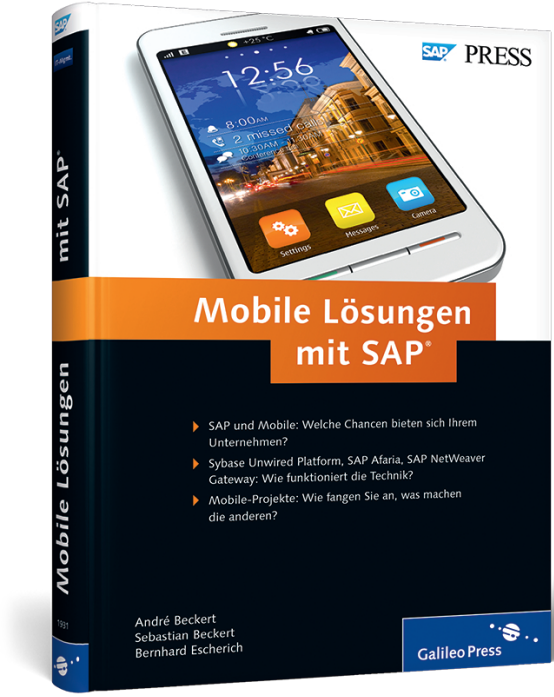
Beckert, Beckert, Escherich

Mobile Lösungen mit SAP®



Galileo Press

Bonn • Boston

Auf einen Blick

Inhalt

Teil III Eigene Mobile-Vorhaben umsetzen

Vorwort

Tablets und Smartphones sind dabei, die Welt der Unternehmens-IT grundlegend zu verändern. Innerhalb der nächsten zwei Jahre werden 200-250 Millionen Tablets verkauft werden. Dabei beträgt die Adaptionsrate für den Unternehmensbereich 50%. Hinzu kommt, dass immer mehr Mitarbeiter ihre eigenen mobilen Geräte im Unternehmen einsetzen möchten, Stichwort »Bring your own device«.

All das macht deutlich, dass die Consumerization unwiderruflich Einzug in die Unternehmen gehalten hat. Dabei gehen die Konsequenzen für die Unternehmen weit über die bloße Administration von Geräten hinaus. Eine Line of Business kann nun etwa Support-Leistungen, die sie bislang zwingend von der unternehmenseigenen IT bezogen hat, sehr leicht als Service cloudbasiert einkaufen.

Für einen CIO und seinen Bereich stellt sich die Frage, wie man auf diese Entwicklung reagiert: Abwarten und das Beste hoffen? Oder lieber aktiv das Tempo und die Richtung bestimmen?

SAP Global IT bestimmt Tempo und Richtung selbst. Wir haben den Trend als klare Chance begriffen, die wir nutzen. Entscheidend ist dabei der geschäftliche Vorteil. Wir beobachten etwa bei den analytischen Anwendungen auf In-Memory-Basis (SAP HANA) ein starkes Ansteigen der Anwendungszahlen. Das SAP-Management hat von seinen mobilen Geräten aus auf Knopfdruck gesicherten Zugriff auf die aktuellen Zahlen.

Der zentrale Nutzen: Die ständig steigende Datenflut kann effektiver beherrscht werden. Und das heißt: Mit konsequenter Nutzung mobiler Geräte und der entsprechenden Software kann ich heute in der gleichen Zeit das Vierfache an Informationen bewältigen.

Die Zahlen im mobilen Bereich für SAP als Unternehmen zeigen deutlich den Bedarf: Wir haben inzwischen zehn Corporate Devices, die wir unterstützen.

Bei SAP sind derzeit im Einsatz, etwa als firmeneigene Geräte:

- 18.000 iPads
- 14.000 iPhones
- 1.500 Samsung Android-Geräte
- 18.000 BlackBerrys
- 100 RIM Playbooks

Darüber hinaus nutzen derzeit bereits 1.500 Mitarbeiter private Geräte im Rahmen von »Bring Your Own Device« beruflich, Tendenz steigend.

Diese Zahlen beruhen auf unserer Strategie, die die notwendigen Elemente für den mobilen Bereich klar bestimmt: geräteunabhängig zu agieren, ein Mobile Device Management zur sicheren Administration der Geräte einzusetzen, kurze Entwicklungszyklen für neue Anwendungen anzustreben und eine klare Anwendungsplanung für die nächsten 18 Monate sowie eine klar definierte mobile Plattform als Basis zu sichern.

Dabei bieten wir den Mitarbeitern selbst, aber auch Kunden, die gleichen Erlebnismöglichkeiten, wie sie sie etwa von Stores großer Hersteller kennen. An zentralen Standorten können sie in eigens dafür eingerichteten Mobile Solution Centern die einzelnen Geräte und Anwendungen unter Anleitung direkt ausprobieren.

Die Zeiten für einen CIO waren selten so spannend wie heute. Mit Themen wie »Big Data« und »Social Media« gilt es, weiteren Trends zu begegnen. Klar, mobile Anwendungen sind da sicherlich kein Allheilmittel. Sie sind aber notwendig, um die Unternehmens-IT in den nächsten Jahren sinnvoll zu gestalten.

In diesem Sinn freue ich mich über das Erscheinen dieses Buches und wünsche Ihnen viel Erfolg bei Ihrem Mobile-Projekt.

Oliver Bussmann
Executive Vice President und Chief Information Officer
SAP AG

Einleitung

Smartphones und Tablet-PCs verändern unser tägliches Leben immer wieder neu, und – man mag es gut oder schlecht finden – wir können überall und jederzeit online sein, uns informieren oder mit anderen kommunizieren. Da nun, da wir dies schreiben, gerade Sommerurlaubszeit ist und in einer großen deutschen Tageszeitung ein umfangreicher Artikel erschien, wie Smartphones unsere Urlaube beeinflussen, wird uns selbst bewusst, dass wir kaum noch auf diese Annehmlichkeiten verzichten können. Wir schreiben dieses Buch innerhalb der kurzen Zeit von sechs Monaten, und jeder von uns Autoren war während dieser Zeit im Urlaub. Durch die mobilen Endgeräte konnten wir auf unseren Laptops weiter schreiben und auf Basis einer cloudbasierten Projektplattform von SAP gleichzeitig an den Kapiteln arbeiten und uns austauschen. Mit unseren Smartphones waren wir in der Lage, miteinander per Telefon, Chat und Skype zu kommunizieren und das unabhängig von Ländergrenzen.

Unter dem Stichwort *Consumerization* wird die technologische Revolution der mobilen Endgeräte zusammengefasst, getrieben durch den Endverbraucher. Diese Geräte und ihre Anwendungsmöglichkeiten sind aus unserem alltäglichen Leben nicht mehr wegzudenken, was die beeindruckenden Verkaufszahlen von iOS- und Android-Geräten bestätigen. Das mobile Telefonieren gehört mittlerweile zum Alltag der Menschen wie das Zähneputzen. Laut einer Berechnung, die SAP durchgeführt hat, gibt es auf der Welt inzwischen mehr Mobiltelefone als Zahnbürsten. Und diese Zahl wird noch steigen, bedenkt man, dass an einem einzelnen Tag doppelt so viele Smartphones verkauft, wie Babys geboren werden. Die Gewohnheit geht so weit, dass laut einer Forsa-Studie aus dem Jahr 2012 60% der 600 befragten deutschen Jugendlichen zwischen 14 und 19 Jahren das Smartphone bzw. das Handy wichtiger ist als das Liebesleben.

Der Einfluss der mobilen Endgeräte macht auch vor Unternehmen nicht halt. Die Mitarbeiter möchten selbstverständlich ihre privaten Geräte auch bei der Arbeit nutzen. Durch sie sind neue Formen der

Unternehmenskommunikation, neue Geschäftsprozesse und damit neue Geschäftsfelder möglich. Die Zahl der Mobile-Projekte in den Unternehmen, und damit verbunden die Investitionen, steigen unaufhörlich. Im Unterschied zum Beispiel zu klassischen Portalprojekten, ist die Mobile-Technologie eine Technologie, die alle Lebensbereiche umfasst.

In verschiedenen Funktionen beschäftigen wir uns seit mehr als zwölf Jahren mit dem Thema Mobile bei SAP und haben zum Beispiel die Arbeitszeiterfassung über Handys im September 2001 auf dem Personalwirtschaftskongress vorgestellt, in Arbeitsgruppen der DSAG und BITKOM mitgearbeitet sowie zahlreiche Kundenprojekte durchgeführt.

Zielsetzung und Zielgruppe

Nun ist eine kritische Masse von Projekten erreicht, in denen es nicht mehr vornehmlich um Ankündigungen und Pilotprojekte mit dem entsprechenden Marketing geht, sondern um reale Projektdurchführungen. Aufgrund unserer Erfahrungen aus den Pilotvorhaben und unseres Interesses an dem Thema SAP und Mobile, hat sich eine Vielzahl von Gesprächen und Interviews ergeben, in denen wir andere an unseren Erfahrungen bei SAP teilhaben ließen. Uns ist bewusst, dass die Kunden SAP eine gewisse Grundskepsis entgegenbringen, da sich über die Jahre im Mobile-Bereich einiges geändert hat. Wir möchten mit diesem Buch aufzeigen, dass sich auf der Grundlage dieser verschiedenen Technologien und der SAP-Zukäufe aus dem Mobile-Umfeld eine umfassende strategische Mobile-Plattform von SAP entwickelt hat. Das Buch verfolgt vor allem ein Ziel: Grundlagen zu vermitteln, die auch dann noch für SAP-Kunden Bestand haben, wenn sich technisch etwas ändert.

Das Buch bietet Ihnen einen Einstieg und Strategieleitfaden zum Thema SAP und Mobile. Es richtet sich an IT-Manager auf allen Ebenen, an Berater von Fachabteilungen großer Firmen sowie an alle SAP-Experten mit technischem und funktionalem Hintergrund. Sie erhalten mit diesem Werk einen umfassenden Einblick in das Thema und werden in die Lage versetzt, eine eigene Mobile-Strategie zu entwickeln. Sie lernen, was SAP anbietet und wie diese Produkte und Infrastrukturen einen Mehrwert für Ihr Unternehmen stiften. Sie lernen die Technologie der wichtigsten SAP-Mobile-Plattform-Komponenten kennen, erfahren, welche Erfordernisse ein Mobile-Projekt

mit sich bringt und welche Erfahrungen andere Unternehmen bereits gemacht haben.

Aufbau des Buches: Teil I

Teil I dieses Buches, »Mobile Anwendungen und die SAP-Lösungen«, vermittelt Ihnen einen grundlegenden Überblick über die neue Mobile-Plattform von SAP und versetzt Sie in die Lage, die Informationen einzuordnen, die Sie bislang schon erhalten haben. Dabei werden konkret diese Fragen beantwortet: Welche Herausforderungen kommen bei einem Mobile-Projekt auf mich zu? Was bringt mir diese neue Plattform, und wie unterscheidet sie sich von den bisherigen Ansätzen von SAP?

Kapitel 1, »Mobile Anwendungen und Geräte in Unternehmen: Vom produktiven Chaos zum strategischen Ansatz«, beschreibt die derzeitige Situation in vielen Unternehmen und Organisationen, in denen Mitarbeiter ihre privaten Geräte nutzen und die geprägt ist von vielen innovativen Anwendungen, die Mitarbeiter für das Unternehmen erstellen, ohne dass ein Projekt offiziell gestartet wurde. Anhand von zwei Beispielen, SAP und dem Krankenhaus Charité in Berlin, zeigen wir Ihnen, wie diese Unternehmen mobile Anwendungen zum Bestandteil ihrer Strategie gemacht haben und welche Erfahrungen dabei gesammelt wurden. Dieses Kapitel beinhaltet darüber hinaus eine Übersicht über die verschiedenen mobilen Endgeräte und Plattformen als Grundlage für die weiteren Ausführungen.

Kapitel 2, »Der Technologiezoo und die IT-Abteilung«, baut auf den beiden im ersten Kapitel vorgestellten Projektbeispielen auf und zeigt Ihnen, welche Herausforderungen hinsichtlich des Managements der mobilen Endgeräte, aber auch hinsichtlich des Themas Sicherheit konkret bei einem Projekt im Bereich Mobile auf Sie zukommen.

Kapitel 3, »Der Datenschützer, die Personalvertretungen und mobile Anwendungen«, vertieft und erweitert das Thema Sicherheit und Datenschutz und zeigt Ihnen, welche Anforderungen hiermit verbunden sind.

Kapitel 4, »Ein kurzer Rückblick: SAP und mobile Anwendungen«, wirft einen Blick zurück auf die bisherigen Lösungen von SAP im Mobile-Bereich. Dabei beschreiben wir, welche Anforderungen, insbesondere bei der Unterstützung der unterschiedlichen mobilen Technologieplattformen, die SAP-Lösungen bislang nicht abdecken konn-

ten. Anschließend werfen wir aber auch schon einen Blick voraus und erklären Ihnen, welche Bestandteile Sie weiter verwenden können, wenn Sie bereits mobile Lösungen von SAP einsetzen, die nicht auf der neuen SAP-Mobile-Plattform beruhen, und welche nicht.

Kapitel 5, »Die neue SAP-Mobile-Plattform«, stellt Ihnen die neue SAP-Mobile-Plattform im Überblick vor, bestehend aus der Sybase Unwired Platform, SAP NetWeaver Gateway und SAP Afaria. Dabei greifen wir auf die vorangegangenen Kapitel zurück und erklären, wie die neuen Lösungen die aufgezeigten Anforderungen – Unterstützung unterschiedlicher mobiler Plattformen, Sicherheitsanforderungen etwa bei Verlust des Gerätes sowie allgemein Management der mobilen Geräte – lösen können.

Kapitel 6, »SAP-Apps im Überblick«, bietet Ihnen eine Orientierungshilfe, um in der schnell wachsenden Menge von mobilen SAP-Anwendungen den Überblick zu behalten. Wir beschreiben in diesem Kapitel die mobilen Anwendungen, die bisher von SAP und Partnern entwickelt wurden. Damit Sie sich in dieser Fülle von Anwendungen nicht verlieren, zeigen wir Ihnen, wie SAP selbst diese Anwendungen in Gruppen aufgeteilt hat: Process Apps, Industry Apps, Employee Productivity Apps und SAP BusinessObjects Apps. Dabei stellen wir dar, welche Technologiekomponenten von den einzelnen Anwendungen genutzt werden. Sie können damit selbst einschätzen, mit welchen Anwendungen Sie sofort starten können, da Sie bereits über die notwendigen Systemvoraussetzungen verfügen.

Der erste Teil des Kapitels hilft Ihnen weiter, wenn Sie gerade erst damit beginnen, sich mit mobilen Anwendungen zu beschäftigen. Im zweiten Teil finden Sie die benötigten Informationen, wenn Sie schon wissen, welche Prozesse Sie mit mobilen Lösungen unterstützen möchten, und nun nach den richtigen Ideen für eine Umsetzung suchen.

Teil II

Teil II, »Die neuen SAP-Mobile-Lösungen unter der Haube«, vermittelt Ihnen vertiefte technische Informationen. Dabei sind die einzelnen Kapitel modular aufgebaut. Zu Beginn erhalten Sie einen detaillierten Überblick; anschließend beschreiben wir die notwendigen Details. Wenn Sie aus dem Anwendungsbereich kommen und die technischen Details nicht vertiefend behandeln möchten, können Sie so selbst entscheiden, ob Sie an einem bestimmten Punkt aus einem Kapitel aussteigen möchten, und erhalten dennoch die für Sie not-

wendigen Informationen. Nach der Lektüre des zweiten Teils wissen Sie, wie Sie Ihre Systemlandschaft verändern müssen, wenn Sie die neue Plattform oder Teile davon einsetzen möchten.

Kapitel 7, »Sybase Unwired Platform«, gibt Ihnen einen detaillierten Überblick über diese Komponente. Wie zeigen Ihnen, wie die Sybase Unwired Platform die unterschiedlichen mobilen Plattformen unterstützt.

Kapitel 8, »SAP NetWeaver Gateway«, bietet einen detaillierten Überblick über SAP NetWeaver Gateway und beschreibt seine Bedeutung für die Verbindung zwischen den mobilen Anwendungen und den SAP-Backend-Systemen. Sie erhalten auch Hinweise darauf, wie Sie Gateway in anderen Szenarien außerhalb des Mobile-Bereichs einsetzen können.

Kapitel 9, »SAP Afaria«, enthält detaillierte Informationen zum Bereich SAP Afaria und erklärt, wie diese Lösung Ihnen beim Management Ihrer mobilen Endgeräte helfen kann und welche Vorteile sie im Bereich Security bietet. Sie erfahren, wie SAP Afaria in Bezug auf bestehende Device-Managementplattformen einzuordnen ist.

Kapitel 10, »Systemlandschaften im Überblick«, beschäftigt sich mit der häufigsten Kundenfrage: »Wie machen es andere?« Diese Frage wird in Bezug auf die Systemlandschaften aufgegriffen. Ausgehend von einem Kundenbeispiel und einer häufig anzutreffenden SAP-Systemlandschaft wird aufgezeigt, welche Komponenten mit der SAP-Mobile-Plattform hinzukommen und was hier zu verändern ist.

Kapitel 11, »Eine neue App entsteht«, zeigt Ihnen, welche Schritte für den Entwicklungsprozess einer mobilen Anwendung notwendig sind.

Kapitel 12, »Der SAP Store«, stellt die Funktionsweise des SAP Stores für mobile Anwendungen vor, mit dem sich wesentliche neue Geschäftschancen für SAP-Berater, aber auch -Kunden, entwickeln können. Dieses Kapitel zeigt die Funktionsweise und die Prinzipien des Shops und beantwortet zudem die Frage, was Sie tun müssen, wenn Sie eine gute Idee für eine mobile Anwendung haben und diese vermarkten möchten.

Teil III

Teil III, »Eigene Mobile-Vorhaben umsetzen«, beschreibt die konkreten Informationen und Handlungsanweisungen, die Sie in die Lage versetzen, ein eigenes Mobile-Projekt zu realisieren. Ob Sie sich bereits mit dem Thema Mobile beschäftigt haben und konkret wissen möchten, wie Sie ihr Vorhaben umsetzen können, oder ob Sie noch ganz am Anfang stehen und einen Startpunkt für Ihr Vorhaben suchen – hier erhalten Sie die notwendigen Tipps für die Vorgehensweise basierend auf den Erfahrungen, die wir in verschiedenen Mobile-Projekten gesammelt haben. Wir veranschaulichen die Projektschritte anhand zweier durchgehender Beispiele, einer Stadtverwaltung mit ihren Bürgerservices und eines Unternehmens aus dem Retail-Bereich.

Kapitel 13, »Die richtigen Personen und das richtige Know-how für Ihr Projekt«, berücksichtigt die Tatsache, dass ein Projekt im Mobile-Bereich Know-how erfordert, das zum Teil in traditionellen SAP-Abteilungen so nicht gegeben ist. Der Leser erhält hier klare Empfehlungen, welche zusätzlichen Kenntnisse er und seine Kollegen benötigen und wer in einem Projektteam vertreten sein sollte. Auch auf unsere Erfahrungen im Bereich der Qualifizierung für die SAP-Beratung im Mobile-Bereich greifen wir hier zurück.

In **Kapitel 14**, »Bestandsaufnahme und Mobile-Reifegrad«, wird das im ersten Teil des Buches angesprochene Thema »produktives Chaos« bei den bisherigen Mobile-Vorhaben verschiedener Unternehmensabteilungen wieder aufgegriffen. Wir zeigen, wie Informationen mit Checklisten gesammelt werden können und welche Kommunikation sinnvoll ist, um zu vermeiden, dass ein Projektteam als Bremser innovativer Ansätze in den Fachbereichen wahrgenommen wird. Ein Reifegradmodell bildet den Ausgangspunkt für die Entwicklung einer Mobile-Strategie im SAP-Bereich.

Kapitel 15, »Eine Mobile-Strategie für Ihr Unternehmen«, schlägt Ihnen basierend auf dem Reifegradmodell aus Kapitel 14 ein Vorgehensmodell für die Erarbeitung einer Mobile-Strategie vor. Wir stellen Ihnen dazu Musterdokumente auf der Basis unserer Projekterfahrungen zur Verfügung. Anhand konkreter Beispiele lernen Sie, wie Sie den Mehrwert mobiler Lösungen darstellen und beziffern können.

Kapitel 16, »Die richtigen mobilen Anwendungen für Ihr Projekt finden«, macht den Schritt von Ihrer Idee in einem Geschäftsbereich zum konkreten Szenario. Anhand der in Kapitel 6 vorgestellten SAP-Apps zeigen wir Ihnen, wie Sie eine mobile Anwendung modellieren können.

Kapitel 17, »Ihre Mobile-Infrastruktur einrichten«, baut auf den im zweiten Teil dieses Buches bereitgestellten Informationen zur Architektur auf und geht auf die konkreten Projektschritte in diesem Bereich sowie auf das Thema Sizing ein, um Ihnen eine Abschätzung der Kosten zu ermöglichen.

Kapitel 18, »Datenschutz und Sicherheit für Ihr Vorhaben«, enthält fundierte Informationen, wie Sie konkret Empfehlungen des Bundesamtes für die Sicherheit in der Informationstechnik mit den SAP-Lösungen umsetzen können. Für die Zusammenarbeit mit den Datenschutzbeauftragten und den Personalvertretungen stellt Ihnen dieses Kapitel Checklisten bereit und erklärt die wichtigsten inhaltlichen Punkte aus den notwendigen Konzepten.

Kapitel 19, »Projekt- und Risikomanagement«, beschreibt, welche besonderen Ansätze das Projektmanagement für ein Mobile-Projekt erfordert, da es wesentlich agiler und dynamischer als in einem herkömmlichen SAP-Projekt sein muss. Wir stellen dar, welche Verhaltensweisen sich bewährt haben, und liefern ein Projektvorgehensmodell. Im Bereich des Risikomanagements gehen wir auf typische Risiken ein und zeigen Ihnen, wie Sie diesen begegnen können.

In **Kapitel 20**, »Erfahrungen und Lehren aus der Praxis«, erhalten Sie einen Überblick über die Erfahrungen und Lektionen, die wir aus unseren Mobile-Projekten gezogen haben. Durch unsere Einbindung in die entsprechenden SAP-internen Gruppen können wir Ihnen dabei auch Erfahrungen aus Projekten darstellen, die wir nicht selbst betreut haben.

Kapitel 21, »Ausblick: Die mobile Zukunft der SAP«, zeigt Ihnen die groben Linien auf, welche Richtung SAP im Bereich der mobilen Lösungen einschlagen wird, sodass Sie Anhaltspunkte für Ihre eigenen Planungen gewinnen. Wir gehen in diesem Zusammenhang sowohl auf den Bereich der Mobile-Plattform als auch auf den der mobilen Anwendungen ein.

Hinweise zur Lektüre

In diesem Buch finden Sie mehrere Orientierungshilfen, die Ihnen die Arbeit mit dem Buch erleichtern sollen.

In den Informationskästen sind Inhalte zu finden, die wissenswert und hilfreich sind, aber etwas außerhalb der eigentlichen Erläuterungen stehen. Damit Sie die Informationen in den Kästen sofort einordnen können, haben wir die Kästen mit Symbolen gekennzeichet:

[+] Die mit diesem Symbol gekennzeichneten *Hinweise* geben Ihnen Informationen zu weiterführenden Themen oder wichtigen Inhalten, die Sie sich merken sollten.

[»] Dieses Symbol macht Sie auf Begriffserklärungen und *Definitionen* aufmerksam, die für das Verständnis des Kapitels wichtig sind.

[zB] *Beispiele*, durch dieses Symbol kenntlich gemacht, weisen auf Szenarien aus der Praxis hin und veranschaulichen die dargestellten Inhalte.

Danksagung

Nach sechs Monaten intensiver Arbeit ist ein Buch über die mobilen Lösungen von SAP entstanden, das einen aktuellen und umfassenden Blick auf einen der wichtigsten Wachstumsmärkte von SAP wirft. Neben den Autoren war eine Reihe anderer Menschen an diesem Buch beteiligt, die wir hier würdigen und bei denen wir uns an dieser Stelle bedanken möchten. Aufgrund der Komplexität, der Schnelllebigkeit und der Dynamik, die mit dem Thema Mobile verbunden sind, ist es für das Schreiben dieses Buches besonders wichtig gewesen, die richtigen Informationen zum richtigen Zeitpunkt zur Verfügung zu haben. Wir möchten dem erfahrenen SAP MAM- und MAU-Experten Steffen Focke für seinen Input zu der Historie mobiler SAP-Technologien und außerdem Matthieu-Patrick Schapranow vom Hasso-Plattner-Institut für seine fachliche Zuarbeit bezüglich der Oncolyzer-App danken. Großer Dank geht auch an das Team von SAP Solution Experience, in erster Linie an Jochen Rundholz für die zahlreichen fachlichen Tipps und Hinweise. Für die notwendige Hilfestellung beim Lizenzmodell der mobilen Lösungen möchten wir Carsten Homeyer von SAP danken.

Des Weiteren geht unser Dank an die Teams aus Entwicklung, Solution Management, Vertrieb, Presales und Beratung bei SAP, die die App für die mobile Patientenakte auf den Markt gebracht haben und

von denen wir in zahllosen Gesprächen und Diskussionen sehr viel profitiert haben. Darüber hinaus hat das Buch sehr stark von der Mobile-Community von SAP profitiert, in der wir viele Informationen über Projekte und Erfahrungen erhalten haben, sodass das Buch nicht nur auf unseren eigenen Projekterfahrungen aufbaut. Wertvollen Input zum Thema SAP Afaria verdanken wir Shiral Tailor von der SAP AG.

Der größte Dank geht aber an unsere Kunden, die mit uns die Pilotprojekte im Mobile-Bereich gemeinsam umgesetzt haben und von deren Ideen für neue Anwendungen wir sehr profitiert haben.

Alle, die wir vergessen haben, besonders hier zu erwähnen, mögen uns verzeihen, der Dank liegt auf unserer Seite.

Da ein Buch einen Verlag und ein fleißiges Lektorat braucht, möchten wir Florian Zimniak und Janina Schweitzer von SAP PRESS herzlichst danken, die uns von der Buchidee an jederzeit unterstützt und betreut haben.

Zuletzt genannt, aber für uns am wichtigsten, ist der Dank an unsere Familien. Sie mögen unsere oftmals geistigen und physischen Abwesenheiten sowie die endlosen Nachtschichten entschuldigen. Erst ihre Geduld und Pflege haben dieses Buch ermöglicht.

Wir Autoren hoffen darauf, Ihr Interesse und die gleiche Begeisterung für das Thema Mobile und die damit verbundenen Lösungen von SAP zu wecken, und wünschen viel Erfolg bei der ersten Umsetzung von Mobile-Projekten in Ihrem Unternehmen.

Die Themen Datenschutz und mögliche Sicherheitsrisiken werden bei der Einführung mobiler Anwendungen oft intensiv diskutiert. Dieses Kapitel gibt Ihnen einen Überblick über mögliche Fallen in diesen Bereichen und beschreibt die Konzepte, die notwendig sind, um diese zu vermeiden.

3 Der Datenschützer, die Personalvertretungen und mobile Anwendungen

Dieses Kapitel vermittelt Ihnen einen Überblick über die Themen Datenschutz und Sicherheitsrisiken beim Einsatz mobiler Anwendungen. In unseren Mobile-Projekten haben wir häufig mit Datenschützern und Personalvertretungen in Unternehmen über diese Themen gesprochen. Unsere Erfahrungen aus diesen Gesprächen lassen wir in dieses Kapitel einfließen. Zu Beginn möchten wir zunächst ein kurzes Gedankenexperiment mit Ihnen durchführen, das wir vielfach und mit sehr guten Ergebnissen bei Diskussionen mit Entscheidungsträgern vor der Umsetzung von Mobile-Projekten verwendet haben.

Daran anschließend werden wir Ihnen im ersten Teil dieses Kapitels einen Überblick darüber geben, mit welchen Gefahren und besonderen datenschutzrechtlichen Anforderungen Sie bei einem Mobile-Projekt konfrontiert sind. Danach gehen wir auf die Anforderungen und Schutzbedürfnisse ein, die sich aus den Vorgaben des Datenschutzes und den Wünschen der Personalvertretungen ergeben. Von besonderem Interesse ist hier der Ansatz, dass immer mehr Unternehmen ihren Mitarbeitern erlauben, eigene Geräte für dienstliche Zwecke zu verwenden (BYOD) und damit eine in den allermeisten Unternehmen existierende Praxis anerkennen.

Für die Herausforderungen, die sich hieraus ergeben, zeigen wir Ihnen im dritten Teil des Kapitels die entsprechenden Lösungsmöglichkeiten im Überblick auf. Diese betreffen sowohl die notwendigen Regelungen

(Policy) als auch die technischen Vorkehrungen. Gerade für den Bereich der Richtlinien gehen wir hierbei auch wieder auf unsere Erfahrungen mit Personalvertretungen und Datenschützern ein.

Dieses Kapitel gibt Ihnen einen grundlegenden Überblick über die genannten Themen. Angesichts der Bedeutung der Themen greifen wir sie in Kapitel 18, »Datenschutz und Sicherheit für Ihr Vorhaben«, noch einmal auf und vertiefen sie im Hinblick auf die konkrete Umsetzung eines Mobile-Projektes.

Anonymisierte Fallbeispiele

In diesem Kapitel sowie in Kapitel 18, »Datenschutz und Sicherheit für Ihr Vorhaben«, werden wir einzelne Sachverhalte anhand von Fallbeispielen verdeutlichen. Angesichts der möglichen Brisanz der Themen haben wir die Fälle anonymisiert, um Rückschlüsse auf die realen Unternehmen und Organisationen zu verhindern. Für unsere Beschreibung der Gegebenheiten bei SAP stützen wir uns auf bereits publizierte Informationen, um zu vermeiden, dass wir als Insider interne Informationen weitergeben. Die große Offenheit unseres CIOs Oliver Bussmann in zahlreichen Vorträgen und Publikationen ermöglicht es aber dennoch, Ihnen hier sehr gute und hilfreiche Einblicke geben zu können.

3.1 Ein Gedankenexperiment vorweg

Unternehmen ohne mobile Endgeräte

Lassen Sie uns dieses Kapitel damit beginnen, dass wir Wünsche von Entscheidungsträgern, die Mobile-Projekten skeptisch gegenüber stehen, in einem Gedankenexperiment einmal Realität werden lassen. Stellen Sie sich vor, dass Sie alle Smartphones und Handhelds aus dem Unternehmensalltag verbannen. Dies bedeutet natürlich auch, dass Sie die Nutzung solcher Geräte in den Räumen Ihres Unternehmens grundsätzlich untersagen müssen. Wer würde sonst Ihre Kollegen daran hindern, Daten aus einem System bei Ihnen im Unternehmen auf ihre Smartphones zu übertragen? Im äußersten Fall kann dies geschehen, indem sie diese Informationen abtippen oder den Bildschirm abfotografieren, um eventuelle E-Mail-Filter zu umgehen, die Ihr Unternehmen verwendet, um den Versand kritischer Dateien zu blockieren. Alle Mitarbeiter des Unternehmens müssten ihre mobilen Endgeräte vor Arbeitsbeginn abgeben. Die Pförtner und Empfangsmitarbeiter müssten diese entgegennehmen. Bei mehreren Tausend Mitarbeitern müssten hier sicherlich einige Neueinstellung vorgenommen werden, um den Andrang am Morgen

zu bewerkstelligen und alle Ein- und Ausgehenden nach mitgebrachten Endgeräten zu befragen und diese einzusammeln. Zudem müssten Taschenkontrollen vorgenommen werden, um zu verhindern, dass Mitarbeiter unbefugt doch ihre Geräte mitbringen.

Unrealistische Umsetzung

Sie werden uns sicherlich zustimmen, dass ein solches Szenario nur außerordentlich schwer umzusetzen ist. Stellen Sie sich dabei ganz einfach vor, dass ein Mitarbeiter an der Rezeption von Ihrem Vorstand verlangt, ihm sein privates iPhone oder ein sonstiges Gerät auszuhändigen. Spätestens an dieser Stelle werden die meisten von Ihnen einen solchen Ansatz als unrealistisch empfinden, es sei denn, Sie arbeiten in einem besonders abgesicherten Sicherheitsbereich, wie zum Beispiel in einem Rüstungsunternehmen.

Notwendiges Sicherheitskonzept

Die Konsequenz daraus ist aber, dass Sie gar keine Wahl haben als sich mit der Sicherheit mobiler Geräte zu beschäftigen, da sie heute schon Realität in Ihrem Unternehmen sind. Die Schlussfolgerung, die sich daraus für Mobile-Projekte ergibt, ist einfach, dass Sicherheitsbedenken heutzutage kein Grund mehr sein können, sich gegen den Einsatz mobiler Geräte zu entscheiden. Sicherheitsbedenken müssen vielmehr der Anstoß dafür sein, sich mit dem Thema mobile Sicherheit professionell zu befassen.

Im Folgenden werden wir mit Ihnen gemeinsam die verschiedenen Risikobereiche beim Einsatz mobiler Endgeräte genauer betrachten. Dabei ist uns ein Hinweis sehr wichtig: Begehen Sie nicht den Fehler, sich von vornherein auf Diskussionen über Schwachstellen einzelner Betriebssysteme oder Geräte zu fokussieren. Natürlich werden wir Ihnen auch hierzu Hinweise geben. Viel wichtiger ist jedoch Folgendes: Angesichts der schnellen Innovationszyklen der Geräte auf dem mobilen Markt müssen grundlegende Mechanismen in Ihrem Unternehmen eingerichtet sein, mit denen Sie den erkannten Risiken begegnen können. Erst dann hat es Sinn, detailliert Sicherheitslücken von bestimmten Betriebssystemen bzw. Geräten zu betrachten, um etwaigen spezifischen Gefahren im Einzelnen begegnen zu können.

3.2 Die fünf Risikobereiche mobiler Anwendungen

Einordnung der Risiken

In Zusammenhang mit mobilen Anwendungen gibt es fünf Bereiche, in denen Risiken entstehen können. Diese fünf Risikobereiche finden Sie in Abbildung 3.1 in einem Schaubild dargestellt.

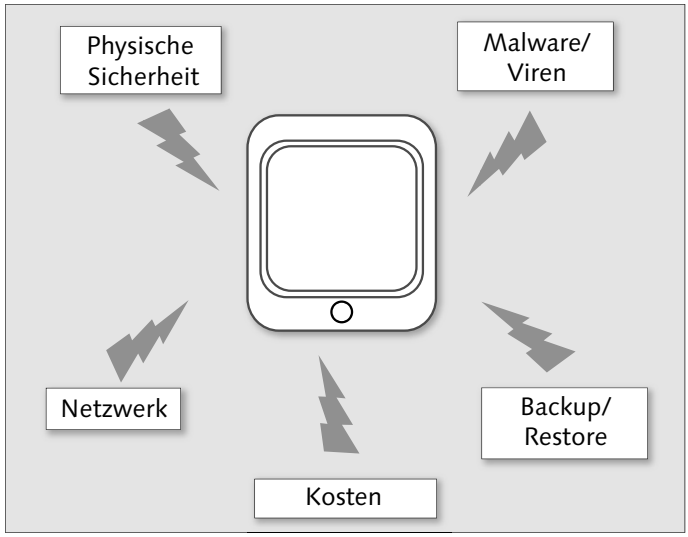


Abbildung 3.1 Risikobereiche für mobile Geräte in Unternehmen/Organisationen

Wir unterscheiden die folgenden fünf Risikobereiche, denen jeweils unterschiedliche Sicherheitsrisiken zugeordnet werden:

- Physische Sicherheit
  - Diebstahl
  - Verlust des Gerätes
  - Verkauf/Weitergabe des Gerätes
  - Verleih des Gerätes
- Malware/Viren
  - Bedrohung durch Schadsoftware
  - Bedrohungen durch risikobehaftete mobile Anwendungen
- Netzwerk
  - Zugang für nicht berechtigte Anwender
- Backup/Restore
  - Löschen von Daten, die Aufbewahrungsregeln unterliegen
  - Speicherung von Daten auf nicht autorisierten Servern
- Kosten
  - hohe Kosten durch nicht sachgemäßen Gebrauch der Geräte

Ausstattung mobiler Endgeräte

Bevor wir nun diese Bereiche im Einzelnen betrachten, zeigen wir Ihnen zunächst einige Kennzahlen, die für das Verständnis der möglichen Risiken und Gefahren wichtig sind.

Beim Vergleich der in Tabelle 3.1 aufgeführten Ausstattungsmerkmale von drei populären Smartphones wird Ihnen schnell klar werden, welches Risikopotenzial diese Geräte unter Sicherheitsgesichtspunkten für Unternehmen bergen.

Produkt/Merkmal	Galaxy S3	iPhone 4s	OneX
Hersteller	Samsung	Apple	HTC
Betriebssystem	Android 4.0	iOS 5	Android 4.0
Netz in D	HSDPA	HSDPA	HSDPA
RAM-Speicher	1 GB	512 MB	1 GB
Hauptkamera	8 MP	8 MP	8 MP
Speicher	16/32/64 GB	16/32/64 GB	32 GB
Videoaufnahmen	1080 p	1080 p	1080 p
Wifi/Bluetooth/GPS	Ja	Ja	Ja

Tabelle 3.1 Gängige Smartphones mit ihren Ausstattungsmerkmalen

Hohe Speicherkapazität

Wenn Sie die in Tabelle 3.1 genannten Ausstattungsmerkmale der Smartphones mit den Leistungsmerkmalen von früheren Rechnern in Ihrem Unternehmen vergleichen, fällt auf, dass die mobilen Geräte heute Charakteristika aufweisen, die denen von Servern in der Vergangenheit ähneln. Dies gilt insbesondere für die Speicherkapazitäten. Zudem bedeuten zusätzliche Ausstattungsmerkmale wie Kameras weitere potenzielle Gefahrenquellen für schutzwürdige Daten in Ihrem Unternehmen.

Mit einer einfachen Rechnung können Sie den Schutzbedarf in Ihrem Unternehmen ermessen:

1. Addieren Sie die Speichergröße der drei Dateien in Ihrem Unternehmen, die die geschäftskritischsten Daten enthalten (Kundendaten, Vertriebslisten, Patientendaten oder Schuldnerdaten).
2. Wenn Sie die so errechnete Summe durch den Speicherplatz dividieren, der für Dateien auf einem mobilen Endgerät zur Verfügung steht, erhalten Sie sicherlich ein Ergebnis >100.

Durch diese große Speicherkapazität können Sie auf Smartphones und Tablets Hunderte von geschäftskritischen Dateien speichern. Sie können sicher davon ausgehen, dass derartige Dateien in der Realität tatsächlich auf mobilen Geräten in Ihrem Unternehmen im Umlauf sind.

3.2.1 Physische Sicherheit

Sicherheitsrisiken für die Geräte

Vor dem Hintergrund der in Abschnitt 3.2, »Die fünf Risikobereiche mobiler Anwendungen«, präsentierten Kennzahlen mobiler Endgeräte gewinnen einige Statistiken zu physischen Sicherheitsrisiken eine besondere Bedeutung:

- **Diebstahl**
  Da moderne Smartphones sehr begehrt sind und Diebe zum Teil mehrere Hundert Euros für ein gestohlenes Gerät erzielen können, ist die Zahl der Diebstähle hoch und weist eine steigende Tendenz auf. So werden pro Jahr rund 300.000 Smartphones in Deutschland gestohlen.
- **Verlust**
  Die meisten modernen Smartphones passen in eine Jacken- oder Hosentasche. Das ist handlich, sie können daher allerdings auch leicht verloren gehen. In einer aktuellen Studie rangieren Hotels und Restaurants ganz oben auf der Rangliste der Plätze, an denen Menschen ihre Geräte verlieren. Das Ausmaß der Zahlen wird Sie jedoch wahrscheinlich genauso überraschen wie uns: Laut einer aktuellen Studie des Branchenverbandes BITKOM hat im Durchschnitt jeder zehnte Deutsche schon einmal sein Handy verloren.

[zB] **Geräteverlust bei einem Gesundheitsdienstleister**

Ein Beispiel aus dem Jahr 2011 belegt, wie real die Gefahren durch verlorene Endgeräte bereits sind. In diesem Jahr wurden bei einer europäischen Gesundheitsbehörde mehrere nicht besonders gesicherte Laptops mit Patientendaten aus einem Lagerraum gestohlen. Die Laptops enthielten Millionen von Patientendaten inklusive der Behandlungshistorie. Besonders negativ wirkte sich hierbei aus, dass die Daten auf den Endgeräten nicht verschlüsselt waren.

- **Verkauf/Weitergabe des Gerätes**
  Moderne Smartphones und Tablets gelten oftmals schon nach kurzer Zeit als veraltet. Denken Sie etwa daran, dass die Firma Apple

bislang im Durchschnitt jedes Jahr eine neue Version des iPads herausgebracht hat. Aus diesem Grund werden Smartphones und Tablets häufiger als andere Geräte weiterverkauft oder zum Beispiel an Verwandte oder Freunde weitergegeben.

- **Verleih des Gerätes**
  Eine Variante des vorangehenden Punktes ist der kurzfristige Verleih der Geräte. Hier zeigt sich die Auswirkung der Flatrate-Tarife, mit denen viele Smartphones vertrieben werden. Zwar geschieht der Verleih oftmals im familiären Umfeld – zum Beispiel surfen die Kinder eines Mitarbeiters über das private WLAN-Netz –, aus der Sicht des Datenschutzes ist dies jedoch natürlich ein unhaltbarer Zustand. Die Vorstellung, dass etwa ein Jugendlicher beispielsweise Patientendaten auf einem nicht besonders gesicherten iPad abrufen und lesen kann, treibt sicherlich nicht nur einem Datenschutzbeauftragten Schweißperlen auf die Stirn.

3.2.2 Malware/Viren und die unterschiedlichen Betriebssysteme

Arten von Malware

Die Gefahr von Schadprogrammen (Malware) ist den meisten Anwendern aus dem PC-Bereich bekannt. Hinter dem Begriff *Malware* verbergen sich eine Reihe von Anwendungen, die von dem Benutzer nicht gewünschte Funktionalitäten auf seinem Rechner ausführen. Dabei unterscheiden Experten *Computerviren*, die Kopien von sich auf den infizierten Rechner schreiben, *Würmer*, die sich über das Netz verbreiten, und *Trojaner*, die sich in einem vermeintlch hilfreichen Programm verbergen.

All diesen Anwendungen ist jedoch eines gemeinsam: Sie erzeugen einen Schaden, indem sie zum Beispiel Kreditkarteninformationen oder Passwörter abgreifen und zu kriminellen Zwecken nutzen. Aus diesem Grund besteht eine der wichtigsten Sicherheitsvorkehrungen für jeden Privatanwender, aber auch für die IT-Abteilungen von Unternehmen, darin, für die Verwendung eines aktuellen Antivirenprogramms zu sorgen. Im dynamischen und noch recht jungen Markt der Smartphones und Tablets ist die Situation in diesem Bereich noch ein klein wenig anders gelagert und, kurz gesagt, noch dynamischer als diejenige, die Sie aus dem PC-/Laptopbereich kennen.

Sicherheitskonzepte der Hersteller

Anwender experimentieren in der Regel gerne mit ihren mobilen Geräten und nutzen vielfältige mobile Anwendungen. Die unterschiedlichen Hersteller mit ihren Betriebssystemen verfolgen dabei auch unterschiedliche Ansätze bezüglich der Sicherheit dieser Programme. Da in diesem Zusammenhang die Charakteristika der jeweils verfolgten Sicherheitsphilosophien der Endgeräteanbieter deutlich werden, stellen wir Ihnen in diesem Kapitel nicht nur mögliche Gefahren durch gefährliche mobile Anwendungen vor, sondern vermitteln Ihnen vielmehr das grundlegende Wissen, mit dem Sie einschätzen können, ob das jeweilige Betriebssystem und damit die entsprechenden Geräte für Sie einsetzbar sind. Wir knüpfen dabei an die Ausführungen zu den verschiedenen Herstellern und deren Plattformen in Kapitel 1, »Mobile Anwendungen und Geräte in Unternehmen: Vom produktiven Chaos zum strategischen Ansatz«, an.

Sicherheit bei Apple iOS

Mit dem überwältigenden Erfolg des iPhones und des iPads hat Apple mobile Anwendungen zu einem Massenphänomen im Konsumentenbereich gemacht und dieser Geräteklasse damit zum Durchbruch verholfen. Mit dem Eindringen in den Unternehmensbereich hat Apple den Zugang zu einer Domäne erzielt, die vorher im Wesentlichen von den BlackBerry-Geräten der Firma RIM beherrscht wurde. Dies führt immer wieder dazu, dass Administratoren und IT-Verantwortliche die Sicherheitsfunktionalitäten der iOS-Plattform (siehe Abschnitt 1.2.1, »Apple iOS«) an den bekannten Funktionalitäten der BlackBerry-Plattform messen.

Apple iOS 5

Mit der iOS-Version 5 wurden noch einmal wesentliche Funktionalitäten für den Einsatz in Unternehmen eingeführt. So wurden etwa die Schnittstellen für Mobile Device Management-Lösungen, auf die wir in Kapitel 9, »SAP Afaria«, noch ausführlich eingehen werden, erweitert. Zudem können Administratoren nun Anwender daran hindern, E-Mails von ihrem Firmen-Account an ihre private E-Mail-Adresse zu senden. Für die Abwehr von Malware ist es von Belang, dass mobile Anwendungen daran gehindert werden können, E-Mails im Hintergrund zu verschicken, zum Beispiel mit vertraulichen Informationen.

Geschlossenes System

Apples Betriebssystem beruht im Wesentlichen darauf, dass das Unternehmen sowohl die Hardware selbst als auch das Betriebssys-

tem sowie die mobilen Anwendungen kontrolliert. So werden alle Apps von Apple einer Überprüfung unterzogen, bevor sie im App Store publiziert werden, und sie müssen Apples Sicherheitsstandards beachten. Die Anwender selbst müssen die Apps über den unternehmenseigenen App Store iTunes laden. So finden Sie etwa auch die SAP Apps im App Store von Apple (*http://www.apple.com/de/itunes/*, siehe das Beispiel der Anwendung SAP EMR Unwired in Abbildung 3.2).

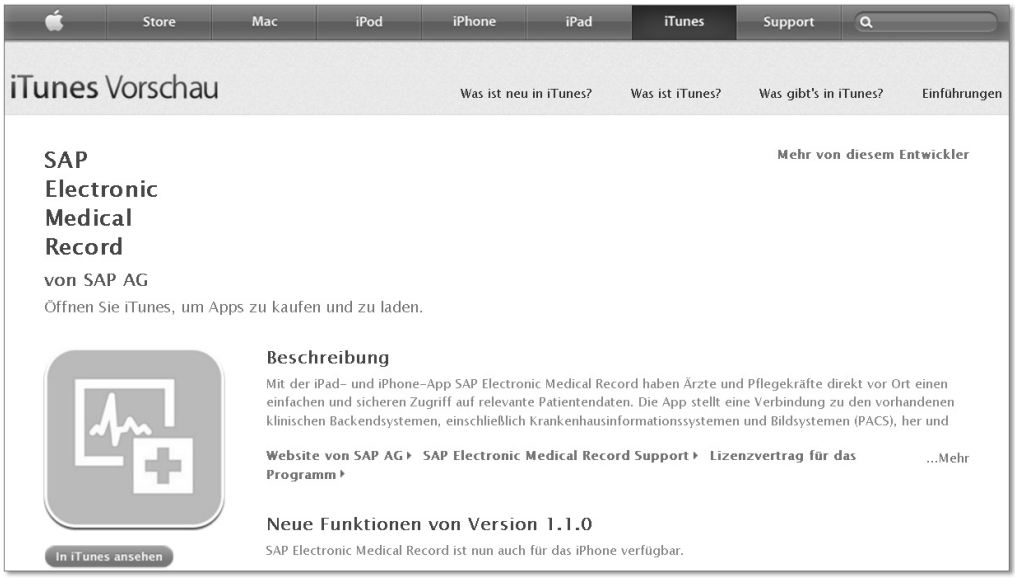


Abbildung 3.2 iTunes als Bezugsquelle für iOS-Apps

Keine externen Schutzprogramme

Apple selbst ist davon überzeugt, dass seine Sicherheitsmechanismen so wirksam sind, dass die Geräte keine zusätzlichen Antivirenprogramme benötigen, die auf PCs gängiger Standard sind. Inwiefern dieser Grundsatz auf Dauer Bestand haben kann, wird die Zukunft zeigen.

Jailbreak

Ein Einfallstor für mögliche Schadsoftware sind Geräte, die einem Jailbreak unterzogen werden. Dabei werden Sicherheitslücken dazu verwendet, alle Sicherheitsmechanismen auszuhebeln und damit dem Anwender die volle Kontrolle über das Gerät zu verschaffen. Fatalerweise erhalten damit aber auch alle mobilen Anwendungen den vollständigen Zugriff auf die Geräte. Böswilligen Anwendungen werden damit alle Tore geöffnet, sodass zum Beispiel alle Arten von

Daten abfließen können. In Kapitel 18, »Datenschutz und Sicherheit für Ihr Vorhaben«, werden wir noch genauer darauf eingehen, wie Sie verhindern können, dass Geräte, die einem solchen Eingriff unterzogen wurden, Zugang zu Ihrem Netzwerk und Ihren Daten erhalten.

Kostenverursachende Apps

In der Vergangenheit sind jedoch auch im iOS-Bereich, wie auch bei einigen anderen Betriebssystemen, darüber hinaus einige mobile Anwendungen aufgetreten, bei denen über Klicks auf Werbeeinblendungen Kosten entstehen konnten. Solche Apps sind daher gute Kandidaten für Ihre schwarze Liste mit verbotenen Anwendungen auf Ihren Geräten. Wir werden in Kapitel 18, »Datenschutz und Sicherheit für Ihr Vorhaben«, noch genauer behandeln, welche organisatorischen Maßnahmen insgesamt geeignet sind, die Sicherheit Ihrer mobilen Anwendungen zu erhöhen.

Für die Sicherheit der Geräte ist es zudem kritisch, dass die Anwender die notwendigen Sicherheitseinstellungen bei Apple-Geräten selbst von Hand vornehmen müssen und diese dann entsprechend auch wieder ändern können. Dies schreit für geschäftlich genutzte Endgeräte geradezu nach einer Administrationslösung, wie wir sie Ihnen in Form von SAP Afaria in Kapitel 9 noch genauer vorstellen werden.

Sicherheit bei Android

Offenes System

Mit dem Betriebssystem Android verfolgt Google einen ganz anderen Ansatz als Apple (siehe Abschnitt 1.2.2, »Android«). Die Offenheit des Systems ist hier oberstes Gebot. Das Betriebssystem selbst ist eine Open-Source-Anwendung auf Linux-Basis. Als Folge dessen verändern die einzelnen Hardwarehersteller, die Android-basierte Geräte vertreiben, immer noch die ursprüngliche Android-Version, die Google ausliefert, sodass es eine Vielfalt von verschiedenen Versionsständen gibt.

Mit *Google play* existiert auch ein von Google bereitgestellter Marktplatz für mobile Android-Anwendungen (*http://play.google.com/store*, siehe Abbildung 3.3). Die Anwender können aber über eine Einstellung an ihren Geräten auch Anwendungen aus anderen Quellen installieren. Google hat bekannt gegeben, dass es alle Apps auf seinem Marktplatz automatisch von einem Tool, dem *Google Bouncer*, auf Schadsoftware überprüft.

Abbildung 3.3 Google play als Quelle für Android-basierte mobile Anwendungen

Schutz durch Antivirenprogramme

Der offene Ansatz von Android hat zwei Folgen: Einerseits stehen Antivirenprogramme in durchaus nennenswerter Zahl zur Verfügung, mit denen die Sicherheit der Geräte überprüft werden kann, so wie Sie es von Ihrem Microsoft Windows-PC kennen. Auf der anderen Seite ist aber auch eine steigende Anzahl von Angriffen auf Android-Geräte zu verzeichnen. So sind etwa seit dem Trojaner *GGTracker* immer wieder Angriffe zu beobachten, bei denen SMS-Funktionalitäten genutzt werden, um den Anwender zu schädigen.

Rooting

Leider ist auch bei Android-basierten mobilen Endgeräten eine Art Jailbreak möglich. Hierbei nutzen die Angreifer einen in Linux vorhandenen Superuser, um alle Sicherheitsvorschriften auszuhebeln und die volle Kontrolle über das Gerät zu erlangen, das heißt es zu *rooten (siehe Abschnitt 2.1, »Herausforderungen durch »Bring Your Own Device«)*. Die Gefahren, die hierbei entstehen, liegen auf der Hand, deswegen sind auch hier Gegenmaßnahmen notwendig, wenn Sie diese Geräte in Ihrem Unternehmen einsetzen möchten.

Verschlüsselung

Allerdings sind in der Version 4 von Android wesentliche Funktionalitäten für den Sicherheitsbereich – insbesondere bei der Verschlüsselung – hinzugekommen. So können die Daten auf einem Android-Gerät nun vollständig verschlüsselt werden. Die Entwicklung sicherer Anwendungen wird zudem durch die Einführung einer Schlüsselbund-API besser unterstützt. Diese vereinfacht zum Beispiel die sichere Authentifizierung eines Benutzers durch eine App wesentlich.

Bei einem geeigneten Mix der organisatorischen und technischen Vorkehrungen, mit denen wir Sie in Kapitel 18, »Datenschutz und Sicherheit für Ihr Vorhaben«, auch für den Android-Bereich bekannt machen werden, sind unserer Einschätzung und Erfahrung nach auch Android-Geräte für den Unternehmenseinsatz geeignet. SAP selbst hat auf seiner letzten Kundenmesse bekannt gegeben, dass es gemeinsam mit Samsung daran arbeitet, die Android-Geräte dieses Herstellers für den professionellen Einsatz in Unternehmen weiter zu optimieren. Erste Ergebnisse sind hier mehr als 100 APIs für sicherheitsrelevante Bereiche der Initiative Samsung for Enterprise (SAFE).

Sicherheit bei Microsoft Windows Phone 7

Microsoft hat in der Vergangenheit verschiedene Anläufe unternommen, um am Markt für mobile Anwendungen ähnlich erfolgreich zu werden wie im Bereich der Office-Produkte und des Betriebssystems Windows. Im Jahr 2010 hat Microsoft eine neue Plattform für mobile Endgeräte vorgestellt, Windows Phone (siehe Abschnitt 1.2.3). Verwechseln Sie dies insbesondere in Bezug auf die Sicherheitsaspekte jedoch nicht mit dem älteren Windows Mobile. Letzteres erlaubte etwa dem jeweiligen Anwender den vollen Zugriff auf alle Dateien.

Restriktives Sicherheitskonzept

Demgegenüber ist Windows Phone unter Sicherheitsaspekten wesentlich neu gestaltet worden:

- Restriktive Zugriffsbeschränkungen wurden eingeführt. So existieren zum Beispiel keine Hintergrundprogramme, was Malware das Leben wesentlich erschwert.
- SMS können nicht aus einer mobilen Anwendung heraus versendet werden. Damit können keine hohen Kosten durch den nicht gewollten Versand von Premium-SMS entstehen.
- Es gibt keine Funktionalitäten für Screenshots. Denken Sie hier etwa an die Möglichkeit, dass sonst bei einem Gesundheitsdienstleister kritische Patientendaten mit einem Screenshot gespeichert werden könnten.

Allerdings können Sie auch bei Windows Phone als Anwender die volle Kontrolle über das Gerät erlangen, ähnlich dem Jailbreak bei Apple-Geräten. Für das Laden der mobilen Anwendungen hat Microsoft den Windows Marketplace etabliert (*http://www.windowsphone.com/de-DE/apps*, siehe Abbildung 3.4). Ähnlich wie Apple überprüft Microsoft alle Apps, bevor Sie auf dem Marketplace eingestellt werden.

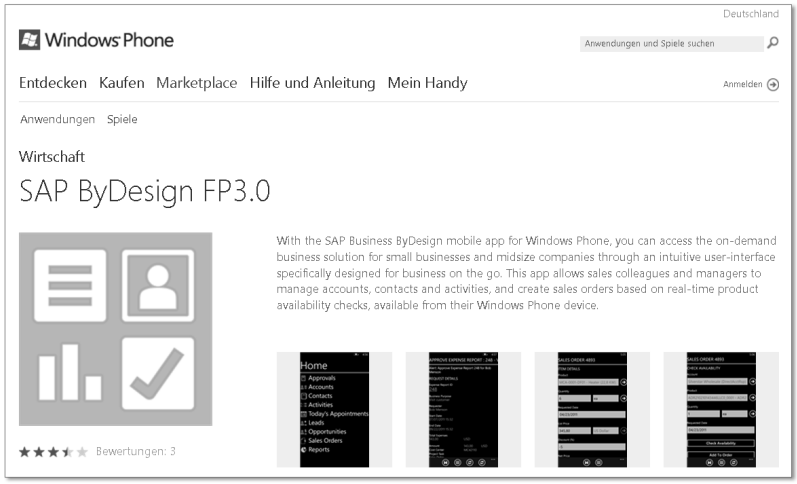


Abbildung 3.4 Windows Marketplace als Quelle für Windows Phone-Anwendungen

Insgesamt ist die Zahl der mobilen Anwendungen für Windows Phone noch verhältnismäßig klein, sodass eine Beurteilung in puncto Sicherheit derzeit schwierig ist.

Sicherheit beim BlackBerry

Umfassende Sicherheitsfunktionalitäten

Über einen längeren Zeitraum waren die BlackBerry-Geräte der Firma Research in Motion (RIM) das Maß aller Dinge bei mobilen Geräten in Unternehmen. In Abschnitt 1.2.4, »BlackBerry OS«, sind wir ja bereits auf die Lösungen der Firma RIM eingegangen. Für den Sicherheitsbereich ist dabei zu beachten, dass die Lösung der Firma nicht nur aus den Geräten selbst und dem BlackBerry OS besteht, sondern auch eine Client-Server-Komponente umfasst. Die ausgereiften Sicherheitsfunktionalitäten des BlackBerry Enterprise Servers (BES) ermöglichen deswegen eine positive Einschätzung in Sachen Sicherheit. Diese Bewertung wurde auch nicht nachhaltig durch zeitweilige Debatten darüber getrübt, ob staatliche Stellen Zugriff auf den Datenverkehr und die Server der Firma RIM erlangen können.

Durch die zunehmende Konkurrenz vor allem der Apple-Geräte ist die Popularität der BlackBerrys stark gesunken. Inzwischen verfügt auch RIM mit der BlackBerry App World über einen Marktplatz, von dem mobile Anwendungen heruntergeladen werden können, wie bei den anderen Anbietern auch nach einer Freigabe der Apps durch RIM (*http://de.blackberry.com/services/appworld/*, siehe Abbildung 3.5).

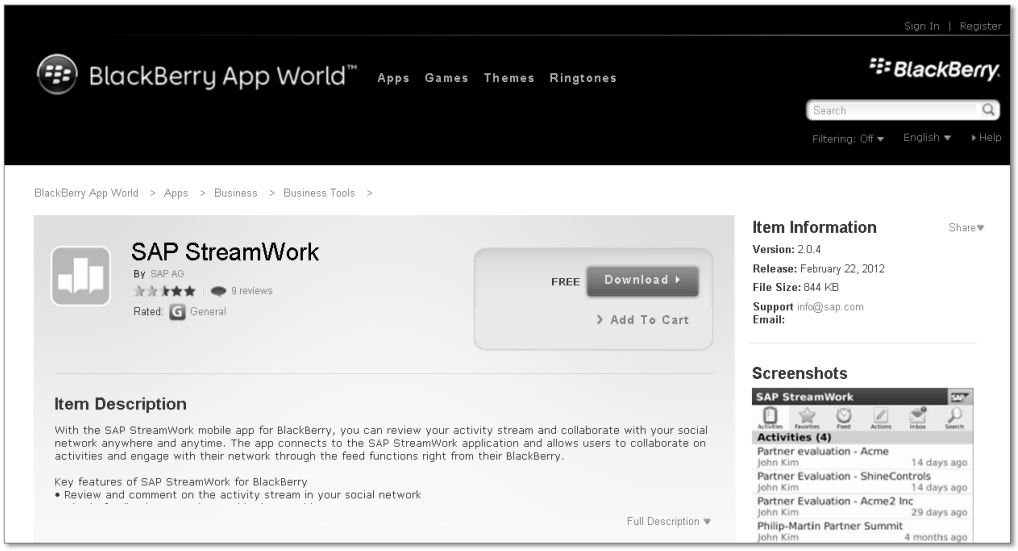


Abbildung 3.5 BlackBerry App World als Quelle für BlackBerry OS-basierte Anwendungen

Eine Einschätzung möglicher Gefahren bei zukünftigen Geräten dieser Firma fällt jedoch verhältnismäßig schwer, da zum gegenwärtigen Zeitpunkt nicht exakt einzuschätzen ist, wie sich die Plattform weiterentwickeln wird, da RIM in letzter Zeit massiv an Marktanteilen verloren hat.

Bei der Lektüre dieses Abschnittes haben Sie unter Umständen Ausführungen zu den Nokia-Geräten vermisst. Der Grund dafür ist einfach: Nokia hat angekündigt, in Zukunft auf Windows Phone zu setzen. Somit sind die entsprechenden Ausführungen zu Windows Phone auch für die Geräte des finnischen Herstellers gültig.

3.2.3 Netzwerk

Virtual Private Network

Die Verwendung mobiler Geräte in Ihrer Organisation oder Ihrem Unternehmen für dienstliche Zwecke setzt voraus, dass Sie den Anwendern Zugang zu Ihrem Server gewähren. In den meisten Organisationen existieren bereits technische Lösungen, mit denen etwa Laptop-Anwender über ein Virtual Private Network (VPN) eine gesicherte Verbindung zum Unternehmensnetzwerk aufbauen können. Über ein VPN-Gateway auf einem Server kann ein Benutzer eine Verbindung zwischen einem mobilen Endgerät und dem Unternehmensnetzwerk aufbauen, die verschlüsselt ist. Wahrscheinlich haben

Sie eine solche Lösung auch heute schon bei sich im Unternehmen für Laptops im Einsatz. Ein anderer Anwender hat auf diese Weise keinen Zugang zu diesem sicheren Netzwerk.

Die Notwendigkeit einer solchen Maßnahme liegt dabei auf der Hand, da es für die Sicherheit Ihrer Daten fatal wäre, wenn sich nicht berechtigte Personen Zugang zu Ihrem Unternehmensnetzwerk verschaffen würden.

Identifikation mobiler Endgeräte

Für den Bereich der mobilen Endgeräte geht es bei der Sicherung der Datennetze daher vor allem darum, die bestehenden VPN-Lösungen für den mobilen Bereich zu adaptieren. Hierfür besteht zunächst die Notwendigkeit, die Geräte zu identifizieren und einem Anwender klar zuordnen zu können. In Kapitel 18, »Datenschutz und Sicherheit für Ihr Vorhaben«, werden wir darstellen, welche Möglichkeiten Sie in diesem Zusammenhang haben.

3.2.4 Backup/Restore

Die gesetzlichen Vorschriften erfordern nicht nur Vorkehrungen, um einen Abfluss von Daten und die Einsichtnahme in diese durch nicht berechtigte Dritte zu verhindern. Ebenso wichtig ist es für Sie, dafür Sorge zu tragen, dass keine Daten gelöscht werden, die gesetzlichen Aufbewahrungsregeln unterliegen.

Datensicherung

Dies ist eine besondere Herausforderung bei mobilen Endgeräten. Die Nutzer dieser Geräte denken durch den meist noch sorglosen Umgang mit diesen Geräten als zum Beispiel mit Laptops noch weniger daran, Datensicherungen vorzunehmen.

Die Anbieter der Betriebssysteme bieten hier Speicherkonzepte in Form von cloudbasierten Lösungen. Aus der Sicht des Datenschutzes entsteht damit jedoch eine neue mögliche Gefahr, nämlich die Speicherung von Daten auf Servern, die nicht unter der Kontrolle des Unternehmens stehen und mit deren Anbietern unter Umständen keine klare vertragliche Regelung geschlossen wurde.

3.2.5 Kosten

Hohe Mobilfunkrechnungen rangieren in den letzten Jahren konstant oben auf der Liste der Gründe, warum sich Jugendliche als eine Hauptnutzergruppe von mobilen Endgeräten verschulden. Wir gehen aufgrund unserer Erfahrungen natürlich davon aus, dass es

sich bei den Anwendern in Ihrem Unternehmen um verantwortungsbewusste Menschen handelt, die keine exzessiven Smartphone-Rechnungen produzieren. Dennoch sollten Sie das Risiko hoher Kosten berücksichtigen und die aktiv lenken.

Kostenfallen

Dabei geht es beispielsweise um Vertriebsmitarbeiter, die einen wichtigen Termin im Ausland wahrnehmen und für ihre in diesem Rahmen gezeigte Präsentation in letzter Minute noch große Dateien laden müssen. Auf diese Weise werden hohe Roaming-Kosten verursacht. Das in Unternehmen derzeit oftmals existierende, und in Kapitel 1 bereits angesprochene »produktive Chaos« mit innovativen Insellösungen in vielen Bereichen erschwert es Ihnen, gute Tarifkonditionen bei Ihrem Telekommunikationsanbieter zu erzielen. Daher ist es wichtig, dass Sie diesen Risikofaktor nicht außer Acht lassen und den Überblick über die Kosten behalten, die durch mobile Anwendungen und Geräte in Ihrem Unternehmen entstehen, sowie deren Transparenz jederzeit aufrechterhalten.

Im Bereich der Kosten ist das Themen Lizenzen für Sie von Bedeutung. Privat erworbene Apps der Mitarbeiter sind zum Teil nicht für eine kommerzielle Verwendung freigegeben. Besonders wichtig wird dieses Thema für Sie, wenn Sie Mitarbeitern über BYOD-Regelungen gestatten, private Geräte für dienstliche Zwecke zu nutzen. Das Thema BYOD werden wir in Abschnitt 3.3.3, »BYOD als besondere Herausforderung«, und insbesondere in Kapitel 18, »Datenschutz und Sicherheit für Ihr Vorhaben«, noch weiter vertiefen.

3.3 Anforderungen des Datenschutzes und der Personalvertretungen

Aus der Sicht des Datenschutzes und der Personalvertretungen müssen sich die Regelungen zum Einsatz mobiler Geräte in den Unternehmen in die bestehenden Regelungen einbetten lassen.

Als Autoren dieses Buches sind wir weder Juristen noch Betriebsräte, sodass wir Ihnen in diesem und den folgenden Abschnitten selbstverständlich weder eine Rechtsberatung noch eine Darstellung der konkreten Positionen von Arbeitnehmervertretern liefern können. Was wir Ihnen jedoch bieten können, sind unsere Erfahrungen aus unseren bisherigen Projektaktivitäten und Gesprächen mit den Verantwortlichen zu diesen Themen.

3.3.1 Was Ihre Datenschutz- und Sicherheitsrichtlinien beachten sollten

Rechtliche Voraussetzungen

In rechtlicher Hinsicht sind die mobilen Geräte genauso zu behandeln wie andere IT-Geräte. Damit ist § 9 des Bundesdatenschutzgesetzes (BDSG) anwendbar, der fordert, dass die Unternehmen sowohl technische als auch organisatorische Maßnahmen zum Datenschutz ergreifen müssen. Hinzu kommen die entsprechenden gesetzlichen Vorschriften zum Risikomanagement, denen zum Beispiel Aktiengesellschaften unterliegen. Weitere gesetzliche und regulatorische Anforderungen für bestimmte Industrien wie etwa die Sozialgesetzbücher, die Haushaltsordnungen des Bundes und der Länder oder etwa auch das Arzneimittelgesetz unterstreichen die Notwendigkeit solcher Bemühungen. Im Folgenden haben wir eine Liste der Punkte zusammengestellt, die in den Datenschutz- und Sicherheitsrichtlinien geregelt wurden, die in unseren Projekten festgelegt wurden. Wie immer bei solchen Dokumenten gibt es jedoch eine Fülle von möglichen Ansätzen, von sehr detaillierten Richtlinien mit einer Fülle von Regelungen bis hin zu sehr allgemein gehaltenen Dokumenten.

In Kapitel 18, »Datenschutz und Sicherheit für Ihr Vorhaben«, werden wir einen Vorschlag für eine solche Regelung (*Policy*) vorstellen und dieses Thema noch weiter vertiefen.

Fragen für eine Sicherheitsregelung

Folgende Aspekte bedürfen in Mobile-Projekten auf die eine oder andere Weise einer Regelung:

- Welche Mitarbeitergruppen sind zur geschäftlichen Nutzung von Smartphones und Tablets berechtigt (zum Beispiel Vertriebsmitarbeiter, Führungskräfte ab einer bestimmten Ebene)?
- Welche Ausstattungsmerkmale soll es pro Gerät und pro Mitarbeitergruppe geben (zum Beispiel entweder Smartphone oder Tablet, Tablet nur mit WLAN)?
- Welche Regelungen werden für den Bereich BYOD getroffen (beispielsweise Kostenübernahme, Freiwilligkeit der Teilnahme)?
- Welche Grundsätze werden für die private Nutzung der dienstlichen Geräte festgehalten?
- Welche Dienste der Smartphones dürfen genutzt werden (insbesondere Telefon, Mail, SMS)?

- Welche Maßnahmen werden zum Diebstahlsschutz des Smartphones ergriffen (Aufbewahrung der Geräte, Aufkleber zur Kennzeichnung der Geräte als Firmeneigentum)?
- Welche Maßnahmen erfolgen bei sonstigen Verlusten des Gerätes?
- Welche Maßnahmen erfolgen beim Verlust der SIM-Karte von Firmengeräten?
- Ist die Weitergabe der Smartphones gestattet?
- Werden die mobilen Endgeräte über ein Mobile Device Management verwaltet?
- Welchen Support gibt es für die Geräte?
- Ist eine Löschung der auf den Geräten enthaltenen Daten mittels Mobile Device Management bei Verlust, Rückgabe des Gerätes oder Austausch eines defekten Gerätes vorgesehen?
- Was sind die erforderlichen Mindeststandards bei den Sicherheitseinstellungen (zum Beispiel Ortungsdienste nicht verwenden)?
- Welche Basiskonfigurationen werden bei den Geräten vorgenommen?
- Wie wird die Installation von Updates der Hersteller geregelt?
- Welche Vorgaben gibt es für Passwörter?
- Welche Vorgaben gibt es für die Installation von mobilen Anwendungen (gegebenenfalls schwarze Liste für verbotene mobile Anwendungen und weiße Liste für erlaubte)?
- Wie muss die Speicherung von dienstlichen und privaten Daten erfolgen?
- Wie ist der Backup der Daten geregelt?
- Ist die Verwendung von cloudbasierten Diensten der Anbieter erlaubt?
- Gibt es Zugriffsbeschränkungen für bestimmte Funktionalitäten (zum Beispiel Ortungsdienste)?
- Wie wird das Umgehen technischer Sperren der Geräte (zum Beispiel Jailbreak bei iOS-Geräten) vermieden?
- Wie wird eine Kostenkontrolle ermöglicht (Tarife)?
- Wie wird mit Kosten umgegangen, die durch mobile Anwendungen entstehen?

Bewusstsein in den Mitarbeitervertretungen

Eine Erfahrung aus den von uns durchgeführten Mobile-Projekten war dabei für uns besonders interessant und unterschied sich zum Teil auch von herkömmlichen IT-Projekten. Den Personalvertretungen und Betriebsräten ist bewusst, dass viele Mitarbeiter außerordentlich daran interessiert sind, ein Tablet oder Smartphone als Dienstgerät zu erhalten oder ein privates Gerät mit einer von der Firma bezahlten SIM-Karte nutzen zu können. Aus diesem Grund sind sie durchaus zu Zugeständnissen auch in kritischen Bereichen (insbesondere der Löschung der Daten auf einem Gerät bei einem Verlust des Gerätes) bereit, wenn sie von Beginn an in die Diskussionen des Projektes eingebunden sind. Daher können wir Ihnen nur dringend empfehlen, schon bei den ersten Überlegungen die Arbeitnehmervertreter einzubeziehen.

Themen der Mitarbeitervertretungen

Erfahrungsgemäß sind es drei Fragen, auf die Personalvertretungen beim Einsatz mobiler Geräte ihr besonderes Augenmerk richten:

- Welche Mitarbeiter erhalten mobile Geräte, und wie ist eine etwaige Auswahl gegebenenfalls begründet?
- Ist die Freiwilligkeit bei einer BYOD-Regelung gegeben oder versucht das Unternehmen hier auf dem Rücken der Mitarbeiter Kosten zu sparen?
- Welche Kontrollmöglichkeiten sind beim Einsatz einer Gerätemanagementlösung gegeben, und wie wird ein möglicher Missbrauch vermieden (verhaltensabhängige Leistungskontrolle)?
- Falls Sie ein Experte auf diesem Gebiet sind, können Sie zu Recht einwenden, dass unter Umständen einige durch die hier aufgeführten Fragen berührten Bereiche gar nicht zwingend der Mitbestimmung unterliegen. Wir sind aber auf der Basis der gesammelten Erfahrungen zu dem Schluss gekommen, dass eine kompromissbereite Haltung vonseiten der Arbeitgeber hier zwingend erforderlich ist.

3.3.2 Zugelassene Geräte versus andere Geräte

Bei allen Regelungen, die Sie für Ihre Mobile-Projekte treffen, empfehlen wir Ihnen, von Beginn an eine Klassifizierung der Geräte vorzunehmen. Dies erlaubt es Ihnen, die Richtlinien so anzupassen, dass die Anwender nicht generelle Regelungen (beispielsweise das Verbot, Firmendaten auf dem Endgerät zu speichern) als ungerechtfertigte Einschränkung ihrer Arbeitsmöglichkeiten empfinden.

Klassifizierung nach Genehmigungsstatus

Eine solche Klassifizierung beruht im Wesentlichen auf dem Genehmigungsstatus der Geräte, das heißt, es wird zwischen erlaubten und verbotenen Geräten unterschieden.

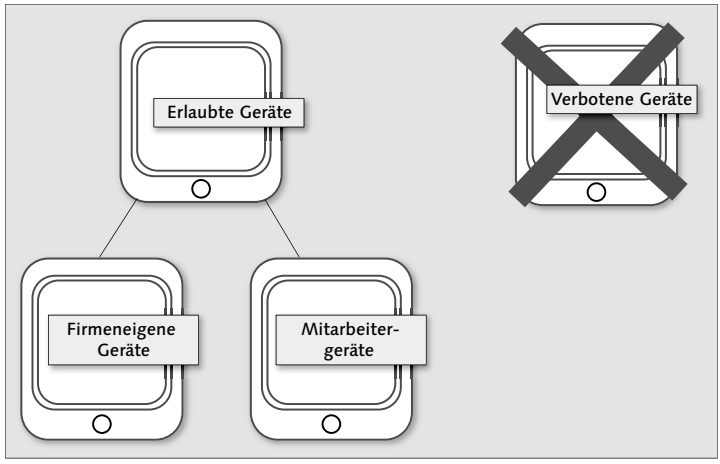


Abbildung 3.6 Klassifizierung von mobilen Geräten in einem Unternehmen mit BYOD-Regelung

Die Darstellung in Abbildung 3.6 geht von dem Maximalfall aus, dass Sie es zulassen, dass Mitarbeiter ihre eigenen Geräte mitbringen und diese im Rahmen einer BYOD-Regelung nutzen dürfen.

Klassifizierung mit und ohne BYOD

Wie wir bereits angesprochen haben, kann es durchaus Fälle geben, in denen Unternehmen keine BYOD-Regelung anwenden möchten. In diesem Fall vereinfacht sich die Klassifizierung wesentlich, wie Sie in Abbildung 3.7 sehen.

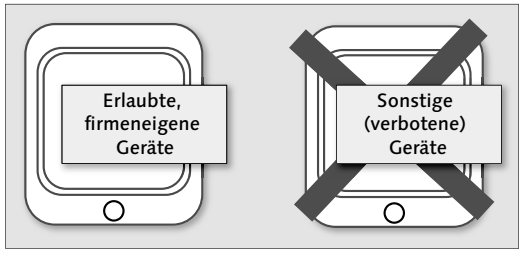


Abbildung 3.7 Klassifizierung von mobilen Geräten in einem Unternehmen ohne BYOD-Regelung

In einem Unternehmen mit einer solchen Regelung dürfen nur die firmeneigenen Geräte verwendet werden. Dass wir eine solche Rege-

lung für außerordentlich schwer umsetzbar halten, haben wir bereits betont.

Erlaubte und nicht erlaubte Geräte

Grundsätzlich ziehen Unternehmen, die diese oder eine ähnliche Klassifizierung erfolgreich anwenden, verschiedene Gesichtspunkte heran, wenn sie darüber entscheiden müssen, welches Gerät in welche Kategorie eingeordnet wird. Aus Sicherheitsgesichtspunkten haben sich folgende Kriterien bewährt:

- zugelassene Betriebssysteme
- zugelassene Version/Hersteller
- Schnittstellen zur eingesetzten MDM-Lösung

Mit dem ersten Kriterium legen Sie fest, welche Plattform Sie sicherheitstechnisch als grundsätzlich geeignet einstufen. In diesem Zusammenhang gehört inzwischen in den meisten Unternehmen die Ansicht der Vergangenheit an, dass nur BlackBerry-Geräte als geeignet eingestuft werden.

Kriterien zur Beurteilung

Folgende Punkte werden immer wieder diskutiert, wenn es darum geht, die einzelnen Betriebssysteme und Versionen mobiler Endgeräte zu beurteilen:

- Mindeststandards für Passwörter bei Gebrauch des Gerätes
- hardwareseitige Verschlüsselung der Daten auf dem Gerät
- Fernlöschung der Daten auf dem Gerät
- Sicherheitslage bezüglich der verwendeten mobilen Anwendungen
- Schutz vor Malware/Viren

In Ihrem Unternehmen existieren sicherlich schon Sicherheitsvorgaben für den IT-Bereich. Diese werden beispielsweise Vorgaben zur Verwendung von Passwörtern enthalten. Auf der Basis solcher Regelungen können Sie sehr schnell bewerten, inwiefern eine mobile Betriebssystemplattform verwendet werden kann.

Verschlüsselung

In der Vergangenheit wurde von diesen fünf Sicherheitsthemen in Bezug auf Betriebssysteme und Versionen mobiler Endgeräte das Thema Verschlüsselung durchaus kritisch gesehen. So unterstützt etwa Android erst ab Version 4.0 (Ice Cream) vollumfänglich die hardwareseitige Verschlüsselung. Dies weist schon auf eine gewisse Besonderheit der Android-Geräte beim Thema Betriebssysteme und

Versionen hin. Hier ist immer ein gewisser »Zoo« (siehe Kapitel 2, »Der Technologiezoo und die IT-Abteilung«) verschiedener Android-Versionsstände bei den unterschiedlichen Endgeräteherstellern zu beobachten. So gehen etwa Schätzungen davon aus, dass die Zahl der Android-Geräte, die Mitte 2012 die neueste Version verwendeten, noch im einstelligen Bereich lag.

3.3.3 BYOD als besondere Anforderung

In den bisherigen Kapiteln wurde das Thema »Bring Your Own Device« (BYOD) bereits mehrfach angesprochen. Diese Überlegungen systematisieren wir in diesem Abschnitt. In Kapitel 18, »Datenschutz und Sicherheit für Ihr Vorhaben«, werden wir die dadurch erforderlichen Maßnahmen weiter vertiefen.

Das Thema BYOD stellt besondere Anforderungen an die Verantwortlichen in einem Unternehmen bzw. einer Organisation, wenn es darum geht, Risiken zu vermeiden, da sie die Privatgeräte der Mitarbeiter nicht unter Kontrolle haben.

Sicherheitsfragen zu BYOD

Bei der Betrachtung dieses Themas stellt sich sofort eine Reihe von Fragen:

- Wie wird vermieden, dass Datenschutzbestimmungen, Risikomanagementpflichten und Gesetze verletzt werden?
- Wie wird der Schutz des geistigen Eigentums des Unternehmens sichergestellt?
- Wer haftet für etwaige Schäden bei Verstößen gegen gesetzliche Bestimmungen?
- Wer trägt die Kosten für den Einsatz der privaten Geräte für dienstliche Zwecke?

Die Liste ließe sich sicherlich noch feiner untergliedern und wesentlich erweitern. In Presseartikeln und auf Kongressen formulieren einige Juristen auch immer wieder rechtliche Bedenken gegen die Verwendung privater Geräte und empfehlen, dass die Nutzung privat angeschaffter Geräte für Unternehmenszwecke generell untersagt wird. Aus der Sicht eines Arbeitsrechtlers mag eine Regelung angemessen erscheinen, die die Verwendung privater Geräte im dienstlichen Bereich verbietet. Aus der Sicht eines IT-Verantwortlichen oder des Leiters eines Fachbereiches geht ein solcher Ansatz jedoch an der

Realität vorbei. Daher stellt sich aus unserer Sicht in den allermeisten Unternehmen nicht mehr die Frage, ob eine BYOD-Regelung erstellt wird, sondern wie diese ausgestaltet wird.

Rechtliche Notwendigkeit von Richtlinien

Werden entsprechende Regelungen nicht rechtzeitig getroffen, besteht die Gefahr, dass Sie eine ungewollt weit gefasste BYOD-Regelung fördern. Die Juristen sprechen in einem solchen Fall von »betrieblicher Übung«. Dies bedeutet nichts anderes, als dass Arbeitnehmer nach einiger Zeit ein Recht zur Nutzung ihres privaten Gerätes im Betrieb dadurch erwerben, dass der Arbeitgeber dies stillschweigend duldet, da er nicht explizit widerspricht.

Festlegung der Richtlinieninhalte

Aus diesem Grund ist das erste wesentliche Element der BYOD-Regelungen in Ihrem Unternehmen die Frage, was Sie für den Bereich BYOD grundsätzlich regeln möchten. Hier gibt es drei Alternativen:

- Soll es ein generelles Verbot des Einsatzes privater Geräte zu dienstlichen Zwecken geben?
- Soll es eine generelle Zulassung von privaten Geräten geben und wenn ja, mit oder ohne zusätzliche Regelungen?
- Sollen nur bestimmte Geräte zugelassen werden und wenn ja, mit oder ohne zusätzliche Regelungen?

Es wird Sie nach der Lektüre unserer bisherigen Ausführungen sicherlich nicht überraschen, dass wir die dritte Alternative dringend empfehlen und als realistische Handlungsoption ansehen.

Koordination der Verantwortlichen

Für die konkrete Ausgestaltung der BYOD-Richtlinie ist die Zusammenarbeit aller relevanten Stellen notwendig:

- Personalvertretungen
- Datenschutzbeauftragte
- Sicherheitsbeauftragte
- IT-Verantwortliche
- Personalabteilung
- Management

Anders als bei den firmeneigenen Geräten hat das Unternehmen bei mobilen Endgeräten aus dem Privatbesitz seiner Mitarbeiter nicht von Haus aus das Recht, auf die mobilen Geräte zuzugreifen und sie zu administrieren. Zudem gibt es auf diesen Geräten per se immer eine Vermischung von dienstlichen und privaten Daten.

Richtlinieninhalte

Folgendes muss demzufolge in einer BYOD-Richtlinie im Detail geklärt werden:

- zugelassene Geräte (inklusive genaue Versionsnummer)
- erlaubte Eingriffe des Unternehmens
  - Administration (beispielsweise Patches)
  - Remote-Löschen der Daten
- Anforderungen an die Sicherheitseinstellungen und die Basiskonfiguration des Gerätes (beispielsweise Ausschaltung von Ortungsdiensten)
- zugelassene mobile Anwendungen mit Firmendaten auf dem Gerät
- zugelassene mobile Anwendungen allgemein
- Zugriff auf private Daten durch Arbeitgeber bei Missbrauchsverdacht
- Zugriff auf das Firmennetz (virtualisierter Desktop)
- Aufbewahrungsregelungen für geschäftliche Daten
- Kostenübernahme für Verbindungskosten
- Kostenregelung für privat genutzte mobile Anwendungen
- Haftungsregelungen bei Schäden

Datenschutzrecht

Wir empfehlen Ihnen, bei all diesen Punkten ein besonderes Augenmerk auf die datenschutzrechtliche Bewertung der Verarbeitung von personenbezogenen Daten zu richten. Rechtlich muss hierbei darauf geachtet werden, dass keine Datenübermittlung an den Arbeitnehmer vorliegt, da dies zusätzliche Maßnahmen erfordern würde. So müsste ein Unternehmen entweder die Zustimmung jedes einzelnen Betroffenen (beispielsweise Kunden, Versicherungsnehmer, Patienten) einholen oder mit dem Arbeitnehmer einen Vertrag über eine Auftragsdatenvereinbarung schließen. Beide Wege sind nahezu nicht praktikabel. Aus diesem Grund wählen Unternehmen hier einen anderen Weg. Diese kritischen Daten werden in mobilen Anwendungen gespeichert, die vollständig von den Unternehmen über ein Mobile Device Management kontrolliert werden können. Damit wird die Forderung des Datenschutzes erfüllt. Dabei ist es natürlich nicht möglich, dass das Unternehmen die Daten auf den Endgeräten im Einzelnen ansehen und etwa die Eingaben des Mitarbeiters in

Echtzeit kontrollieren kann, da dies in den Bereich der verhaltensabhängigen Leistungskontrolle fallen würde.

Zudem muss eine weitere Forderung der Datenschützer darin bestehen, dass insbesondere für Privatgeräte die Speicherung kritischer Daten auf dem Gerät durch mobile Anwendungen nach Möglichkeit vermieden wird. In Kapitel 18, »Datenschutz und Sicherheit für Ihr Vorhaben«, werden wir Ihnen am Beispiel der mobilen Patientenakte (siehe Abschnitt 1.4.2, »Mobility am Beispiel der Charité Berlin) aufzeigen, wie diese Forderung durch SAP schon bei der Entwicklung dieser mobilen Anwendung berücksichtigt wurde. In Kapitel 18 werden wir insbesondere auch darauf eingehen, was Sie bei der Entwicklung eigener mobiler Anwendungen beachten müssen, damit diese die notwendigen Sicherheitsstandards erfüllen.

3.4 Maßnahmen zur Vermeidung von Gefahren und Risiken bei mobilen Anwendungen

Bei der Behandlung des Themas Sicherheit möchten wir es vermeiden, einen Fehler zu machen, der zum Teil bei Diskussionen in diesem Bereich zu beobachten ist, nämlich eine Fülle von Gefahren aufzuzeigen ohne direkt Lösungen anzubieten. Deswegen möchten wir jetzt den Schwenk vollziehen und Ihnen im Folgenden vorstellen, welche organisatorischen und technischen Maßnahmen Sie ergreifen können, um möglichen Risiken von Beginn an erfolgreich zu begegnen.

Grundsätze für die mobile Sicherheit

Grundlegend für den Umgang mit dem Thema mobile Sicherheit sind aus unserer Sicht vier Kernaussagen:

- Mobile Sicherheit ist die Summe aus organisatorischen Maßnahmen und technischen Hilfsmitteln.
- Je weniger verschiedene mobile Geräte bzw. Plattformen eingesetzt werden, umso einfacher ist es, einen guten Sicherheitsstand herzustellen.
- Ohne ein MDM-Tool ist eine wirkungsvolle Absicherung der Endgeräte in einem größeren Unternehmen mit einem vertretbaren Aufwand kaum zu leisten.
- Bei allen organisatorischen Vorkehrungen und technischen Hilfsmitteln bewahrheitet sich besonders im mobilen Bereich der

Index

A

B

C

D

E

F

G

H

I

J

K

L

M

N

O

P

Q

R

S

T

U

V

W

X

Y

Z