auf allen mobilen Endgeräten ausgelegt. Sie bieten in der Regel nicht den Funktionsumfang und das Anwendererlebnis einer Web App, sondern sind darauf ausgerichtet, die jeweils maßgeblichen Inhalte und Dienste optimiert für ein mobiles Endgerät über einen Browser zur Verfügung zu stellen (z. B. die Fahrplanauskunft auf der Website eines Verkehrsbetriebs).

- **Mobilportal**
  Siehe mobil optimierte Website

- **Native App**
  Als native App werden Apps bezeichnet, die ausschließlich in der jeweiligen Programmiersprache der Plattform (z. B. Objektive C für Apple iOS) programmiert wurden. Versionen derselben App für unterschiedliche Plattformen müssen dabei in der Regel von Grund auf neu entwickelt werden. Native Apps zeichnen sich in der Regel durch eine hohe Performance aus, da Sie die Hardware des jeweiligen Geräts optimal ausnutzen können. Darüber hinaus nutzen sie oftmals eine Reihe von Geräte-Features wie Offline-Speicherung, Kamera, Ortungs- und Lagesensoren etc.

- **Penetrationstest**
  Ein Penetrationstest ist die sicherheitstechnische Analyse eines Systems, einer App oder einer IT-Infrastruktur mit den Mitteln eines Hackers. Dieser Test ist ein legaler und strukturierter Hackerangriff.

- **Rooting**
  Das Pendant zum → Jailbreaking auf Android-Geräten. Nach dem Rooting steht dem Nutzer der normalerweise gesperrte Administrator-Account (»root«) zur Verfügung.

- **Sandbox**
  Eine Sandbox ist ein isolierter Bereich, in dem Software ausgeführt werden kann, ohne dass Sicherheitslücken in dieser Software auf Bereiche außerhalb der Sandbox Zugriff haben. Eine Sicherheitslücke in einem Browser mit Sandbox kann beispielsweise nicht auf andere Ressourcen des Rechners zugreifen.

- **SDK**
  Ein Software Development Kit (SDK) ist eine Sammlung von Werkzeugen und Anwendungen, die dazu dient, eine Software zu erstellen. Mit einem solchen Kit ist es Softwareentwicklern möglich, eigene Anwendungen zu erstellen. Alle Anbieter mobiler Betriebssysteme und Plattformen bieten solche kostenlosen SDKs an, mit denen Programmierer native Applikationen für die jeweilige Plattform entwickeln können (z. B. Apple iOS SDK, Android SDK oder Windows Phone SDK).

- **Shadow-IT**
  Eine nicht reglementierte Nutzung von privaten Endgeräten im Unternehmen nennt man Shadow-IT. Dies ist der Fall, wenn Mitarbeiter private Geräte oder Software nutzen, um damit auf geschäftliche Ressourcen und Daten zuzugreifen, auch wenn dies nicht gestattet und entsprechend geregelt ist. Typische Beispiele hierfür sind die Weiterleitung von geschäftlichen E-Mails an private E-Mail-Konten, die Ablage von Unternehmensdaten in sogenannten Public Clouds wie z. B. Dropbox oder das Umgehen von Sicherheitsbarrieren, um mit einem

privaten Gerät auf geschäftliche Anwendungen und Daten zuzugreifen.

- **Smartphone**
  Smartphones sind Mobiltelefone, die in der Regel über einen berührungsempfindlichen Bildschirm gesteuert werden. Im Vergleich zu herkömmlichen Handys verfügen Sie über mehr Rechenleistung und Arbeitsspeicher. Außerdem können Sie über WLAN oder das Mobilfunknetz auf das Internet zuzugreifen. Smartphones bündeln die Funktionen mehrerer Geräte in einem (z. B. Organizer, Navigationsgerät, Kamera, MP3-Player). Der Funktionsumfang von Smartphones kann durch Anwendungen, sogenannte Apps, erweitert werden.

- **Tablet Computer, Tablet**
  Tablets sind kompakte und tragbare Computer, die über einen berührungsempfindlichen Bildschirm gesteuert werden und daher keine Hardwaretastatur benötigen. In der Regel beträgt ihre Bildschirmdiagonale zwischen 7 und 10 Zoll. Tablets können über WLAN oder das Mobilfunknetz auf das Internet zuzugreifen. Sie zeichnen sich durch eine Akkulaufzeit von mehreren Stunden im Betrieb und eine Standby-Zeit von mehreren Tagen aus. Anwendungen, sogenannte Apps, erweitern den Funktionsumfang von Tablets.

- **Threat Modelling**
  Threat Modelling ist eine formalisierte Bedrohungsanalyse, die das Ermitteln von sicherheitsrisiken ermöglicht.

- **Web App**
  Anders als native Apps werden Web Apps mit Hilfe von Webtechnologien (z.B. HTML5, CSS3, JavaScript etc.) programmiert. Webbasierte Apps werden üblicherweise in einem in das Betriebssystem integrierten Browser ausgeführt. Die Fähigkeiten von Web Apps sind daher begrenzt durch den Funktionsumfang, den dieser Browser bereitstellt. Der Zugriff auf Hardware-Funktionen, wie Kamera oder GPS- und Lagesensoren ist bei Web Apps nur teilweise möglich. Web Apps versuchen ähnlich wie → Hybrid Apps das Anwendererlebnis nativer Apps nachzubilden.

- **Wireframe**
  Als Wireframe werden frühe Entwürfe der Benutzeroberfläche einer Anwendung bezeichnet, bei der lediglich Platzierung und Funktion der einzelnen Elemente relevant sind. Farben und Texte hingegen spielen bei diesem schematischen Entwurf keine Rolle. Wireframes sind dazu geeignet, künftige Anwender frühzeitig in den Entwicklungsprozess einzubinden, um so zu einer möglichst nutzerfreundlichen Oberfläche zu gelangen.

Der BITKOM vertritt mehr als 2.100 Unternehmen, davon rund 1.300 Direktmitglieder mit 140 Milliarden Euro Umsatz und 700.000 Beschäftigten. 900 Mittelständler, mehr als 100 Start-ups und nahezu alle Global Player werden durch BITKOM repräsentiert. Hierzu zählen Anbieter von Software & IT-Services, Telekommunikations- und Internetdiensten, Hersteller von Hardware und Consumer Electronics sowie Unternehmen der digitalen Medien und der Netzwirtschaft.

BITKOM

Bundesverband Informationswirtschaft,
Telekommunikation und neue Medien e.V.

Albrechtstraße 10 A
10117 Berlin-Mitte
Tel.: 030.27576-0
Fax: 030.27576-400
bitkom@bitkom.org
www.bitkom.org