

Kapitel 2

Technische Aspekte

A. Besonderheiten von Apps gegenüber sonstiger Software

I. Entwicklung von Apps

Die Entwicklung einer App für Smartphones unterscheidet sich nicht grundsätzlich von der Erstellung von Software für andere Geräte wie einem Desktop-Computer. Es ergeben sich aber durch die Anforderungen der mobilen Plattform auch spezielle **Anforderungen** an die Entwicklung der Apps, die wir im Folgenden diskutieren. 1

II. Software Design für Apps

1. Besondere Anforderungen mobiler Softwareprojekte

Zentral für das **Software Design** einer App ist der Umstand, dass es für ein mobiles Gerät entwickelt wird. Hieraus ergeben sich einige zentrale Anforderungen, die sich von anderen Softwareprojekten unterscheiden: 2

- Bedienung durch Multi-Touch-Interfaces,
- begrenzter Platz des Displays,
- eventuell geringe Bandbreite der Internetverbindung,
- Richtlinien und Vorgaben des Plattformbetreibers.

Im Gegensatz zu einer Website sollte sich eine App auf die wichtigen Bestandteile eines Dienstes fokussieren und dabei dem Nutzer nicht nur Inhalte der Website anbieten, sondern ermöglichen, die **Kernfunktionen eines Dienstes** zu bedienen.¹ 3

PRAXISTIPP

Fokussieren Sie sich auf die wichtigsten Funktionen Ihres Dienstes und legen Sie bei der Umsetzung Wert auf eine einfache Bedienbarkeit.

¹ Diverse Fachliteratur zum Thema Interaktionsdesign für Mobile Applikationen ist in den letzten Jahren erschienen, u.a. *Hoover/Berkman* und *Clark*.

2. Besondere Möglichkeiten mobiler Plattformen

a) Sensoren

- 4 Plattformen wie Googles Android oder Apples iOS gestatten Apps Zugriff auf einige **Sensoren** der Geräte. So kann eine App den Standort des Benutzers abfragen, den das Gerät mithilfe eines GPS-Sensors ermittelt hat. Weitere gängige Sensoren sind:
- Helligkeitssensor zur Messung der Umgebungshelligkeit,
 - Bewegungssensor zur Bestimmung der Beschleunigung des Geräts,
 - Gyrosensor, der die Lage des Geräts wiedergibt,
 - Mikrofon,
 - Fotokamera.
- 5 Die Verarbeitung dieser Daten innerhalb einer App kann erstaunliche **Synergien** ermöglichen. Ein einfaches Beispiel ist die Anreicherung eines Fotos mit den Ortungsdaten eines GPS-Sensors.

b) Stetige Internetverbindung

- 6 Die Tatsache, dass ein Smartphone, zumindest in der Theorie, kontinuierlich mit dem **Internet** verbunden ist, eröffnet eine Reihe von Anwendungsfeldern.

c) Überall und zu jeder Zeit

- 7 Eine wesentliche Besonderheit mobiler Plattformen gegenüber herkömmlichen Computern liegt in der Tatsache begründet, dass ein Nutzer in vielen verschiedenen Situationen Zugriff auf das Gerät hat. Applikationen wie ein Fahrtenbuch oder eine Navigationsanwendung machen erst im richtigen Kontext Sinn.

d) Push-Nachrichten

- 8 Mittels **Push-Nachrichten** können kurze Meldungen an den Nutzer gesendet werden. Dies kann sowohl von einer App lokal ausgehen als auch von einem Server im Internet, deren Dienste eine Applikation verwendet. So kann eine App auch Nachrichten versenden, wenn sie selber nicht aktiv ist. Ein typisches Beispiel findet sich in Kalender-Apps: Eine Erinnerung an einen Termin wird auch angezeigt, wenn der Kalender gerade nicht benutzt wird.

3. Hardware-Vielfalt

Es gibt viele verschiedene Hersteller von Android-Smartphones. Um einen Unique Selling Point zu erzeugen, passen Hersteller das Android-Betriebssystem an. Zudem existiert eine große Anzahl von Geräten mit verschiedenem Funktionsspektrum (Bildschirmgröße, Leistung des Prozessors usw.). Dies kann, je nach Applikation, zu einem hohen **Anpassungs- und Testaufwand** führen. Es ist unmöglich, auf allen Geräten zu testen. Nicht nur die Anzahl der Varianten führt hier zu einem Problem, auch die geographische Verfügbarkeit. Einige Smartphones werden nur in einzelnen Ländern oder Regionen (Asien) vermarktet.

Apple bietet wenig Vielfalt in den einzelnen Produktlinien. Die verschiedenen Versionen des iPhones unterscheiden sich nicht grundsätzlich. Ebenso sind die Unterschiede der Softwareversionen gering. Googles Android-Betriebssystem hingegen wird von unterschiedlichen Hardwareherstellern eingesetzt. Dies hat zu einer Vielfalt an verschiedener Hardware gesorgt. Das Betriebssystem unterscheidet sich zwischen einzelnen Versionen teilweise erheblich.

III. Der App Store: Beispiel Apple

1. Entwickler-Account

Um eine App in den Marktplatz platzieren zu können, benötigt der Entwickler einen Zugang, den sog. Entwickler-Account, für den eine **jährliche Gebühr** gezahlt werden muss. Apple bietet zurzeit vier verschiedene Zugangsarten an:²

- iOS Developer Program Individual – Kosten: 99 US-\$. Einzelpersonen können Apps über den App Store vertreiben.
- iOS Developer Program Company – Kosten: 99 US-\$. Firmen mit einem Entwicklerteam können Apps über den App Store vertreiben.
- iOS Developer Program Enterprise – Kosten: 299 US-\$. Firmen mit einem Entwicklerteam können Apps ausschließlich innerhalb der eigenen Firma veröffentlichen.
- iOS Developer University Program – kostenlos. Für den Einsatz in Forschung und Lehre.

² Apple Developer Programs, abrufbar unter: <https://developer.apple.com/programs>.

PRAXISTIPP

Beginnen Sie frühzeitig, den geeigneten **Account** für Ihren Anwendungsfall zu erstellen. Es kann in der Praxis einige Tage dauern, bis ein Account durch Apple freigeschaltet wird.

- 12 Neben der Berechtigung, Apps in Apples App Store zu platzieren, eröffnet ein Entwickler-Account Zugang zu einer Vielzahl an Hinweisen, Beispielen und der notwendigen Software, um Apps zu programmieren. Diese Entwickler-Software steht ausschließlich für die Apple-Plattform zur Verfügung. Ein MAC-Computer ist also Voraussetzung für die Entwicklung von Apps für iPhone, iPad oder iPod Touch. Für einige Länder müssen zusätzlich Unterlagen für die Steuerbehörde ausgefüllt werden.

PRAXISTIPP

Für die Programme „Company“ und „Enterprise“ ist eine sog. **D-U-N-S Nummer** zwingend erforderlich. Dabei handelt es sich um einen international anerkannten Zahlencode, der zur Identifizierung von Firmen verwendet wird. Eine D-U-N-S Nummer kann bei der Firma Dun & Bradstreet (D&B)³ kostenlos beantragt werden.

2. Review-Prozess

- 13 Bevor eine App im App Store veröffentlicht werden kann, muss sie einen Begutachtungsprozess, das sog. **Review**, durch Apple durchlaufen. Während dieses Prozesses wird geprüft, ob eine Applikation den Voraussetzungen zur Veröffentlichung im App Store entspricht. Eine abschließende Aufstellung der Kriterien gibt es nicht. Im Dokument „App Store Review Guidelines“⁴ werden einige Themen konkret angesprochen, doch Apple behält sich vor, Apps zurückzuweisen, die „*in Inhalt oder Funktion eine gewisse Grenze überschreiten*“. Letztlich kann keine belastbare Aussage getroffen werden, ob eine App für den App Store zugelassen wird.

■ **Prüfen** Sie Ihre App mithilfe der „App Store Review Guidelines“ und ergänzenden Anmerkungen.

³ Vgl. dazu http://www.dnbgermany.de/wp-content/uploads/2011/07/DnB_DUNSBrosch2010_screen3.pdf.

⁴ App Store Review Guidelines, abrufbar unter: <https://developer.apple.com/appstore/resources/approval/guidelines.html>.

- **Testen** Sie Ihre App auf den aktuellen Soft- und Hardware-Versionen.
- Stellen Sie sicher, dass alle notwendigen **Metadaten** wie Beschreibungstexte und Vorschaubilder eingetragen wurden. Apple bietet hierzu eine Checkliste an.

Eine praxistaugliche Vorgehensweise ist primär die Vermeidung der bekannten 14 Ursachen, die einer App den Zutritt zum App Store verwehren. Ein Konzept sollte bereits im Vorfeld hinsichtlich seiner Veröffentlichbarkeit geprüft werden.

Nach dem **erfolgreichen Review** wird die App automatisch im App Store veröffent- 15licht. Statusänderungen werden per E-Mail kommuniziert. Es kann einige Stunden dauern, bis die App für alle Nutzer sichtbar ist.

PRAXISTIPP

Wenn eine Applikation zum **Review** eingereicht wird, kann zwischen automatischer Veröffentlichung und einer Veröffentlichung durch den Entwickler gewählt werden. Somit können Sie eine vorzeitige Veröffentlichung vermeiden.

3. Testen von Apps

Wie in jedem Softwareprojekt ist das **Testen** der Software ein zentraler Be- 16standteil des Entwicklungsprozesses. Fehler in der Programmierung und Umsetzung von Anforderungen sollen möglichst früh erkannt und behoben werden. Je komplexer eine Software ist, desto aufwändiger kann es sein, alle Zustände einer Software zu erreichen, in die sie ein Endanwender versetzen kann. Besonders bei Apps mit einem aufwändigen Review-Prozess ist es sehr wichtig, Probleme frühzeitig schon während der Entwicklung zu beheben. Nachdem die App im App Store veröffentlicht ist, dauert es eine Woche, bis eine Korrektur, selbst für triviale kleine Fehler, beim Kunden ankommt.

PRAXISTIPP

Neben manuellen Tests durch einen Menschen sollten schon im Programmcode **automatisierte Tests** erstellt und einzelne Programmteile auf ihr korrektes Verhalten getestet werden.

Es gibt verschiedene Ansätze, einen möglichst umfassenden **Testprozess** zu im- 17plementieren. Wir verweisen auf weiterführende Literatur zum Thema.⁵ Das Thema Testen wurde über die letzten Jahre als äußerst wichtig erkannt und es

⁵ Dazu Beck.

existieren einige sehr gute Vorgehensmodelle. In der Praxis lässt sich jedoch beobachten, dass schon sehr einfache Maßnahmen sehr viel bewirken.

PRAXISTIPP

Es ist besser, einen sehr einfachen Prozess heute in der Praxis einzusetzen, als erst morgen einen Besseren.

- 18 Neben diesen sog. **Komponententests** (engl. unit test) gibt es noch weitere Tests, die auf anderen Ebenen stattfinden. Es wird im Wesentlichen zwischen den folgenden Testarten unterschieden:

a) Komponententests

- 19 Komponententests finden auf **Programmcodesebene** statt und werden durch den Entwickler selbst erstellt. Sie sollten möglichst bei jeder Änderung im Programmcode durchlaufen werden.

b) Integrationstest

- 20 Integrationstests sollen die **fehlerfreie Zusammenarbeit einzelner Softwarekomponenten** sicherstellen. Ebenso wie Komponententests finden Integrationstests auf der Ebene des Programmcodes statt.

c) Systemtest

- 21 Systemtests betrachten das **Programm als Gesamtsystem**. Es werden alle an das Programm gestellten Anforderungen betrachtet. Systemtests finden auf Benutzerebene statt.

d) Abnahmetest

- 22 Diese Testart dient der Abnahme des **fertigen Softwareprodukts** durch den Kunden. Auf einen ersten Blick könnte ein Prozess mit nur einem Abnahmetest als ausreichend erscheinen. Das Problem ist jedoch, dass der Abnahmetest viel zu spät erfolgt. Tests schon am Beginn eines Projekts können nur automatisierte Tests auf Ebene der Komponenten leisten. Zudem haben Tests in der Entwicklungsphase einen positiven Einfluss auf die Qualität des Programmcodes.⁶

⁶ Dazu Pryce/Freeman.

PRAXISTIPP

Fragen Sie Ihren Dienstleister, ob neben einem reinen Systemtest auch automatisierte Tests einzelner Komponenten implementiert werden.

4. Continuous Integration

Continuous Integration (CI) oder **Kontinuierliche Integration** bezeichnet die Idee, dass jede Änderung im Programmcode unmittelbar zu einer automatischen Erzeugung des Endprodukts führt. Bei Apps bedeutet dies, dass eine installierbare App zum Testen erzeugt wird, nachdem eine Änderung durchgeführt wurde. 23

Continuous Integration geht Hand-in-Hand mit **Software-Tests**. Zum einen dienen Komponententests zum automatisierten Überprüfen des Systems: Nur wenn die Komponententests erfolgreich sind, wird eine neue Version erzeugt. Diese dient dann als Basis für System- und später auch Abnahmetests. Continuous Integration stellt sicher, dass die App bei allen Testern und eventuell bei einem Auftraggeber immer in der aktuell letzten Version getestet werden kann. 24

PRAXISTIPP

Eine Investition in Continuous Integration sollte direkt am Beginn eines Projekts erfolgen.

5. Updates

Jede Änderung an einer App muss den Review-Prozess erneut durchlaufen. Es wird nicht zwischen einer neuen App und einem Update unterschieden. Dies betrifft sowohl Änderungen zur **Fehlerbehebung** als auch neue Funktionen. Dies führt dazu, dass auch zeitkritische Änderungen nicht unmittelbar möglich sind, auch wenn dies für die Nutzer mit erheblichen Problemen verbunden ist. Es besteht die Möglichkeit, einen Review-Prozess mit Priorität bei Apple zu erbitten; dieser wird aber in nur gravierenden Fällen ausnahmsweise gewährt. Gründe können sicherheitskritische Fehler sein.⁷ 25

PRAXISTIPP

Einer App kann der Zugang zum App Store verwehrt bleiben. Dies sollte allen Beteiligten bewusst und vertraglich geklärt sein. Planen Sie in Ihrem Projekt

⁷ Formular zum Antrag eines beschleunigten Review-Prozesses, abrufbar unter: <https://developer.apple.com/appstore/contact/appreviewteam/index.html>.

Zeit für ein zweites Review-Verfahren ein. Apple bietet die Möglichkeit, ein beschleunigtes Review zu erbitten.

6. Kundenfeedback

- 26 Der App Store bietet Kunden die Möglichkeit, eine App zu bewerten. Diese Bewertung setzt sich aus der Vergabe von einem bis fünf Sternen und einem optionalen Freitext zusammen. Diese **Bewertung** ist für jeden Kunden einsehbar. Leider können Sie als Anbieter nicht direkt auf eine Rezension antworten oder Rückfragen an den Verfasser stellen. Somit kann durch Missverständnisse oder Einzelfälle leicht ein verzerrtes Bild entstehen.

PRAXISTIPP

Bieten Sie dem Nutzer eine Möglichkeit **Feedback** direkt aus der App an Sie zu senden. Somit kann ein Dialog stattfinden und eine potenziell negative Bewertung in ein Lob für Ihren Support verwandelt werden. Stellen Sie die wichtigsten Fragen und Antworten in einem speziellen Bereich in Ihrer App zur Verfügung. Diese Inhalte sollten dynamisch nachgeladen werden, damit sie ohne ein Update erweitert werden können.

IV. Wirtschaftliche Aspekte

- 27 Das Konzept App hat Einfluss auf die **wirtschaftlichen Aspekte**. Traditionell wird Software zu relativ hohen Preisen pro Stück verkauft, auch weil sich Kleinstbeträge durch den Aufwand, der durch den Abrechnungsprozess entsteht, nicht rechnen.

1. Verkauf der App

- 28 Der günstigste mögliche Preis einer App bei Apple liegt bei unter 1 € (89 Cent). Vor allem für einfache Spiele und kleine Dienstprogramme kann ein solcher Preis nur bei sehr hohen Stückzahlen interessant sein, da die Abwicklung des Kaufs durch die Plattform übernommen wird. Der Entwickler bekommt 70 % des **Verkaufspreises** ausgezahlt. Bis Sommer 2012 zahlte Apple rund 2,5 Mrd. US-

\$ an App-Entwickler aus,⁸ inzwischen sollen die Auszahlungen auf 7 Mrd. US-\$ angestiegen sein.⁹

2. Werbefinanziert

Sowohl Apple und Google selbst als auch externe Dienstleister bieten Werkzeuge an, mit denen man Werbung in Apps anzeigen kann. Jede Anzeige bzw. jeder Klick auf die Werbung wird vergütet. Bei Apps mit sehr vielen täglichen Programmstarts kann **Werbung** eine interessante Alternative zum Verkauf darstellen. Wichtig ist aber, dass die App wirklich häufig eingesetzt wird, damit pro Nutzer auch genug Werbung angezeigt wird. Bei selten genutzten Apps, z.B. sehr speziellen Werkzeugen oder saisonalen Apps, kann die Nutzungshäufigkeit so gering sein, dass sich Werbung im Vergleich zu einem Verkauf nicht lohnt.

3. In-App-Käufe

In-App-Käufe erlauben es dem Entwickler, Inhalte oder zusätzliche Funktionen direkt in der App zu verkaufen. Somit kann die Einstiegsschwelle niedrig gehalten werden und eine Monetarisierung ist auch nach dem initialen Verkauf möglich. Apple bietet verschiedene Arten von In-App-Käufen an:

Consumables sind Verbrauchsgüter, die jedes Mal erworben werden müssen, wenn der Kunde sie benötigt. Beispielsweise fallen SMS-Guthaben oder zusätzliche Spielversuche unter diese Kategorie.

Non-Consumables sind Käufe, die einem Kunden nach dem einmaligen Erwerb auf allen Geräten unbegrenzt zur Verfügung stehen, beispielsweise eine Exportfunktion oder zusätzliche Level eines Spiels.

Subscriptions-Abonnements können kostenfrei, automatisch verlängerbar oder zeitlich begrenzt sein. Unter diese Kategorie fallen neben regelmäßig erscheinenden Ausgaben einer digitalen Zeitung auch Services wie der Zugang zu einem Online-Archiv.¹⁰

⁸ Apple Keynote 2012, abrufbar unter http://www.youtube.com/watch?v=TrXBcK21G_o.

⁹ Vgl. dazu <http://www.internetworld.de/Nachrichten/Mobile/Zahlen-Studien/App-Statistik-von-Apple-Milliarden-fuer-Entwickler-72702.html>.

¹⁰ In-App Purchase Guidelines, abrufbar unter: <https://developer.apple.com/appstore/in-app-purchase/In-App-Purchase-Guidelines.pdf>.

PRAXISTIPP

In-App-Käufe müssen ebenfalls ein Review-Verfahren durchlaufen. Prüfen Sie daher im Vorfeld, unter welche Kategorie Ihre Leistung fällt und ob Ihr Vorhaben den Richtlinien für In-App-Käufe entspricht.

4. Freemium-Modell

- 34 Das sog. **Freemium-Modell** stellt den Benutzern Grundfunktionalität kostenlos zur Verfügung. Premiumdienste, wie sie z.B. im Firmeneinsatz nötig sind, müssen dann zusätzlich bezahlt werden. Freemium kann eine kostenlose (oder günstige) Basisversion mit Werbung und In-App-Käufen verbinden.¹¹

B. Gefährdung der Datensicherheit/Malware durch Apps

I. Datensicherheit

- 35 Datensicherheit in Computersystemen ist ein komplexes und schnell wachsendes Thema. Im Folgenden kann nun ein Überblick über die wesentlichen Aspekte vermitteln.

1. Betriebssystemebene

- 36 Mobile Geräte entwickeln sich seit Jahren vermehrt zum **Universalwerkzeug**. Diese Entwicklung wird durch mehrere Faktoren begünstigt. Smartphones sind heute in vielerlei Hinsicht dem Desktop-Computer ähnlicher als den Telefonen früherer Generationen, die Hardware der einzelnen Geräte unterscheidet sich nicht mehr so stark. Infolge dessen gibt es eine Konzentration bei Smartphone-Betriebssystemen. Deutlich wird es daran, dass die Thematisierung von Smartphone-Betriebssystemen heute üblich ist, wie z.B. iOS von Apple oder Android von Google, während die Betriebssysteme bei älteren Telefonen in der Regel unbekannt blieben.
- 37 Eine Konzentration auf wenige Betriebssysteme/Plattformen ermöglicht es erst, dass Drittanbieter Software für Smartphones schreiben und die Geräte nicht mehr nur mit Software des Geräteherstellers daher kommen. Im Zuge der Ver-

¹¹ Dazu *Anderson*.

breitung der Plattformen rücken diese zunehmend in den Fokus der Hersteller von **Viren und Malware**.

2. Benutzerdaten

Abgesehen von den neuen Möglichkeiten bei der Software bestechen moderne Smartphones aber auch damit, dass viele neue Hardware-Technologien in die Geräte integriert werden. Eine Geräte-Erweiterung wie ein Gyrosensor, der ermitteln kann, in welcher Lage man ein Gerät hält, mag dabei unkritisch sein. Erweiterungen wie GPS hingegen ermitteln personenbezogene Daten, und Technologien wie Bluetooth und WLAN ermöglichen sogar den Kontakt mit dem Smartphone von außen.

Auf Smartphones werden **sicherheitsrelevante Daten gesammelt**, die durch immer vielfältigere Nutzung anfallen. Je mehr Software installiert oder Hardware integriert ist, desto größer die Gefahr eines Fehlers, der Unberechtigten Zugang zum Smartphone und somit Zugang zu den eigenen Daten verschafft.

PRAXISTIPP

Installieren Sie nur Software, die Sie unbedingt brauchen. Entfernen Sie ungenutzte Software.

Schalten Sie alle Kommunikationsteile am Gerät ab, wenn Sie diese nicht brauchen.

Mit fallenden Kosten für Datenverbindungen sind immer mehr mobile Geräte permanent mit dem Internet verbunden. Im Gegensatz zu Technologien wie **WLAN** oder **Bluetooth** spielt beim Internet die Distanz zum mobilen Gerät keine Rolle. Schadhafte Programme, die auf dem mobilen Gerät installiert sind, können vom anderen Ende des Globusses ausgenutzt werden, um Zugriff auf das Smartphone herzustellen.

3. Das Prinzip „sandbox“

Um dies zu verhindern, werden Apps in einer „**sandbox**“ installiert. Eine „sandbox“ ist eine geschlossene Umgebung, in der die App ausgeführt werden darf. Damit soll sichergestellt werden, dass kein Zugriff auf das Betriebssystem oder auf die Daten von anderen Apps möglich ist. Ist eine App fehlerhaft, so wird lediglich der Zugriff auf die „sandbox“ der schadhaften App ermöglicht, der Rest des Systems bleibt unversehrt.

- 42 In extremen Fällen ist die schadhafte Software des Betriebssystems des Smartphones selbst und aus der „sandbox“ kann ausgebrochen werden. Das bekannteste Beispiel hierfür ist der „**Jailbreak**“ unter Apples iOS. Hierbei wird durch die Überlistung der „sandbox“ Zugriff auf das Betriebssystem verschafft und Software installiert, die den Zugriff auf das System permanent ermöglicht. Sobald das Betriebssystem zugreifbar ist, gilt das auch für alle Daten der installierten Apps. Nur die Apps, die eigene Maßnahmen zur Sicherung ihrer Daten treffen, sind dann noch vor dem Zugriff sicher.

4. Daten sicher auf dem Gerät speichern

- 43 Apps sollten sensible Daten wie Passwörter nicht in den Einstellungen der App speichern, sondern die **Schlüsselverwaltung** des Betriebssystems verwenden. Diese können nur mit einem Masterpasswort gelesen werden, das nirgendwo gespeichert wird. Andersgeartete sensible Daten sollten verschlüsselt auf dem Smartphone gespeichert werden. Auch die Schlüssel für die Verschlüsselung können der Schlüsselverwaltung des Betriebssystems anvertraut werden.¹²

PRAXISTIPP

Um Daten zugreifbar zu machen, muss man nicht unbedingt eine App und das Betriebssystem des Smartphones aushebeln. Manchmal wird dieser Zustand herbeigeführt, ohne dass man es mitbekommt. Erstellt man ein Backup des Smartphones auf einem anderen Computer, dann sind die Backup-Kopien meist nicht verschlüsselt. Auf Daten, die eine App unverschlüsselt gespeichert hat, ist nun auf dem Computer, auf dem man das Backup gemacht hat, recht leicht zuzugreifen.

5. Daten sicher übertragen

- 44 Ein Teil der sensiblen Daten, die gespeichert werden, bestehen aus Zugangsdaten zu Online-Diensten oder aus persönlichen Daten. Diese werden bei Benutzung der Online-Dienste ins Internet übertragen. Dabei ist der Weg vom Smartphone zum Online-Dienst nicht als vertrauenswürdig anzusehen. Jeder, der Verfügung über einen der Knotenpunkte auf dem Weg hat, kann die vorbeikommenden Daten lesen. Um dies zu verhindern, sollten die Daten während der Übertragung **verschlüsselt** sein.

¹² Dwivedi/Clark/Thiel, S. 3.

PRAXISTIPP

Apps sollten beim Übertragen von sensiblen Daten ins Internet eine verschlüsselte Verbindung benutzen. Momentan sind das überwiegend **SSL-Verbindungen**. Prüfen Sie bei den Online-Diensten, die Sie benutzen, ob deren Schnittstellen eine gesicherte Übertragung anbieten.

6. Daten sicher in der Cloud speichern

Viele Daten werden nicht nur kurzfristig ins Netz übertragen, sondern in **Cloud-Diensten** wie Amazon S3¹³ oder Dropbox gespeichert. Hierbei sind die Daten während der Übertragung verschlüsselt, aber nicht unbedingt im benutzten Online-Service. Amazon S3 ist lediglich ein Speicher-Dienst, hier ist man selbst in der Pflicht, die eigenen Daten zu verschlüsseln. Bei Dropbox werden die Daten vom Online-Dienst **Dropbox** verschlüsselt, bevor sie dort gespeichert werden. Die Daten sind somit verschlüsselt, doch der Online-Dienst ist in der Lage, die Daten zu entschlüsseln. Im Falle von Dropbox hat die US-Regierung einen vergleichsweise einfachen Zugriff auf die dort gespeicherten Daten. Die Modalitäten richten sich hier nach dem Land, in dem der Online-Dienst beheimatet ist.

PRAXISTIPP

Hinterlegen Sie keine sensiblen Daten in Online-Services, solange nicht sichergestellt werden kann, dass die Daten ausreichend verschlüsselt sind. Es sollte geprüft werden, ob eine zusätzliche Absicherung möglich ist. Ein ideales Szenario zeichnet sich dadurch aus, dass die Daten **verschlüsselt** werden, bevor sie das Gerät verlassen.

7. Zugriff auf persönliche Daten

Bei **Social Media** ist es heute üblich, allerhand Daten abzufragen und ins Internet zu übertragen. Dies betrifft persönliche Daten des Benutzers, Adressbuch, Kalender, die aktuelle Position oder gar die eindeutige Identifizierungsnummer des benutzten Geräts. Es ist oftmals nicht nachvollziehbar, ob diese Daten für den Betrieb des Dienstes nötig sind und wie sie verwendet werden. Oft entsteht der Eindruck, die Daten werden lediglich gesammelt.

¹³ Amazon Simple Storage Service (Amazon S3), abrufbar im Internet unter <http://aws.amazon.com/de/s3/>.

PRAXISTIPP

Apps sollten nur diejenigen Daten übertragen, die für den Betrieb des Dienstes unerlässlich sind. Sie sollten dem Nutzer klare Hinweise geben, welche Daten übertragen und wie sie verwendet werden.

8. Authentizität von Daten

- 47 In manchen Anwendungsfällen ist der komplette Schutz der Daten, wie er bisher besprochen wurde, keine Option. In diesen Fällen soll der lesende Zugriff gewährt werden, die Daten sollen aber vor **Manipulation** geschützt sein. Je wichtiger die Daten, desto weniger kann man sich dann auf den Schreibschutz verlassen, den das Betriebssystem vorgibt. Der Schutz vor Manipulation lässt sich auf zwei Wegen herstellen:

a) Asymmetrisches Verschlüsselungsverfahren

- 48 Werden Daten durch ein asymmetrisches Verschlüsselungsverfahren¹⁴ verschlüsselt, so existieren zwei Schlüssel, einer zum Verschlüsseln und ein anderer zum Entschlüsseln. Ist man im Besitz des Schlüssels, der entschlüsseln kann (gern öffentlicher Schlüssel oder **Public Key** genannt), kann man Daten lesen, aber man ist nicht in der Lage, Daten zu verschlüsseln, die mit dem gleichen Schlüsselpaar wieder lesbar sind. Das Schreiben von Daten wird hiermit verhindert.

b) Signierte Daten

- 49 Im zweiten Fall werden die Inhalte nicht verschlüsselt, sondern signiert. Die **Signatur** zeigt an, von welcher Quelle die Daten stammen. Werden die Daten manipuliert, so verliert die Signatur ihre Gültigkeit und die Verbindung zwischen Inhalt und Quelle besteht nicht mehr. Auf diesem Weg wird das Schreiben nicht verhindert, aber es wird nachprüfbar, ob die Daten authentisch sind oder nicht.

PRAXISTIPP

Apps sollten Daten zum Schutz vor Manipulation verschlüsseln oder signieren.

¹⁴ Schmech, S. 159.

Beide Verfahren haben ihre Vor- und Nachteile. Je nach Anwendungsfall ist es 50
sogar üblich, beide Verfahren zu kombinieren. Die Daten werden dann ver-
schlüsselt und signiert.

9. Datenverlust und Verfügbarkeit

Daten sind für uns nur dann sinnvoll, wenn wir mit ihnen arbeiten können. Das 51
Thema der **Datensicherheit** umfasst ebenso die Verfügbarkeit von Daten.
Ständige Verfügbarkeit ist besonders in verteilten Systemen wie dem Internet
von großer Bedeutung.

Verfügbarkeit kann temporär eingeschränkt werden, wenn Systeme ausfallen, 52
auf denen benötigte Daten gespeichert sind. Im schlimmsten Fall – dem Verlust
der Daten – wird die Verfügbarkeit permanent eingeschränkt. In den meisten
Fällen kann Verfügbarkeit durch Redundanz kompensiert werden. Das betrifft
Systeme, die redundant ausgelegt sind, ebenso, wie Backups von Daten anzu-
legen.

PRAXISTIPP

Erstellen Sie Sicherheitskopien von ihren Daten. Legen Sie Systeme, die Daten
zur Verfügung stellen, redundant aus.

II. Sicherheit im Unternehmenseinsatz

Viele Daten in Unternehmen werden als besonders schützenswert betrachtet. 53
Die Veröffentlichung von **firmeninternen Daten** oder der Verlust kann einem
Unternehmen wirtschaftlichen Schaden zufügen. Der sensible Umgang mit
Daten ist sehr wichtig. Unternehmen betreiben mitunter großen Aufwand, ihre
Daten sicherzuhalten. Die Anwendung/Benutzung von mobilen Geräten öffnet
neue Probleme in diesem Bereich.

1. Einsatz privater Smartphones

Brauchte man für die berufliche Ausübung seines Berufs ein Mobiltelefon, so 54
war es vor wenigen Jahren noch üblich, dass man dafür ein zweites Telefon
bekam. Die Überlassung des Firmentelefons für private Zwecke und die Ent-
wicklung von **Dual-Sim-Karten** eröffneten die Möglichkeit, ein Gerät für beide
Zwecke zu benutzen.

- 55 Dem gesteigerten Komfort und der Flexibilität stehen Probleme bei der Datensicherheit gegenüber. Wird das Smartphone geschäftlich benutzt, so hat man z.B. Zugriff auf das firmeninterne Adressbuch. In der privaten Benutzung werden Apps verwendet, die Zugriff auf das Adressbuch anfordern. Über diesen Weg können firmeneigene Daten ins Internet gelangen.

PRAXISTIPP

Bevor man einer App den Zugriff auf Daten gewährt, sollte überprüft werden, ob nicht der Zugriff auf Daten erlaubt wird, die einem nicht gehören.

2. Anbindung externer Dienste

- 56 Jederzeit Zugriff auf seine Arbeitsergebnisse und benötigte Dokumente zu haben, ist besonders dort wichtig, wo es mehrere Orte gibt, an denen gearbeitet wird. Viele **Cloud-Dienste** wie Dropbox bieten den nötigen Komfort, jederzeit Zugriff zu haben. Wie weiter oben schon besprochen, ist es schwierig, die Sicherheit der Daten zu gewährleisten.

PRAXISTIPP

Vor Benutzung eines Online-Dienstes sollte beim Arbeitgeber vorher um Erlaubnis gefragt werden.

- 57 Viele Unternehmen untersagen die Ablage von firmeninternem Material in anderen Online-Services. Zugriff auf firmeninterne Daten wird hier per **VPN (Virtual Private Network)** realisiert. Mitarbeiter bekommen hierfür einen verschlüsselten Zugang zum firmeninternen Netz. Befindet sich auf dem Smartphone eine schadhafte App, so kann diese Zugriff auf firmeninterne Daten und Strukturen erlangen.

PRAXISTIPP

Beenden Sie die Verbindung in Firmennetze, wenn Sie ungesicherte Apps benutzen.

- 58 Stellen Sie selbst eine Software her, die im Unternehmen eingesetzt werden soll, ziehen Sie in Betracht, einen **externen Gutachter** zurate zu ziehen. Die Möglichkeiten reichen von der Beauftragung eines externen Entwicklers für ein Sicherheitsaudit bis hin zur Beauftragung von Spezial-Anbietern wie dem TÜV.