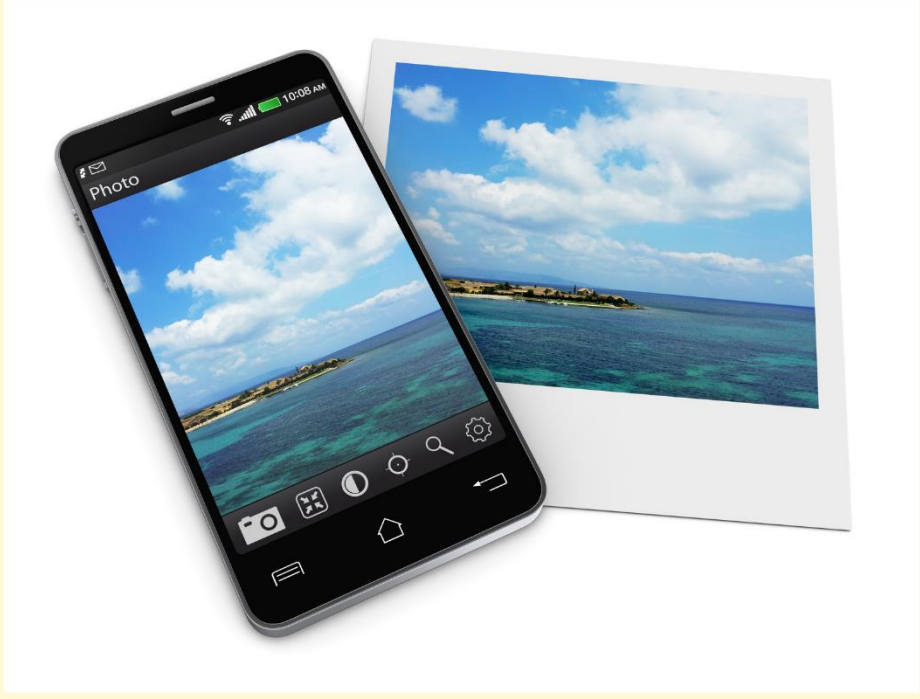
# Einfache Sicherheit für Smartphones und Tablets




Ronald Schlager

# 1. Vorwort

## 1.1. Über das Buch

Das Buch hilft Ihnen als privater oder firmenmäßiger Nutzer mobiler Geräte wie Smartphones oder Tablet Computers, Ihre Geräte und Daten sowohl physisch wie auch logisch zu schützen.

## 1.2. Wer sollte das Buch lesen?

Das Buch habe ich für Sie als privater oder firmenmäßiger Nutzer mobiler Geräte unabhängig von Ihren Vorkenntnissen geschrieben. Hier finden Sie wichtige Informationen, um Ihre Mobilgeräte, aber auch das Betriebssystem, Ihre Apps und Ihre Privat- bzw. Firmendaten, die Sie auf Ihren Geräten speichern, sowohl physisch als auch logisch zu schützen.

## 1.3. Hinweis auf das Copyright



## 1.4. Haftungsausschluss

Firmennamen, Handelsmarken oder Produktnamen sind meist geschützt. Die im (e)Buch enthaltenen Informationen wurden sorgfältig recherchiert. Sie stellen Informationen dar, die zur Entscheidungsfindung beitragen sollen. Aufgrund des Buchinhalts getroffene Entscheidungen und Maßnahmen fallen in den Verantwortungsbereich des Lesers. Obwohl ich das (e)Buch nach bestem Wissen und Gewissen geschrieben habe, kann ich Fehler nicht gänzlich ausschließen. Seitens des Autors wird jede Haftung abgelehnt.

## 1.5. Autor, Publisher

Ronald Schlager, schlager communications services GmbH
Web: https://www.schlager-cs.co.at/

## 1.6. Quelle des Fotos auf der Titelseite

© lucadp - Fotolia.com

# 2. Inhalt des (e)Buchs

1. Vorwort ..... 1
1.1. Über das Buch ..... 1
1.2. Wer sollte das Buch lesen? ..... 1
1.3. Hinweis auf das Copyright ..... 1
1.4. Haftungsausschluss ..... 1
1.5. Autor, Publisher ..... 1
1.6. Quelle des Fotos auf der Titelseite ..... 1
2. Inhalt des (e)Buchs ..... 2
3. Begriffsdefinitionen ..... 4
4. Mobiles Arbeiten und mobiles Leben ..... 10
4.1. Vorteile des mobilen Arbeitens ..... 10
4.2. Die Zukunft der Arbeit ..... 11
5. Risiken und Tücken unsicherer mobiler Geräte ..... 13
5.1. Physikalische Sicherheit ..... 13
5.2. Temperatur ..... 13
5.3. Batterien / Akkus ..... 13
5.4. Verlorengegangene oder gestohlene Geräte ..... 13
5.5. Nicht vertrauenswürdige mobile Geräte ..... 14
5.6. Nicht vertrauenswürdige Anwendungen ..... 14
5.7. Daten in mobilen Geräten ..... 15
5.8. Malware ..... 15
5.9. Nicht vertrauenswürdige Netzwerke ..... 16
5.10. Soziale Netze ..... 16
5.11. Nicht vertrauenswürdige Inhalte ..... 17
5.12. Ortsspezifische Dienste, Ortung ..... 17
6. Wer ist für mobile Sicherheit verantwortlich? ..... 18
6.1. Mobile Anwender wie Sie und ich ..... 18
6.2. Mobilfunk-Dienstanbieter ..... 18

6.3. Systemhersteller ....18
6.4. Firmen und Organisationen, Ausbildner, IT-Manager ....19
7. Wie Sie Ihr mobiles Gerät schützen ....20
7.1. Schutz vor physischer Beschädigung ....20
7.2. (Luft-)Feuchtigkeit ....20
7.3. Temperatur, Sonnenlicht ....20
7.4. Batterien, Akku ....21
7.5. Verlorengegangene oder gestohlene Geräte ....21
7.6. Vertrauenswürdige Geräte ....22
7.7. Gerätezugriff ....22
7.8. Vertrauenswürdige und unsichere Apps ....23
7.9. App Stores ....23
7.10. Software Updates ....24
7.11. Schadprogramme ....24
7.12. Vertrauenswürdige Netze ....24
7.13. Soziale Netze ....26
7.14. Teilen und Tauschen von Dateien ....26
7.15. Vertrauenswürdiger Inhalt ....26
7.16. Standort- und ortsspezifische Dienste ....27
7.17. Datenschutz ....27
7.18. Datensicherung und -wiederherstellung ....28
8. Zusammenfassung ....30
9. Anhang ....31
9.1. Über den Autor ....31
9.2. Weitere Bücher des Autors ....31
9.3. Seminare des Autors ....33
9.4. Profilbeschreibungen des Autors ....33

# 3. Begriffsdefinitionen

Ich setze voraus, dass Sie Anwender eines privaten oder von Ihrem Arbeitgeber bereitgestellten mobilen Gerätes sind und interessiert sind, Ihr Mobilgerät, die Anwendungsprogramme (Apps) und die mobilen Daten zu schützen und für einige Zeit zu nutzen.

Sie finden in diesem (e)Buch keine Anweisungen, wie Sie Ihr mobiles Gerät oder die darauf gespeicherten Daten beschädigen können oder wie Sie gefährliche Programme installieren, das Betriebssystem knacken, Passwörter stehlen oder irgend etwas anderes Verbotenes durchführen können.

Zuallererst möchte ich ein paar Begriffe erklären, die ich in diesem (e)Buch verwende.

**Android**
Ist ein freies und Open Source Betriebsssystem, ursprünglich von einer kleinen Firma entwickelt, die von Google im Jahr 2005 gekauft wurde. Ist ein Linux-Derivat, unterstützt von Google und anderen Herstellern, die die Open Handset Alliance bilden.

**Anwendungsprogramm, (“application program”)**
Ist ein Programm zur Datenverarbeitung (der Hauptanwendung eines Computers).

**Anwendungsprogramm-Schnittstelle**
Ist eine Schnittstelle zwischen einzelnen Programmen für die Zusammenarbeit dieser Programme.

**Apple iOS**
Ist ein geschlossenes, herstellerspezifisches Betriebssystem von Apple für Apple iPhone, iPod oder iPad (Umstellung ab Juni 2019 auf iPadOS).

**Betriebssystem**
Ist ein Programm, das die Computer-Hardware verwaltet und spezifische Dienste zur Nutzung der Hardware für andere Programme, die auf dem gleichen Computer laufen (z.B. Datenverarbeitsprogramme, Anwendungsprogramme), anbietet.

Ein Betriebssystem für mobile Geräte (mobile operating system) läuft auf einem Smartphone oder Tablet Computer und bietet Software-Funktionen und eine Programmumgebung für vorinstallierte oder vom Benutzer (oder dem Arbeitgeber) installierte Anwendungsprogramme („Apps"). Die Anwendungsprogramme unterstützen mobile Anwender bei ihren geschäftlichen oder privaten Aufgaben.

### Bluetooth™

Ist eine Funktechnik zum Informationsaustausch zwischen einem Computer und seinen Peripheriegeräten über kurze Distanzen (bis 100 Meter oder mehr).

### Bring Your Own Device (BYOD)

Ist eine Geschäfts- (und IT-) Politik, um Mitarbeitern die offizielle Nutzung Ihrer privaten mobile Geräte für Arbeitszwecke zu erlauben. Der Einsatz von Geschäftsanwendungen und –daten parallel zur Nutzung privater Apps und Daten ist ausdrücklich erlaubt, aber sehr umstritten.

### Computer

Ist ein programmierbares Gerät zur Lösung bestimmter Aufgaben. Es besteht aus Hardware (Gehäuse, elektronische Bauteile, Kabel, usw.) und Software (auch: Programm, Reihe von Arbeitsanweisungen, die der Computer ausführen soll).

### Computernetzwerk

Ist die Infrastruktur für Computer zum Informationsaustausch mit anderen Rechnern über verfügbare Pfade (über physische Verbindungen und möglicherweise unterschiedliche Netzwerkelemente).

### Informationstechnologie (IT)

Darunter versteht man die Nutzung von Computer- und Kommunikationstechnologie zur Suche, Ein- und Ausgabe, Speicherung oder Verarbeitung von Information. Der Austausch von Informationen zwischen Computer ist erforderlich, um komplexe Aufgaben zu lösen.

### Internet

Wie Sie wissen, ist das Internet das weltweit größte Computernetzwerk für den Informationsaustausch zwischen Benutzern. Das Internet nutzen private Anwender, aber auch

Firmenmitarbeiter für Geschäftszwecke, Menschen in Ausbildung, Mitarbeiter verschiedener Organisationen, Militärs und viele andere Anwender.

### Kommunikationssystem

Ist eine Gruppe von Funktionen und Diensten innerhalb eines Computers zum Informationsaustausch zwischen Computersystemen, um komplexe Datenverabeitungsaufgaben zu lösen.

### Mobile App

Kurzform für mobiles Anwendungsprogramm. Mobile Apps werden speziell für mobile Geräte wie Smartphones oder Tablet Computer programmiert.

### Mobiltelefon

Ist ein Gerät zum Telefonieren, das einfache Telefondienste und das Short Message Service (SMS) von öffentlichen Mobilfunknetzen bereitstellt.

### Protokoll

Ist die “Sprache” eines Programms in einem Computer zur Kommunikation mit anderen Programmen anderer Computer.

### Schnittstelle

Ist das Bindeglied zwischen einem Computer und anderen Elementen wie andere Computer oder Peripheriegeräte zur Datenein- und –ausgabe oder zum Datenaustausch.

### Smartphone

Ein Smartphone ist ein intelligenter Computer in einem speziellen, kleinen Gehäuse, meist mit einer relativ großen, hochauflösenden Farbbildschirm, der berührungsempfindlich (“Touchscreen”) ist und damit Programme bedienbar macht. Hauptanwendungen sind neben Telefonie der Internet-Zugang und die Nutzung darüber angebotener Dienste wie Chat, soziale Netzwerke (z.B. WhatsApp, Facebook, Instagram, Twitter) sowie der Zugang zu Firmennetzen.

In einem Smartphone sind viele technische Funktionen eingebaut wie z.B. Kamera(s), Navigation, Radio, Fernsehen, Multimedia-Abspielprogramme und verschiedene Sensoren für Umgebungslicht, Position, Beschleunigung, Magnetfeld, Lage und vieles andere.

Verschiedene Schnittstellen dienen zur kabelgebundenen oder drahtlosen Kommunikation mit anderen mobilen Geräten, Computer, verschiedene Peripheriegeräte, die über USB-Ports verfügen oder zur Internet-Anbindung (apropo: das ist unser größtes Sicherheitsproblem).

## System

In diesem (e)Buch ist ein System ein Computer zur Informationsverarbeitung inklusive Peripheriegeräte (wie Harddisk, Drucker, Monitor) und Benutzer.

## Tablet Computer

Ein Tablet Computer ist ein intelligenter mobiler Computer in einem speziell flachen Gehäuse unterschiedlicher Größe ähnlich wie ein Buch und einem hochauflösenden, meist berührungsempfindlichen Farb-Bildschirm (“Touchscreen”). Anwender nutzen den Tablet Computer sowohl beruflich zum Arbeiten als auch privat zur Unterhaltung. Beispiele für berufliche oder firmenmäßige Nutzung sind Verkaufsunterstützung, Unterstützung bei der Entscheidungsfindung und vieles anderes. Der Einsatz als Telefonapparat steht nicht im Vordergrund.

Viele der unterstützten Leistungsmerkmale und Funktionen sind denen von Smartphones sehr ähnlich.

## Universal Serial Bus (USB)

Ist ein Bussystem zur lokalen Vernetzung eines Computers über Kupferkabel oder Funk mit Peripheriegeräten wie Smartphones, Kameras, Harddisk-Laufwerke und viele andere Geräte.

## Verwaltungsaufgaben für mobile Anwender und Geräte

Hat eine Firma firmenspezifische Mobilgeräte oder private Geräte (Stichwort: Bring Your Own Device) in das Unternehmensnetzwerk einzubinden, muß sie sehr komplexe Verwaltungsaufgaben erfüllen. Ich möchte Ihnen hier einige Verwaltungsaufgaben vorstellen (die englischen Begriffe sind in Klammern angeführt):

### Verwaltung mobiler Geräte (Mobile Device Management)

Mobile Geräte müssen über ihren gesamten Lebenszyklus, von der Beschaffung und der Installation, dem Betrieb bis zur Außerbetriebnahme und eventuell sogar inklusive Recycling, verwaltet werden.

**Verwaltung mobiler Anwendungen**
**(Mobile Application Management)**
Die Verwaltung mobiler Anwendungen umfaßt Funktionen und Dienste zur vereinfachten Entwicklung, Verteilung und Anwendung mobiler Anwendungen (“Apps”) für Unternehmen.

**Verwaltung mobiler Daten (Mobile Data Management)**
Die Verwaltung mobiler Daten beinhaltet Funktionen für den Zugriff, das Laden, Speichern, Verarbeiten und Löschen von Daten in mobilen Geräten inklusive dem Schutz vor Verlust oder Missbrauch dieser Daten.

**Verwaltung der mobilen Sicherheit**
**(Mobile Security Management)**
Firmenanwendungen und -daten auf mobilen Geräten sind nach bestimmten Sicherheitsrichtlinien einzusetzen. Es sind Funktionen erforderlich, um die Daten zu sichern, vor unautorisierten Zugriffen zu schützen und das Kopieren oder Übertragen von Daten zu unsicheren Geräten oder Orten zu verhindern.

**Verwaltung der durch Mobilgeräte verursachten Kosten**
**(Mobile Expense Management)**
Verbindungsentgelte für Telefonate und Datenmengengebühren sinken dank moderner Serviceverträge oder den Einsatz von neuen Technologien wie Telefonieren über das Internet. Durch internationale Roaming-Abkommen und EU-weite Regelungen sanken die Kosten weiter.
Datennetzbetreiber erhöhen im nationalen Bereich ihre Bandbreiten (das sind die Bitübertragungsgeschwindigkeiten) ohne ihre Gebühren aufgrund großer Konkurrenz zu erhöhen. Die Nutzung öffentlicher Dienste hat sich stark gewandelt.
Internationale Verbindungen oder Dienste verursachen bei bestimmten Nutzungsformen hohe Roamingkosten.
Kostenkontrolle und die Blockade teurer Dienste ist eine Aufgabe, die einige Unternehmen besonders fordert. Der Einsatz dieser Programme hilft der Firma, die entstandenen Kosten zu kontrollieren und gegebenenfalls zu begrenzen.

## Wi-Fi oder Wireless Local Area Network (WLAN)

Wireless Fidelity oder Wireless Local Area Network ist eine spezifische Netzwerktechnologie zum drahtlosen Informationsaustausch (z.B. mit Funksignalen) über bis zu mehrere

hundert Meter (abhängig von vielen Faktoren). Die Technologie ist sowohl im In-house-Bereich als auch für den Outdoor-Internet-Zugang in Verwendung.

# 4. Mobiles Arbeiten und mobiles Leben

## 4.1. Vorteile des mobilen Arbeitens

Heute ist der Einsatz mobiler Geräte für private und berufliche Zwecke bereits alltäglich. Die Anforderungen an Geräte, Mitarbeiter und Unternehmen sind vielfältig, hier finden Sie ein paar Beispiele:

Firmen benötigen flexible Arbeitsflächen einerseits für Ihre internen Mitarbeiter, die in Ihren Büros arbeiten, andererseits für mobile Mitarbeiter, die Ihr Büro nur kurzzeitig nutzen.

Mobile Mitarbeiter wollen zu Hause oder während sie reisen arbeiten.

Es gibt viele Aufgaben, die Sie mobil erledigen können, z.B. Telefonate, E-Mails senden und empfangen, Systemverwaltung, Projektmanagement, Verkaufen und viele andere.

Das Institut der Deutschen Wirtschaft identifizierte die Auswirkungen von mobilem Arbeiten auf die Mitarbeiter.

Hier finden Sie weitere Details der Studie:
https://www.iwkoeln.de/fileadmin/publikationen/2017/356407/IW-Trends_3_2017_Mobiles_Arbeiten.pdf

Es gibt vieles, das Sie mobilisieren können:

**Clients:**
Die Mobilität der Geräte nimmt zu. Laptops, Notebooks und Personal Digital Assistants (PDAs) waren die ersten mobile Geräte, heute sind es Smartphones and Tablets.

**Anwendungen (Apps):**
Neue Anwendungen sind in Entwicklung oder bereits in Einsatz. Sie werden für die Betriebssystem-Plattformen Apple iOS oder Android entwickelt.

**Daten:**
Ihr Arbeitgeber bietet Ihnen Firmeninformationen in Form binärer Daten auf stationären zentralen Computersystemen zur Verarbeitung oder zum Download an.

Ihr mobiles Gerät greift auf die zentral gespeicherten Daten zu, ohne sie auf Ihr Mobilgerät zu laden. Soferne der Zugriff der externen Geräte auf die zentral gespeicherten Daten kontrolliert erfolgt, ist diese Lösung sehr sicher.

Lädt sich Ihr Mobilgerät die bereitgestellten Daten in den lokalen Speicher des Geräts zur Verarbeitung, kann die zentrale IT-Abteilung diese nicht mehr unmittelbar kontrollieren. Sie benötigt dann weitere Programme zur Verwaltung diese mobilen Daten (siehe Unterkapitel Verwaltung mobiler Daten, Mobile Data Management).

## 4.2. Die Zukunft der Arbeit

Beachten Sie einige wenige, aber sehr interessante Trends über die Zukunft der Arbeit:

- Mobiles Arbeiten wird normal (arbeiten Sie wo immer Sie sind, zu jeder Zeit, mit beliebigen Menschen, produktiver als im Büro).
- Wir müssen mit Kollegen, Kunden oder externen Partnern zusammenarbeiten, um unsere Arbeit zu verrichten. Antworten auf gestellte Fragen werden früher erwartet, da wir mit mobilen Geräten arbeiten.
- Smartphones sind die bevorzugten Kommunikationswerkzeuge.
- Mobile Werkzeuge reduzieren Betriebskosten.
- Anwender von Smartphones sind höher motiviert als Anwender von Desktop Personal Computer (sie verwenden ihre Geräte rund um die Uhr sowohl für ihre Arbeitgeber als auch privat)

Quelle (teilweise):
http://thefutureofwork.net/assets/Mobile_Workforce_Survey2012_Exec_Summary_Final.pdf

Vor einiger Zeit las ich ein sehr interessantes Buch über die Zukunft der Arbeit. Die Autorin ist Frau Lynda Gratton. Die deutsche Ausgabe trägt den Titel “Job Future – Future Jobs: Wie wir von der neuen Arbeitswelt profitieren”. Sie erklärt sehr anschaulich, wie Mobilisierung sowie neue Computer- und Kommunikationstechnologien unser aller Leben und Arbeiten beeinflussen kann. Der für mich wichtigste Aspekt dabei ist, dass wir selbst entscheiden, wie wir unser Leben und Arbeiten mit Hilfe der

neuen Technologien gestalten. Die Autorin bietet dazu viele praktische Beispiele.

Es gibt andere Bücher und Websites, die sich mit einer 4 Stunden Arbeitswoche (Stichworte: “four hour work week (4HWW)”) beschäftigen. Sie alle spielen mit unseren Träumen von Unabhängigkeit, Entscheidungsfreiheit und einem freien Leben irgendwo auf der Erde. Das sehr häufig diskutierte Buch stammt von Timothy Ferriss (siehe https://fourhourworkweek.com/). Die Bücher verfolgen alle ähnliche Ideen. Eine der wichtigsten ist die Steigerung der Mobilität durch Einsatz von mobilen Technologien und das zu Tun, was Sie tun wollen, an jedem beliebigen Ort der Welt.

Ich schließe daraus, dass wir leistungsfähige (mobile) Technologien besitzen, die uns erlauben, unsere eigene Zukunft zu gestalten. Es ist unsere Entscheidung, wie wir diese Technologien nutzen. Wir sind aber auch für die Sicherheit unserer mobilen Systeme, Anwendungen und Daten, die wir täglich nutzen, selbst verantwortlich und wir haben zu lernen, wie wir Risiken minimieren und Tücken vermeiden.

# 5. Risiken und Tücken unsicherer mobiler Geräte

Das folgende Kapitel beschreibt verschiedene Risiken, denen unsere mobilen Geräte ausgeliefert sind.

## 5.1. Physikalische Sicherheit

Versehentliche Flüssigkeitstropfen bei der Reinigung des Gehäuses mit einem feuchten Tuch oder ein vergossenes Getränk auf unserem mobilen Gerät kann passieren. Dringt die Feuchtigkeit in die Elektronik ein, gehen Bauteile kaputt. Das Smartphone-Gehäuse ist aus Glas, Polykarbonat oder Aluminium. Fällt das Smartphone auf eine harte Oberfläche, bricht das Gehäuse oder das Display. Beachten Sie, dass der Touchscreen sehr druckempfindlich ist und spitze Gegenstände die Oberfläche zerkratzen. Fingerabdrücke auf dem Touchscreen behindern die Lesbarbeit und greifen Oberflächen an.

## 5.2. Temperatur

Sehr hohe oder niedrige Temperaturen können das Gehäuse, den Bildschirm oder die Elektronik des mobilen Gerätes zerstören.

## 5.3. Batterien / Akkus

Entladen Sie Ihre Batterien / Akkus nicht vollständig. Volle Entladungen verkürzen die Lebensdauer Ihrer Akkus. Beachten Sie auch mechanische Verformungen oder sehr starke Hitzeentwicklungen.

## 5.4. Verlorengegangene oder gestohlene Geräte

Ihr Smartphone oder Tablet Computer speichert wichtige persönliche Informationen oder Firmendaten. Es zeichnet Ihre Aktivitäten auf, sammelt Daten Ihres Kommunikations- oder Konsumverhaltens und Bildschirmfotos der Seiten, die Sie besuchten, um nur einige wenige zu nennen.

Diebe sind vielleicht daran interessiert, wo Sie sich aufhalten und wie lange, welche E-Mails Sie erhalten haben, welche Bankkonten

Sie nutzen und vieles andere. Der einfachste Weg, um all diese Informationen zu erhalten ist es, Ihr Gerät zu stehlen, um physisch auf das Gerät zuzugreifen und diese Daten auszulesen.

Ein anderer Grund, warum Ihr Gerät gestohlen wird, ist viel einfacher. Für diese Diebe bringt Ihr Gerät unmittelbar ein Einkommen.

## 5.5. Nicht vertrauenswürdige mobile Geräte

Sie wollen unsichere Apps installieren oder die eingebauten Sicherheitsbeschränkungen Ihres mobilen Gerätes aus irgendwelchen Gründen umgehen? Es gibt illegal Softwarepakete und illegal Dienstleister zum Knacken Ihres Gerätes (“rooting” oder “jailbreaking”). Ist das Geräte einmal “offen” ist es potentiell unsicher und Schadprogramme lassen sich leicht installieren und ausführen. Diese Geräte sind dann aus Sicht Ihres Arbeitgebers nicht mehr vertrauenswürdig.

## 5.6. Nicht vertrauenswürdige Anwendungen

Viele Apps sind gratis. Seien Sie vorsichtig! Die Entwickler der Apps haben vielleicht spezielle Ziele, die sie mithilfe ihrer Apps erreichen wollen. Apps können versteckte Schadprogramme enthalten, um Ihre Bankkontodaten auszuspionieren und an verdächtige Personen weiterzuleiten. Die Software sammelt vielleicht Daten, die sie tatsächlich nicht benötigt.

Oder haben Sie eine Erklärung, wozu z.B. meine Taschenlampen-App Ortsinformationen meines Smartphones benötigt? Ich benötige diese Information während der Nutzung der App sicher nicht. Aber wer sonst ist an diesen Daten interessiert? Sie wären erstaunt, wüssten Sie, welche Daten Ihr mobiles Gerät sammelt und an jemanden für Sie völlig unbekannten sendet.

Entwickler mobile Apps besitzen unterschiedliche Kenntnisse und nutzen verschiedene Entwicklungswerkzeuge. Da kommen schon einige Programmfehler in den Apps vor. Die Apps kommunizieren mit anderem Apps am gleichen oder in fremden Systemen, oder beeinflussen die Arbeitsweise anderer Apps. Sie umgehen eventuell auch eingebaute Sicherheitsbeschränkungen.

Private Apps oder solche für den persönlichen Gebrauch (z.B. Multimedia Player, Spiele, soziale Netzwerke, etc.) unterbrechen unsere Arbeitszeit und führen zu geringerer Produktivität.

Sie haben Ihr mobiles Gerät mit vielen vorinstallierten Apps gekauft. Zusätzlich erhalten Sie weitere Apps zum Download von (hoffentlich) vertrauenswürdigen App Stores. Die Apps benötigen spezielle Berechtigungen, dass sie auf Ihrem mobilen Gerät laufen können. Erinnern Sie sich? Das System fragt Sie jedes Mal während des Installationsvorgangs bzw. bei Updates nach den notwendigen Rechten der App. Seien Sie ehrlich. Haben Sie schon jemals die gesamte Liste gelesen und der App trotzdem die Ausführungsrechte erteilt?

## 5.7. Daten in mobilen Geräten

Sie speichern sehr wahrscheinlich wissentlich oder unwissentlich viele persönliche Daten wie E-Mail-Adressen, Termine für Besprechungen, Geschäftsgeheimnisse, Bankkonto-Daten, persönliche Identitätsdaten, PIN-Codes oder Kreditkartendaten auf Ihrem mobilen Gerät. Ihr Gerät speichert Adressen besuchter Webseiten, Bildschirmdarstellungen, geladenen Fotos, eingegebene Codes usw.

Datendiebe versuchen mit diesen Daten in Ihrem Namen mit Ihrem hart verdienten Geld Waren zu kaufen, die Rechnungen der Diebe zu bezahlen, Ihr Geld auf fremde Konten zu transferieren, uvam. Die Diebe finden heraus, mit welchen Partnern Sie Geschäftsbeziehungen pflegen oder wer Ihre Freunde sind und kontaktieren diese, um weitere Informationen über Sie und Ihr Verhalten, Ihre Vorlieben, Ihre geplanten Treffen oder Urlaubsreisen (Ihr Zuhause ist zu dieser Zeit unbewohnt!) zu gewinnen.

## 5.8. Malware

Schadprogramme (=Malware) sind Programme wie Softwareviren, versteckte Spionageprogramme, Phishing-Software, Hintergrund-Programme zur Überwachung oder Aufzeichnung Ihrer Benutzerkennungen und Passwörter, Dialer-Programme zum Verbinden mit teuren Premiumtelefondiensten oder Software zum Senden teurer Premium-SMS.

Die Maßnahmen zum Schutz Ihres Gerätes, Ihrer Apps und Ihrer Daten vor Schadprogrammen für mobile Geräte sind die gleichen wie für Ihren Desktop-Computer oder Notebook.

## 5.9. Nicht vertrauenswürdige Netzwerke

Wireless Local Area Network- (WLAN- oder Wi-Fi-) Technologie nutzt Funksignale zum Informationsaustausch. Diese Signale breiten sich in bestimmte Richtungen oder in alle Richtungen aus (hängt vom Antennentyp und seinen Charakteristika ab). Die Funksignale werden von vielen Oberflächen und Gegenständen reflektiert und erreichen so Gebiete, in denen der Empfang nicht gewünscht ist.

Jedes Gerät, das diese Signale empfängt, könnte Ihre transferierten Informationen kopieren. Bei Wireless Local Area Networks nutzen Hacker möglicherweise spezielle Software zum Aufzeichnen Ihrer Daten und zur Analyse Ihrer Kommunikation (z.B. Ihre empfangenen oder gesendeten E-Mails, Ihre genutzten Passwörter für Ihr Bankkonto, etc.). Wie Sie sehen, ist das sehr unsicher und Sie sollten den Einsatz von Wireless Local Area Networks (WLAN) für den Zugriff auf Firmendaten von unterwegs unterlassen. Ist der Zugriff über WLAN unbedingt erforderlich, sprechen Sie mit Ihrem Systemadministrator über Ihre Sicherheitsbedenken. Das gleiche gilt für Zugriffe auf Ihr Bankkonto oder andere Dienste, die einen gewissen Grad an Vertraulichkeit und Geheimhaltung fordern.

## 5.10. Soziale Netze

Die Nutzung soziale Netze wie WhatsApp, Instagram, Facebook, Tumblr, Twitter, Xing oder LinkedIn wirft Fragen nach Ihrer Privatsphäre (Veröffentlichung zu vieler pivater Daten) auf. Soziale Netze sind auch sehr gute Datenquellen (Firmen verwenden Software zur Analyse veröffentlichter Informationen in sozialen Netzen für z.B. Marketingzwecke) oder können potentiell missbräuchlich genutzt werden (z.B. in dem sie im Namen bekannter Persönlichkeiten oder fiktiver Personen Nutzerprofile anlegen, um jemanden zu schädigen) und vieles anderes mehr. Die private Nutzung soziale Netze während Ihrer Arbeitszeit unterbricht außerdem Ihre produktive Phase.

## 5.11. Nicht vertrauenswürdige Inhalte

Manche Anbieter von Daten, Beschreibungen, Programmen, usw. versuchen offensichtlich oder versteckt, Sie mit Falschinformation in die Irre zu leiten, zu verunsichern oder an Ihr wohlverdientes Geld zu gelangen. Gerade auf scheinbar nützlichen Diskussionsforen, durch Newsletter, E-Mails usw. wird Ihnen Falschinformation als reale Tatsache angeboten.

Auch QR- (Quick Response-) Codes sind einfach zu nutzen. Eine App nimmt ein Foto des graphischen Codes auf und wandelt diesen in einen Link auf eine Webseite um, die Ihr Smartphone lädt. Ein manipulierter oder bewusst angebrachter QR-Code leitet Ihr mobiles Gerät auf eine gefährliche Webseite um, bietet Ihnen dort Falschinformation oder startet von dort aus seine Attacken gegen Ihr mobiles Gerät.

## 5.12. Ortsspezifische Dienste, Ortung

Ihr mobiles Gerät unterstützt sehr wahrscheinlich Navigationsdienste. Die Positionsdaten speichert Ihr mobiles Gerät und verschiedene Apps greifen auf diese Daten zu. Die Navigationssoftware greift auf die Positionsdaten zu und hilft Ihnen, Ihren Standort oder Ihren Weg zum Ziel zu finden.

Ihre Positionsdaten sind aber auch für Werbetreibende, Diebe, Sicherheitsorganisationen und viele andere für deren Zwecke interessant.

# 6. Wer ist für mobile Sicherheit verantwortlich?

## 6.1. Mobile Anwender wie Sie und ich

Wir sind für unsere eigenen privaten mobilen Geräte verantwortlich. Aber auch für Firmengeräte haben wir Verantwortung zu übernehmen. Wir nutzen diese Geräte, arbeiten mit Apps und Unternehmensdaten an unterschiedlichen Orten. Wir sind verpflichtet, auf die Geräte physisch und logisch zu achten und sie zu schützen.

Veröffentlicht Ihre IT-Abteilung Sicherheitsrichtlinien, so lesen Sie diese sorgfältig durch und beachten Sie die Hinweise. Wer diese Anweisungen und Regeln missachtet, riskiert rechtliche Konsequenzen.

## 6.2. Mobilfunk-Dienstanbieter

Viele Netzbetreiber bieten Sicherheitsdienste zum Schutz Ihrer mobilen Geräte. Diese beinhalten Massenmail-Filter, Virusüberprüfungen, Firewalldienste, E-Mail-Adress-Filter und vieles mehr. Nutzen Sie diese Dienste und schaffen Sie damit eine weitere Sicherheitsstufe.

## 6.3. Systemhersteller

Systemhersteller sind Entwickler, Hardware-Produzenten, Betriebssystem- und App-Entwickler oder App-Anbieter.

Kaufen Sie Ihr mobiles Gerät von vertrauenswürdigen Quellen. Installieren Sie Apps, um Ihr Gerät persönlich zu gestalten. Achten Sie aber auf vertrauenswürdige Entwickler und App-Anbieter (oder App Stores).

## 6.4. Firmen und Organisationen, Ausbildner, IT-Manager

Die Steigerung Ihres Sicherheitsbewusstseins ist mir ein großes Anliegen. Viele Sicherheitsverletzungen resultieren in Datenzerstörung, gestohlenen Daten, Kompromittierung der Identität von Personen oder vielen anderen Problemen.

Lernen Sie, wie Sie sich und Ihre Geräte schützen. Sprechen Sie mit Ihrem IT-Bauftragten über Ihre Sicherheitsbedenken. Besuchen Sie Seminare über Sicherheit bei Computer und mobilen Geräten. Lesen Sie Fachartikel oder recherchieren Sie im Internet nach den Themen, die Sie besonders interessieren.

Denken Sie daran: der schwächste Punkt in einer Kette von Sicherheitsmaßnahmen ist immer der Mensch.

# 7. Wie Sie Ihr mobiles Gerät schützen

## 7.1. Schutz vor physischer Beschädigung

Zu aller erst schützen Sie Ihr Smartphone durch eine Schutzhülle oder ein Schutzgehäuse. Achten Sie auch darauf, dass das Gerät nicht wegrutschen kann (dagegen helfen rutschfeste Auflagen). Abhängig von Ihrer generellen Gerätenutzung und den Umgebungsbedingungen gibt es viele verschiedene Spezialgehäuse oder Schutzhüllen. Ganz leichte oder dünne Schutzhüllen bieten einfachen mechanischen Schutz. Ein wasserdichtes, robustes Gehäuse schützt Ihr Gerät auch vor Feuchtigkeit. Manche Gehäuer erlauben die Nutzung selbst unter schwierigen Wetterbedingungen oder Unterwasser.

Ein Bildschirmschutz (z.B. eine duchsichtige Folie) schützt Ihre Anzeige vor Schmutz und Fingerabdrücken.

## 7.2. (Luft-)Feuchtigkeit

Normale Luftfeuchtigkeit ist für Ihr mobiles Gerät kein Problem. Wird Ihr Gerät aber richtig nass, schalten Sie das Gerät sofort aus und legen es in einen Behälter mit Reis oder grobkörniges Salz (eingeschlossen in einen leichten Stoffbeutel, um direkten Kontakt zu verhindern). Schließen Sie den Behälter und warten Sie ein paar Tage. Diese Materialien absorbieren Feuchtigkeit und trocknen damit Ihr Gerät. Danach schalten Sie Ihr Gerät wieder ein.

Reinigen Sie Ihr mobiles Gerät regelmäßig oder wann immer Sie Schmutz oder Fingerabdrücke (enthalten korrosive Säure) auf Ihrem Gerät erkennen. Nutzen Sie am besten Mikrofasertücher und kein oder nur sehr wenig Wasser auf dem Tuch. Nutzen Sie nie sonstige Flüssigkeiten. Das Gehäuse ist in der Regel nicht wasserbeständig oder widerstandsfähig gegenüber anderen Chemikalien (sie können Polykarbonat auflösen oder korrodieren).

## 7.3. Temperatur, Sonnenlicht

Halten Sie die Umgebungstemperatur des Gerätes niedrig. Halten Sie das Gerät im Schatten und nutzen Sie es nicht über längere

Zeit in der Sonne. Das führt zu Überhitzungen des Gerätes und die UV-Strahlung zerstört den Kunststoff.

## 7.4. Batterien, Akku

Behandeln Sie Ihre Batterien oder Akkus sorgfältig. Starten Sie den Ladevorgang, wenn noch 20 - 40% an Ladekapazität verfügbar sind. Stecken Sie das Ladegerät nicht zu früh ab. Überladen Sie Ihre Akku aber auch nicht. Lesen Sie die Bedienungsanleitung Ihres Produkt genau und befolgen Sie die vom Hersteller angeführten Punkte.

## 7.5. Verlorengegangene oder gestohlene Geräte

Lassen Sie Ihr Gerät nie unbeaufsichtigt liegen. Geht Ihr privates Gerät verloren oder es wird gestohlen, melden Sie es Ihrem Mobilfunkanbieter und sperren Sie Ihre SIM-Karte. Geht Ihr Firmengerät verloren, erkundigen Sie sich nach den Vorschriften ihres Arbeitgebers und Ihren Verpflichtungen bei Verlust oder Diebstahl.

Versuchen Sie, Ihr Gerät aus der Ferne zu sperren. Erkundigen Sie sich nach Diensten des Geräteherstellers zur Lokalisierung Ihres Gerätes, der Darstellung der aktuellen Position und des zurückgelegten Weges der letzten Stunden auf einer Landkarte. Möglicherweise bietet Ihr Dienstanbieter oder der Hersteller des Gerätes auch die Sperre des kompletten Gerätes oder die Löschung Ihrer Daten an.
Manche Dienste erlauben das Anrufen des gestohlenen Geräts, das dann mit der größtmöglichen Lautstärke läutet, und zwar unabhängig von der aktuellen Geräteeinstellung.

Verwaltet die IT-Abteilung Ihres Arbeitsgebers Ihr mobiles Gerät (mit Hilfe eines Mobile Device Management-Systems) erklären Sie diesen Mitarbeitern unmittelbar Ihre Situation (Verlust oder Diebstahl), damit sie die geeigneten Maßnahmen durchführen. Sind Sie selbst für Ihr Gerät verantwortlich, installieren Sie eine App, die Ihnen hilft, Ihre Daten von der Ferne zu löschen, gewissen Gerätefunktionen zu blockieren, Mails mit Positionsdaten an Sie zu senden und vieles mehr. Verwenden Sie Ihre bevorzugte Internet-Suchmaschine und geben Sie Schlüsselwörter wie “remote wipe”, “remote lock” oder “remotely remove app” ein und Sie erhalten eine

Liste von Links zu interessanten Quellen für mehr Information und geeignete Software.

## 7.6. Vertrauenswürdige Geräte

Beziehen Sie Ihr Mobilgerät (möglichst in Originalverpackung) von vertrauenswürdigen Quellen (z.B. direkte Vertriebspartner der Hersteller, Ihr Arbeitgeber oder Mobilfunk-Netzbetreiber).

Achten Sie darauf, dass Ihr Gerät nicht geknackt wird.

Sobald Ihr Gerät geknackt ist, gibt es keine Beschränkungen für spezielle Apps, die nun alles tun, wozu sie programmiert wurden. Sind Sie sich bewusst, dass Ihre Daten verloren gehen oder gestohlen werden können und es keinen Schutz oder Geheimhaltung mehr gibt. Verwenden Sie diese Geräte nicht für Dienste, die ein gewisses Maß an Sicherheit benötigen wie mobile Bankzugriffe, mobile Bezahlung, Shopping, Kreditkartenzahlungen und anderes. Greifen Sie nicht auf Ihre Firmendaten zu.

## 7.7. Gerätezugriff

Sperren Sie Ihr Gerät mit einem Sperrbildschirm, der Sie nach Eingabe eines PIN-Codes oder eines Passworts fragt, um Ihnen den Zugriff auf das Gerät zu erlauben. Andere Lösungen fordern Sie auf, mit den Fingern eine Figur nachzuziehen, den Fingerabdruck einzulesen oder Ihr Gesicht fotografieren zu lassen. Seien Sie kreativ bei der Festlegung Ihres PIN-Codes (“0000”, “1234” und Ihr Geburtsdatum oder das Ihrer Familienmitglieder sind leicht zu erraten).

Schützen Sie Ihre Hände bei der Eingabe Ihrer Codes vor neugierigen Blicken. Eine Smartphone-Kamera eines Beobachters kann Ihre Eingabe filmen. Selbst Kleinkinder schaffen es durch Beobachtung, Ihre Codes zu nutzen.

Software kann Mehrfachversuche bei PIN-Eingaben überwachen. Erreichen Sie eine definierten Anzahl von fehlerhaften Eingabeversuchen, löscht das Programm alle auf dem Gerät gespeicherten Daten und setzt das Gerät in den Auslieferzustand zurück. Nutzen Sie Ihre bevorzugte Internet-Suchmaschine und geben Sie Begriffe wie “mobile device management“ oder “PIN lock

wipe data" oder ähnliche Wortkombinationen ein, um relevante Suchergebnisse und damit mehr Informationen zu diesem Thema zu erhalten.

Gesichtserkennung ist zur Benutzeridentifikation wenig geeignet. Denken Sie nur an unterschiedliche Stile Ihres Aussehens wie einen Bart oder ein anderes Makeup. Andere Biometriedaten zu Ihrer Identifikation sind Ihre Sprache oder Ihr Fingerabdruck. Es hängt von Ihrem Gerät ab, welche biometrischen Daten erfassbar sind.

Alle oben genannten Benutzer-Identifikationsmethoden haben spezielle Schwachstellen. Es ist nicht mein Ziel, Sie hier in diesem (e)Buch über diese Details zu informieren.

## 7.8. Vertrauenswürdige und unsichere Apps

Installierte mobile Apps auf Ihrem Gerät machen aus Ihrem Mobilgerät ein einmaliges, individuelles System, das genau nach Ihren Wünschen und Bedürfnissen gestaltet ist. Laden und installieren sie Apps, denen Sie vertrauen oder die von sehr bekannten App Stores stammen. Seien Sie vorsichtig bei den Fragen nach den Rechten einer App während der Installation.

Ihre Firma kann "schwarze Listen" von Apps erstellen, die Sie nicht installieren sollten, aber auch "weiße Listen" von Apps, die Sie zu Arbeitszwecken installieren dürfen. Fragen Sie Ihren IT-Manager nach einem Enterprise App Store (ein Server, auf dem Ihr Arbeitgeber vertrauenswürdige Apps zum Download bereitgestellt).

Software kann helfen, unzuverlässige oder unsichere Apps zu erkennen. Suchen Sie mit Ihrer bevorzugten Suchmaschine nach Begriffen wie "security app", "mobile security software" oder "app permission". Sie erhalten eine Liste von Links zu zusätzlichen Quellen, die Ihnen helfen, die richtige Sicherheits-Software für Sie zu finden.

## 7.9. App Stores

Laden Sie nur zuverlässige Apps von sehr bekannten öffentlichen App Stores oder Ihrem Firmen- (Enterprise) App Store. Laden Sie keine Apps von App Stores, deren Namen Sie noch nie gehört

haben oder deren Betreiber Sie nicht kennen. Vertrauenswürdige Store-Betreiber überprüfen ihre Apps bevor sie diese zum Download anbieten. Sind Sie sich aber auch im Klaren, dass es Millionen von Apps gibt und Hacker auch vertrauenswürdige Apps modifizieren, um Ihr Gerät zu infizieren.

## 7.10. Software Updates

Hacker wissen, welches Betriebssystem mit welcher Versionsnummer oder welche häufig eingesetzten Apps welche Sicherheitsmängel und –schwachstellen haben. Sie sind sehr gut ausgebildet und attackieren sehr professionell. Die Anzahl an Attacken steigt dramatisch an. Aktualisieren Sie Ihre Software (die Geräte-Firmware, das mobile Betriebssystem und alle Ihre Apps) so bald und so häufig als irgendwie möglich!

Was können Sie tun, wenn Ihr Gerät für Updates zu alt ist? Nehmen Sie das Angebot Ihres Providers oder Ihres Arbeitgebers in Anspruch, um auf ein neues Gerät umzusteigen. Der erlittene Schaden durch Hackerangriffe oder Datendiebe ist bei weitem größer als die Kosten für ein neues Gerät.

## 7.11. Schadprogramme

Ihr Smartphone oder Tablet Computer arbeitet wie jeder anderer Computer und kann sich durch Schadprogramme infizieren.

Ich empfehle Ihnen als erste Tätigkeit nach der Erstinbetriebnahme Ihres neu erworbenen Gerätes, vertrauenswürdige Sicherheitssoftware zu installieren (diese sollte mindestens den Schutz vor Schadprogrammen und Viren unterstützen).

Alle großen, international tätigen Hersteller von Endgerätesicherheitslösungen für Desktop Computer oder Notebooks bieten passende Apps für Ihr spezielles Gerät an. Vergessen Sie nicht, Ihre Software und die Sicherheitsdatenbanken aktuell zu halten.

## 7.12. Vertrauenswürdige Netze

Sobald die Wireless Local Area Network-Schnittstelle Ihres Gerätes eingeschalten ist, sucht Ihr mobiles Gerät automatisch nach

WLANs und versucht sich zu verbinden. War das erfolgreich, startet es mit der Synchronisation Ihrer E-Mails, aktualisiert das Betriebssystem und Ihre installierten Apps, tauscht Standortinformationen mit wem auch immer aus und führt viele andere Tätigkeiten aus. Aktivieren Sie die WLAN-Schnittstelle nur dann, wenn Sie sicher sind, dass Sie diese auch tatsächlich benötigen. Schalten Sie die Schnittstelle in allen anderen Fällen einfach aus! Durch die Deaktivierung der Schnittstelle benötigt Ihr Gerät auch weniger Strom. Sperren Sie die automatische WLAN-Erkennung ("WLAN auto-detect"), das schützt Sie vor automatischer Einwahl in unsichere Wireless Local Area Networks.

Bluotooth™ nutzen Hacker für den Zugang zu Ihrem Gerät und Ihren Daten. Geben Sie Hackern dazu keine Gelegenheit. Starten Sie die Bluetooth™–Schnittstelle nur bei Bedarf.

Bereitgestellte Mobilfunk-Datendienste (wie Global System for Mobile communication, GSM, Universal Mobile Telecommunications System, UMTS, oder Long Term Evolution, LTE) von öffentlichen, vertrauenswürdigen Mobilfunk-Dienstanbietern sind sicherer als WLAN-Internetzugänge und Hackern fällt es viel schwerer, Ihre Daten dort mitzulesen.

Abhängig von Ihrem Dienstvertrag mit Ihrem Mobilfunkanbieter müssen Sie eventuell mehr bezahlen, wenn die transferierten Datenmengen einen gewissen Wert überschreiten. Um sicherzugehen, dass Sie keine unnötig hohen Kosten verursachen, sperren Sie die Nutzung des Datenübertagungsdienstes.

Fragen Sie Ihren Mobilfunkanbieter, welche Dienste für Sie verfügbar sind. Zusätzlich bieten viele Anbieter Sicherheitsdienste wie Virenchecks und Massenmail-Blockierung oder volle Firewalldienste für Ihren Internet-Zugang. Ich empfehle Ihnen, diese Dienste in Anspruch zu nehmen. Fragen Sie danach!

Wenn Sie nicht wissen, wie sicher Ihr Netzwerk tatsächlich ist, nutzen Sie sichere Virtual Private Network- (VPN-) Verbindungen. Diese Verbindungen laufen über Wireless Local Area Networks oder öffentliche Mobilfunknetze und das öffentliche Internet. Virtual Private Networks fordern üblicherweise bestimmte Formen der Benutzer- und meist auch Geräteidentifikation und sollten Ihre Daten im Hintergrund vor der Übertragung über das Internet verschlüsseln. Damit sind sie vor unerlaubten Lesezugriffen

geschützt. Fragen Sie Ihren IT-Manager oder Ihren Mobilfunkanbieter, welche Software mit welchen Einstellungen Sie benötigen.

## 7.13. Soziale Netze

Arbeitgeber wollen verhindern, dass Ihre Mitarbeiter während der Arbeitszeit soziale Netze wie WhatsApp, Instagram, Facebook, Tumblr, Twitter, Xing oder LinkedIn und andere für Privatzwecke nutzen.

Wird Ihr Mobilgerät durch eine Mobile Device Management Software Ihres Arbeitgebers verwaltet, wird diese versuchen, Ihren Zugriff auf soziale Netze zu blockieren.

Bitten Sie Ihren Arbeitgeber zusätzlich um Unterstützung und Ausbildung zum Erkennen von Sicherheitsgefahren und –bedenken sowie beim Umgang mit sozialen Netzen. Sie profitieren auch im privaten Umgang mit den sozialen Netzen von Ihrer erworbenen Kompetenz.

## 7.14. Teilen und Tauschen von Dateien

Nutzen Sie Tauschdienste für Dateien im beschränkten Maße und nur für Ihre privaten Dateien. Speichern Sie keine Firmendaten auf Cloud-Plattformen (außer auf den von Ihrem Arbeitgeber ausdrücklich erlaubten) und sozialen Netzen. Übertragen Sie dabei Ihre Daten nie über unsichere Netze wie Wireless Local Area Networks (WLAN). Für unternehmenswichtigen Dateiaustausch fragen Sie Ihren IT-Verantwortlichen, welche Plattformen und welche Apps vertrauenswürdig sind und von Ihrem Arbeitgeber ausdrücklich vorgeschrieben wurden.

## 7.15. Vertrauenswürdiger Inhalt

Laden Sie Daten, Beschreibungen, Fotos, Videos, usw. nur von vertrauenswürdigen Quellen. Nutzen Sie Foren, Newsletter, E-Mails usw. nur von bekannten Anbietern.

QR- (Quick Response-) Codes sind sehr einfach zu nutzen. Bevor Sie einen QR-Code einscannen, überprüfen Sie das Trägermaterial. Wie wurde der Code auf das Trägermaterial

aufgebracht? Sind mechanische Manipulationen erkennbar? Ist die Information rund um den QR-Code von vertrauenswürdigen Quellen? Wenn Sie sich nicht sicher sind, lesen Sie den Code nicht ein.

## 7.16. Standort- und ortsspezifische Dienste

Viele Apps geben Ihre Standortdaten an wen auch immer weiter. Wollen Sie verhindern, dass jeder weiß, wo Sie sich aufhalten? Dann sperren Sie die Standort-Funktion auf Ihrem Gerät. Damit haben auch Diebe keine Information, dass Sie außer Haus sind und genügend Zeit haben, Ihre Wohnung oder Ihr Haus leer zu räumen. Nebenbei sparen Sie auch noch Strom Ihres Akkus.

## 7.17. Datenschutz

Den besten Schutz Ihrer Daten erreichen Sie dadurch, dass Sie diese nicht auf Ihrem Mobilgerät speichern.

Den zweitbesten Schutz erreichen Sie durch Verschlüsselung. Verschlüsselung hilft Ihnen, entweder alle Datendateien im Gerät oder nur spezifische Dateien vor unerlaubtem Lesen zu schützen. Denken Sie auch an Ihre E-Mails und Chat-Verläufe. Viele Betriebsysteme haben diese Funktion bereits eingebaut. Abhängig vom Betriebssystem sind unterschiedliche Einstellungen vorzunehmen. Zur selektiven Verschlüsselung von Dateien und E-Mails benötigen Sie meist spezielle Software, die Sie von renomierten App Stores beziehen können.

Ihre Daten, die Ihr Gerät über Netze überträgt, schützen Sie ebenfalls am besten durch Verschlüsselung. Dazu benötigen Sie separate Programme, die Sie über Ihren Arbeitgeber erhalten oder von App Stores laden. Weitere Schutzmaßnahmen finden Sie im Kapitel “Vertrauenswürdige Netze”.

Bevor Sie Ihr Mobilgerät zur Reparatur einsenden oder außer Betrieb nehmen und entsorgen, löschen Sie alle Daten und entfernen Sie Ihre SIM- und SD-Karten. Das gleiche gilt auch für den Verkauf oder die Weitergabe an andere Nutzer.

## 7.18. Datensicherung und -wiederherstellung

Die einfachste Art, Daten (E-Mails, Kontakte, Textdateien, Präsentationen, Fotos, Videos, usw.) Ihres Mobilgerätes zu sichern, ist das Kopieren der Daten auf Ihre SD-Karte im Mobilgerät. Nehmen Sie die Karte heraus und stecken Sie diese in ein anderes Gerät. Dort importieren Sie die Daten der SD-Karte. SIM-Kartenleser erlauben die Sicherung der auf der SIM-Karte gespeicherten Daten.

Vielleicht verwenden Sie Cloud-Dienste für E-Mails, Kalenderdaten oder andere Informationen. Überprüfen Sie im Detail, welche Daten tatsächlich gesichert werden und wie lange diese gesicherten Daten in dieser Version für Sie verfügbar sind, bevor Sie in der Cloud gelöscht werden. Sichern Sie gegebenenfalls Ihre dort gespeicherte Daten auf lokalen Datenträgern!

Fragen Sie Ihren Arbeitgeber, welche Daten er sichert? Wie geht Ihr Arbeitgeber mit Firmendaten und Ihren privaten Fotos, Videos und anderen privaten Daten auf Ihrem Mobilgerät um?

Eine andere Sicherungsvariante Ihrer mobilen Daten ist die Verbindung Ihres Mobilgerätes mit einem Desktop-Computer oder Notebook über USB-Kabel (das Sie bereits in der Schachtel ihres Mobiltelefons erhalten haben oder das Sie speziell kaufen müssen). Alternativ übertragen Sie Ihre Daten drahtlos über Bluetooth™.

Beziehen Sie Datensicherungssoftware vom Hersteller Ihres Mobilgeräts oder einer anderen (vertrauenswürdigen) Quelle und installieren Sie diese auf Ihrem Computer. Dann transferieren Sie die Dateien direkt von Ihrem Mobilgerät zu Ihrem Desktop-Computer oder laden die gesicherten Daten von dort in Ihr Mobilgerät.

Fragen Sie Ihren Arbeitgeber, ob er Datensicherungsdienste in seiner zentralen IT-Abteilung anbietet oder einen speziellen Cloud-Dienst empfehlen kann, um Ihre mobilen Firmendaten sicher zu speichern.

Zur Sicherung Ihrer privaten Daten können Sie auch öffentliche Cloud-Dienste wie Amazon Drive, Dropbox, Google Drive, Microsoft OneDrive oder andere nutzen. Achten Sie darauf, Ihre Daten vor der Sicherung in der Cloud zu verschlüsseln.

Der Hersteller Ihres Mobilgerätes oder Ihr Mobilfunkanbieter kann ebenfalls Datensicherungsdienste anbieten.

# 8. Zusammenfassung

Jedes Mobilgerät und jeder Benutzer sind schützenswert. Es gibt unterschiedliche Sicherheitsmaßnahmen, wie Sie sich und Ihr Mobilgerät auf einfache Art schützen können:

- Schützen Sie Ihr Gerät vor physischer Beschädigung
- Verhindern Sie Verlust oder Diebstahl Ihrer Mobilgeräte
- Laden Sie den Akku rechtzeitig
- Achten Sie auf moderate Temperatur und wenig Sonnenlicht
- Vermeiden Sie hohe (Luft-)Feuchtigkeit oder Nässe
- Nutzen Sie nur vertrauenswürdige Geräte
- Schützen Sie sich vor Schadprogrammen
- Sperren Sie den Gerätezugriff
- Nutzen Sie nur vertrauenswürdige Netze
- Nutzen Sie nur vertrauenswürdige Apps
- Laden Sie Apps nur von vertrauenswürdigen App Stores
- Führen Sie regelmäßige Software Updates
- Nutzen Sie nur vertrauenswürdigen Inhalt
- Aktivieren Sie Ortung und nutzen Sie ortsspezifische Dienste nur bei Bedarf
- Schützen Sie Ihre Daten durch Verschlüsselung
- Schränken Sie das Teilen und Tauschen von Dateien ein
- Führen Sie Datensicherungen unbedingt durch
- Nutzen Sie soziale Netze nur privat

# 9. Anhang

## 9.1. Über den Autor

Ronald Schlager startete im Jahr 1980 seine berufliche Laufbahn im Markt für Kommunikationstechnologien.

Er verfügt über 10 Jahre Erfahrung in Entwurf und Entwicklung von Hard- und Software für Computerschnittstellen und Schnittstellen von Paketvermittlungssystemen für öffentliche Netzbetreiber.

Er ist Eigentümer des Trainings- und Consulting-Unternehmens schlager communications services GmbH (http://www.schlager-cs.co.at).

Seit 1988 bietet Herr Schlager Wissen über Kommunikationstechnologien, -protokolle und ihre Anwendung an und hilft damit seinen Partnern, erfolgreich in ihrem Beruf zu sein. Er organisiert vollständig neutrale und herstellerunabhängige Seminare und ist Trainer für Entscheidungsträger, Systemintegratoren und Spezialisten sowohl im Provider- und Enterprise-Bereich als auch bei Systemherstellern, -integratoren und Dienstanbietern.

Ronald Schlager ist unabhängiger Consultant und Planer von Kommunikationslösungen.

Er veröffentlicht technische Beschreibungen (z.B. Ratgeber für Entscheidungsträger und Endanwender) und Seminarunterlagen als Print on Demand-Bücher oder elektronische Bücher (eBooks).

## 9.2. Weitere Bücher des Autors

„Unified Communications – Buyer's Guide – Deutsche Ausgabe“
„Unified Communications – Buyer's Guide“ (Englisch)
„Auswahl von Enterprise-VoIP-Systemen“ (Deutsch)
“Einsparungspotentiale der IP-Telefonie“ (Deutsch)

„Corporate Telephony Strategies for Enterprise Customers and Organizations” (Englisch)

„Auswahl von Videokonferenzlösungen“ (Deutsch)
„Selecting Video Conferencing Solutions“ (Englisch)

“IPv4 and IPv6 Addresses – An Introduction“ (Englisch)
“IPv6-Adressen – Typen, Einsatz und Verwaltung“ (Deutsch)

“The OSI Model – simply explained” (Englisch)
“Das OSI-Modell – einfach erklärt” (Deutsch)

Folgende Seminarunterlagen sind verfügbar:

“Basics in Data Communications – Part 1/3: Tutorial“ (Englisch)
“Basics in Data Communications – Part 2/3: Tutorial“ (Englisch)
“Basics in Data Communications – Part 3/3: Tutorial“ (Englisch)

“From ISDN to SIP” (Englisch)

“Fundamentals of Local Area Networks – Part 1/2” (Englisch)
“Fundamentals of Local Area Networks – Part 2/2” (Englisch)

“IP-based Video Surveillance” (Englisch)

“Mobilfunk-Technologien – Teil 1 von 3” (Deutsch)
“Mobilfunk-Technologien – Teil 2 von 3” (Deutsch)
“Mobilfunk-Technologien – Teil 3 von 3” (Deutsch)

“Mobile Enterprise Management” (Deutsch)

“SIP – The Key to VoIP (Part 1 of 2)” (Englisch)
“SIP – The Key to VoIP (Part 1 of 2)” (Englisch)

“Voice over IP: Chances, Changes, Challenges” (Englisch)

“Voice over IP-Technologie – Teil I.1” (Deutsch)
“Voice over IP-Technologie – Teil I.2” (Deutsch)
“Voice over IP-Technologie – Teil II” (Deutsch)

“Wide Area Network Services” (Deutsch)

Weitere Informationen über Bücher in verschiedenen Formaten und weiteren Verlagen und Vertriebskanälen finden Sie hier:
https://www.schlager-cs.co.at/buecher/

## 9.3. Seminare des Autors

Seminare folgender Themengebiete sind verfügbar (mit Linkclick erhalten Sie die Seminarthemen im Detail):

Kommunikationstechnologien und -dienste
M2M, Industrie 4.0 und das Internet of Things (IoT)
Switching- und Routing-Technologien
Mobility
Security
‚Voice over IP', ‚Video over IP', ‚Unified Communications'
Protokolle

## 9.4. Profilbeschreibungen des Autors

Profilbeschreibungen von Ronald Schlager finden Sie auf folgenden Plattformen:

Ronald Schlager´s Bio
Amazon
LinkedIn
Smashwords
Twitter
Xing