

Beckert, Beckert, Escherich

## Mobile Lösungen mit SAP®



**Galileo Press**

Bonn • Boston

# Auf einen Blick

## TEIL I Mobile Anwendungen und die SAP-Lösungen

1	Mobile Anwendungen und Geräte in Unternehmen: Vom produktiven Chaos zum strategischen Ansatz .....	31
2	Der Technologiezoo und die IT-Abteilung .....	63
3	Der Datenschützer, die Personalvertretungen und mobile Anwendungen .....	79
4	Ein kurzer Rückblick: SAP und mobile Anwendungen .....	109
5	Die neue SAP-Mobile-Plattform .....	121
6	SAP-Apps im Überblick .....	137

## TEIL II Die neuen mobilen Lösungen von SAP unter der Haube

7	Sybase Unwired Platform .....	199
8	SAP NetWeaver Gateway .....	239
9	SAP Afaria .....	275
10	Systemlandschaften im Überblick .....	299
11	Eine neue App entsteht .....	317
12	Der SAP Store .....	349

## TEIL III Eigene Mobile-Vorhaben umsetzen

13	Die richtigen Personen und das richtige Know-how für Ihr Projekt .....	369
14	Bestandsaufnahme und Mobile-Reifegrad .....	389
15	Eine Mobile-Strategie für Ihr Unternehmen .....	407
16	Die richtigen mobilen Anwendungen für Ihr Projekt finden .....	429
17	Ihre Mobile-Infrastruktur einrichten .....	451
18	Datenschutz und Sicherheit für Ihr Vorhaben .....	469
19	Projekt- und Risikomanagement .....	497
20	Erfahrungen und Lehren aus der Praxis .....	515
21	Ausblick: Die mobile Zukunft der SAP .....	529

# Inhalt

Vorwort .....	17
Einleitung .....	19

## Teil I Mobile Anwendungen und die SAP-Lösungen

### 1 Mobile Anwendungen und Geräte in Unternehmen: Vom produktiven Chaos zum strategischen Ansatz 31

1.1	Die Smartphone-Revolution .....	31
1.2	Übersicht und Verbreitungsgrad von Mobile- Betriebssystemen .....	36
1.2.1	Apple iOS .....	38
1.2.2	Android .....	39
1.2.3	Windows Phone .....	40
1.2.4	BlackBerry OS .....	41
1.2.5	Symbian .....	41
1.2.6	HP webOS .....	42
1.2.7	Weitere Betriebssysteme für mobile Endgeräte .....	42
1.3	Übersicht mobiler Endgeräte .....	42
1.3.1	Smartphones .....	44
1.3.2	Mobiltelefone .....	45
1.3.3	Tablet-PCs .....	46
1.3.4	Notebooks/Subnotebooks/Laptops/ Netbooks .....	46
1.3.5	Personal Digital Assistant (PDA) .....	47
1.3.6	Portable Media Player .....	47
1.4	Unternehmen werden mobil – zwei Erfahrungsbeispiele .....	48
1.4.1	Mobility bei der SAP AG .....	48
1.4.2	Mobility am Beispiel der Charité Berlin .....	52
1.5	Zusammenfassung .....	62

### 2 Der Technologiezoo und die IT-Abteilung ..... 63

2.1	Herausforderungen durch »Bring Your Own Device« .....	66
-----	--	----

2.2	Herausforderungen durch Mobility .....	67
2.2.1	Die Sicht auf die mobilen Endgeräte .....	67
2.2.2	Die Sicht auf die Infrastruktur .....	69
2.3	Herausforderungen für das Endgerätemanagement .....	70
2.4	Herausforderungen durch die Anwendungs- entwicklung und -verwaltung .....	72
2.5	Herausforderungen für die Unternehmens- sicherheit .....	74
2.6	Zusammenfassung .....	76

### **3 Der Datenschutz, die Personalvertretungen und mobile Anwendungen ..... 79**

3.1	Ein Gedankenexperiment vorweg .....	80
3.2	Die fünf Risikobereiche mobiler Anwendungen .....	81
3.2.1	Physische Sicherheit .....	84
3.2.2	Malware/Viren und die unterschiedlichen Betriebssysteme .....	85
3.2.3	Netzwerk .....	92
3.2.4	Backup/Restore .....	93
3.2.5	Kosten .....	93
3.3	Anforderungen des Datenschutzes und der Personalvertretungen .....	94
3.3.1	Was Ihre Datenschutz- und Sicherheitsrichtlinien beachten sollten .....	95
3.3.2	Zugelassene Geräte versus andere Geräte ...	97
3.3.3	BYOD als besondere Anforderung .....	100
3.4	Maßnahmen zur Vermeidung von Gefahren und Risiken bei mobilen Anwendungen .....	103
3.4.1	Organisatorische Vorkehrungen .....	104
3.4.2	Technische Vorkehrungen .....	106
3.5	Zusammenfassung .....	107

### **4 Ein kurzer Rückblick: SAP und mobile Anwendungen ..... 109**

4.1	SAP Mobile Sales (MSA) .....	110
4.2	SAPConsole (WebSAPConsole) .....	111

4.3	SAP NetWeaver Mobile/SAP Mobile Infrastructure .....	112
4.4	Mobile Web Dynpro Online .....	117
4.5	Zusammenfassung .....	119
<b>5</b>	<b>Die neue SAP-Mobile-Plattform .....</b>	<b>121</b>
5.1	Sybase Unwired Platform .....	124
5.2	SAP NetWeaver Gateway .....	128
5.3	SAP Afaria .....	131
5.4	Zusammenfassung .....	135
<b>6</b>	<b>SAP-Apps im Überblick .....</b>	<b>137</b>
6.1	Klassifizierung mobiler Anwendungen .....	138
6.1.1	Native Anwendungen .....	139
6.1.2	Webanwendungen .....	140
6.1.3	Hybride Anwendungen .....	141
6.1.4	Container-Anwendungen .....	142
6.1.5	Online-/Offlineanwendungen .....	143
6.2	SAP Store .....	144
6.3	SAP-App-Navigator .....	147
6.3.1	Employee Productivity Apps (Personal) .....	149
6.3.2	Employee Productivity Apps (Finanzen) .....	160
6.3.3	Employee Productivity Apps (Vertrieb) .....	166
6.3.4	Employee Productivity Apps (Sonstige) .....	175
6.3.5	Process Apps .....	182
6.3.6	Industry Apps .....	188
6.3.7	Business Intelligence Apps .....	192
6.3.8	Zusammenfassung .....	196

## **Teil II Die neuen mobilen Lösungen von SAP unter der Haube**

<b>7</b>	<b>Sybase Unwired Plattform .....</b>	<b>199</b>
7.1	Die Sybase Unwired Plattform als Lösung für die Unternehmensmobilisierung .....	201
7.2	Architektur der Sybase Unwired Plattform .....	204
7.3	Systemanforderungen und Installation .....	213

- 7.4 Sicherheitsaspekte und Authentifizierung ..... 217
- 7.5 Kernfunktionen der Sybase Unwired Platform ..... 226
  - 7.5.1 Mit Datenquellen verbinden ..... 226
  - 7.5.2 Mobile Anwendungen erstellen ..... 227
  - 7.5.3 Mobile Anwendungen konsumieren ..... 234
  - 7.5.4 Mobile Anwendungen und Geräte kontrollieren ..... 235
- 7.6 Zusammenfassung ..... 237

**8 SAP NetWeaver Gateway ..... 239**

- 8.1 Funktionen von SAP NetWeaver Gateway ..... 239
- 8.2 Plattformübergreifende Integration mithilfe von OData ..... 246
  - 8.2.1 Open Data Protocol ..... 247
  - 8.2.2 REST-Architekturrichtlinien ..... 249
  - 8.2.3 OData mit SAP-Annotationen ..... 251
- 8.3 SAP NetWeaver Gateway-Architektur und -Komponenten ..... 254
- 8.4 Empfehlungen für den Aufbau einer Gateway-Systemlandschaft ..... 260
- 8.5 Gateway-Serviceentwicklung ..... 265
- 8.6 Zusammenfassung ..... 273

**9 SAP Afaria ..... 275**

- 9.1 Notwendigkeit eines Mobile Device Managements ..... 275
- 9.2 Mit SAP Afaria mobile Daten, Anwendungen und Geräte zentral verwalten ..... 279
  - 9.2.1 Bereitstellung und Inbetriebnahme ..... 281
  - 9.2.2 Produktive Nutzung ..... 282
  - 9.2.3 Außerbetriebnahme/Deaktivierung ..... 283
  - 9.2.4 Geräteverwaltung mithilfe von Richtlinien ..... 284
- 9.3 Was spricht für den Einsatz von SAP Afaria? ..... 288
  - 9.3.1 Anmeldung und Aktivierung von privaten mobilen Endgeräten ..... 288
  - 9.3.2 Anwendungsverwaltung ..... 289

9.3.3	Zentrale Administrationskonsole .....	290
9.3.4	Berichte und Statistiken .....	291
9.4	Architekturüberblick und Komponenten .....	292
9.5	Zusammenfassung .....	296
<b>10 Systemlandschaften im Überblick .....</b>		<b>299</b>
10.1	Historisch gewachsene SAP-Systemlandschaften .....	299
10.2	Wie machen es andere? Ein Beispiel für eine neue Systemlandschaft .....	307
10.3	Mobilisierung der Systemlandschaft .....	312
10.4	Zusammenfassung .....	316
<b>11 Eine neue App entsteht .....</b>		<b>317</b>
11.1	Konzepte mobiler Anwendungen .....	318
11.1.1	Die SUP-Verbindungsoptionen .....	325
11.1.2	Hybrider Web-Container .....	326
11.2	Sybase Mobile Software Development Kit .....	328
11.3	Prozess der mobilen Anwendungsentwicklung .....	333
11.3.1	MBO-Entwicklung .....	335
11.3.2	Entwicklungsprozess für Hybrid-Web- Container-Anwendungen auf MBO-Basis ...	338
11.3.3	Entwicklungsprozess für mobile Onlineanwendungen auf Basis von OData .....	340
11.3.4	Entwicklungsprozess für mobile Offlineanwendungen .....	344
11.4	Zusammenfassung .....	347
<b>12 Der SAP Store .....</b>		<b>349</b>
12.1	SAP-Zertifizierung für mobile Anwendungen .....	353
12.1.1	Zum Start: Informationen finden .....	353
12.1.2	SAP-Partner werden .....	355
12.1.3	SAP-konforme Anwendungen entwickeln ..	359
12.1.4	Vermarktung der mobilen Anwendung .....	362
12.1.5	Kosten für das Partnerprogramm .....	364
12.2	Zusammenfassung .....	364

**Teil III Eigene Mobile-Vorhaben umsetzen**

<b>13 Die richtigen Personen und das richtige Know-how für Ihr Projekt ..... 369</b>	
13.1	Benötigte Rollen und Fähigkeiten im Projekt ..... 370
13.1.1	Zuordnung der Rollen nach Projekttypen ..... 374
13.1.2	Projektleiter ..... 376
13.1.3	Prozessexperte ..... 377
13.1.4	UI-Experte ..... 378
13.1.5	Entwickler ..... 379
13.1.6	Administrator ..... 379
13.1.7	Architekt und Sicherheitsexperte ..... 380
13.2	Wissensaufbau und Qualifizierung ..... 380
13.3	Ein schneller Check: Wo stehen Sie mit Ihrem Mobile-Vorhaben? ..... 384
13.3.1	Grundvoraussetzungen ..... 384
13.3.2	Design der Benutzeroberfläche ..... 385
13.3.3	Administration ..... 386
13.3.4	Entwicklung ..... 387
13.4	Zusammenfassung ..... 387
<b>14 Bestandsaufnahme und Mobile-Reifegrad ..... 389</b>	
14.1	Vom produktiven Chaos zum geregelten Vorgehen ..... 390
14.2	Ansätze zur Informationserhebung in Ihrem Unternehmen ..... 393
14.2.1	Aufbau einer Mobile-Community ..... 395
14.2.2	Prototyp auf Basis der App SAP StreamWork ..... 397
14.2.3	Bestandsaufnahme erweitern ..... 400
14.3	Zwei Anwendungsbeispiele für die Umsetzung eines Mobile-Projekts ..... 400
14.4	Wie reif ist Ihr Unternehmen im Mobile-Bereich? – Reifegradmodell ..... 404
14.5	Zusammenfassung ..... 406

## 15 Eine Mobile-Strategie für Ihr Unternehmen ..... 407

- 15.1 Kernelemente und Umfang einer Mobile-Strategie ..... 408
  - 15.1.1 Geschäftsziele und -vorgaben ..... 410
  - 15.1.2 Portfolio mobiler Lösungen ..... 412
  - 15.1.3 Unterstützte Hardwareplattformen und Betriebssysteme ..... 415
  - 15.1.4 Mobile-Anwendungsplattform ..... 417
  - 15.1.5 Verwendung und Verwaltung mobiler Endgeräte sowie Sicherheitsaspekte ..... 418
- 15.2 Schritte für die Erarbeitung einer Mobile-Strategie ..... 418
- 15.3 Fallbeispiele für eine Mobile-Strategie ..... 426
  - 15.3.1 Mobile-Strategie einer Stadt: Beispielsburg ..... 426
  - 15.3.2 Mobile-Strategie eines Konsumgüterherstellers: Essglück ..... 427
- 15.4 Zusammenfassung ..... 428

## 16 Die richtigen mobilen Anwendungen für Ihr Projekt finden ..... 429

- 16.1 Die »Killer-App«: Mythos oder Realität? ..... 429
- 16.2 Auswahl und Umsetzungsweise der mobilen Anwendungen für das Projekt ..... 437
  - 16.2.1 Kaufen oder Selbermachen? ..... 437
  - 16.2.2 Fokussierung auf die strategisch wichtigen mobilen Anwendungen ..... 439
  - 16.2.3 Die Mischung macht's ..... 440
  - 16.2.4 Vorsicht vor einem überladenen Projekt ..... 441
- 16.3 Fallbeispiel: Apps für Beispielsburg und Essglück ..... 442
  - 16.3.1 App-Portfolio: Beispielsburg ..... 442
  - 16.3.2 App-Portfolio: Essglück ..... 444
- 16.4 Neue mobile Anwendungen und Prozesse modellieren ..... 446
- 16.5 App-Checkliste für eilige Leser ..... 448
- 16.6 Zusammenfassung ..... 449

**17 Ihre Mobile-Infrastruktur einrichten ..... 451**

- 17.1 Projektschritte zur Einrichtung der Infrastruktur ..... 451
  - 17.1.1 Installation von SAP NetWeaver Gateway ..... 453
  - 17.1.2 Installation von Sybase Unwired Platform und SAP Afaria ..... 456
- 17.2 Dimensionierung der Infrastruktur ..... 460
  - 17.2.1 Initiales Sizing für Onlineanwendungen auf OData-Basis ..... 463
  - 17.2.2 Initiales Sizing für HTML5-/JavaScript-basierte Hybrid-Container-Anwendungen ..... 465
  - 17.2.3 Installationsoptionen und Kostenabschätzung ..... 465
- 17.3 Zusammenfassung ..... 468

**18 Datenschutz und Sicherheit für Ihr Vorhaben ..... 469**

- 18.1 Sicherheitsrichtlinien in der Praxis ..... 470
  - 18.1.1 Balance zwischen Sicherheit und Akzeptanz ..... 470
  - 18.1.2 Geltungsbereich der Policies ..... 472
  - 18.1.3 Klassifizierung der Daten ..... 472
  - 18.1.4 Welche Geräte dürfen verwendet werden? ..... 475
  - 18.1.5 Was darf/muss mit den mobilen Endgeräten getan werden? ..... 476
  - 18.1.6 Was ist im Bereich BYOD erlaubt? ..... 477
  - 18.1.7 Beispiel-Policy eines Unternehmens für den Einsatz mobiler Geräte ..... 478
- 18.2 Technische Sicherheitsmaßnahmen ..... 481
  - 18.2.1 Unsichere Geräte erkennen ..... 482
  - 18.2.2 Sichere mobile Anwendungen ..... 485
  - 18.2.3 Sicheres Backup ..... 490
  - 18.2.4 Kosten ..... 492
- 18.3 Zusammenfassung ..... 494

<b>19</b>	<b>Projekt- und Risikomanagement .....</b>	<b>497</b>
19.1	Projektmanagement in Mobile-Projekten .....	497
19.1.1	Projektmanagementmodelle .....	499
19.1.2	Schnellstartlösungen für die rasche und risikoarme Implementierung .....	505
19.1.3	Projektmanagement für zwei Fallbeispiele .....	510
19.2	Risikomanagement in Mobile-Projekten .....	512
19.3	Zusammenfassung .....	514
<b>20</b>	<b>Erfahrungen und Lehren aus der Praxis .....</b>	<b>515</b>
20.1	Erfahrungen im Bereich der Geräte, der Infrastruktur und der Entwicklung .....	516
20.2	Erfahrungen im Bereich der Rahmbedingungen und organisatorischen Themen .....	521
20.3	Zusammenfassung .....	528
<b>21</b>	<b>Ausblick: Die mobile Zukunft der SAP .....</b>	<b>529</b>
21.1	Mobile-Plattformen .....	530
21.2	Mobile Anwendungen und Mobile-Services .....	534
21.3	Zusammenfassung .....	541
	Die Autoren .....	543
	Index .....	545

# 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 Adaptionrate 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.

**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?

Aufbau des  
Buches: Teil I

**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 Plattform, 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 gekennzeichnet:

- [+]** 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.

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.

Unrealistische  
Umsetzung

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.

Notwendiges  
Sicherheitskonzept

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

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.

Einordnung  
der Risiken

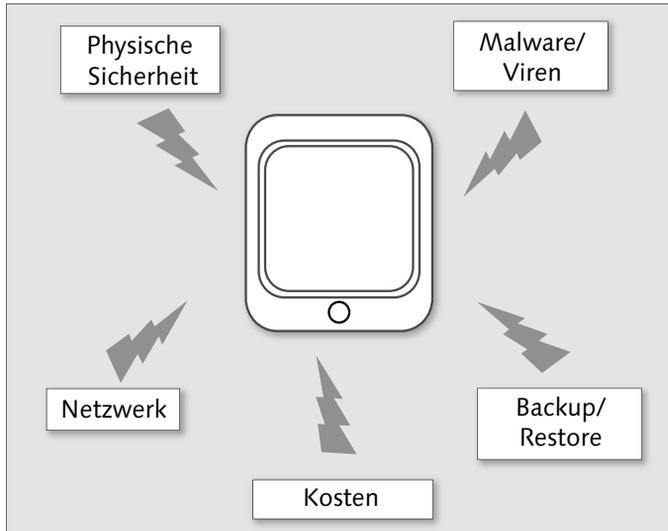


Abbildung 3.1 Risikobereiche für mobile Geräte in Unternehmen/Organisationen

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 berechnigte 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

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

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.

Hohe Speicherkapazität

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

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 gestohlenen 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

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 vermeintlich hilfreichen Programm verbergen.

Arten von Malware

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.

Sicherheits-  
konzepte 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 Betriebssystem

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).

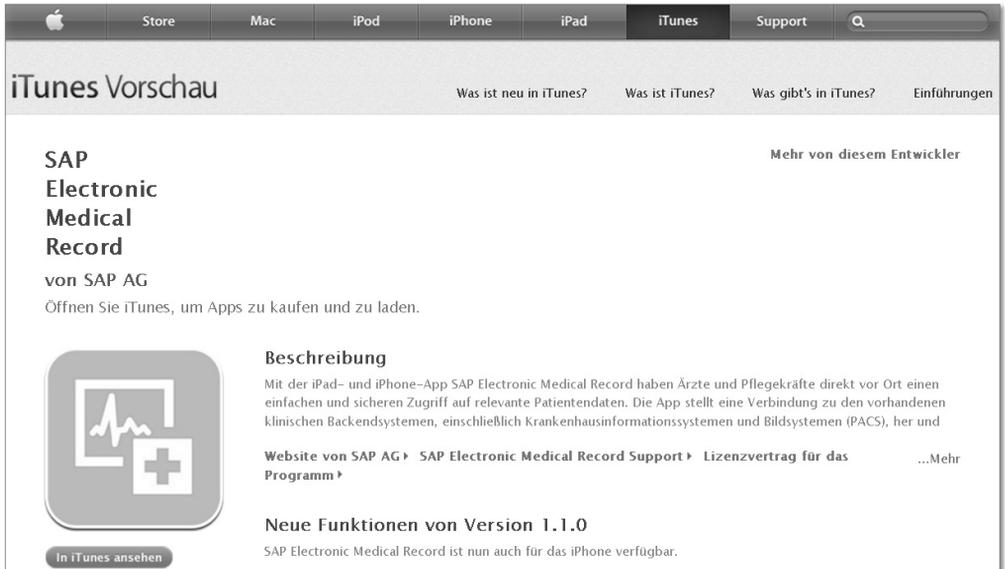


Abbildung 3.2 iTunes als Bezugsquelle für iOS-Apps

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.

Keine externen  
Schutzprogramme

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

Jailbreak

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.

Kosten-  
verursachende  
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

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.

Schutz durch Antivirenprogramme

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.

Rooting

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.

Verschlüsselung

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.windows-phone.com/de-DE/apps>, siehe Abbildung 3.4). Ähnlich wie Apple überprüft Microsoft alle Apps, bevor Sie auf dem Marketplace eingestellt werden.

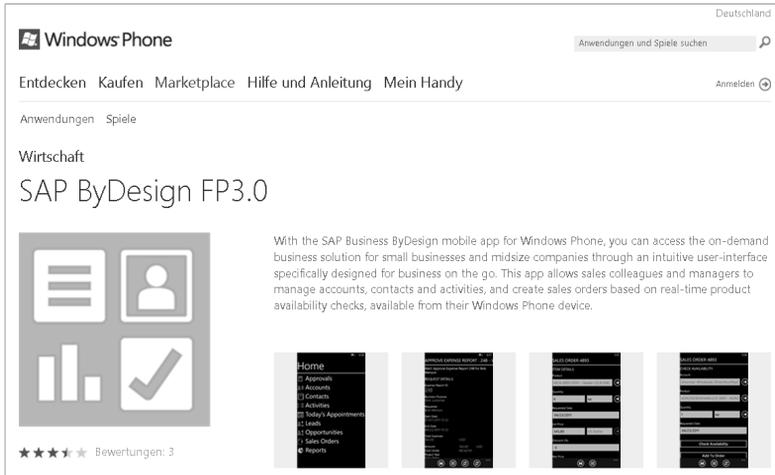


Abbildung 3.4 Windows Marketplace als Quelle für Windows Phone-Anwendungen

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

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).

Umfassende  
Sicherheits-  
funktionalitäten

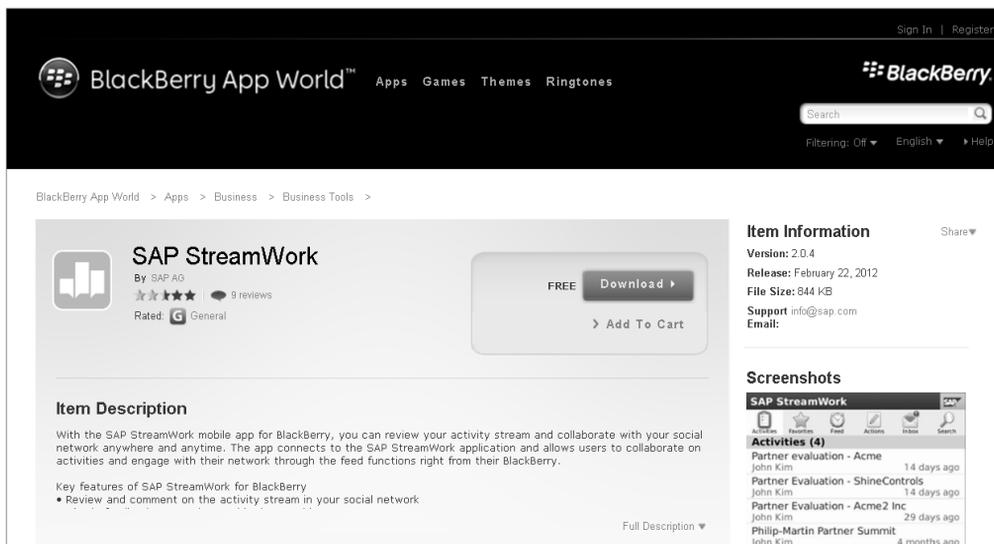


Abbildung 3.5 BlackBerry App World als Quelle für BlackBerry OS-basierte Anwendungen

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 berechnete Personen Zugang zu Ihrem Unternehmensnetzwerk verschaffen würden.

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 zuzuordnen zu können. In Kapitel 18, »Datenschutz und Sicherheit für Ihr Vorhaben«, werden wir darstellen, welche Möglichkeiten Sie in diesem Zusammenhang haben.

Identifikation  
mobiler Endgeräte

### 3.2.4 Backup/Restore

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

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.

Datensicherung

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

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.

Rechtliche  
Voraussetzungen

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.

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

Fragen für eine  
Sicherheits-  
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?

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.

Bewusstsein  
in den Mitarbeiter-  
vertretungen

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

Themen der  
Mitarbeiter-  
vertretungen

- ▶ 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.

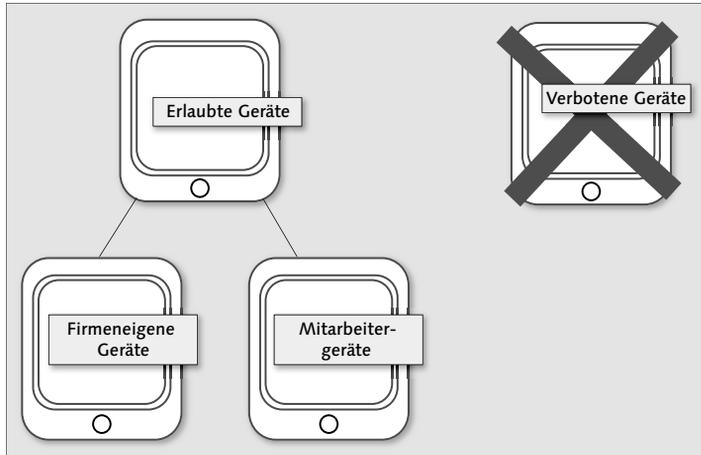


Abbildung 3.6 Klassifizierung von mobilen Geräten in einem Unternehmen mit BYOD-Regelung

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.

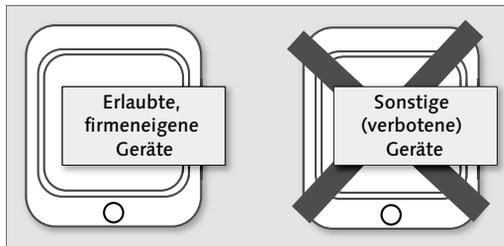


Abbildung 3.7 Klassifizierung von mobilen Geräten in einem Unternehmen ohne BYOD-Regelung

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.

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:

Erlaubte und nicht erlaubte Geräte

- ▶ 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.

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

Kriterien zur Beurteilung

- ▶ 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.

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

Verschlüsselung

Versionen hin. Hier ist immer ein gewisser »Zoo« (siehe Kapitel 2, »Der Technologiezoo und die IT-Abteilung«) verschiedener Android-Versionenstände 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.

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.

Rechtliche  
Notwendigkeit  
von Richtlinien

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:

Festlegung der  
Richtlinieninhalte

- ▶ 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.

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

Koordination der  
Verantwortlichen

- ▶ 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.

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

Grundsätze für die mobile Sicherheit

- ▶ 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

---

ABAP 212, 229, 253, 301  
ABAP Dictionary 252  
ABAP Workbench 257  
ABAP-Klasse 253, 266  
ActiveSync 308  
Add-on 239, 257  
Administrationskonsole 135, 282,  
287, 295  
Administrator 71, 210, 219, 372, 374,  
379  
Adobe PhoneGap 142, 348, 532  
Afaría Enterprise Application Store  
289  
Afaría → SAP Afaría  
Afaría-Client 293  
Afaría-Datenbank 294  
Afaría-Self-Service-Portal 289  
Afaría-Server 294  
Agentry → Syclo Agentry  
Air-Print-Schnittstelle 489  
Akkulaufzeit 308  
Android 39, 88, 482  
Anlagevermögen, mobiles 277  
Antivirenprogramm 87  
Antivirus-and-Firewall-Manager 133  
Anwendergruppe 472  
Anwendungsentwicklung → mobile  
Anwendung, Entwicklung  
Anwendungs-ID 235  
Anwendungsmanagement 200  
Anwendungsplattform 138  
Anwendungsregistrierung 235  
Anwendungsschnittstelle 335  
Anwendungssystem → mobile Anwen-  
dung  
Anwendungsverwaltung 289  
API 243, 266  
App Gallery 420  
App → mobile Anwendung  
App Store 39, 44, 281, 349  
Appcelerator Titanium 348, 532  
Apple iCloud 490  
Apple iOS 38, 295, 481  
Sicherheit 86  
Version 4.0 483

Version 4.2.1 483  
Version 5 86, 479  
Apple iPad 46, 86, 309, 435  
Apple iPhone 86, 352  
Apple iPod 48  
Apple iTunes 87, 353, 490  
Application Code 138  
Applikationsserver 69  
Arbeitspaket 453  
Arbeitsspeicher 47, 60, 454  
Architekt, für mobile Lösungen 372,  
380, 452  
ASP.NET 244  
Asset-Management-Komponente 71  
Atom Publishing Protocol (AtomPub)  
129, 242, 247  
Atom Syndication Format 129, 247  
Attribut 206  
Ausfallsicherung 215, 459  
Außendienst 64, 111, 308, 539  
Außerbetriebnahme 283  
Authentifizierung 218, 220, 231, 234,  
318

## B

---

Backend-Konnektor 445  
Backend-System 206, 211, 318, 334  
Backup 82, 93, 277, 490  
Backup- und Restore-Komponente 71  
Backup-Manager 133  
Bandbreite, Optimierung 71  
Bankensektor 195  
BAPI 254, 272  
BAPI-Wrapper 346  
Barcode-Scanner 44  
Basis-Authentifizierung 221, 235  
Benachrichtigung 464  
Benchmarking 462  
Benutzername 221  
Benutzeroberfläche 333, 385  
Benutzerschnittstelle 252  
Bereitstellungsphase 281  
Best Practice 453  
betriebliche Übung 101

- Betriebssystem 38, 67, 99, 214, 476, 517
  - Bibliothek 324
  - BlackBerry 34, 91, 110, 430, 492, 519
  - BlackBerry Enterprise Server 492
  - BlackBerry OS 41
  - Blog 146
  - BOR-Generator 272
  - Bring Your Own Device (BYOD) 63, 75, 79, 98, 276, 477
    - Richtlinie* 101, 105
    - Sicherheit* 100
  - Buchhaltung 160
  - Budget 523
  - Bundesamt für die Sicherheit in der Informationstechnik (BSI) 384, 474
  - Bundesdatenschutzgesetz (BDSG) 95
  - Business Case 524
  - Business Enablement and Provisioning 259
  - Business Intelligence (BI) 192, 291, 301
  - Business Object Repository (BOR) 256
  - BYOD → Bring Your Own Device (BYOD)
- C**
- 
- Cache 319
  - Cache-Datenbank 207, 231
  - Cache-Management 331
  - Caching-Algorithmus 58
  - Cascading Style Sheet (CSS) 141, 204
  - Central Hub Deployment 262, 455
  - Certificate Authority Server 294
  - Certification Authority 224
  - Charité 52, 61
  - Citizen Office 307
  - Citrix 67
  - Client-Server-Architektur 32, 300
  - Cloud 93, 124, 240, 308, 352, 490, 506, 530, 535
  - Cluster 215, 459
    - Architektur* 466
    - Datenbank* 207
    - Management* 236
  - Code-Generator 255
  - Communication Station 111
  - Community → Mobile-Community
  - Consumer App Store 349
  - Consumerization 63, 370, 433
  - Container-Anwendung 142
  - Content-Generator 245, 267, 271
  - Controller 45
  - Cookie 223
  - CPU 454
  - CRUD 335
  - Customer Relationship Management 110
  - Customizing 147
- D**
- 
- Data Change Notification 221
  - Data Orchestration Engine (DOE) 199, 311, 325, 332, 344
  - Data Tier 207, 209, 215, 220, 458
  - Data Vault 219
  - Data-Quellen-Provider 256
  - Datenanbindung 227
  - Datenbank 199
  - Datendiebstahl 277
  - Datenebene → Data Tier
  - Datenmissbrauch 237
  - Datenmodell 267, 332, 335
  - Datenquelle 206, 318, 337
  - Datenreplikation 323
  - Datenschutz 79, 94, 280, 469
  - Datenschutzbeauftragter 372
  - Datenschutzrecht 102, 472
  - Datensicherheit 202
  - Datensicherung 93
  - Datensynchronisierung 202, 308, 318, 319, 330
  - Deaktivierung 283
  - demilitarisierte Zone (DMZ) 133, 206, 264
  - Design 385, 446
  - Design tool 127
  - Desktop-PC 46
  - device-agnostic 415
  - Device-Management-Standard 132
  - Diagnose-Komponente 71
  - digitales Zertifikat 224, 235
  - Discman 47
  - Display 308
  - DOE → Data Orchestration Engine (DOE)

DOE-Konnektor 200, 325  
 Dokumentenmanager 133  
 Domain 235  
 Download 477  
 Drei-Knoten-Ansatz 215  
 Drucken 487  
 Dual-Use 494  
 Duet Enterprise 240  
 Dynpro 254  
 Dynpro-Screen 272

## E

---

Early Adopter 412  
 E-Book-Reader 47  
 Echtzeit 167  
 Eclipse 211, 232, 243, 329  
 Effizienz-Fan 392  
 Eigenentwicklung 402  
 Einkauf 177  
 E-Mail 430, 477  
   *dienstliche Nutzung* 476  
   *private Nutzung* 476  
   *Sicherheit* 34, 105  
 E-Mail-Konto 281  
 Embedded Deployment 262, 455  
 Employee Productivity App 147, 149,  
   166, 433, 440, 540  
 Emulator 339  
 Encryption Key 219  
 Endgeräte-Mobility 33  
 Enrollment 285, 481  
 Enrollment-Server 294  
 Enterprise App Store 349  
 Enterprise Information System (EIS)  
   199, 220, 362  
 Enterprise Mobility 67  
 Enterprise Service 131  
 Enthusiast 392  
 Entität 251  
 Entwickler für mobile Lösungen 374,  
   379  
 Entwicklerlizenz 356, 364  
 Entwicklungsplattform 73, 227, 321  
 Entwicklungsprozess 317, 333  
 Entwicklungsumgebung 117, 139,  
   211, 232, 243  
 Entwicklungswerkzeug 324  
 Erwartungsmanagement 520

## F

---

Facebook 75, 146  
 Failover 215, 459  
 Fall-zu-Fall-Integration 306  
 Feldbeschreibung 252  
 Festplattenkapazität 454  
 Field Service 110  
 Firewall 205, 282  
 Firmennetzwerk 63  
 Fortbildung 158  
 Fragebogen 393  
 Freitextsuche 252

## G

---

Gartner 122  
 Gartner-Quadrant 531  
 Gateway → SAP NetWeaver Gateway  
 Gateway-Content 259  
 Gateway-Design-time 256, 272  
 Gateway-Enablement 259  
 Gateway-Konsument 256  
 Gateway-Server 258  
 Gateway-Service 240, 257, 265  
 Gateway-Verbrauchsmodell 273  
 Generic Interaction Layer (GenIL)  
   244, 260  
 Geräte-Management 65, 131, 200,  
   209, 284, 308, 410  
 Geräte-ressource 65  
 Gesamtbetriebskosten 202, 237  
 Geschäftslogik 323, 333  
 Geschäftsprozess 203, 391  
 Geschäftsziel 439  
 Google 39, 88  
 Google Cloud Print 489  
 Google play 88  
 GPS-Funktion 44  
 Groupware  
   *Funktionalität* 47  
   *System* 41  
 Groupware-Anwendung 240  
 Gruppe 284  
 GW\_CORE 258, 262, 455

## H

---

Haftungsregelung 102  
 HANA Oncolyzer 58, 536  
 HANA-Appliance 537  
 Handheld 43  
 Hasso-Plattner-Institut für Software-  
 systemtechnik (HPI) 60  
 Hewlett-Packard webOS 42  
 Hosting-Service 135  
 HTML 112  
 HTML4 141  
 HTML5 52, 140, 204, 232, 243, 261,  
 324, 348  
 HTML5-/JavaScript-Schnittstelle 212  
 HTML-Adapter 210  
 HTTP 249  
 HTTP(S) 221, 245, 270  
 HTTP(S)-Request-Methode 247  
 Hybrid App Designer 212  
 hybride Anwendung 141, 212, 228,  
 232, 333  
 hybrider Web-Container 203, 212,  
 228, 236, 326, 333, 338  
 Hybrid-Web-Container-Anwendung  
 212, 228, 460

## I

---

iCloud 490  
 Identity Management 520  
 Implementierungsprozess 453  
 Industry App 147, 188  
 Informationserhebung 393  
 Infrastruktur  
   *Dimensionierung* 451  
   *Sizing* 460  
 Infrastrukturdienst 328  
 initiales Sizing 463  
 In-Memory-Plattform 535  
 In-Memory-Technologie 58  
 Innovation  
   *anwendergetriebene* 32  
   *IT-getriebene* 32  
 integrierte Entwicklungsumgebung  
 255  
 Interaktionsmuster 384  
 Internet 34  
 Internet Information Server 295

Internetbrowser 291  
 Intranet 472  
 Inventarisierung 70  
 Inventarmanager 134  
 iOS → Apple iOS  
 iPad → Apple iPad  
 iPhone → Apple iPhone  
 IT-Abteilung 63, 390  
 IT-Infrastruktur 69  
 IT-Leiter 371  
 IT-Projekt 498  
 IT-Sicherheitskonzept 105  
 IT-Skeptiker 392  
 iTunes → Apple iTunes  
 IT-Unternehmensrichtlinie 64, 72,  
 522  
 IW\_BEP 259, 262, 267, 322  
 IW\_CBS 259  
 IW\_CNT 259  
 IW\_FND 258, 262, 455  
 IW\_SCS 259, 264, 455

## J

---

J2EE-Engine 301  
 Jailbreak 66, 87, 292  
 Jailbreak-Erkennung 482  
 Java DataBase Connectivity (JDBC)  
 199, 248  
 Java VM 67  
 Java-Database-Connektor 325  
 JavaScript 141, 204, 232, 324  
 JavaScript Object Notation 221

## K

---

Kennwort 75, 281  
 Kick-off-Workshop 315  
 Killer-App 429, 540  
 Know-how 527  
 Know-how-Transfer 511  
 Komplettlösung 203  
 Konfiguration 210, 332  
 Konfigurationsmanagement 71  
 Konfigurationsmanager 133  
 Konnektivität 65, 69, 331  
 Kosten 82, 102  
   *BYOD* 492

*Kostenkontrolle* 292  
*Risiko* 93  
 Kundenauftrag 168, 173  
 Kundenmanagement 171  
 Kundenzufriedenheit 411

## L

---

Laptop 43, 46, 92, 308  
 Lastverteilung 215, 459  
 Laufzeitserver 206  
 Laufzeitumgebung 67, 117  
 Layer 140  
 LC-Display 47  
 Lebenszyklus 262  
 Lieferant 179  
 Live-Demonstration 505  
 Lizenz 300, 314, 467  
   *BYOD* 494  
   *Named-User-Lizenz* 467  
   *transaktionsbasierte* 467  
 Lizenzmanager 134  
 Load Balancing 215, 459  
 Logfile 209  
 Logfile-Analyse 236  
 Logistik 179  
 Log-Protokoll 362  
 lokaler Anwendungs-Content 259  
 Look and Feel 329  
 Look Book 475  
 Lösungsarchitekt → Architekt für  
   mobile Lösungen  
 Lösungspaket 509

## M

---

Mac OS X 39  
 magisches Dreieck 498  
 Mainframe 32, 300  
 Malware 82, 90  
 Manager Self Service (MSS) 536  
 Marketing-Fan 393  
 Masterplan 502  
 Materialmanagement 170  
 MBO → Mobile Business Object  
   (MBO)  
 MBO-Framework 127  
 Mehrbenutzersystem 33

Meldung 175  
 Messaging-Datenbank 208, 220  
 Metadata Provider Class (MPC) 268  
 Microsoft .NET 111, 243  
 Microsoft Failover Cluster 216  
 Microsoft Office 240, 494  
 Microsoft SharePoint 240  
 Microsoft Windows Phone 40, 90  
 Middleware 138, 205, 236  
 Mitarbeiterproduktivität 411  
 Mitarbeitersuche 149  
 Mitarbeitertraining 453  
 Mitarbeiterzufriedenheit 411  
 mobile Anwendung 33, 34, 67, 72,  
   87, 145, 234, 349, 373, 392, 402,  
   409, 429  
   *Auswahl* 429  
   *Bereitstellung* 235  
   *branchenspezifische* 440  
   *Checkliste* 448  
   *Design* 446  
   *Download* 349  
   *Entwicklung* 73, 126, 204, 229, 317,  
     375, 527, 533  
   *externe* 422  
   *interne* 424  
   *Kaufen oder Selbermachen* 437  
   *Klasse* 137  
   *Kosten* 88  
   *leichtgewichtige* 326  
   *modellieren* 446  
   *Portfolio* 408, 441, 448  
   *Provisionierung* 142  
   *prozessspezifische* 440  
   *Risikobereich* 81  
   *Sicherheit* 485  
   *Sizing* 461  
   *Spezifikation* 447  
   *Systemintegration* 527  
   *Update* 143  
   *Vermarktung* 364  
   *Zulassung* 102  
 mobile Application → mobile Anwen-  
   dung  
 Mobile Asset Management (MAM)  
   113  
 Mobile Asset Management for Utilities  
   (MAU) 113  
 Mobile Business Intelligence 430,  
   511, 536

- Mobile Business Object (MBO) 127, 142, 206, 210, 226, 321, 332, 339
  - Mobile Consumer Application Platform (MCAP) 122, 138, 532
  - Mobile Device Management (MDM) 70, 71, 99, 107, 122, 275, 279, 374, 386, 487, 502, 522, 531
  - Mobile Enterprise Application Platform (MEAP) 74, 122, 138, 307, 533
  - mobile Patientenakte → SAP EMR
    - Unwired
  - Mobile Web Dynpro Online 117
  - mobile Webseite → Webanwendung
  - Mobile-Betriebssystem 36, 203, 329
    - Marktanteil 36
    - Sicherheit 37
  - Mobile-Client-Schnittstelle 311
  - Mobile-Community 389, 393, 525
    - Moderator 394
    - Prototyp 398
  - Mobile-Entwicklungspfad 123
  - MobileGrafix 111
  - Mobile-Infrastruktur 203, 315, 451, 519
  - Mobile-Plattform 124, 279, 305, 410, 416, 530
  - Mobile-Projekt 79, 95, 305, 438, 497
    - Bestandsaufnahme 389
    - Budget 391
    - Dokumentation 391
    - Erfahrung 515
    - Know-how 369
    - Rolle 369
  - mobiler Workflow 430
  - mobiles Arbeiten 33
  - mobiles Bezahlen 110, 430, 530, 540
  - mobiles Endgerät 34, 42, 67, 234, 308
    - Administration 102
    - Ausstattung 83
    - Auswahl 516
    - Diebstahl 84
    - Hersteller 99
    - Integration 331
    - Klassifizierung 98
    - Konfiguration 277
    - Lebenszyklus 278, 408
    - Policy 476
    - Registrierung 209, 220
    - Sicherheit 69, 131
    - Speicherkapazität 83
    - Verlust 84
    - Wartung 68
    - Weitergabe 84
    - Zulassung 102
  - mobiles Szenario 305, 410
    - Bewertung 424
    - externes 424
    - internes 425
  - Mobile-Service 124
  - Mobile-Strategie 124, 299, 389, 407, 419, 451, 472, 501
  - Mobile-Systemlandschaft 207
  - Mobile-Workflow-Anwendung →
    - Hybrid-Web-Container-Anwendung
  - Mobilisierung 304, 451
  - Mobility 33, 63
    - Sicherheitsrisiko 79
  - Mobiltelefon 31, 45
  - Mock-up 452
  - Model-Repository 130
  - Modifikation 66
  - MP3-Player 47
  - Multifingergeste 39
  - Multikanalzugang 115
  - Multiprojektmanagement 502
  - Multitasking-Betriebssystem 42
  - Multitouchscreen 44, 46
  - mySAP Mobile Business 110
- 
- ## N
- 
- Nachrichtendienst 208
  - native Anwendung 139, 143, 203, 229, 324, 517
    - native Offlineanwendung 460
    - native Onlineanwendung 460
  - native Objektschnittstelle 212
  - .NET Compact Framework Runtime 67
  - Netzwerk 82
    - Sicherheit 92
  - Netzwerk-Port 209
  - Netzwerkverbindung 68, 319
  - Notebook 43, 46
  - Nutzeranforderung 435

## O

---

Objektschnittstelle 327  
 OData 51, 242, 243, 247, 371  
 OData Channel 213, 252, 257, 265, 268, 341, 465  
 OData mit SAP-Annotationen (OData4SAP) 251  
 OData Software Development Kit 128, 203, 208, 212  
 OData-Parser 331  
 OData-Protokoll 204, 210, 230, 265, 324, 330  
 OData-Schnittstelle 232  
 OData-SDK → OData Software Development Kit  
 OData-Service 322  
 offener Standard 533  
 öffentliche Verwaltung 190  
 Offlineanwendung 143, 230, 311, 318, 330, 344, 357  
 OMA Device-Management-Client 132  
 on demand 532, 541  
 on premise 308  
 Onboarding 209, 220, 234  
 On-demand-Lösung 352  
 OneTouch 134  
 Online Data Proxy 210, 213, 229, 323  
 Onlineanwendung 139, 143, 230, 311, 318, 340, 356  
 Onlinedatenzugriff 128  
 Open Data Protocol (OData) → OData  
 Open DataBase Connectivity (ODBC) 248  
 Open Handset Alliance 39  
 Open Mobile Alliance (OMA) 132  
 Open Web Application Security Project (OWASP) 485  
 OpenSearch 252  
 Operation 206  
 Ortsflexibilität 65  
 Over The Air (OTA) 131, 282, 311

## P

---

Package-Server 294  
 Paket 210  
 Paketlizenzmodell 467  
 Palmtop 43

Parser 332  
 Partner-App 50, 146, 195  
 Passwort 99, 221  
 Patch-Manager 134  
 Peer-Analyse 423  
 People Integration 115  
 Performance 464  
 Persistenz 331  
 Personal Computer (PC) 31  
 Personal Digital Assistant (PDA) 31, 44, 47, 109  
 Personal Information Manager 109  
 Personalanwendung 149  
 Personalisierung 370  
 Personalvertretung 79, 94, 392  
 PHP 243  
 Picture Archiving and Communications Systems (PACS) 57  
 Pilotimplementierung 504  
 Pilotprojekt 522  
 Plattformlösung, integrierte 200  
 Plug-in 127, 255  
 Pocket-PC 43, 47  
 Podcast 158  
 Policy → Sicherheitsrichtlinie  
 Port 282  
 Portable Media Player 47  
 Portal 301  
 Process App 147  
 Product Availability Matrix (PAM) 454  
 Produktionsphase 504  
 produktive Nutzung 282  
 Produktportfolio 312  
 Produktprofil 362  
 Profitabilität 411  
 Programmierschnittstelle 232, 335  
 Programmiersprache 334  
 Projektleiter 373  
 Projektmanagement 497  
 Projektmanagement, iteratives 501  
 Projektphase 499  
 Projektplan 526  
 Projektzeit 391  
 Provider 46  
 Proxy-Objekt 270  
 Proxy-Server 295  
 Prozessdesign 453  
 Prozessexperte 373, 377  
 Prozessintegration 301

Prozessor 454  
 Public Key 225  
 Public Key Infrastructure 226  
 Push 322  
 Push-Benachrichtigung 330  
 Push-Kanal 130, 202, 242

## Q

---

Qualifizierung 380  
 QWERTZ-Tastatur 41

## R

---

Radio Frequency Identification 111  
 Rapid Application Development (RAD) 127  
 Rapid Deployment Solution (RDS) 314, 453, 507, 523, 540  
 Realtime 49  
 Recalls Plus 537  
 Redundanz 215, 237  
 Reifegradmodell 404  
 Reisekostenabrechnung 160  
 Relay Server Outbound Enabler 216  
 Relay-Server 147, 206, 216, 322  
 Remote 289  
 Remote Function Call (RFC) 246, 254, 325  
 Remote Lock 283  
 Remote Wipe 283  
 Remote-Kontrolle 134  
 Remote-Zugriff 65, 75  
 Representational State Transfer (REST) → REST  
 Request for Quotation 180  
 REST 51, 130, 237, 242, 249, 320  
 RESTful 213, 248, 250  
 RESTful-Webservice 325  
 Restore 82, 93  
 Reverse Proxy 207, 322  
 RFC 272  
 RFC-Generator 272  
 Risikomanagement 497, 512  
 Roaming 292, 492  
 Rolle 218  
 Roll-out 281, 504  
 Rooting 66, 89

Root-Konto 66  
 Routenplaner 179  
 Ruggedized Device 392, 518  
 Rule of Three 122  
 Runtime Data Provider Class (DPC) 268  
 Runtime Wrapper 141

## S

---

SAINT 455  
 Samsung Galaxy S 519  
 SAP Access Approver 164  
 SAP Afaria 49, 88, 107, 121, 131, 199, 209, 216, 275, 308, 386, 418, 475, 483, 506, 507, 531  
*Afaria-Server* 458  
*Architektur* 293  
*Bericht* 291  
*Jailbreak-Erkennung* 482  
*Release 7.0* 135  
*Vorteil* 297  
 SAP AG 48  
 SAP Application Performance Standard (SAPS) 462, 466  
 SAP Best Practice 315  
 SAP Business ByDesign 302  
 SAP Business Suite 131, 254, 264, 302, 325  
 SAP BusinessObjects Explorer 119  
 SAP BusinessObjects-App 147, 192  
 SAP Cart Approval 177  
 SAP Citizen Connect 190, 442, 510  
 SAP Clinical Task Tracker 435  
 SAP Community Network 213, 358, 383, 387, 454  
 SAP CRM 309, 442  
 SAP CRM Mobile Service 112  
 SAP CRM Sales 182, 309, 442, 452, 511  
 SAP Customer and Contacts 171  
 SAP Customer Briefing 167  
 SAP Customer Financial Fact Sheet 172  
 SAP Customer Relationship Management (CRM) 167, 182  
 SAP Developer Center 357  
 SAP Developer Network 506  
 SAP EAM Work Order 187

- SAP ECC 6.0 301
- SAP EHS Safety Issue 175
- SAP Electronic Medical Record Unwired 190
- SAP Employee Lookup 145, 149
- SAP EMR Unwired 53, 433, 447, 473, 540
- SAP Enhancement Package (EHP) 301
- SAP ERP Order Status 174
- SAP ERP Quality Issue 178
- SAP Field Service 185
- SAP GRC Policy Survey 166
- SAP GUI 111
- SAP GUI für HTML (WebGUI) 112
- SAP HANA 60, 244, 438, 535
- SAP HANA Oncolyzer 58, 536
- SAP HCM Interview Assistant 155
- SAP HCM Manager Insight 156
- SAP HR Approvals 153
- SAP Idea Place 358
- SAP Incident Management System 175
- SAP Innovation Center Potsdam 61
- SAP Integration and Certification Center (SAP ICC) 355
- SAP Internet Transaction Server (SAP ITS) 112
- SAP Java Connector 199
- SAP Learning Assistant 158
- SAP Leave Request 151
- SAP Logon Ticket 223
- SAP Material Availability 170
- SAP Mobile Apps 195, 352, 468
  - Partner-Center* 353
  - Partnerprogramm* 358
- SAP Mobile Direct Store Delivery (MDS) 113
- SAP Mobile Engine 112
- SAP Mobile Infrastructure 112, 117, 303
- SAP Mobile Sales 110
- SAP Mobile Sales Online 119
- SAP Mobile Time and Travel (MTT) 113
- SAP Mobility Toolbox 143
- SAP NetWeaver 301
- SAP NetWeaver 2004 113
- SAP NetWeaver Application Server 112, 117, 301
- SAP NetWeaver Application Server ABAP 128, 239, 254
- SAP NetWeaver Business Process Management (BPM) 131
- SAP NetWeaver Business Warehouse (BW) 244
- SAP NetWeaver Business Warehouse Accelerator 119
- SAP NetWeaver Composition Environment 302
- SAP NetWeaver Developer Studio 117
- SAP NetWeaver Gateway 121, 128, 147, 199, 203, 210, 229, 239, 242, 306, 323, 340, 356
  - Architektur* 255
  - Bereitstellungsoptionen* 455
  - Entwicklungsprozess* 271
  - Kerntechnologie* 256
  - Systemvoraussetzung* 453
- SAP NetWeaver Mobile 112, 303, 311
- SAP NetWeaver Mobile Infrastructure 200
- SAP NetWeaver Portal 223
- SAP NetWeaver Process Integration (PI) 131
- SAP NetWeaver-Plattform 112, 113
- SAP Payment Approvals 163
- SAP Policyholder Lookup 188
- SAP R/3 110, 301
- SAP Real Spend 536
- SAP Retail Execution 184
- SAP Safety Issue 473
- SAP Sales Order Notification 168
- SAP Service Marketplace 456, 461
- SAP Standard Application Benchmark 462
- SAP Store 49, 137, 144, 147, 313, 349
  - Architektur* 351
  - für Smartphone* 146
  - Listung* 363
  - Ordermanagement* 145
  - Suche* 144
- SAP StreamWork 240, 397
- SAP Support Portal 454
- SAP Timesheet 152
- SAP Transport Notification and Status 179
- SAP Transport Tendering 180
- SAP Travel Expense Approval 161
- SAP Travel Receipt Capture 160
- SAP Web Application Server → SAP NetWeaver Application Server

- SAP-Add-on-Installationswerkzeug (SAINT) 455
- SAP-App 137, 397, 438
  - Download* 147
  - Installation* 147
  - Sicherheit* 438, 486
- SAP-App-Navigator 137, 440
- SAP-Backend-System 239, 262
- SAP-Beratung 314, 453
- SAPConsole 111, 303
- SAP-Mobile-Plattform 50, 58, 121, 142, 199, 279, 299, 307, 318, 348, 417, 451, 525, 529
- SAP-Partner 124, 137, 314, 352
- SAP-Partner-App → Partner-App
- SAPS → SAP Application Performance Standard (SAPS)
- SAP-Schulung 380
- SAP-Standard-App 523
- SAP-Strategie 534
- SAP-Systemlandschaft 299
- SAP-Zertifizierungsteam 361
- Schnellstartlösung 314, 460
- Schutzbedarfsklasse 474
- schwarze Liste 88
- Screen Scraping 272, 455
- Screenshot 90, 504
- Scrum-Methode 377
- SDMA-Modellierungstool 346
- Self-Service-Portal 295
- Sencha Touch 348
- Sensa Touch 532
- Sensor 44
- Serverparameter 209
- Service 33
- Service Builder 271
- Service Call 468
- Service Control Center 145
- Service Manager 539
- Service Provider Infrastructure (SPI) 244, 260
- Servicedokument 273
- Servicedokumenten-URL 235
- serviceorientierte Architektur (SOA) 300
- Session-Manager 134
- Sicherheit 469, 520
  - Datenklassifizierung* 472
  - organisatorische Vorkehrung* 104
  - physische* 82, 84
  - technische Maßnahme* 481
  - technische Vorkehrung* 106
- Sicherheitscheck 105
- Sicherheitsexperte 373, 380
- Sicherheitskonzept 81, 86
- Sicherheitsmanagement 72
- Sicherheitsmanager 134
- Sicherheitsrichtlinie 80, 95, 104, 281, 392, 470, 478
- Sicherheitsschlüssel 223
- SIM-Karte 46
- Single Host 461
- Single Sign-on (SSO) 222, 235, 288
- Siri 435
- Sizing 451
- Sizing-Übersicht 465
- Skalierbarkeit 203, 312, 323, 459
- Smartphone 31, 44, 308
- SMS 90
- SMS Integration Suite 134
- SOAP 130
- Software as a Service 124
- Software Development Kit (SDK) 126, 251, 324
- Softwarelebenszyklus 300
- Software-Management-Komponente 71
- Softwaremanager 134
- soziales Netzwerk 75, 240, 395
- Speicherkapazität 283
- Spracherkennungssystem 435
- Standard-App 374, 385, 438
- Steuerungs-SMS 132
- Subskription 210, 219
- SuccessFactors 490, 535
- Support 65, 290, 309, 356, 395, 518
- Supportability 328
- Sybase 121, 195, 200, 279
- Sybase 365 195, 532
- Sybase Control Center (SCC) 125, 209, 236, 337
- Sybase Data Tier → Data Tier
- Sybase Mobile Software Development Kit 205, 211, 231, 232, 318, 331, 457
- Sybase Product Download Center 213
- Sybase Relay Server 458
- Sybase Unwired Platform (SUP) 51, 121, 126, 147, 199, 240, 246, 261, 280, 310, 317, 357, 387, 456, 531

*Anwendungsentwicklung* 127, 228  
*Hardwareanforderung* 457  
*Installation* 213  
*Kernfunktion* 204  
*Release 2.0* 203  
*Release 2.1* 204, 229  
*Sicherheit* 217  
*Systemvoraussetzung* 214  
 Sybase Unwired Platform Runtime  
   205, 207, 457  
 Sybase Unwired Server 125, 206,  
   207, 211, 216, 337  
 Sybase Unwired Workspace 126,  
   211, 232, 335, 457  
 Sybase-Infocenter 456  
 Syclo 143, 531, 538  
 Syclo Agentry 531, 539  
 Symbian 41, 46  
 synchronisierte Anwendung 139  
 Synchronisierung 219  
   *meldungsbasierte* 231  
   *replikationsbasierte* 231  
 Systemadministration 436  
 Systemalias 256  
 Systemanbindung 206  
 Systemlandschaft 299, 459

## T

---

Tablet 31, 46, 308, 530  
 Telecom-Expense-Management-Funktionalität (TEM) 292, 493  
 Testlizenz 506  
 Testsystem 356, 523  
 Thing Type 251  
 Things 433  
 Token 223  
 Trainingsangebot 352  
 Transaktion  
   *SE80 (ABAP Workbench)* 270  
   *SEGW (Service Builder)* 271  
 Transaktionsservice 302  
 Transparenz 301  
 Trend 530  
 Trojaner 89  
 Twitter 75, 146

## U

---

Überwachungsdatenbank 209  
 UI-Experte 373, 378  
 UI-Komponente 332  
 Umsatzwachstum 411  
 UMTS 493  
 Unified Agent Service 210  
 Unternehmensdaten 66, 282, 309  
 Unternehmensrichtlinie 165, 470,  
   502  
 Unternehmensstrategie 408  
 Unternehmensziel 307  
 Unwired Server → Sybase Unwired  
   Server  
 Update 221  
 Upgrade 71  
 Urlaubsantrag 151, 433  
 USB-Anschluss 488  
 User  
   *automatische Erstellung* 221  
   *manuelle Erstellung* 221  
 User Interface 252, 328, 446

## V

---

Verbindungs-Provider 242  
 Verschlüsselung 76, 99, 282, 318  
 Versicherungsbranche 188  
 Verteilungsplattform 205  
 Vertrieb 167, 182  
 Verwaltung 235  
 Virenschutz 282  
 Virtual Private Network (VPN) 49, 92  
 virtueller Zugang 477  
 Virus 82  
 Visual Studio 232, 243, 329  
 Voice over IP 133  
 Vorstellungsgespräch 155  
 VPN-Tunnel 482

## W

---

Walkman 47  
 Wasserfallmodell 500  
 Web Dynpro 112, 117  
 Webanwendung 140, 348  
 WebSAPConsole 111  
 Webserver 69, 210

Webservice 129, 199, 213, 302, 311  
Webservice-Endpunkt 256  
Webstandard 128, 242  
Wireless LAN (WLAN) 44, 493  
Work Order Manager 539  
Workflow 339  
Workflow Forms Editor 212, 232  
Workflow-Anwendung → Hybrid-  
Web-Container-Anwendung  
Workshop 421  
World Wide Web Consortium 132

## X

---

X.509-Zertifikat 225  
Xcode 232, 243, 327  
Xing 75  
XML 270

## Y

---

YouTube 145, 146, 383

## Z

---

Zeiterfassung 152  
Zertifikat 219, 331  
Zertifizierungsprozess 353  
Zertifizierungstest 362  
Zielfestlegung 411  
Zugriffsberechtigung 164  
Zugriffskontrolle 218  
Zwei-Knoten-Ansatz 215