IT-Sicherheit im Handwerk


# Mobiles Arbeiten

## & Bring Your Own Device (BYOD)

Dozentenhandbuch

Gefördert durch:
Bundesministerium für Wirtschaft und Energie
aufgrund eines Beschlusses des Deutschen Bundestages

TASK FORCE
IT-SICHERHEIT IN DER WIRTSCHAFT
Mehrwert und Schutz für Rechner.

Das diesem Buch zugrundeliegende Verbundvorhaben "IT-Sicherheitsbotschafter im Handwerk - qualifizierte, neutrale Botschafter für IT-Sicherheit im Handwerk finden, schulen und Awarenesskonzepte erproben (ISiK)" wurde mit Mitteln des Bundesministeriums für Wirtschaft und Energie (BMWi) im Rahmen der Task Force "IT-Sicherheit in der Wirtschaft" gefördert und durch den Projektträger im Deutschen Zentrum für Luft- und Raumfahrt (PT-DLR) betreut.

Die Task Force "IT-Sicherheit in der Wirtschaft" ist eine Initiative des Bundesministeriums für Wirtschaft und Energie, die gemeinsam mit IT-Sicherheitsexperten aus Wissenschaft, Wirtschaft und Verwaltung vor allem kleine und mittelständische Unternehmen für IT-Sicherheit sensibilisieren und dabei unterstützen will, die Sicherheit der IKT-Systeme zu verbessern. Weitere Informationen zur Task Force und ihren Angeboten sind unter: *www.it-sicherheit-in-der-wirtschaft.de* abrufbar.

Herausgeber: Institut für Technik der Betriebsführung (itb) im
Deutschen Handwerksinstitut (DHI) e.V.
Kriegsstraße 103a • 76135 Karlsruhe (Konsortialführer)

Kompetenzzentrum IT-Sicherheit
und Qualifizierte Digitale Signatur (KOMZET) der
Handwerkskammer Rheinhessen
Dagobertstraße 2 • 55116 Mainz (fachliche Leitung)

Westfälische Hochschule
Institut für Internet-Sicherheit – if(is)
Neidenburger Straße 43 • 45877 Gelsenkirchen
(Kooperationspartner)

Interessengemeinschaft des Heinz-Piest-Instituts für Handwerkstechnik (HPI) an der Leibniz-Universität Hannover
Wilhelm-Busch-Straße 18 • 30167 Hannover
(Kooperationspartner)



**ISBN** **978-3-944916-13-2**

Verlag: Handwerkskammer Rheinhessen
Dagobertstraße 2 • 55116 Mainz
*www.hwk.de*

# Autorenteam

**Malte G. Schmidt**

Studierter Journalist (Bachelor of Arts) und wissenschaftliche Hilfskraft am Institut für Internet-Sicherheit – if(is) der Westfälischen Hochschule. Veröffentlichungen in Fachpublika sowie in Zeitschriften und Zeitungen (Bereich Feuilleton).

**Falk Gaentzsch**

Bachelor of Science und wissenschaftlicher Mitarbeiter am Institut für Internet-Sicherheit – if(is) an der Westfälischen Hochschule in Gelsenkirchen. Projektleiter für das Projekt „IT-Sicherheit im Handwerk“.

Schwerpunkte:
IT-Sicherheit & Awareness
Cloud-Computing
Virtualisierung

**Prof. Norbert Pohlmann**

Informatikprofessor für Verteilte Systeme und Informationssicherheit sowie geschäftsführender Direktor des Instituts für Internet-Sicherheit - if(is) an der Westfälischen Hochschule in Gelsenkirchen.

# Einleitung

Die Digitalisierung der Welt hat jeden Sektor gesellschaftlichen Lebens durchdrungen und hat natürlich keinen Halt gemacht vor deutschen Handwerksbetrieben. 99,7 Prozent aller kleinen und mittelständischen Unternehmen (KMU) nutzen Informationstechnologie während ihrer täglichen Geschäftsprozesse (vgl. Bundesministeriums für Wirtschaft und Technologie, 2012); das bedeutet im Umkehrschluss, dass nur ein einziges von 300 Unternehmen auf IT verzichtet. Möchte man einen Handwerksbetrieb ohne internetfähiges Gerät finden, muss man lange suchen, denn die Chancen dafür stehen schlecht – nämlich bei Eins zu Dreihundert. PCs, Notebooks, Smartphones und Tablets gehört mittlerweile genauso zum Handwerker wie die Kelle zum Maurer oder der Pinsel zum Maler. Mobile Endgeräte ermöglichen es, zahlreiche Arbeitsvorgänge von unterwegs aus zu erledigen, wie beispielsweise die Auftragsdaten eines Kunden direkt vor Ort zu erfassen oder einfach dienstliche E-Mails zu versenden. Ihr hoher Nutzwert für KMU spiegelt sich im Verbreitungsgrad wider: Ein Drittel aller Handwerksbetriebe nutzt Tablet-PCs, zwei Dritteln stehen Smartphones zur Verfügung (vgl. IT-Sicherheit im Handwerk, 2013). Die Akzeptanz zur Nutzung privater Endgeräte für dienstliche Zwecke ist groß: In rund zwei Dritteln aller deutschen Unternehmen unterschiedlicher Größe kommen Privatgeräte zum Einsatz (vgl. Dell, 2012).

### Die Hälfte aller Unternehmen ohne sichere Passwörter

Leider ist ein vertrauensvoller Umgang mit den Geräten oftmals nicht gegeben, denn das Thema IT-Sicherheit ist in vielen Handwerksbetrieben unpopulär. Nur die Hälfte aller Betriebe nutzt sichere Passwörter für Geräte und den Zugriff auf das Unternehmensnetzwerk und ändert diese regelmäßig. Drei Viertel der Betriebe schützen sensible Daten nicht mit einem Verschlüsselungsmechanismus. Die Verantwortlichen in jedem zweiten Handwerksbetrieb geben an, ihre Mitarbeiter seien eher nicht oder überhaupt nicht geschult im vertrauensbewussten Umgang mit IT.

Im Betriebsalltag stehen sämtliche Arbeitsprozesse, die mithilfe von IT-Geräten erfolgen, unter der Prämisse der Praktikabilität. Handwerksbetriebe nutzen dann IT, wenn sie Vorgänge erleichtert, beispielsweise in den Bereichen EDV, Logistik, Management et cetera. Das Thema IT-Sicherheit muss sich dieser Praktikabilität oftmals unterordnen. Aus Sicht vieler Unternehmer „stören“ Sicherheitsmaßnahmen eher, als dass sie nutzen. Zeit-, Kosten- und Ressourcenaufwand stehen für sie in keinem Verhältnis zu den Vorteilen. Das hat zwei Ursachen: Erstens sind die Erfolge von IT-Sicherheit keine greifbaren. Sie sind unsichtbar, zumindest solange, bis den Unternehmen Schäden aufgrund von fahrlässigem Umgang mit IT entstehen. Ein Fünftel aller Handwerksbetriebe negiert sämtliche Risiken vollends (vgl. IT-Sicherheit im Handwerk, 2013). „Bei uns ist noch nie etwas passiert“ ist das Totschlagargument, das vielen IT-Beratern seitens der Verantwortlichen im Unternehmen entgegengebracht wird. So einfach wird dann oft die Relevanz des gesamten Themas zunichte gemacht und die Risiken ausgeblendet.
Zweitens herrscht oft große technische Unwissenheit vor. Funktionen werden nicht hinterfragt, eingeübte Abläufe nicht verändert. Gleichzeitig nehmen die Gefahren für die Unternehmensnetzwerke zu, Schadsoftware wird immer raffinierter, Angriffe Krimineller erfolgen immer gezielter. Die Vergangenheit zeigt: Neue Technologien fördern stets auch neue Gefahren zu Tage. Dabei ist der technische Fortschritt gut und wichtig, sollte aber mit überlegter und vertrauensvoller Nutzung einhergehen.

## Zielgruppe des Handbuchs

Dieses Buch richtet sich nicht nur an erfahrene IT-Nutzer, denen das Wort „Phishing“ kein Fremdwort ist und insbesondere an die, die für andere zu Ansprechpartnern in Sachen IT-Sicherheit werden wollen. Es richtet sich genauso an diejenigen, die noch keine Berührungspunkte mit Sicherheitsthemen haben, ja vielleicht sogar erst noch von der Relevanz dieser Themen überzeugt werden wollen.

So werden im ersten Kapitel dieses Handbuchs grundlegende Begriffe geklärt und generelle Fragen beantwortet. Kapitel 2 zeigt auf, warum IT-Sicherheitsmaßnahmen überhaupt wichtig sind. Konkrete Tipps zum Schutz eines Handwerksbetriebes werden in Kapitel 3, 4 und 5 gegeben. Dabei erfolgt eine Auseinandersetzung auf drei Ebenen: Zunächst erfahren Sie, wie Sie die Sicherheit aller mobilen IT-Geräte erhöhen (Kapitel 3). Dieser sogenannte Basisschutz ist jedoch nicht ausreichend. Daher geht es in Kapitel 4 darum, wie die Mitarbeiter eines Betriebes sensibilisiert werden können, um Sicherheitsrisiken zu minimieren. Darüber hinaus können Verantwortliche in den Betrieben auf einer organisatorischen Ebene durch Richtlinien und Management zum Schutz des Unternehmensnetzwerks beitragen. Beachten Sie dazu die Hinweise in Kapitel 5. Im nachfolgenden Kapitel 6 werden die zuvor aufgeführten Ratschläge an zwei Praxisbeispielen verdeutlicht. Nach Darstellung der erforderlichen Sicherheitsmaßnahmen erfahren Sie in Kapitel 7, wie sich die Maßnahmen im Betrieb umsetzen lassen. Abschließend finden Sie eine Checkliste der wichtigsten Tipps (Kapitel 8) und nützliche Links zu weiterführenden Informationen (Kapitel 9).

Viel Erfolg beim Schutz Ihrer mobilen Endgeräte![1][2][3][4][5]

---

[1] *Zugunsten besserer Lesbarkeit wird in diesem Handbuch auf genderneutrale Sprache verzichtet.*

[2] *Kostenlose Software-Produkte, die insbesondere im Kapitel 3. Schutz auf der Geräteebene – Basisschutz genannt werden, gelten zum Zeitpunkt der Erstellung dieses Handbuchs insofern als lizenzfrei und damit kostenlos, als dass sie zunächst nur im Hinblick auf private Nutzung betrachtet wurden. Ob diese Produkte auch im Unternehmenseinsatz kostenlos eingesetzt werden können, müssen Anwender im Einzelfall selbst prüfen.*

[3] *Anleitungen zu Software- und Systemeinstellungen können je nach Produktversion abweichen. Die hier gegebenen Anleitungen orientieren sich an den Smartphone- und Tablet-Betriebssystemversionen iOS 7, Android 4.3, Windows Phone 8 und Blackberry10 OS. Anwender sollten bei Abweichungen ihre Geräte-Handbücher zu Rate ziehen.*

[4] *Als Tipp gekennzeichnete Textabschnitte (fett und mit rotem Strich markiert) können unmittelbar an Unternehmer und Mitarbeiter weitergegeben werden.*

[5] *Vielen Dank an Carsten Balan*

# Seminarziele

Ziel dieses Handbuchs ist es, Anwender grundlegend für die Gefahren des mobilen Arbeitens zu sensibilisieren, aktuelle Schutzmaßnahmen zu präsentieren sowie Verantwortlichen in Unternehmen einen Leitfaden zur Einführung eines BYOD-Konzeptes (siehe Kapitel 5.4) an die Hand zu geben, sofern sie sich trotz aller Risiken zum Einsatz von Privatgeräten entschließen. Dargestellte Risiken und Lösungsansätze werden mit zahlreichen Beispielen illustriert und zielen stets auf die Bedürfnisse kleinerer und mittelständischer Unternehmen ab (siehe Kapitel 6).

Mit Abschluss des Seminars sind Sie in der Lage:

- Ein Grundverständnis über das Thema „Mobiles Arbeiten“ vermitteln zu können.
- Sicherheitsrisiken und Schutzmaßnahmen für Smartphones, Tablets und Laptops zu kennen.
- Mitarbeiter für den verantwortungsvollen Umgang mit den Geräten zu schulen.
- Arbeitgeber bei der Erarbeitung von Unternehmensrichtlinien für mobiles Arbeiten zu unterstützen.
- Bei der Einführung eines BYOD-Konzept beratend tätig zu sein.

# Inhaltsverzeichnis

# 1. Mobiles Arbeiten (BYOD)

In diesem Kapitel geht es darum, grundlegende Begriffe zu klären sowie die vier populärsten Geräteklassen des mobilen Arbeitens zu identifizieren.

## 1.1 Begriffsklärung

„Mobiles Arbeiten“ beschreibt den Umstand, ortsunabhängig jede auf Informations- und Kommunikationstechnik gestützte Tätigkeit ausführen zu können – sei es von Zuhause aus (im Homeoffice), unterwegs im Zug, im Hotel, auf der Dienstreise, bei Außendienstterminen (beim Kunden vor Ort) oder auf der Baustelle. Zwischen dem mobilen Arbeitsplatz und der zentralen Betriebsstätte besteht dabei eine Verbindung durch elektronische Kommunikationsmittel. Mobiles Arbeiten ist mittlerweile sehr beliebt, es gibt einen Trend zur größeren Flexibilität in der Wahl der Arbeitsumgebung. Begünstigt wurde diese Entwicklung durch technische Fortschritte bei Laptop, Smartphone und Tablet-PC. Die Geräte wurden leistungsfähiger, leichter, günstiger und komfortabler in der Bedienung. So können nun an jedem Ort mit einer Internetverbindung E-Mail-Anwendungen und viele weitere Dienste genutzt werden.

***BYOD beschreibt die Möglichkeit für Mitarbeiter, ihr Privatgerät für betriebliche Zwecke nutzen zu dürfen.***

In Zusammenhang mit mobilem Arbeiten steht der Begriff „Bring Your Own Device (BYOD)“. Gemeint ist die Tatsache, dass Mitarbeiter ihre eigenen mobilen Endgeräte wie Smartphones und Tablets, aber auch Laptops und PCs für berufliche Zwecke nutzen. Mit diesen privaten, selbst ausgewählten Geräten greifen Sie auf Daten, Anwendungen und Infrastrukturen des Unternehmens zu. Sinngemäß bedeutet BYOD also „Bring dein eigenes Gerät mit (zur Arbeit)“. Das Gegenteil zu BYOD ist CYOD (Chose Your Own Device), hierbei stellt der Arbeitgeber dem Arbeitnehmer oft eine Auswahl an mobilen Endgeräten zur Verfügung (siehe S. 114).

## 1.2 Netbooks, Notebooks, Smartphones und Tablets – Grundlagen

Nachfolgend ein Überblick über die mobilen Endgeräte, die in Unternehmen große Beachtung finden.

### Notebooks

Notebooks sind tragbare Personal Computer. In ihrer Funktionalität gleichen sie den Desktop-PCs (Schreibtisch-Rechner), da sie aufgrund hochwertiger Grafikkarten und leistungsstarken Prozessoren rechenintensive Software ausführen können. Ein Notebook wird oft mit dem Begriff „Laptop“ synonym bezeichnet, obgleich unter diese Bezeichnung auch die Netbooks fallen. Üblicherweise kommen Notebooks mit einigen Anschlüssen, Schnittstellen für Wechseldatenträger (z.B. Universal Serial Bus, kurz: USB und Secure Digital Memory Card, kurz: SD-Karte), Monitor (Video Graphics Array, kurz: VGA und High Definition Multimedia Interface, kurz: HDMI), Netzwerk (Local Area Network, kurz: LAN) und Funkübertragungstechnologien wie Bluetooth daher. Darüber hinaus besitzen sie oft ein DVD- oder Blu-Ray-Laufwerk.


*Abbildung 1: Notebook („IBM Thinkpad R51"; André Karwath, 2004)*

## Netbooks

Netbooks sind kleine Notebooks mit einer durchschnittlichen Bildschirmdiagonale von zehn Zoll und kleinerer Tastatur. Aufgrund ihrer Größe und ihres leichten Gewichts sind sie besonders für den mobilen Einsatz ausgelegt, müssen aber in puncto Leistungsfähigkeit und Ausstattung größere Kompromisse eingehen. So kommen sie üblicherweise mit vergleichsweise geringer Festplattengröße daher, sodass Anwender oft Cloud-Dienste zur Kompensation nutzen. Netbooks wurden besonders für die flexible Internetnutzung entworfen und bestechen durch ihren niedrigen Preis gegenüber den Notebooks. Ihnen fehlen üblicherweise DVD-Laufwerke und weitere Anschlüsse.

***Für weitere Informationen bezüglich Cloud-Computing, nutzen Sie das gleichnamige Handbuch oder entsprechende Fachliteratur.***

*Abbildung 2: Netbook („HP 2133 Mini-Note PC (front view compare with pencil)"; VIA Gallery, 2008)*

## Smartphones

Herkömmliche Mobiltelefone, umgangssprachlich Handys genannt, sind darauf ausgelegt, die Funktion eines tragbaren Telefons zu erfüllen.
Die Einführung Apples iPhone im Jahr 2007 krempelte den gesamten Mobiltelefonmarkt um. Die Smartphones wurden infolge aus einer Nischen-Geräteklasse zum marktbeherrschenden Gerätetypus. In 2013 wurden laut dem Marktforschungsunternehmen Gartner weltweit 986 Millionen Smartphones verkauft (vgl. Gartner, 2014), 26 Millionen davon in Deutschland (vgl. BITKOM, 2014). Heute sind vier von fünf verkauften Mobiltelefone in Deutschland Smartphones, klassische Handys haben laut BITKOM dagegen nur noch einen Anteil von vier Prozent am gesamten Marktvolumen (ebenda).

Im Gegensatz zu klassischen Handys weisen Smartphones heutzutage in ihrer Funktionalität eher eine Ähnlichkeit zu Computersystemen auf, die an tragbare PCs im Hosentaschenformat erinnert. Internetnutzung und E-Mail-Korrespondenz via Smartphone ist heute Gang und Gäbe. Das Global Positioning System (GPS) ermöglicht eine präzise Standortbestimmung der Geräte sowie Karten- und Navigationsfunktion. Applikationen, sogenannte Apps, lassen den Funktionsumfang beliebig erweitern. So können heute klassische Büro-Anwendungen wie eine Textverarbeitung oder Tabellenkalkulation, aber auch branchenspezifische Firmenanwendungen auf dem Smartphone genutzt werden.

*Abbildung 3: Smartphones („App Store on Smartphone"; Intel Free Press, 2013)*

Wie auch beim klassischen Desktop-PC kommen Smartphones mit immer leistungsfähigerer Hardware und besserem Betriebssystem daher. Dabei verteilt sich die Nutzung der Betriebssysteme wie folgt:

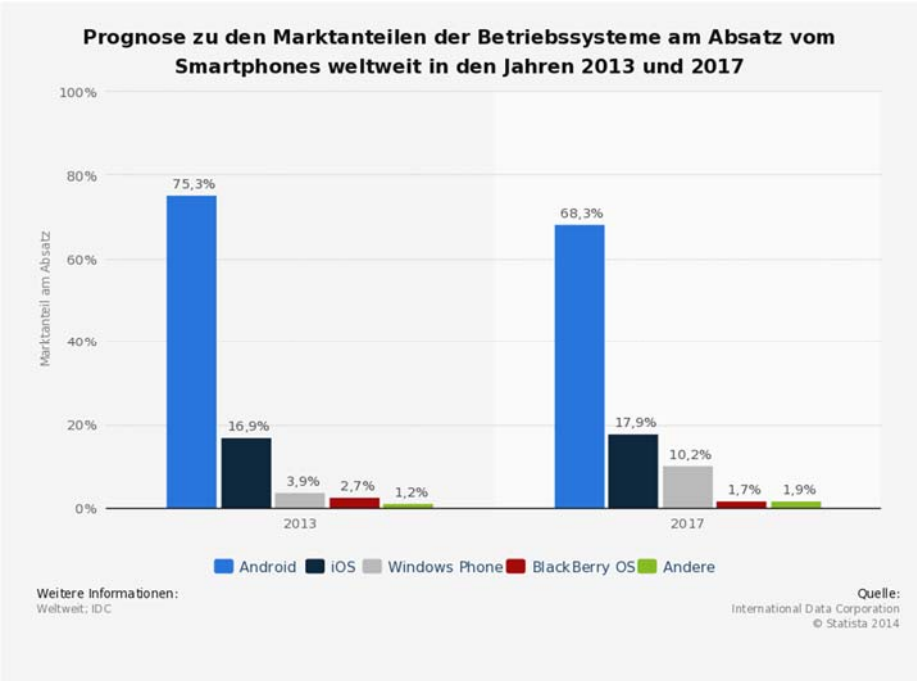



*Abbildung 4: Prognostizierte Marktanteile der Smartphone-Betriebssysteme (International Data Coorporation nach Statista 2013)*

## Tablet-PCs

***Tablet-PCs gleichen in ihrer Funktionalität eher Smartphones als Laptops oder Desktop-PCs.***

Tablet-Computer sind tragbare flache Computer, deren Displays beinahe die gesamte Größe der Gehäuse einnehmen. Sie lassen sich über ihr Display, einem berührungsempfindlichen Touchscreen, mit den Fingern, einem speziellen Stift oder in Verbindung mit einer Tastatur steuern. Ihre Anschluss-vielfalt ist stark eingeschränkt, viele besitzen einen USB-Anschluss und einen HDMI-Anschluss zur Verbindung mit einem Monitor oder Fernseher. In ihrer Funktionalität gleichen sie eher dem Smartphone als dem Desktop-PC: Der Software-Umfang lässt sich analog zum Smartphone mithilfe von Applikationen, kurz Apps, erweitern (siehe nachfolgendes Kapitel). Im Jahr 2013 wurden laut Bundesverband Informationswirtschaft, Telekommunikation und neue Medien (BITKOM) über fünf Millionen Geräte in Deutschland verkauft, jedes dritte

deutsche Unternehmen setzt Tablets aufgrund ihrer großen Flexibilität im Betriebsalltag ein (vgl. BITKOM, 2013d).

*Abbildung 5: Tablet-PC („swipe telecom"; Swipe Telecom Tablet PC Company, 2012)*

### Weitere mobile Endgeräte

Neben den oben genannten Geräten ist der Einsatz weitere mobiler Geräteklassen denkbar. So ist beispielsweise mit heutigen E-Book-Readern, tragbaren Lesegeräten für elektronische Bücher, auch die Internetnutzung möglich. Daneben gibt es eine Reihe von kleinen Handhelds, tragbaren elektronischen Geräten, wie dem Personal Digital Assistant (PDA), der Basisfunktionen zur Textverarbeitung und eine Kalender- und Adressverwaltung ermöglicht.

# 2. Risiken

Die Vorteile von mobilen Geräten sind enorm, privat, aber auch beruflich. Die neuen Risiken leider auch! Die Masse der mobilen Geräte sind für den Consumer-Markt entwickelt worden und bieten oft eine unzureichende IT-Sicherheit.

Mobile Geräte stellen ein erhöhtes Risiko dar, da sie auch außerhalb der Unternehmensmauern verwendet werden können. Die Geräte und die darauf gespeicherten Daten sind deshalb größeren Gefahren ausgesetzt.

Aufgrund ihrer Größe und ihres Gewichts sind die Geräte an jedem Ort einsetzbar – und können leicht vergessen, verloren oder gestohlen werden. Dadurch können unter anderem gesetzliche Bestimmungen verletzt werden, wenn vertrauliche Daten an unbefugte Dritte geraten. Zudem entsteht ein finanzieller Verlust.

Eine weitere Bedrohung besteht bei der mobilen Internetnutzung, sei es via UMTS oder über andere Unternehmensnetzwerke. Sie können sich nicht ohne weiteres sicher sein, dass in der Netzwerkverbindung bis hin zum Internet niemand mit lauscht. Die Gefahr eines digitalen Spitzels ist gerade bei drahtlosen Verbindungen in einem fremden Netzwerk, zum Beispiel das eines Unternehmens oder eines Internet-Cafés, besonders gegeben.

Als kleine Computer im Hosentaschen-Format sind mobile Geräte auch den Gefahren stationärer PCs ausgesetzt: In der Studie „IT-Sicherheit im Handwerk“ nennt die Hälfte der befragten Handwerksunternehmer Schadprogramme wie Viren, Würmer und Trojaner als größtes Risiko für ihre IT-Sicherheit (vgl. hier und im Folgenden: IT-Sicherheit im Handwerk, 2013). Weitere Problemfelder sehen sie hauptsächlich in den Bereichen Onlinebanking, Spam und Datenmanipulation und -verlust. Ihren Mitarbeitern attestieren 50 Prozent der Befragten jedoch kein ausreichendes beziehungsweise gar kein Bewusstsein für IT-Sicherheitsthemen.
Nachfolgend sollen IT-Gefahrenpotenziale besprochen und die Konsequenzen offengelegt werden, die Unternehmen bei Missachtung in Kauf nehmen.

## 2.1 Drahtlose Kommunikation und ihre Tücken

Nachfolgend ein Überblick über drahtlose Kommunikationstechnologien, ihren Risiken und möglichen Schutzmaßnahmen.

### 2.1.1 Wireless LAN (WLAN) und Hotspots

**Beschreibung**

- Wireless Local Area Network (drahtloses lokales Netzwerk)
- Ersetzt die kabelgebundene Netzwerktechnik
- Aufbau über drahtlose Router oder Wireless Access Points
- Verschiedene Verschlüsselungstechnologien (WEP, WPA, WPA 2)
- Synonym: WiFi

**Anwendungsmöglichkeiten**

- Netzwerkzugang an öffentlichen Plätzen (z.B. Flughäfen, Bahnhöfen, Bibliotheken, Restaurants, Cafés), Zuhause und in Unternehmen

**Risiken**

- Besonders angreifbar bei unverschlüsselter Kommunikation innerhalb eines öffentlichen oder unzureichend verschlüsselten WLAN-Netzes (unzureichend: Standards WEP und WPA); Folge: Datenverlust
- Man-in-the-Middle-Angriff[6] ermöglicht Abhören und Manipulation der Kommunikation der im Netzwerk befindlichen Teilnehmer

**Sicherheitsempfehlungen (siehe:** *4.3 Sicherheit bei drahtloser Kommunikation***)**

- WLAN-Schnittstelle deaktivieren und nur bei Bedarf aktivieren
- In den WLAN-Einstellungen die Option „automatisch verbinden, sobald Netzwerk in Reichweite“ deaktivieren
- Meidung öffentlicher WLAN-Netze; stattdessen besser: Nutzung des mobilen Internets, da Angriffe schwieriger[7]
- Kontrolle der WLAN-Verschlüsselung vor Verbindungsaufbau; aktueller Standard: WPA2
- Einsatz von Verschlüsselungstechniken (VPN und SSL/TLS)
- Nutzung einer aktuellen Firewall
- Für Betreiber des WLAN-Netzes: sinnfreie Benennung des Netzwerks (SSID-Name), die nicht auf verwendete Geräte oder den Einsatzort zurückzuführen sind; Deaktivierung der Router-Fernkonfiguration; Vergabe eines sicheren Netzwerksschlüssels; regelmäßige Firmware-Aktualisierung

***Für weitere Informationen bezüglich WLAN-Sicherheit, nutzen Sie das gleichnamige Handbuch oder entsprechende Fachliteratur.***

[6] *Man-in-the-Middle-Angriff: Ein Angreifer kann den Netzwerkverkehr über eine durch ihn kontrollierten Datenknoten, beispielsweise ein WLAN-Router, abfangen, mitlesen und manipulieren.*

[7] *Hinweis: Die Nutzung des mobilen Internets bietet ebenfalls keinen ausreichenden Schutz vor Datenabgriff. Die massenhafte Nutzerüberwachung durch Nachrichtendienste wie der NSA kann hier als Beleg aufgeführt werden. Es sind also (weitere) Verschlüsselungsmechanismen erforderlich.*

### 2.1.2 Bluetooth

**Beschreibung**

- Funktechnik für eine kabellose Datenübertragung über kurze Distanzen von (normalerweise) bis zu zehn Metern; mithilfe spezieller Hardware können auch Entfernungen bis zu hundert Metern überbrückt werden
- Kommunikation mit anderen Bluetooth-Geräten (PIN-Vergabe erforderlich)

**Anwendungsmöglichkeiten**

- Einsatz vor allem bei Smartphones und Tablets
- Bluetooth-Pairing mit Bluetooth-fähigen Geräten zum Austausch von Dateien
- Kommunikation mit einem Drucker
- Kabellose Freisprechanlagen im Auto, Headsets, Lautsprecher-Verbindung

**Risiken**

- Permanente Sichtbarkeit des Anwendergeräts, wenn Bluetooth-Funktion aktiviert ist
- Bluetooth-Tracking: Erstellung von Bewegungsprofilen über eine Verkettung von mehreren Bluetooth-Geräten (Angreifer muss sich in der Nähe befinden)
- Bluesnarfing: Unbefugter Zugriff auf gespeicherte Textnachrichten (SMS), Adress- und Kalenderdaten bei Verwendung bestimmter Geräte oder veralteter Bluetooth-Versionen
- Steuerung des Zielgeräts mithilfe von AT-Befehlen (z.B. Senden von SMS)

**Sicherheitsempfehlungen (siehe:** *4.3 Sicherheit bei drahtloser Kommunikation***)**

- Bluetooth deaktivieren und nur bei Bedarf aktivieren
- Nicht die Gerätekennung als Bluetooth-Namen verwenden
- Keine sensiblen Daten mittels Bluetooth austauschen, sofern sie nicht im Vorfeld verschlüsselt wurden
- Möglichst nur in abhörsicherer Umgebung verwenden (nicht an öffentlichen Plätzen)
- Bluetooth Geräte aber der Version 4.0 bieten nicht nur mehr Sicherheit bei der Datenübertragung, es wurde auch der Fokus auf eine neue Energiesparfunktion gesetzt, dem so genannten „Bluetooth low energy“

### 2.1.3 Mobilfunkstandards (GPRS, GSM, EDGE, UMTS, HSDPA, LTE)

**Beschreibung**

- Mobilfunkstandards zur drahtlosen Kommunikation über Mobilfunk-Sendemasten
- Zur Nutzung notwendig: Teilnehmerauthentifikation via International Mobile Station Equipment Identity (IMEI-Nummer)
- Unterschiedliche Datenübertragungsgeschwindigkeiten und Verschlüsselung je nach Standard (GSM 9,6 kBit/s, GPRS 115 kBit/s, EDGE 236 kBit/s, UMTS 384 kBit/s, HSDPA 14,4 MBit/s, LTE 150 MBit/s)

**Anwendungsmöglichkeiten**

- Telefonie, Übertragung von Kurzmitteilungen (SMS) und Internetnutzung

**Risiken**

- Ungezielter Lauschangriff über eine in der Nähe befindlichen Antenne ermöglicht Abhören aller im Sendebereich befindlichen Teilnehmer, dies betrifft insbesondere die Standards GSM, GPRS und EDGE
- Gezielter Man-in-the-Middle-Angriff bei einigen Mobilfunkstandards möglich; Folge: Abhören und Manipulation der Kommunikation eines Ziels; Voraussetzung: IMEI-Nummer des Opfers muss bekannt sein
- Die zurzeit genutzte Verschlüsselung zwischen dem mobilen Geräte und der Basisstation ist nicht sicher genug.

**Sicherheitsempfehlungen (siehe:** *4.3 Sicherheit bei drahtloser Kommunikation***)**

- Nutzung von Apps/Programmen, die eine verschlüsselte Kommunikation (z.B. über TLS/SSL) ermöglichen, besser noch sind Apps die eine Ende-zu-Ende verschlüsselte Kommunikation ermöglichen
- Deaktivieren von Schnittstellen, die nicht benötigt werden
- Es sollten aktuelle Übertragungstandards verwendet werden, UMTS (3G) gilt als sicher und LTE (4G) als sehr sicher (Stand 2014)

### 2.1.4 Global Positioning System (GPS)

**Beschreibung**

- Globales Navigationssatellitensystem
- Satelliten senden ständig ihre aktuelle Position aus, sodass GPS-Empfänger am Boden ihre eigene Position und die Bewegungsgeschwindigkeit bestimmen können

**Anwendungsmöglichkeiten**

- Standortbestimmung/Ortung (z.B. in Navigations-Apps, Enterprise-Apps zur Flottenkontrolle)
- Zeitmessung (z.B. Geschwindigkeitsangabe in Navigations-Apps)

**Risiken**

- Unbemerkte Standortübermittlung und Erstellung von Bewegungsprofilen (Tracking) durch (unsichere) Apps
- Datenschutzrechtliche Risiken, sofern Mitarbeiter nicht über Standortkontrolle durch Arbeitgeber informiert wurden; in größeren Unternehmen wird die Zustimmung des Betriebsrats benötigt
- GPS-Spoofing: Störung von Positionsdaten durch Imitation von Satellitensignalen

**Sicherheitsempfehlungen (siehe:** *4.3 Sicherheit bei drahtloser Kommunikation***)**

- GPS deaktivieren und nur bei Bedarf aktivieren
- Kontrolle der Zugriffsrechte bei der Installation einer App
- Ausdrücklicher Hinweis der Ortung durch Arbeitgeber bei Flottenkontrolle: *„Der Arbeitgeber hat den Einsatz des Ortungssystems durch geeignete Maßnahmen für den Beschäftigten erkennbar zu machen und ihn über den Umfang der Aufzeichnungen und deren regelmäßige oder im Einzelfall vorgesehene Auswertung zu informieren“ (*§32g BDSG[8])

[8] *BDSG – Bundesdatenschutzgesetz*

### 2.1.5 Near Field Communication (NFC)

**Beschreibung**

- Kontaktlose Kurzstreckenfunktechnik zum Datenaustausch über kurze Strecken von circa zehn Zentimetern
- Kommunikation zwischen zwei Teilnehmern (z.B. zwei Smartphones mit NFC-Chips oder ein Smartphone und „NFC-Tag“ (Etikett) oder eine EC-/Kreditkarte mit NFC-Chip und ein (Bank-)Terminal)
- Übertragungswege: passiv (Initiator[9] sendet Magnetfeld aus, Target[10] empfängt) oder aktiv (beide Teilnehmer senden abwechselnd ein Magnetfeld aus)
- max. Übertragungsrate: 424 kbit/s

**Anwendungsmöglichkeiten**

- Micro-Payment für bargeldloses Bezahlen von Kleinbeträgen (ggf. in Verbindung mit PIN-Eingabe); Beispiele: Sparkasse Girogo, Visa payWave, Maestro PayPass, Deutsche Bahn Touch and Travel, Google Wallet
- Aktivierung von Informationen und Diensten (z.B. Nachrichten, Fahrpläne)
- Authentifikation (Zugangs- und Zugriffskontrollen)

**Risiken**

- Automatische Datenübertragung, sobald elektromagnetisches Feld durch den Initiator aufgebaut wird: Datenauslese (z.B. Kreditkartennummer und Ablaufdatum), mögliche Folge: Datenmissbrauch
- Lauschangriff mit Hilfe einer in der Nähe befindlichen Antenne
- Malware-Infektion durch korrumpierten NFC-Tag (z.B. auf Smart Postern)
- Man-in-the-Middle Attacken

**Sicherheitsempfehlungen (siehe:** *4.3 Sicherheit bei drahtloser Kommunikation***)**

- SIM-Karten mit NFC-Sicherheitsmodul (Secure Element) präferieren, sofern möglich
- NFC-Schutzhülle für Smartphone und Kreditkarten verwenden
- Nutzung der NFC-Technologie mit Sicherheitsbeauftragtem im Unternehmen und/oder der Unternehmensführung abklären
- NFC bei Smartphones deaktivieren und nur bei Bedarf aktivieren
- Dienstleister und Anwendungen im Vorfeld auf Seriosität und Sicherheitsvorkehrungen prüfen; auf vollständige Verschlüsselung bei Datenübertragung achten
- Keine sensiblen (Unternehmens-)Daten via NFC übertragen
- Basisschutz auf dem Smartphone einrichten
- Bei Geräteverlust NFC-Bezahldienste sperren lassen

[9] *Initiator, ist die Instanz die eine Kommunikation auslöst.*
[10] *Target, ist die Instanz mit der eine Kommunikation aufgebaut und abgewickelt wird.*

### 2.1.6 Quick-Response-Codes (QR-Codes)

**Beschreibung**

- Quadratische Abbildungen aus schwarzen und weißen Punkten, die codierte Informationen bereitstellen
- QR-Codes werden in der Regel mithilfe von Smartphone- und Tablet-Kameras und QR-Code Reader interpretiert

*Abbildung 6: QR-codierte URL zum Ziel https://www.it-sicherheit-handwerk.de*

**Anwendungsmöglichkeiten**

- Verweis auf Internetseiten (z.B. in Zeitschriften und auf Postern)
- Grafische Codierung von (SMS-)Text, Kontakt- und Kalenderdaten, E-Mailadressen, Geo-Koordinaten, Telefonnummern und WLAN-Zugangsdaten

**Risiken**

- Überklebte QR-Codes beispielsweise auf Plakaten, die auf präparierte Websites verweisen, um personenbezogene Nutzerdaten abzugreifen
- Datenverlust aufgrund der fahrlässigen Codierung sensibler Daten (z.B. WLAN-Zugangsdaten) an Orten, die von Dritten einsehbar sind und so unberechtigt ausgelesen werden können
- USSD-Angriff[11]: Verlust von sämtlichen gespeicherten Daten sowie Sperrung der SIM-Karte möglich (siehe Kapitel *3.2.4 Personal Firewall*)

**Sicherheitsempfehlungen (siehe:** *4.3 Sicherheit bei drahtloser Kommunikation***)**

- Sensibilisierung der Mitarbeiter hinsichtlich der Gefahren
- QR-Code-Scanner verwenden, der die codierte Ziel-Adresse anzeigt, bevor sie aufgerufen wird
- Schutz vor USSD-Manipulation:
  Anfälligkeit prüfen[12]; ggf.: Installation der App „NoTelURL“

[11] *USSD-Angriff: Konnte auf angreifbaren Android-Geräten genutzt werden, um Systemeinstellungen zu verändern.*
[12] Siehe hierzu: *http://www.heise.de/security/dienste/USSD-Check-1717811.html;*

## 2.2 Viren, Würmer, Trojaner

***Malware bedroht heutzutage alle intelligenten Geräte im Netzwerkverbund.***

Die Vorstellung, Schädlinge (Malware) wie Viren, Würmer und Trojaner stellen lediglich eine Gefahr für herkömmliche Desktop-PCs oder allenfalls für Laptops dar, ist überholt. Die Digitalisierung hat uns eine Vielzahl neuer intelligenter Geräte beschert, die Teil sämtlicher Lebens- und Arbeitsbereiche sind: intelligente Produktionsmaschinen, Digitalkameras, Smartphones, Tablet-PCs, Smart-TV-Fernseher oder sogar Smart-Fridges (intelligente Kühlschränke) und Smart-Cars – sie alle sind anfällig für Schädlinge, erst recht, wenn sie Zugang zum Internet haben. Sicherheitsexperten sind der Ansicht, dass bekannte Schadsoftware, die in den vergangenen Jahrzehnten auf Desktop-PCs und Laptops abzielte und sich professionalisierte, plötzlich eine Vielzahl neuartiger Gerätetypen gefährdet. Gleichzeitig lässt sich jedoch bewährte Software zum Virenschutz der Desktop-PCs nicht eins zu eins auf die jungen Gerätetypen übertragen. Trotz des oft defizitären Stands der IT-Sicherheit dieser Geräte stehen sie dennoch in direkter Verbindung mit den anderen Geräten im Netzwerkverbund und nehmen teil am globalen Datenaustausch des Internets.

### Sechsmal mehr Smartphone-Schädlinge in 2013

***Premium-SMS-Abzocke ist die populärste Angriffsmethode bei Smartphones. Insgesamt gibt es laut Juniper knapp 300.000 Schädlinge, die speziell auf Smartphones abzielen.***

Laut einer Studie des Netzwerkausrüsters Juniper stieg die Zahl der Schadprogramme für Smartphones zwischen 2012 und 2013 um 614 Prozent an (vgl. Juniper Networks Inc, 2013). Kriminelle konnten vor allem mit korrumpierten Textnachrichten (SMS) Erfolge erzielen. Zwei Drittel aller von Juniper erfassten Angriffe auf Smartphones erfolgten mithilfe von verseuchten SMS, die infolge den Betroffenen teure Premium-SMS-Dienste aufzwangen. Diese Art der Angriffe ist beileibe nicht die einzig mögliche.

Für eine Vireninfektion kann bereits der Besuch einer kompromittierten Website genügen, um das gesamte System und womöglich den gesamten Netzwerkverbund anzustecken. Die Ausprägungen der verschiedenen Schädlinge erscheint unendlich: Aktuell zählt der Virenschutz-Hersteller McAfee 120 Millionen verschiedene Malware-Varianten in seiner Datenbank (vgl. McAfee, 2013), Juniper zählte allein 270.000 Smartphone-spezifische Schädlinge (vgl. Juniper Networks Inc, 2013). Es kann zwischen drei Typen von Schädlingen unterschieden werden:

### Computervirus

***Ein Virus reproduziert sich, indem er sich unter Zutun des Anwenders unbemerkt in andere Computerprogramme einschleust.***

Die bekannteste Form ist die des Computervirus (meist nur Virus genannt). Mit diesem Begriff werden oftmals auch die anderen zwei Typen von Schädlingen synonym verwendet, da die Abgrenzung bisweilen nicht einfach ist. Ein Computervirus ist ein Computerprogramm, das sich verbreitet und reproduziert, indem es sich heimlich in andere Computerprogramme einschleust. Ist es einmal aktiviert, kann es unbemerkt Software oder sogar Hardware des betroffenen Anwendersystems manipulieren. Naturgemäß verfolgen die Urheber von Computerviren meist die Absicht, Schäden beim Anwendersystem hervorzurufen und/oder es zu ihren Gunsten zu verändern.

Um sich auf andere Geräte übertragen zu können, ist ein Virus auf die Mithilfe des Nutzers angewiesen – der Nutzer hilft natürlich unbeabsichtigt, er ahnt nichts von der Vireninfektion. So kann der Virus beispielsweise eingebettet in ein infiziertes PDF-Dokument über einen USB-Stick auf den Rechner des Kollegen übertragen werden.
Die Auswirkungen einer Infektion mit einem Computervirus sind sehr unterschiedlich. Es kann zu kleineren, kaum wahrnehmbaren Störungen während der Ausführung von

Software kommen oder zu komplettem Datenverlust beziehungsweise dem vollständigen Hardwaredefekt.

### Computerwurm

Der zweite Schädlingstyp ist der Computerwurm. Computerwürmer vervielfältigen sich ebenfalls, sobald sie (vom Nutzer unbemerkt) ausgeführt wurden. Sie sind selbstständige Programme, die sich an einer unauffälligen Stelle im System mit einem harmlos klingenden Dateinamen niederlassen. Von dort aus manipulieren sie installierte Software und das Betriebssystem des Anwenders. Bei der Verbreitung auf andere Systeme sind sie nicht mehr auf die Mithilfe des Anwenders angewiesen. Sie machen sich beispielsweise Sicherheitslücken oder schwache Passwörter von E-Mail-Programmen zunutze, um eine Kopie von sich selbst automatisiert an eingetragene E-Mail-Adressen zu versenden. Öffnet ein Adressat dann den Anhang einer solchen E-Mail, beginnt das perfide Spiel auf seinem System von Neuem. Diese Verbreitungsmethode verbraucht bisweilen so viele Ressourcen in einem Netzwerkverbund, dass es sogar zu einem Serverausfall in Unternehmen kommen kann.

***Würmer lassen sich oft mit einem harmlos klingenden Namen an einer unauffälligen Stelle im System nieder. Sie können sich selbstständig verbreiten, indem sie beispielsweise Kopien von sich selbst via E-Mail verteilen.***

### Trojanisches Pferd

Bei einem Trojanischen Pferd (kurz: Trojaner) handelt es sich um eine der griechischen Mythologie entliehene Bezeichnung eines Schadprogrammes, das der Anwender unter falschen Vorzeichen aktiviert. Entsprechend dem mythologischen Vorbild stellen sich die digitalen Trojaner nach außen als nützliche oder unterhaltende Anwendung dar, mit dem Ziel, vom Nutzer ausgeführt zu werden. So kann sich eine Datei „Bildschirmschoner.exe“ in Wahrheit als Schadprogramm entpuppen, das Dateien löscht, Online-Banking-Passwörter mitliest oder gleich die Kontrolle über das Anwendersystem übernimmt. Dabei ist unerheblich, ob die nach außen dargestellte Funktion des Bildschirmschoners tatsächlich funktioniert oder nicht. Der schädigende und/oder spionierende Teil der Anwendung läuft im Verborgenen, parallel zur Oberfläche des Bildschirmschoners. Nachfolgend zwei Trojaner-Beispiele für das Android-Betriebssystem:

***Trojaner tarnen sich als nützliche oder unterhaltende Anwendung, führen im Hintergrund jedoch Prozesse aus, um beispielsweise Daten zu stehlen oder Passwörter mitzulesen.***

Der Fake Player tarnt sich als App zur Wiedergabe von Medieninhalten. Wird sie gestartet, erscheint eine Nachricht in russischer Sprache auf dem Display des Geräts, in der darum gebeten wird zu warten. Währenddessen versendet das Gerät vom Anwender unbemerkt SMS-Nachrichten, die zur Inanspruchnahme eines teuren SMS-Premium-Dienstes führen (vgl. Lamberty, 2012).
Beim Start des Trojaners GingerMaster werden dem Nutzer vordergründig ästhetische Fotos weiblicher Models gezeigt. Im Hintergrund nutzt die Schadsoftware eine Sicherheitslücke im Android-Betriebssystem aus, die bis zur Android-Version 2.3 klaffte und ab Version 2.3.1 behoben wurde. So erlangte die Software die sogenannten Root-Rechte, die weitreichendsten Zugriffsrechte zur Konfiguration und Erweiterung des Systems – dies ist gleichbedeutend mit der Aushebelung sämtlicher Sicherheitsvorkehrungen. Nun kann sie nach Belieben weitere Software auf dem Gerät installieren, ohne dass sie dafür die Genehmigung des Nutzers bräuchte. Gleichzeitig verrät sie dem unbekannten Angreifer pikante Geräteinformationen wie die Telefonnummer und die SIM-Karten-PIN (ebenda).

***Zwei Drittel aller Unternehmen haben laut SecuMedia bereits Malwarevorfäll erlebt.***

Zusammenfassend lässt sich feststellen: Die Gefahr einer Malware-Infektion im betrieblichen Umfeld ist real. Zwei Drittel der Unternehmen aus Deutschland haben bereits Malwarevorfälle erlebt, ein Drittel erlitten in den Jahren 2010 bis 2012 Schadensfälle aufgrund von Viren, Würmern und Trojanern (vgl. SecuMedia, 2013)[13].

## 2.3 Programme und Apps als Sicherheitsrisiken

***Software-Schwachstellen in veralteter Software ist eines der größten Einfallstore für Schädlinge. Angreifer zielen auf diejenigen Programme ab, die einen hohen Verbreitungsgrad haben wie beispielsweise die Browser-Plug-Ins Java und Flash.***

Veraltete Software ist eines der größten Einfallstore für Schadprogramme. Kriminelle nutzen Software-Schwachstellen aus, um Schädlinge in das System des Anwenders zu schleusen. Dabei finden Angreifer immer neue Schlupflöcher. Gängige Programme mit hoher Reichweite ziehen die Aufmerksamkeit vieler Angreifer auf sich – werden hier Schwachstellen gefunden, dienen sie als vielversprechender Nährboden für ihre Schädlinge. Viele Nutzer einer Software versprechen viele infizierte Systeme. Aus diesem Grund müssen Software-Hersteller wie Oracle, dessen Browser-Plugin Java laut Herstellerangaben auf einer Milliarde Desktop-PCs und drei Milliarden mobilen Endgeräten installiert ist, ständig auf der Hut sein: Es gilt, Sicherheitslücken zu entdecken und mittels Sicherheitsupdates zu versiegeln. Oft wird erst bei der Identifikation einer Schwachstelle bekannt, dass diese bereits aktiv durch Kriminelle ausgenutzt wird. Bis ein entsprechendes Sicherheitsupdate erscheint und durch Anwender eingespielt wird, vergeht zusätzliche Zeit, die Kriminelle zum Verbreiten von Malware nutzen können. So kann es passieren, dass aufgrund einer Schwachstelle im Adobe Reader – ein weitverbreitetes Programm zur Darstellung von PDF-Dokumenten – kompromittierte PDF-Dateien im Betrieb die Runde machen und reihenweise diejenigen Geräte mit einem Virus infizieren, die eine veraltete Version des Adobe Readers nutzen.

Neben der Infiltration bestehender Software (Programme und Apps) versuchen Kriminelle allerdings auch neue Produkte aus dem Boden zu stampfen, um so Malware in Umlauf zu bringen. Beispiele dafür sind die in Kapitel *2.2 Viren, Würmer, Trojaner* vorgestellten Android-Apps, die sich als Trojaner entpuppen.

### 2.3.1 Bezugsquellen

Potenzielle Gefahrenquellen sind die Bezugsorte von Software-Produkten. Viele IT-Anwender laden Software von unbekannten Internetseiten herunter, auf die sie mittels Google-Suche gestoßen sind. Dabei machen sie sich keine Gedanken darüber, wer eigentlich der Betreiber einer bestimmten Website ist und welche Absichten er mit seinem Angebot verfolgt.
Fahrlässigkeit in der Auswahl von Software-Bezugsquellen kann dazu führen, dass sich Mitarbeiter statt der gewünschten Software Schadprogramme auf den mitgebrachten Geräten installieren oder installiert haben und damit das gesamte Unternehmensnetzwerk gefährden. Das Sicherheitsrisiko potenziert sich, wenn die Installa-

[13] *In „<kes>/Microsoft Sicherheitsstudie“ führt die Zeitschrift <kes> in Kooperation mit Microsoft alle zwei Jahre eine Befragung unter KMU und einigen Großunternehmen durch, um den Stand der IT-Sicherheit zu untersuchen. Dabei äußern sich die Befragten auch zu Schadensfällen und geben Prognosen ab. Die Zahlen stammen aus der Studie von 2012, bei der 133 beantwortete Fragebogen ausgewertet werden konnten.*

tion von Software in den Unternehmensrichtlinien nicht geregelt ist und kein aktuelles Virenschutz-Programm installiert ist.

***App-Downloads aus inoffiziellen App Markets sind gefährlich, da hier möglicherweise weniger Kontrollmechanismen im Vergleich zu den offiziellen Markets zugrunde liegen.***

Gleiches gilt natürlich auch für die Installation von Apps aus unbekannten Quellen. Es ist davon auszugehen, dass das Risiko einer Schadcode-Infektion bei denjenigen Applikationen größer ist, die nicht aus den offiziellen App Markets (iOS: App Store; Android: Google Play; Windows 8: Windows Store; Windows Phone: Windows Phone Store; Blackberry: Blackberry World) stammen. Grund dafür sind die Sicherheitsrichtlinien der App Markets, die App-Entwickler erfüllen müssen, damit sie ihre App über die jeweilige Plattform anbieten dürfen. Allerdings gibt es hier zum Teil gravierende Unterschiede in der Härte der Auflagen. Apples App Store hat hier vergleichsweise strenge Anforderungen.

***Auch die Prüfmechanismen der offiziellen Markets können nicht verhindern, dass es Schadsoftware in die offiziellen Download-Kataloge schafft.***

Trotz der Sicherheitsvorkehrungen gelten auch die offiziellen App Stores als Distributionsmöglichkeit für Schadsoftware – und zwar deshalb, weil nicht jede der über zwei Millionen angebotenen Apps in den App Stores der vier populärsten Betriebssysteme (vgl. Statista, 2014) im Detail auf Schädlinge überprüft werden kann. So kommt es, dass der Trojaner Rootcager, der bei Ausführung auf Android-Geräten versucht, Root-Rechte zu erlangen, über den offiziellen Android Store vier Tage lang unter verschiedenen App-Namen vertrieben wurde. Laut Symantec, einem Software-Hersteller für Sicherheitsprodukte, haben sich in dieser Zeit 50.000 bis 200.000 Nutzer den Rootcager über den App Store heruntergeladen (vgl. Hamada nach Lamberty, 2012). Nutzer sollten sich daher vor der Installation einer Software oder App umfassend über diese informieren, weitere Hinweise hierzu im Kapitel 4.1.

### 2.3.2 App-Zugriffsrechte

Das Installieren von Applikationen (Apps) auf Smartphones und Tablets ist unter Sicherheitsaspekten grundsätzlich problematisch[14]. Damit eine App bestimmte Programmfunktionen zur Nutzung bereitstellen kann, braucht sie in vielen Fällen Zugriff auf gewisse Ressourcen des Gerätes, auf dem sie installiert werden soll. Eine Navigations-App kann nur dann eine navigierende Funktion aufweisen, wenn ihr die Möglichkeit eingeräumt wird, in Kommunikation mit dem GPS-Satelliten treten zu dürfen, um die Position des Gerätes auf der Landkarte bestimmen zu können.

***Mit der App-Installation gewährt der Nutzer Zugriffsrechte zu Geräteressourcen. Die Auswahl der zu fordernden Berechtigungen obliegt den Urhebern einer App.***

Es wird zwischen Hardware-Ressourcen, dazu gehören die drahtlosen Schnittstellen (z.B. WLAN und Bluetooth) oder auch die Kamera und Software-Ressourcen wie dem Telefonbuch, dem Kurznachrichten-Speicher (SMS) und den Systemeinstellungen unterschieden. Es obliegt den Urhebern einer App, festzulegen, welche Zugriffrechte ihre App einfordern soll. Genau hier liegt der Knackpunkt: Anwender können nie sicher sein, was die Urheber einer App mit den freigegebenen persönlichen Daten machen. Dienen erlaubte Zugriffe auf Ressourcen wirklich nur dazu, um die beschriebenen Funktionalitäten einer Anwendung zu ermöglichen? Welche Daten fließen im Verborgenen ab und welche Sicherheitseinstellungen werden durch die App verändert? Gibt es Sicherheitsvorkehrungen, die die Datenübertragung zwischen Gerät und Herstellerserver vor äußeren Angriffen abschirmen? Die Datensicherheit der Nutzer ist also stark abhängig von der Intention der App-Betreiber.

[14] *Gleiches gilt natürlich auch für die Installation von Software auf Laptops, mit dem Unterschied, dass ein Laptop womöglich durch eine wirksamere Security Suite besser vor Datenabfluss geschützt sein kann.*

### Geforderte versus tatsächlich benötigte Zugriffsrechte

***Werden mehr Zugriffsrechte gefordert, als die Funktionen der Anwendung vermuten lassen, ist die Seriosität des App-Urhebers fraglich.***

Viele Anwendungen fordern bei der Installation mehr Berechtigungen ein, als sie überhaupt für ihre Funktionalitäten benötigen. Eine missbräuchliche Verwendung der zusätzlich geforderten Zugriffsrechte muss dann vermutet werden. Erfolgt auf den Privatgeräten der Mitarbeiter keine saubere Abschirmung des dienstlichen Bereichs (siehe Kapitel *2.10.1. Trennung von privaten und beruflichen Daten* und *5.4.3. Trennung zwischen Unternehmens- und Privatbereich auf den Geräten*) landen plötzlich Geschäfts-E-Mails, dienstliche Kontaktinformationen und Kundendaten auf den Servern eines Herstellers für eine harmlos wirkende App. Tabelle 1 zeigt am Beispiel der Android-App „Brightest Taschenlampe“ (Downloadzahl 939.031[15]) eine Gegenüberstellung der geforderten mit den tatsächlich technisch notwendigen Zugriffsrechten.

| Berechtigung | Auswirkungen | Technisch notwendig? |
|---|---|---|
| Bilder und Videos aufnehmen | In diesem Fall: Steuerung des Kameralichts | ja |
| Standby-Modus deaktivieren | Verhindert, dass die Taschenlampe nach kurzer Zeit automatisch deaktiviert wird | ja |
| Lichtanzeige steuern | Erlaubt es, die Bildschirmhelligkeit zu maximieren | ja |
| USB-Speicherinhalt ändern/löschen | Ermöglicht es, Werbung und Daten zwischenzuspeichern | nein |
| Uneingeschränkter Internetzugriff | Blendet Werbung ein und sendet Informationen zur Personalisierung dieser an AdWhirl | nein |
| Telefonstatus lesen und identifizieren | Sammelt Informationen, um das Gerät eindeutig identifizieren zu können | nein |
| Genauer und ungefährer Standort | Weitere Informationen zur Personalisierung der Werbung | nein |
| System-Tools (Verschiedenes) | Ermöglicht einen Überblick über installierte Apps | nein |

*Tabelle 1: Vergleich der geforderten und technisch notwendigen Zugriffsrechte der App „Brightest Taschenlampe" (vgl. Lamberty, 2012)*

### Rechtevergabe bei Android

Je nach Betriebssystem unterscheidet sich die Kontrolle und Vergabe der von der App eingeforderten Zugriffsrechte. Googles Betriebssystem Android basiert auf einem Berechtigungssystem, das zwischen einer Vielzahl unterschiedlicher Zugriffsberechtigungen unterscheidet.

| Android-Berechtigungen | |
|---|---|
| Name | Erläuterung |
| Telefonnummern direkt anrufen | Verleiht Apps die Möglichkeit, unbemerkt vom Anwender oder mit dessen Zutun Telefonnummern anzuwählen. |
| Kurznachrichten senden | Ermöglicht es Anwendungen, SMS zu versenden – entweder transparent für den Nutzer (mit dessen Zutun) oder unbemerkt. |

[15] *Stand: 18.08.2013*

| | |
|---|---|
| USB-Speicherinhalte ändern oder löschen | Erlaubt Zugriff auf den Gerätespeicher, sodass gespeicherte Daten ausgelesen, bearbeitet oder verändert werden können. |
| Kontakte lesen, Meine Kontakte ändern | Berechtigt eine Anwendung, auf die Kontakte des Anwenders zugreifen und diese verändern zu können. |
| YouTube, YouTube-Nutzernamen | Diese Berechtigungen ermöglichen Anwendungen den Zugriff auf das YouTube-Konto des Nutzers. |
| Lesezeichen für Webseiten setzen und das Webprotokoll aufzeichnen | Hiermit erhalten Apps Zugriff auf Browserdaten wie Verlauf und Lesezeichen. |
| Vertrauliche Protokolldaten lesen | Erlaubt es einer App, die Protokolldaten des Anwendersystems zu lesen. Die Protokolldaten enthalten meist sensible Informationen. |
| Telefonstatus lesen und identifizieren | Ermöglicht es einer App, zu ermitteln, ob mit dem Gerät des Nutzers telefoniert wird. Außerdem werden die Identifikationsnummern des Smartphones (IMEI und IMSI) übermittelt. |
| Genauer (GPS-)Standort | Ermöglicht Zugriff auf Standortdaten des Nutzers. |
| Ungefährer (netzwerkbasierter) Standort | Wie GPS, bloß ungenauer. |
| Bluetooth-Verbindungen herstellen | Voraussetzung, um Bluetooth-Verbindungen herzustellen. |
| Uneingeschränkter Internetzugriff | Berechtigt eine Anwendung dazu, eine Internetverbindung herzustellen und Daten zu versenden. |
| Netzwerkstatus/WLAN-Status anzeigen | Eine Anwendung erhält mit dieser Berechtigung Informationen über das genutzte Netzwerk (WLAN, 3G etc.). |
| Bekannte Konten suchen | Berechtigt eine App, Benutzerkonten des Anwenders zu suchen und sich mit ihnen zu verbinden. |
| Kontoliste verwalten | Mit dieser Berechtigung ist eine App in der Lage, bestehende Konten zu entfernen, Passwörter zu löschen oder neue Konten hinzuzufügen. |
| Als Kontoauthentifizierer fungieren | Ermöglicht einer Anwendung, Authentifizierungsfähigkeiten des Konto-Managers zu verwenden. Konten können so erstellt und abgerufen werden; Passwörter können festgelegt werden. |
| Google Mail: Konten auf dem Gerät verwenden, hinzufügen oder entfernen | Ermöglicht einer App den Zugriff auf das Google-Mail-Konto des Nutzers. |
| Install Packages (Apps installieren) | Berechtigt eine Anwendung dazu, andere Anwendungen zu installieren. |
| Über andere Apps ausführen | Hiermit kann eine App die Benutzeroberfläche anderer Apps verändern. |
| Standby-Modus deaktivieren | Berechtigt eine App dazu, den Standby-Modus auszuschalten. |
| Synchronisierungseinstellungen lesen | Berechtigt eine App dazu, festzustellen, ob im Hintergrund Synchronisationen laufen (z.B. mit Google Mail). |
| Hintergrundprozesse beenden | Ermöglicht einer App, andere laufende Apps zu beenden. |
| Sicherheitseinstellungen für das System ändern | Nur für Entwickler: Hiermit können Sicherheitseinstellungen des Systems verändert werden. |
| App permanent ausführen | Ermöglicht es einer App, einen Teil des Arbeitsspeichers permanent zu besetzen, um beispiels- |

| | |
|---|---|
| | weise schneller starten zu können. |
| Beim Start ausführen | Ermöglicht es einer App, bei Systemstart automatisch zu starten. |
| Vibrationsalarm steuern | Erlaubt es einer App, Vibrationsalarm auszulösen. |
| Bilder und Videos aufnehmen | Berechtigt zur Aufnahme von Fotos und Videos (bemerkt oder unbemerkt vom Nutzer). |

*Tabelle 2: Android-Zugriffsberechtigungen (vgl. Heister, 2012)*

***Das Berechtigungssystem unter Android funktioniert nach einem Alles-oder-Nichts-Prinzip.***

Dabei erhalten Android-Nutzer vor der Installation einer App einen Überblick über die Berechtigungen, die eine Anwendung zur Inbetriebnahme einfordert. Dies gilt sowohl für die Installation von Apps aus dem offiziellen Market als auch für die Installation von Apps aus Drittquellen. Das Berechtigungssystem unter Android funktioniert nach einem Alles-oder-nichts-Prinzip. Entweder der Nutzer akzeptiert alle geforderten Zugriffe oder die Installation der App muss abgebrochen werden. Eine Selektion einzelner Rechte ist nicht möglich.

Ausnahme ist Android ab der Version 4.3, hier ist ein nachträgliches Hinzufügen oder Entfernen der von einer App geforderten Rechte möglich.

### Rechtevergabe bei Apple iOS

Apples Betriebssystem iOS hat vor Version 6 kein vergleichbares Berechtigungssystem. Nutzer können hier lediglich entscheiden, ob Anwendungen Standortinformationen des Gerätes abfragen und senden dürfen. Standortinformationen sind beispielsweise auch in Fotos enthalten, sodass beim Zugriff auf die Mediengalerie ein entsprechender Dialog erscheint. Auf welche weiteren Ressourcen Apps zugreifen, ist für den Nutzer intransparent und unkontrollierbar. Er muss blind darauf vertrauen, dass die durch Apple geprüften Anwendungen des App Stores den Datenschutz der Nutzer gewährleisten. Aus diesem Grund erntete Apple viel Kritik, beispielsweise als bekannt wurde, dass die iOS-App des sozialen Netzwerks Path ungefragt die Adressbuchdaten der Nutzer auf den Unternehmensservern abspeichert (vgl. Süddeutsche.de, 2012).

***Ab iOS6 haben Apple-Nutzer die Möglichkeit, Zugriffsrechte bei App-Ausführung zu verwehren oder diese nachträglich zu entziehen.***

Als Reaktion auf die Kritik der Datenschützer führte Apple in der iOS-Version 6 mehr Kontrollmöglichkeiten für Nutzer ein. Anwender können nun analog zum Android-Berechtigungssystem Rechte gewähren, sobald eine App auf persönliche Daten oder andere Apps wie Facebook und Twitter zugreifen will. So obliegt die Entscheidung dem Nutzer, ob zum Beispiel auf Ortungsdienste, Kontakte und Fotos zugegriffen werden darf. Im Unterschied zum Google-Betriebssystem können Nutzer von iOS 6 jedoch auch nachträglich den Anwendungen Zugriffsrechte wieder entziehen.

| iOS-Berechtigungen | |
|---|---|
| Name | Erläuterung |
| Ortungsdienste | Ermöglicht einer App die Lokalisierung des Gerätestandorts. |
| Kontakte | Berechtigt eine App zum Lesen der Kontakte. |
| Kalender | Berechtigt eine App zum Zugriff auf den Kalender des Benutzers. |
| Erinnerungen | Ermöglicht es einer App, die Erinnerungen des Nutzers einzusehen. |
| Fotos | Ermöglicht einer App, Fotos aufzunehmen. |
| Bluetooth | Voraussetzung zur Nutzung der Bluetooth-Funktion einer App. |

| | |
|---|---|
| Mikrofon | Ermöglicht Zugriff auf das Mikrofon. |
| Aktivitätsdaten | Ermöglicht Zugriff auf Aktivitätsdaten, die anzeigen, wie lange der Besitzer eines iPhone 5s täglich gegangen, gerannt und Auto gefahren ist oder sich nicht bewegt hat, solange er das iPhone mit sich geführt hat. |
| Twitter und Facebook | Ermöglicht Apps den Zugriff auf das Nutzerkonto in den sozialen Netzwerken Facebook und Twitter. |

*Tabelle 3: iOS-Zugriffsberechtigungen (vgl. Aschermann, 2013)*

### Rechtevergabe bei Windows

Bei Smartphones mit Windows-Phone-Betriebssystem müssen Nutzer – analog zum Android-Berechtigungssystem – Apps alle geforderten Zugriffsrechte gewähren, um sie installieren zu können. Eine Übersicht der Zugriffsrechte und ihrer Bedeutung unter Windows Phone zeigt die Tabelle 4.

***Analog zum Android-Berechtigungssystem müssen Windows-Nutzer alle Zugriffsrechte gewähren, um eine Anwendung installieren zu können.***

| Windows-Phone-Berechtigungen | |
|---|---|
| Name | Erläuterung |
| Kalender | Mit dieser Berechtigung kann eine App Kalendereinträge des Nutzers lesen. |
| Kontakte | Berechtigt eine App dazu, die Kontakte des Nutzers zu lesen. |
| Identität des Handys | Berechtigt eine Anwendung dazu, die Identität des Smartphones sowie einige technische Gerätemerkmale zu ermitteln. |
| Identität des Eigentümers | App ist dazu berechtigt, die Windows Live Anonymous ID zu ermitteln. Diese ID erlaubt keine tatsächlichen Rückschlüsse auf den Handy-Besitzer (auch wenn dies der Name suggeriert). |
| Kamera | Erlaubt eine Anwendung den Zugriff auf die Gerätekamera. |
| Ortungsdienste | Berechtigt zum Zugriff auf die GPS-Koordinaten des Geräts. |
| Musik- und Videobibliothek | Berechtigt dazu, die Multimedia-Dateien des Gerätespeichers einzusehen und zu verändern. |
| Mikrofon | Ermöglicht einer App den Zugriff auf das Gerätemikrofon. |
| Datendienste | Erlaubt es einer Anwendung, eine Internetverbindung herzustellen. |
| Push-Benachrichtigungsdienst | Ermöglicht das Versenden von Push-Benachrichtigungen. |
| Bewegungs- und Richtungssensor | Erlaubt einer App den Zugriff auf die Sensoren des Telefons. |
| Xbox LIVE | Ermöglicht die Synchronisation mit dem Xbox-LIVE-Konto. |

*Tabelle 4: Windows-Phone-Zugriffsrechte (vgl. Kalus, 2013)*

Möchte sich ein Nutzer von Windows 8 oder Windows RT eine App aus dem Windows Store auf sein Laptop oder Tablet laden, erhält er auf der Beschreibungsseite im Store Auskunft darüber, welche Zugriffsrechte er mit der Installation der jeweiligen App bestätigt. Eine separate Einverständniserklärung wie bei Windows Phone wird nicht angezeigt. Er kann sich anschließend in den Einstellungen der App die freigegebenen Berechtigungen ansehen, jedoch nicht ändern.

***Im Unterschied zu Android können Windows 8-Nutzer geforderte Zugriffsrechte lediglich auf der Beschreibungsseite im Market ansehen; es gibt keinen dezidierten Dialog bei der App-Installation.***

### Rechtevergabe bei BlackBerry

***BlackBerry 10 ermöglicht auch die separate Freigabe bestimmter Zugriffsrechte beim Ausführen einer App.***

BlackBerry-Geräte haben unter BlackBerry 10 weitreichende Einstellmöglichkeiten bei der Rechtevergabe. Wenn Apps nach der Installation erstmals auf den Geräten ausgeführt werden, können Nutzer einzelne Anwendungsberechtigungen vergeben und andere ablehnen – außer, die Hersteller einer App machen die Freigabe sämtlicher Zugriffsrechte zur Nutzungsbedingung (ohne die Zustimmung sämtlicher Rechte kann die App dann gar nicht erst installiert werden), wie es oft bei importierten Android-Apps der Fall ist. Im Regelfall können Nutzer fortwährend Änderungen an der Rechtevergabe einer App vornehmen, um so Ressourcen-Zugriffe zu steuern. Sie erhalten in den Geräteeinstellungen zudem einen Überblick über sämtliche Berechtigungen, die installierte Apps erhalten haben.

### Malware-Anfälligkeit der Apps

Zusätzlich zur Problematik der Rechtevergabe kommt die Malware-Anfälligkeit der Apps. Es gibt keine fehlerfreie Software. Das bedeutet, dass potenziell jede Anwendung – auch wenn sie die Kontrollinstanzen der Markets erfüllt – Schwachstellen aufweist. Angreifer können diese ausnutzen, um Schädlinge auf die Geräte der Anwender zu überspielen und Daten abzugreifen.

## 2.3.3 Fokus WhatsApp – Instant Messenger mit Tücken

***WhatsApp ist eine der beliebtesten Apps überhaupt. Der Hersteller des Instant Messengers gilt allerdings nicht als besonders sicherheitsbewusst.***

Den WhatsApp-Messenger nutzen laut Herstellerangaben rund 600 Millionen Menschen (Stand August 2014) – damit gehört die App zu den beliebtesten überhaupt. Bei dieser Smartphone-Applikation handelt es sich um einen Dienst für den Nachrichtensofortversand (Instant Messaging). Im Gegensatz zu SMS werden die Nachrichten innerhalb der WhatsApp-Gespräche (Chats) über das Internet versandt (mithilfe der Mobilfunknetze oder über WLAN). Neben Textnachrichten ist auch der Versand unter anderem von Fotos, Video- und Audiodateien möglich.
Daraus ergibt sich die große Popularität der Applikation: Nutzer brauchen zunächst lediglich die Gebühren für die Nutzung des mobilen Internets zu zahlen, gesonderte Gebühren für SMS- oder MMS-Gebühren entfallen.
Im Februar 2014 kaufte Facebook WhatsApp auf. Die Übernahme wurde von zahlreichen Medienberichten begleitet und rief europäische Datenschützer auf den Plan. Mit Blick auf den hohen Kaufpreis von 19 Milliarden Dollar befürchten sie, dass Facebook vorhandene Nutzerdaten mit den personenbezogenen Daten der WhatsApp-Nutzer zusammenführen könnte, um Kapital daraus schlagen zu können. Außerdem kritisieren sie die Monopolstellung von Facebook, die sich aus der weitreichenden Konzentration der Kommunikation von Millionen Nutzern ergebe (vgl. z.B. Klemm, 2014; Kwasniewski, 2014)

## Sicherheitsrisiken bei Nutzung

Problematisch ist die Nutzung der Applikation aufgrund bekannt gewordener Sicherheitsprobleme, die die Medien attestierten[17]. WhatsApp überträgt laut dem ARD-Magazin Ratgeber Internet die Namen und Rufnummern seiner Nutzer unverschlüsselt an seine amerikanischen Server. Auf diesen würden auch sämtliche Gesprächsinhalte zunächst zwischengespeichert, bevor sie an die Empfänger weitergeleitet würden. Man wisse nicht, für wie lange die Daten dort genau gespeichert liegen, so der Journalist Jörg Schieb in der Sendung vom 17. August 2013 (Schieb, 2013).

***Gesprächsinhalte werden auf den Servern des Herstellers zwischengespeichert, bevor sie an den Adressaten übermittelt werden.***

Das Online-Nachrichtenportal Heise online hat Ende 2012 mehrfach deutlich gemacht, wie leicht sich die Account-Übernahme eines bestehenden WhatsApp-Nutzeraccounts für geübte Hacker gestaltete (vgl. Eikenberg, 2012). Die Redakteure benötigten lediglich die Seriennummer (IMEI) des Zielgeräts und die zugehörige Rufnummer – beides leicht zu erbeutende Informationen – und konnten infolge unter falschem Namen WhatsApp-Nachrichten senden und empfangen.
Erfolgsversprechenden Phishing- und Social-Engineering-Angriffen (siehe Kapitel *2.5 Phishing und Social Engineering*) war nach der Übernahme eines WhatsApp-Accounts Tür und Tor geöffnet. Mittlerweile ist das Problem zwar behoben, es ist aber immer noch symptomatisch für die marode Sicherheitsphilosophie des Unternehmens.

Viele Nutzer beklagen sich zudem über Nachrichten unbekannter Rufnummern, die Spam und Links zu Schadcode-kompromittierten Websites enthalten. Folgt ein Nutzer unbedacht diesen Links, kann es zu einer Vireninfektion seines Geräts kommen.
Das Bezahlsystem zur Abo-Verlängerung gilt ebenfalls als unsicher. Wie heise online berichtete, ist die Dateneingabe im Bezahlverfahren nicht mittels einer SSL-Verschlüsselung abgesichert (siehe Kapitel *4.4.1 HTTPS*), sondern erfolgt teilweise ungeschützt (vgl. Eikenberg, 2013). Befindet sich ein Angreifer im gleichen Netzwerk wie sein Opfer, beispielsweise im öffentlichen WLAN eines Cafés, könnte er durch einen Man-in-the-middle-Angriff sein Opfer auf eine präparierte Website lotsen, um sensible Finanzdaten wie Kreditkartendaten oder PayPal-Zugangsdaten vom Nutzer unbemerkt abzugreifen (siehe Kapitel *2.1.1 Wireless LAN (WLAN) und Hotspots*).

***„WhatsApp“ ist problematisch aufgrund bekannt gewordener Sicherheitsprobleme. Eine empfehlenswerte Alternativen ist beispielsweise die App „Threema“ mit echter Ende-zu-Ende-Verschlüsselung.***

Für Unternehmen ergeben sich aufgrund oben genannter Probleme Sicherheitsrisiken. Mitarbeiter die WhatsApp auf Geräten nutzen, die auch im dienstlichen Einsatz sind, versenden Telefonbuchdaten an Server in den USA.

Untersuchungen des Instituts für Internet-Sicherheit im Februar 2014 haben ergeben, dass WhatsApp eine RC4-Verschlüsselung für den Transport der Daten vom Smartphone zu ihren Servern verwendet. RC4 ist veraltet und unsicher, und beispielsweise von der NSA in Echtzeit zu brechen[18]. Bei WhatsApp handelt sich um eine App die keine Ende-zu-Ende-Verschlüsselung verwendet. Das bedeutet, spätestens auf den WhatsApp-Servern liegen die Gespräche, Bilder und Videos im Klartext.
Empfehlenswert ist eine echte Ende-zu-Ende-Verschlüsselung über alle Zwischenstationen, beispielsweise mit der App „Threema“. Bei dieser werden die Daten vom Versender selbst verschlüsselt und können nur vom Empfänger entschlüsselt werden. Hierfür ist es erforderlich, dass sich der eigene geheime Schlüssel sich nur im Besitz

[17] *Natürlich ist WhatsApp nicht der einzige Messenger mit Sicherheitsproblemen. Andere Messenger sind aber weitaus weniger verbreitet.*
[18] *http://www.internet-sicherheit.de/aktuelles/mitteilungen/nachricht/nachricht-detail/zdf-volle-kanne-dominique-petersen-spricht-uebe/*

der betreffenden Person befindet. Weiterführende Informationen im Kapitel *3.2.6 Datenverschlüsselungsmechanismen – Verschlüsselung der Kommunikation.*

### 2.3.4 Geschäftsmodell „Bezahlen mit persönlichen Daten“

Ein grundsätzliches Problem ist das vorherrschende Geschäftsmodell „Bezahlen mit persönlichen Daten“. Hierbei werden die Apps in der Regel kostenlos bereitgestellt, und der Benutzer „bezahlt“ die Apps mit seinen persönlichen Daten. Konkret bedeutet das: Die Finanzierung der App-Entwicklung erfolgt über die Vermarktung persönlicher Daten, die die Anbieter entweder weiter verkaufen oder nutzen, um personalisierte Werbung zu schalten.

## 2.4 E-Mail – von digitalen Postkarten und falschen Absendern

Die E-Mail ist ein einfach zu bedienendes, schnelles und weithin bekanntes Kommunikationsmittel. Es gibt kaum ein Unternehmen, das nicht per E-Mail zu erreichen ist oder E-Mails zur internen Kommunikation einsetzt. Aber auch bei dieser Technologie gibt es bestimmte Gefahren und Verhaltensregeln, auf die achtgegeben werden muss. Nachfolgend ein Überblick mit besonderem Fokus auf Risiken und Sicherheitsempfehlungen. Tiefer gehende technische Informationen in den Handbüchern Netzwerksicherheit und Rechtsverbindliche Kommunikation.

E-Mails

- Elektronische Post, die vom E-Mail-Server des Absenders (z.B. der des Betriebs) zu dem entfernten Server des Empfängers überstellt wird.
- Es wird zwischen drei Arten von Empfängern unterschieden: „An“, „CC“ (Kopie), „BCC“ (Blindkopie)
- Sobald eine E-Mail das eigene Netzwerk verlässt, kann kein Einfluss mehr darauf genommen werden, wie und über welche Server sie weitergeleitet wird

Risiken

- Unverschlüsselte und nicht signierte E-Mails sind theoretisch auf jeder Zwischenstationen komplett einseh- und auch veränderbar. Dies ist vergleichbar mit einer Postkarte, die mit einem Bleistift beschrieben wurde.
    - Einsehbar bedeutet, dass eine E-Mail auf ihrem Weg ohne besonderen technischen Aufwand mitgelesen werden kann: das Schutzziel der Vertraulichkeit ist nicht erfüllt.
    - Veränderbar bedeutet, dass der Absender und der Inhalt einer E-Mail leicht gefälscht werden können. Zudem sind die Zwischenstationen unbekannt – eine E-Mail von Düsseldorf nach Berlin kann auf ihrem Weg zum Beispiel über die USA geleitet werden. Das Schutzziel der Integrität ist nicht erfüllt.
- Einige Risiken unverschlüsselter und unsignierter E-Mails
    - Mitlesen und Veränderungen durch Dritte, zum Beispiel mit dem Ziel der Spionage
    - Vortäuschen falscher E-Mail-Absender durch Angreifer, zum Beispiel mit dem Ziel der gezielten Infektion mit einem Schadprogramm über den E-Mail-Anhang oder einen Link

Sicherheitsempfehlungen

- Versenden Sie keine sensiblen Daten in unverschlüsselten E-Mails.
- Verschlüsseln Sie Ihre E-Mails. Die häufigsten genutzten Technologien zur Verschlüsselung von E-Mails sind:
    - PGP (Pretty Good Privacy)
    - S/MIME (Secure/Multipurpose Internet E-Mail Extensions)
    - passwortverschlüsselte Anhänge
- Adressieren Sie mit Bedacht. Die Empfänger einer E-Mail können alle anderen „An“ und „CC“-Adressaten einsehen.
- Antivirenprogramme sollten automatisiert Anhänge beim Empfang von E-Mails überprüfen
- Prüfen Sie Anhänge vor dem Öffnen mit einem Anti-Viren-Programm.
- Denken Sie daran, dass Absender leicht gefälscht werden können. Seien Sie misstrauisch, wenn Sie verdächtige Inhalte von vertrauten Personen erhalten. Halten Sie im Zweifel telefonische Rücksprache.
- Prüfen Sie den Absender und den Betreff von E-Mails auf Glaubhaftigkeit, bevor Sie diese öffnen.
- Besuchen Sie keine Links in E-Mails, sofern Sie sich über die Vertrauenswürdigkeit der E-Mail nicht sicher sind.

***Hinter Spam kann sich auch ein Angriff auf sensible Daten verbergen. Links in Spam-Mails können auf Webseiten führen, die beispielsweise einen Trojaner direkt auf den Computer laden können.***

***Für weitere Informationen bezüglich Rechtsverbindlicher Kommunikation, nutzen Sie das gleichnamige Handbuch oder entsprechende Fachliteratur.***

### 2.4.1 Spam

Spam- und Junk-E-Mails („Müll-E-Mails“) sind Nachrichten mit unerwünschtem Inhalt. Statistisch gesehen haben neun von zehn E-Mails Spam zum Inhalt. Das Gros des massenhaft verschickten Spams beinhaltet Werbe- und Marketingbotschaften, die die Empfänger zum Kauf eines bestimmten Produkts bewegen sollen. Dabei handelt es sich meistens um die folgenden Produkte und Dienstleistungsangebote in absteigender Häufigkeit: Medikamente, Diätprodukte, Job-Angebote, Dating-Angebote und Glückspiele. Der Vielzahl an Werbebotschaften scheinen keine Grenzen gesetzt.

Teuer kann es für Empfänger von sogenanntem Scam werden, Betrugsversuchen, die ein Ziel verfolgen: das Geld der Empfänger. Betrüger verschleiern ihre Absichten, tarnen sich als seriöse Dienstleister oder harmlose Privatleute, um das Vertrauen der Empfänger zu gewinnen. In Kombination mit oft emotionalen Themen gelingt es Betrügern immer wieder, das Geld der Empfänger zu kassieren. Beispielsweise wenn sie in Nachrichten vorgeben, dass ihre Brieftasche im Urlaub geklaut worden sei und man ihnen doch bitte fünfzig Euro schicken solle, damit sie wieder nach Hause kommen könnten. Oder wenn sie im Namen einer Hilfsorganisation um Spenden für notleidende Kinder in Afrika bitten.

***Absender von Scam verschleiern ihre Absichten und appellieren beispielsweise an die Wohltätigkeit der Empfänger.***

***Nutzen Sie Spam-Filter (zum Beispiel vom E-Mail-Provider), um Ihr Postfach möglichst frei von Spam zu halten.***
***Antworten Sie niemals auf Spam-Mails. Sonst erfährt der Versender, dass Ihre E-Mailadresse wirklich existiert und sendet Ihnen noch mehr Spam.***

***Kaufen Sie keine über Spam beworbene Ware.***

## 2.5 Phishing und Social Engineering

***Phishing-Mails kommen oft im Gewand bekannter Unternehmen und Banken daher, um persönliche Daten der Adressaten abzugreifen.***

Als Unterkategorie von Scamming, dem Trickbetrügen, zielt Phishing auf das Fischen personenbezogener Daten ab. Hier tarnen sich Betrüger beispielsweise als vertrauenserweckende Unternehmen, um an Kundendaten zu kommen. In Nachrichten, die beispielsweise in ihrer Optik und ihrem Stil dem Corporate Design einer Bank nachempfunden sind, bitten sie dann um die Verifizierung der Kundendaten auf einer Internetseite, die in den Nachrichten verlinkt ist. Folgt das nichtsahnende Opfer dann diesem Link, gelangt es auf eine präparierte Website der Betrüger, die ebenfalls in der Optik des Unternehmens gestaltet ist. Werden hier sensible Bankdaten eingegeben, können Betrüger diese fischen und in Konsequenz das Bankkonto des Opfers leerräumen.

### Ein sympathischer Datendieb am Telefon

***Beim Social Engineering Angriffe werden die Gutgläubigkeit und das Vertrauen der Opfer ausgenutzt, um im persönlichen Kontakt sensible Unternehmensdaten abzugreifen.***

Die Betrugsform des Social Engineering („soziale Manipulation“) beinhaltet gegenüber dem Phishen stärker eine zwischenmenschliche Komponente. Ziel der kriminellen Bestrebungen ist es, Personen unter Vortäuschung falscher Tatsachen zu bestimmten Handlungen zu bewegen. Im Unternehmenskontext versuchen Angreifer häufig Mitarbeitern die Zugangsdaten zum Unternehmensserver oder andere sensible Unternehmensinformationen zu entlocken. Die konkreten Angriffe können unterschiedliche Formen annehmen und aufeinander aufbauen. Grundsätzlich suchen Angreifer Kontakt zu Mitarbeitern, die im Besitz vertraulicher Informationen sind. Telefonisch, in sozialen Netzen oder im persönlichen Gespräch geben sie sich als Angehörige des Unternehmens aus, erwecken Sympathie und suggerieren durch bruchstückhafte Informationsfetzen Kenntnis vom Betriebsalltag des Mitarbeiters. Haben sie das Vertrauen des Opfers gewonnen, gelingt es ihnen leicht, Informationen zu erhalten. Beispielsweise könnte eine Person, die sich als Techniker aus der IT-Abteilung ausgibt, um die Zugangsdaten eines Mitarbeiters bitten, damit ein Arbeitsschritt abgeschlossen werden könne. Oder aber eine Person im blauen Overall gibt sich als Handwerker aus und erbittet Zugang zum Büro des Chefs, um Reparaturen durchzuführen. Gezieltes Social Engineering kann verheerende Folgen für ein Unternehmen haben, sofern Mitarbeiter nicht ausreichend sensibilisiert wurden. Die Skala der finanziellen Schäden ist nach oben hin offen.

## 2.6 Unsichere Arbeitsumgebung

Zug, Bus und U-Bahn bieten keine sicheren Arbeitsumgebungen. Im vollbesetzten Verkehrsmittel ist es nicht schwer, Blicke auf die immer größeren Displays der Geräte zu erhaschen. Sitznachbarn haben bisweilen die Gelegenheit, vertrauliche E-Mails oder sogar Kennwörter mitzulesen. Hinzu kommt noch, dass öffentliche WLAN-Netze für den Internetzugang genutzt werden, was bei fehlenden Verschlüsselungsmechanismen gefährlich sein kann (siehe Kapitel *2.1 Wireless LAN (WLAN) und Hotspots*).

***Mitarbeiter gehen beim Arbeiten in unsicherer Umgebung ein großes Risiko ein. Bei besonders fahrlässigem Verhalten müssen sie persönlich haften.***

Trotzdem ist die Nutzung mobiler Endgeräte im öffentlichen Personennahverkehr für viele Menschen sehr attraktiv: Die Hälfte aller Befragten einer Nutzungsstudie des börsennotierten Internetunternehmens Tomorrow Focus AG greifen während der Zugfahrt oder im Flughafen häufig oder sehr häufig zu ihrem Smartphone oder Tablet, um im Internet zu surfen (vgl. Tomorrow Focus Media, 2013). Es ist fraglich, wie viele schnell noch eben die Mails vom Chef beantworten, folgt doch die E-Mail-Korrespondenz laut der Studie an Position zwei der meistgenutzten Smartphone-Funktionen (ebenda). Mitarbeiter gehen beim Arbeiten in frequentierten Umgebungen

ein großes Risiko ein und haften unter Umständen bei grob fahrlässigem Verhalten für etwaige Datenpannen (siehe Kapitel *2.10.3 Datenschutzanforderungen*)

## 2.7 Risiko Jailbreaking und Rooting

***Jailbreaking/Rooting hebelt Sicherheitsmechanismen aus, die der Zugriffsrechtebeschränkung dienen. Kommt es zur Malware-Infektion, ist das manipulierte Gerät schutzlos ausgeliefert.***

Jailbreaking (im Deutschen: „Gefängnisausbruch“) bezeichnet einen technischen Eingriff in das Dateiverzeichnis von Apple-Geräten wie iPhones, iPads, iPods, Apple-TVs mit dem Zweck, Nutzungsbeschränkungen zu entfernen. Dabei wird das von Apple abgeschirmte Dateisystem „aus seinem Gefängnis aufgesperrt“, sodass die Erweiterung des Funktionsumfangs und die Installation von nicht genehmigter Drittanbietersoftware möglich werden. Eine Hauptmotivation für Jailbreaking fußt in dem Wunsch, Apps aus anderen Quellen als dem offiziellen App Store installieren zu können. Auf diese Weise können auch illegale Software-Kopien kostenpflichtiger Apps auf die Geräte geladen werden, ohne dass hierfür bezahlt werden muss. Mit der Geräte-Modifikation erlischt nicht nur die Herstellergarantie, sie ist unter Sicherheitsaspekten auch sehr gefährlich. Anwendungen, die abseits des offiziellen App Stores angeboten werden, unterliegen nicht der Sicherheitskontrolle durch Apple. Das Risiko einer Malware-Infektion aufgrund kompromittierter Software ist hier höher. Der vergleichbare Vorgang bei Android-Geräten nennt sich Rooting. Bei dem Root-Recht handelt es sich unter Android um ein Zugriffsrecht, welches nicht nur dem Nutzer, sondern auch Apps einen tiefen Zugriff auf das System gewährt. Der Nutzer verliert hier die Kontrolle über das Gerät. Damit birgt Rooting Gefahren und ist nicht zu empfehlen.

## 2.8 Geräteverlust und -diebstahl

***Jeder zehnte Deutsche hat laut BITKOM sein Handy schon einmal verloren. Geräteverlust ist ein großes Sicherheitsrisiko für Unternehmen.***

Laut Statistik werden innerhalb eines halben Jahres circa 64.000 Mobiltelefone, Laptops, Handhelds und USB-Sticks in Londoner Taxis liegengelassen (vgl. Karpf, 2006[19]; Fischermann, 2012). Untersuchungen des Bundesverbands Informationswirtschaft, Telekommunikation und neue Medien (BITKOM) ergaben, dass jeder zehnte Deutsche (7,7 Millionen) sein Handy schon einmal verloren hat (vgl. BITKOM, 2012b). Weiteren 3,5 Millionen Bundesbürgern wurde das Mobiltelefon gestohlen, 2,8 Millionen wissen nicht, ob sie ihr Gerät verloren haben oder es gestohlen wurde (ebenda)[20]. Diese Zahlen illustrieren die hohe Wahrscheinlichkeit eines Geräteverlusts. Einer Studie des Sicherheitsherstellers Check Point zufolge, beurteilen IT-Verantwortliche den Verlust mobiler Endgeräte als gefährlichstes Szenario in Hinblick auf die Sicherheit der auf den Geräten gespeicherten Daten (vgl. Checkpoint Software Technologies Ltd, 2013)[21]. Sicherheitsexperten des Instituts für Internet-Sicherheit der Westfälischen Hochschule bestätigen, dass es Dieben trotz Zugriffssperre in der Regel möglich ist, unverschlüsselt gespeicherte Daten auf den erbeuteten Geräten abzugreifen, sofern sie den nötigen Ehrgeiz mitbringen (vgl. Fischermann, 2012). Ein Beispiel: Ein nicht verschlüsseltes Notebook kann von einer Boot-CD gestartet werden. Der Zugriff auf alle Daten, die unverschlüsselt auf der Festplatte liegen, ist dann ohne Enschränkun-

[19] *Im Detail: 55.000 Mobiltelefone, 5.000 Handhelds, 3.000 Laptops und 900 USB-Sticks. Da diese Zahlen zuletzt 2006 von der Sicherheitsfirma Pointsec erhoben wurden, ist davon auszugehen, dass die Anzahl verlorener Geräte heute noch höher ausfallen dürfte.*

[20] *Durchgeführt wurde die repräsentative Befragung vom Marktforschungsinstitut Forsa, das 1.003 Personen ab 14 Jahren befragte. Insgesamt haben 14 Millionen Deutsche schon einmal ihr Handy verloren oder es ist ihnen gestohlen worden.*

[21] *In der Stichprobe enthalten sind 790 IT-Verantwortliche aus den USA, Kanada, Großbritannien, Japan und Deutschland*

gen möglich. Die Anmeldung im Betriebssystem, beispielsweise Windows oder Linux, kann so vollständig übergangen werden. Alternativ könnte die Festplatte leicht ausgebaut werden. Haben Mitarbeiter private Geräte verloren, die sie dienstlich genutzt haben, kann dies unter Umständen rechtliche Konsequenzen für sie nach sich ziehen (siehe Kapitel *2.10 Rechtliche Risiken*).

## 2.9 Schützenswerte Smartphone-Ressourcen

Nachfolgend eine Übersicht über schützenswerte Hardware- und Software-Ressourcen bei Smartphones. Diese kann als Zusammenfassung vorangegangener Risiken betrachtet werden und soll den vertrauensvollen Umgang mit bestimmten Smartphone-Bereichen fördern.

| Schützenswerte Ressourcen eines Smartphones | | |
|---|---|---|
| Anwendung | Schutzbedarf | Begründung |
| Kamera | hoch | Bilder oder Videos von Personen oder Gegenständen können erstellt und gespeichert werden, ohne dass eine Einwilligung besteht. |
| Mikrofon | hoch | Durch den Zugriff auf das eingebaute Mikrofon kann ein Gerät zur Abhöreinrichtung (Wanze) umfunktioniert werden. Private Gespräche können mitgeschnitten und gespeichert werden, ohne dass eine Einwilligung besteht. |
| GPS | hoch | Bewegungsprofile können erstellt werden. |
| NFC-Chip | hoch | Mit Hilfe des NFC-Chips und der Google-Wallet-Anwendung kann ein Benutzer kleinere Beträge überweisen. Erhält ein Angreifer das Passwort für das Google-Konto des Nutzers kann er die Signatur des Chips aufzeichnen und das Konto des Besitzers belasten. |
| Telefonbuch | hoch | Das Telefonbuch speichert nicht nur persönliche Daten, sondern auch Daten Dritter, was einen erhöhten Schutzbedarf begründet. |
| SMS-Anwendung | hoch | Wie auch im Telefonbuch stehen in SMS die Rufnummern der Absender. Des Weiteren findet hier persönliche Kommunikation statt, die geschützt werden muss. |
| Gespeicherte Passwörter | sehr hoch | Passwörter sind beispielsweise unter Android im Klartext gespeichert und können deshalb vom Angreifer frei verwendet werden. Je nach Art der Passwörter kann ein beträchtlicher Schaden angerichtet werden. |
| Speicherkarte (z.B. SD-Karte) | hoch | Die SD-Karte wird oft als Dateiablage sensibler Daten (beispielsweise für Backups) genutzt. Sie ist hoch schutzbedürftig, da sie einerseits sehr leicht aus dem Gerät entwendet und ausgelesen werden kann und andererseits, weil sämtliche (auch unsichere) Anwendungen freien Zugriff auf dort gespeicherte Daten haben, ohne dabei eine Berechtigung einholen zu müssen. |

*Tabelle 5: Schützenswerte Smartphone-Ressourcen (vgl. Lamberty, 2012)*

## 2.10 Rechtliche Risiken

Mit Einführung eines BYOD-Konzepts im Unternehmen gehen zusätzliche rechtliche Risiken einher, die es im Vergleich zur Nutzung firmeneigener Geräte nicht gibt.
Wilfried Reiners, Rechtsanwalt mit Schwerpunkt auf IT-Recht, rät entschieden davon ab, Privatgeräte der Mitarbeiter für betriebliche Zwecke einzusetzen: „Bring Your Own Device bedeutet nach heutigem Recht, stets Datenschutzrechte zu verletzen. Es gibt keine technische Möglichkeit, dies zu verhindern – Unternehmen können also voll haftbar gemacht werden.“ Demnach begehen zahlreiche Unternehmen Rechtsverletzungen, für die sie oft erst im Fall einer publik gewordenen Datenpanne auch tatsächlich belangt werden. Grund dafür ist ein veraltetes Datenschutzgesetz, das sich gegenüber heutigen Nutzungsgewohnheiten unflexibel zeigt. Einzige rechtssichere Möglichkeit in Zusammenhang mit BYOD ist laut Reiners, mit dem Kunden einen Vertrag zur Auftragsdatenverarbeitung abzuschließen, der die Datenweitergabe an Dritte ausdrücklich gestatte. Solch ein circa 15-seitiges Dokument im Vorfeld einer Dienstleistungserbringung zu verlangen, sei aber verständlicherweise höchst unüblich, so Reiners weiter. Für ihn ist klar: „Die hohen rechtlichen Risiken und der mögliche Schaden stehen in keinem Verhältnis zur kurzsichtigen Kosteneinsparung.“
Das Kapitel 7. *Umgang mit BYOD im Betrieb* behandelt die weitere Vorgehensweise, sofern sich ein Betrieb für ein BYOD-Konzept entscheiden sollte.

***BYOD birgt weitaus größere rechtliche Risiken als der ausschließliche Einsatz unternehmenseigener Geräte.***

***Einzige rechtssichere Option laut Rechtsanwalt Reiners: Ein Vertrag zur Auftragsdatenverarbeitung, der die Datenweitergabe an Dritte ausdrücklich gestatte.***

### 2.10.1 Trennung von privaten und beruflichen Daten

Unternehmen tragen für dienstliche, insbesondere für personenbezogene Daten, die volle Verantwortung. Daraus ergibt sich für die Unternehmensleitung die Pflicht, die Erhebung, Nutzung und Verarbeitung personenbezogener Unternehmensdaten, wie beispielsweise Kunden-Stammdaten, vollständig und zu jedem Zeitpunkt zu kontrollieren. Eine Kontrolle der Unternehmensdaten durch den Arbeitgeber ist allerdings nur möglich, sofern hierdurch keine privaten Daten der Mitarbeiter eingesehen, kopiert, verändert oder gelöscht werden. Ein solcher Konflikt besteht dann, wenn Mitarbeiter auf dienstlich genutzten Privatgeräten sowohl private als auch Unternehmensdaten speichern, ohne sie voneinander technisch zu separieren. Dann hat der Arbeitgeber keine Möglichkeit, Unternehmensdaten einzusehen, ohne dabei private Daten der Mitarbeiter zu tangieren. Als Konsequenz verliert er die Kontrolle über die Unternehmensdaten, sodass er entsprechend §7 BDSG haftbar gemacht werden kann, sofern der entsprechende Mitarbeiter gegen die Datenschutzanforderungen des Bundesdatenschutzgesetzes verstößt (siehe Kapitel 2*.10.3 Datenschutzanforderungen*). Ein weiteres Beispiel für einen Kontrollverlust des Arbeitgebers entsteht durch einen Konflikt mit dem Fernmeldegeheimnis, das im nachfolgenden Kapitel behandelt werden soll.

***Die Vermischung von privaten und Unternehmensdaten bedeutet die Verletzung der Kontrollpflicht des Arbeitgebers. Er kann keine Unternehmensdaten mehr einsehen, ohne private Daten der Mitarbeiter zu tangieren.***

### 2.10.2 Fernmeldegeheimnis

***Nutzen Mitarbeiter das Betriebstelefon oder den beruflichen E-Mail-Account auch privat, darf der Arbeitgeber keine Inhalts- und Verbindungsdaten speichern.***

Das Fernmeldegeheimnis kollidiert dann mit der Kontrollpflicht des Arbeitgebers für personenbezogene Unternehmensdaten, wenn er seinen Mitarbeitern gestattet, das betriebliche E-Mail-Konto auch für private Zwecke zu nutzen. In diesem Fall wird der Arbeitgeber nämlich qua Telekommunikationsgesetz zu einem „Anbieter von Telekommunikationsdienstleistungen". Entgegen der oft vorherrschenden Meinung erbringen auch Unternehmen, die Telekommunikationsanlagen für private Nutzung ohne Gewinnerzielungsabsicht bereitstellen, „Telekommunikationsdienstleistungen geschäftsmäßig" (§3 Nr.10 TKG). Dabei ist unerheblich, ob der Arbeitgeber die private Nutzung des betrieblichen Accounts ausdrücklich gestattet – sogar bei Duldung der privaten Nutzung, also bei Nicht-Sanktionierung dieser, greift das Gesetz. Als Konsequenz ist der Arbeitgeber zum Schutz des Fernmeldegeheimnisses seiner Mitarbeiter verpflichtet (§88 TKG). Infolge darf er – bis auf ausdrückliche Ausnahmen (vgl. Institut für IT-Recht, 2010) – keine Inhalts- oder Verbindungsdaten des betrieblichen Accounts mehr überwachen (z.B. bei E-Mail-Archivierung). Er hat dann keine Möglichkeit mehr, Unternehmensdaten in E-Mails zu kontrollieren, sodass er durch den Verstoß des Bundesdatenschutzgesetzes haftbar gemacht werden kann.

### 2.10.3 Datenschutzanforderungen

An dieser Stelle soll ausdrücklich daraufhin gewiesen werden, dass trotz Umsetzung aller nachfolgenden Schutzmaßnahmen weiterhin ein großes Risiko der Rechtsverletzung besteht.

Das Bundesdatenschutzgesetz ist die Grundlage aller Schutzauflagen für den Umgang mit personenbezogenen Daten, die ein Unternehmen einhalten muss. Dem Datenschutzbeauftragten im Unternehmen kommt die Aufgabe zu, die Mitarbeiter auf die Einhaltung der dort festgeschriebenen Anforderungen zu sensibilisieren und zu verpflichten (Hinweise zum Datenschutzbeauftragten im Handbuch *Datenschutz*).

Bei Verstößen gegen das BDSG kann das Unternehmen haftbar gemacht werden. Ausschlaggebend sind der Paragraf neun und die zugehörige Anlage:

***Die Anlage zu §9 BDSG legt die zu treffenden Datenschutzmaßnahmen im Unternehmen fest.***

*„Öffentliche und nicht-öffentliche Stellen, die selbst oder im Auftrag personenbezogene Daten erheben, verarbeiten oder nutzen, haben die technischen und organisatorischen Maßnahmen zu treffen, die erforderlich sind, um die Ausführung der Vorschriften dieses Gesetzes, insbesondere die in der Anlage zu diesem Gesetz genannten Anforderungen, zu gewährleisten. Erforderlich sind Maßnahmen nur, wenn ihr Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht."* (§9 BDSG)

Die Anlage zu diesem Gesetzestext beinhaltet acht Kontrollen personenbezogener (Kunden-)Daten, aus denen sich direkte Maßnahmen ableiten lassen. Diese sollen nachfolgend dargestellt werden (vgl. hier und im Folgenden BITKOM, 2013a).

*„Dabei sind insbesondere Maßnahmen zu treffen, die je nach der Art der zu schützenden personenbezogenen Daten oder Datenkategorien geeignet sind […]."* (Anlage zu §9 Satz 1 BDSG)

### Zutrittskontrolle

*„[…] 1. Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren […].“*

Unternehmen sind in der Pflicht, den physischen Zutritt zu EDV-Anlagen, auf denen personenbezogene (Kunden-)Daten verarbeitet oder gespeichert werden, außenstehenden Personen zu verwehren. Dies kann im Fall von Server- oder Büroräumen durch eine verschließbare Tür und weitere Sicherheitsmechanismen umgesetzt werden. Bei mobilen Endgeräten ist die Umsetzung dieser Anforderungen jedoch kaum möglich. Im besten Fall gelingt es Arbeitgebern, mit den Mitarbeitern Aufbewahrungspflichten zu vereinbaren, sodass die Geräte bei Nicht-Benutzung besser vor dem Zugriff Unbefugter geschützt sind.

***Die Zutrittskontrolle ist bei mobilen Endgeräten praktisch nicht umzusetzen.***

### Zugangskontrolle

*„[…] 2. zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können […].“*

Der Zugang zu EDV-Anlagen muss technisch abgesichert werden. Authentifikationen der zur Verarbeitung der Daten beauftragten Personen sind unumgänglich. Diese werden in der Praxis über Zugriffssperren durch Passwörter, zusätzlichem Besitz (z.B. Chipkarten) et cetera realisiert. Mit dem Grad der Sensibilität der Daten steigt auch der Sicherheitsanspruch an die zu treffende Zugangskontrolle. Probleme in Zusammenhang mit BYOD können sich dadurch ergeben, dass Unbefugte Zugang zu den Privatgeräten der Mitarbeiter erhalten, auf denen personenbezogene Daten verarbeitet werden können oder gespeichert sind. Dies kann schnell passieren, beispielsweise wenn sich Familienangehörige, Freunde oder Bekannte das Smartphone des Mitarbeiters „nur mal schnell zum Telefonieren ausleihen“. Richtlinien hierfür werden in Kapitel 4.1 beschrieben. Auch bei Wartungs- und Supportarbeiten am privaten Gerät durch Dritte können Verstöße des Bundesdatenschutzgesetzes vorkommen, sofern Mitarbeiter im Vorfeld keine entsprechenden Schutzmaßnahmen treffen (z.B. Löschung der sensiblen Daten; spezielle Zugriffssperren für genutzte Dienste).

***Die Anforderungen Zugangs- und Zugriffskontrolle können unter anderem mittels Zugriffssperren, Berechtigungssystem, strengem App-Rechtemanagement und klar definierten Datenspeicherungsroutinen umgesetzt werden.***

### Zugriffskontrolle

*„[…] 3. zu gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können […].“*

Mithilfe der oben genannten Authentifikationen sollte im Unternehmen ein Berechtigungssystem (auch innerhalb verschiedener Software-Produkte) einhergehen, dass den Zugriff des Mitarbeiters auf diejenigen Daten beschränkt, die er für seinen Tätigkeitsbereich benötigt. Andernfalls können sich schnell Probleme mit der Norm der Zugriffskontrolle einstellen, beispielsweise wenn der Vertrieb im Unternehmen auch Zugriff auf Daten der Buchhaltung hat, obwohl er sie nicht benötigen würde (betriebsinterner Konflikt). In der Praxis ist zu beobachten, dass die Ausdifferenzierung der Zugriffsrechte mit der Unternehmensgröße steigt. In einem Drittel aller kleinen Handwerksbetriebe (unter zehn Mitarbeiter) haben alle Mitarbeiter uneingeschränkten Zugriff auf sämtliche Daten (vgl. IT-Sicherheit im Handwerk, 2013).
Verstöße sind unternehmensextern denkbar, wenn auf privaten Geräten der Mitarbeiter Apps mit weitreichenden Zugriffsrechten und Internetverbindung installiert sind, die

gegebenenfalls sensible Unternehmensdaten auslesen und kopieren können. Gleiches gilt auch für schädliche Anwendungen, die oft darauf abzielen, personenbezogene Daten abzugreifen. Auch die Synchronisation mit öffentlichen Cloud-Diensten, beispielsweise mit der Absicht zur Datensicherung, kann den Kontrollverlust über die Daten zur Folge haben, da nicht ausgeschlossen werden kann, dass Unbefugte (z.B. die Betreiber der Cloud-Server) die Daten einsehen und kopieren können.
***Für weitere Informationen bezüglich Cloud-Computing, nutzen Sie das gleichnamige Handbuch oder entsprechende Fachliteratur.***

### Weitergabekontrolle

*„[…] 4. zu gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist […].“*

Die Kontrolle der Weitergabe personenbezogener Daten steht in Korrespondenz mit der zuvor genannten Zugriffskontrolle. Im Fokus der Datenschutzbemühungen sollte die Einschränkung der Kopiermöglichkeit personenbezogener Daten, die Verwendung sicherer Kommunikationswege sowie die sichere Speicherung der Daten stehen. Das Risiko des Datenabflusses beziehungsweise Datendiebstahls ist groß und die Verlustmöglichkeiten vielfältig. In Zusammenhang mit BYOD sind die verantwortungslose Speicherung sensibler Daten auf den Geräten, die Verwendung unverschlüsselter Kommunikation, die Nutzung unsicherer Anwendungen und (Cloud-)Dienste sowie fehlende Diebstahlschutzmaßnahmen zu beobachten. Letztere betreffen auch das Vorgehen bei gestohlenen Geräten. Werden im Vorfeld keine Notfallpläne erstellt und keine (rechtlich unverbindliche) Vereinbarung zur Löschung auch der privaten Daten des Geräts vereinbart, können immense Schäden entstehen, von denen der Arbeitszeitverlust noch der geringste ist. Versenden Mitarbeiter sensible Daten in einer unverschlüsselten E-Mail können sie von Angreifern so leicht gelesen werden wie von einer Postkarte der analogen Briefpost. Dabei schreibt die Anlage des Bundesdatenschutzgesetzes ebenfalls vor, geeignete Verschlüsselungsmechanismen für den Transport der Daten zu wählen:
*„Eine Maßnahme nach Satz 2 Nummer 2 bis 4 ist insbesondere die Verwendung von dem Stand der Technik entsprechenden Verschlüsselungsverfahren.“*

***Sichere (verschlüsselte) Kommunikationswege und ein verantwortungsvoller Geräteumgang impliziert die Weitergabekontrolle.***

Die Verschlüsselung sollte dabei nicht nur den Kommunikationsweg schützen (beispielsweise mithilfe einer VPN-Verbindung, siehe Kapitel *4.4.2. VPN*), sondern auch die Daten selbst mithilfe geeigneter Software wie beispielsweise TrueCrypt[22]. Einige Einsatzmöglichkeiten von TrueCrypt zeigt ein Onlineworkshop im Videoformat[23].

***TrueCrypt wird aktuell nicht weiterentwickelt, steht aber immer noch in Version 7.1a zur Verfügung. Ein unabhängiges Audit [24]hat darüber hinaus ergeben, dass diese Version als sicherer einzuschätzen ist.***

[22] *http://www.heise.de/download/truecrypt.html*
[23] *http://www.internet-sicherheit.de/institut/buch-sicher-im- internet/videos/screenvideos/?tx_bddbflvvideogallery_pi1%5Bvideo%5D=11*
[24] *https://opencryptoaudit.org/reports/iSec_Final_Open_Crypto_Audit_Project_TrueCrypt_Security_Assessment.pdf*

### Eingabekontrolle

*„[…] 5. zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind […].“*

Die Zuordnung von EDV-Tätigkeiten zu bestimmten Personen sind in Unternehmen zu protokollieren. Eine mögliche Abhilfe, die jedoch einen hohen technischen Aufwand erfordert, kann mittels Data Loss Prevention erfolgen. An Grenzen stoßen solche Systeme da, wo die Gefahr besteht, dass versehentlich private Daten der Mitarbeiter aufgezeichnet werden. Dies ist insbesondere bei der Protokollierung privater IT beziehungsweise bei Speicherung der Zugangs- und Inhaltsdaten des auch privat genutzten betrieblichen E-Mail-Accounts der Fall (siehe Kapitel *2.10.2 Fernmeldegeheimnis*). Dieser Umstand bestärkt nochmal die Norm zur Trennung von privaten und beruflichen Daten (Kapitel *2.10.1 Trennung von privaten und beruflichen Daten*).

***Protokollierungssysteme wie die Data Loss Prevention helfen bei der Eingabekontrolle.***

### Auftragskontrolle

*„[…] 6. zu gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können […].“*

Während die Unternehmensleitung bei unternehmenseigener IT der Norm der Auftragskontrolle noch relativ leicht nachkommen kann, stehen ihr bei Privatgeräten der Mitarbeiter hier weniger Kontrollmöglichkeiten zur Verfügung. Überprüfte die Unternehmensleitung die Arbeitsprozesse der Mitarbeiter, die auf ihren privaten Smartphones oder Tablets ablaufen, umfassend, käme es bei unsachgemäßer Trennung von privaten und beruflichen Daten zu Datenschutzkonflikten. Selbst bei ordnungsgemäßer Separierung der beiden Bereiche wäre die Akzeptanz einer solchen als Überwachungsmaßnahme empfundenen Kontrolle bei den Mitarbeitern sehr gering. Der Mittelweg liegt in der Sensibilisierung des Mitarbeiters in Verbindung mit einem Vertrauensvorschub: Der Mitarbeiter sollte so verantwortungsvoll wie möglich mit den Unternehmensdaten auf seinem Privatgerät umgehen. Ihm sollte bewusst gemacht werden, dass Aufsichtsbehörden jeder Zeit die Möglichkeit eingeräumt werden muss, die Unternehmensdaten auf dem Gerät einsehen zu können. Auch hier sei noch einmal erwähnt, dass bei Verstößen des Mitarbeiters gegen das Bundesdatenschutzgesetz das Unternehmen voll haftbar gemacht werden kann.

***Auftragskontrolle ist in Zusammenhang mit BYOD schwierig umzusetzen. Der Arbeitgeber muss jederzeit die Möglichkeit haben, Unternehmensdaten auf den Privatgeräten einzusehen.***

### Verfügbarkeitskontrolle

*„[…] 7. zu gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind […].“*

Die Verfügbarkeitskontrolle ist dann verletzt, wenn das Unternehmen nicht geeignete Backup-Routinen für personenbezogene Daten hat und/oder geeignete Notfallpläne (z.B. bei Diebstahl) und Datenwiederherstellungsoptionen fehlen. Bei Störung oder Verlust der Geräte sind die Daten dann verloren, sodass die Norm der permanenten Verfügbarkeitskontrolle verletzt ist. Auch ist denkbar, dass genutzte Cloud-Dienste vorrübergehend ausfallen, sodass die Daten zeitweise nicht mehr verfügbar sind (weitere Hinweise hierzu im Handbuch *Cloud-Computing*). Die permanente Verfügbarkeit ist auch verletzt, wenn Mitarbeiter krank oder beurlaubt sind und die Unternehmensleitung zeitweise keine Möglichkeit hat, auf die auf dem Privatgerät gespeicherten Daten zuzugreifen.

***Backup-Routinen und Notfallpläne für den Diebstahlschutz werden in Zusammenhang mit der Verfügbarkeitskontrolle relevant.***

Von den Backup-Mechanismen sensibler Daten auf Geräten in Mitarbeitereigentum sollten private Daten der Mitarbeiter ausgenommen sein, da andernfalls der Datenschutz dieser verletzt werden würde. Im besten Fall verbleiben alle Geschäftsdaten auf dem Unternehmensserver und werden nicht lokal auf den genutzten Mobilgeräten gespeichert. Für die Vereinbarung der Vorgehensweise im Fall eines Geräteverlusts ist entscheidend, dass Arbeitgeber und Arbeitnehmer sich nicht nur darauf einigen, ob auch die privaten Daten des Mitarbeiters via Fernlösch-Funktion gelöscht werden dürfen. Sondern auch, in welcher Regelmäßigkeit ein Backup der privaten Daten erfolgt. Auf diese Weise kann der persönliche Schaden reduziert werden.

**Trennungsgebot**

*„[…] 8. zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.“*

***Die Trennung von privaten Unternehmensdaten ist Voraussetzung für die Einhaltung einiger der zuvor genannten Kontrollpflichten.***

In Zusammenhang mit BYOD unterstreicht das Trennungsgebot noch einmal die Relevanz der Trennung zwischen privaten und beruflichen Daten auf den genutzten Geräten. Die zu verschiedenen Zwecken erhobenen personenbezogenen Daten sollten technisch nicht untereinander und schon gar nicht mit privaten Daten der Mitarbeiter vermengt werden. Eine physische (räumliche) Trennung ist jedoch nicht notwendig und auch nicht möglich. Möglichkeiten zur technischen Umsetzung der Trennung werden in Kapitel 5.4.3 behandelt.

### 2.10.4 Datenverlust

Meist sind es menschliche Ursachen, die einen Datenverlust zur Folge haben. Mitarbeiter sind oft nicht geschult in Sachen Datenschutz, sodass sie unachtsam mit Unternehmensdaten umgehen.
Obwohl in erster Linie Unternehmen beziehungsweise die Unternehmensleitung haftbar sind bei Datenpannen, können auch einzelne Mitarbeiter haftbar gemacht werden, wenn sie besonders fahrlässig handeln.

***Die Meldepflicht (§42a BDSG) ist bei Datenpannen unbedingt zu beachten.***

Bei (vermutetem) Abfluss von besonders schutzwürdigen Daten an Dritte, beispielweise bei Geräte-Diebstahl oder bei einem Hacker-Angriff, sind Unternehmen verpflichtet, den Vorfall unverzüglich der betreffenden Datenschutz-Aufsichtsbehörde sowie den vom Vorfall Betroffenen zu melden (vgl. §42a BDSG). Besonders schutzwürdige Daten sind nach §3 Absatz 9 BDSG „Angaben über die rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit oder Sexualleben“ sowie Bank- und Kreditkartendaten, Berufsgeheimnisse und „personenbezogene Daten, die sich auf strafbare Handlungen oder Ordnungswidrigkeiten oder den Verdacht strafbarer Handlungen oder Ordnungswidrigkeiten beziehen“ (§42a BDSG).

***Für weitere Informationen bezüglich des Themas Datenschutz, sowie weiterer Risiken und Empfehlungen, nutzen Sie das gleichnamige Handbuch oder entsprechende Fachliteratur.***

### 2.10.5 Lizenzrechtliche Konflikte

***Lizenzrechtliche Konflikte können sich in Zusammenhang mit BYOD schnell einstellen.***

Kommt ein BYOD-Modell in einem Unternehmen zum Einsatz, besteht eine große Gefahr, Software-Lizenzrechte zu verletzen, sofern im Vorfeld keine Analyse benötigter Nutzungslizenzen durchgeführt wurde. Bei Verwendung von Software außerhalb der vertraglich vereinbarten Zwecke, kann es nach Lizenzkontrollen zu Unterlassungsansprüchen und gegebenenfalls sogar zu Schadensersatzforderungen kommen. Im Unternehmensalltag kann es in zwei Fällen zu Lizenzrechtsverletzungen kommen.

#### Nutzung von Unternehmenssoftware auf dem Privatgerät des Mitarbeiters

Drei verschiedene Definitionen sind üblich: Erstens der Nutzer ist eine bestimmte Person oder ein bestimmter Arbeitsplatz (an dem mehrere Personen arbeiten können), zweitens der Nutzer ist Inhaber zweier Nutzungslizenzen, die er durch die Installation auf zwei Geräten in Anspruch nehmen kann (häufig darf hier die Software nicht an beiden Geräten gleichzeitig ausgeführt werden). Drittens der Nutzer ist das Unternehmen, das heißt, die Software darf auf allen unternehmenseigenen Geräten ausgeführt werden. Gilt beispielsweise letztere Lizenzart würde die Nutzung der Software bei BYOD einen Verstoß darstellen. Daneben gibt es auch Volumen- oder Paketlizenzen, die individuelle Nutzungsregelungen festlegen.

#### Nutzung von Software des Privatgeräts für betriebliche Zwecke

Es ist zu prüfen, ob privat erworbene Software eine Nutzungslizenz für betriebliche Zwecke beinhaltet. Verstößt ein Mitarbeiter gegen Nutzungsbedingungen, kann der Hersteller Unterlassungsansprüche und bei vorsätzlichem Verhalten Schadensersatzforderungen gegen den betreffenden Mitarbeiter stellen. Im schlimmsten Fall kann auch das Unternehmen des Mitarbeiters haftbar gemacht werden, wenn die illegitime Nutzung der Software im Tätigkeitsbereich des Mitarbeiters stattgefunden hat. Für betriebliche Zwecke verwendete Geräte werden als unternehmenseigene gewertet, auch wenn sie sich eigentlich im Besitz der Mitarbeiter befindet. Für eventuelle Unterlassungs- und Nachvergütungsansprüche gegen das Unternehmen ist unerheblich, ob die Unternehmensleitung Kenntnis vom Fehlverhalten des Mitarbeiters hatte oder nicht. Bei Verwendung von Raubkopien für betriebliche Zwecke können zudem Schadensersatzansprüche des Software-Herstellers geltend gemacht werden. Die Unternehmensleitung ist in der Pflicht, stets dafür Sorge zu tragen, dass für betrieblich genutzte Software die passenden Lizenzen zur Verfügung stehen.

## 2.11 Zusammenfassung

**Risiken**

Mobiles Arbeiten bringt zahlreiche Gefahrenpotenziale mit sich. Neben Lauschangriffen auf die drahtlosen Schnittstellen WLAN, Bluetooth und NFC sind weitere technische Risiken denkbar. So steigen Anzahl und Verbreitung von Schädlingen wie Viren, Würmer und Trojaner zunehmend und stellen eine Bedrohung für alle Nutzer mobiler IT-Geräte dar.

In puncto Handhabung der Geräte kann ein allzu leichtfertiger Umgang schnell negative Konsequenzen nach sich ziehen. Phishing, die Verwendung unsicherer Apps besonders in Hinblick auf den Datenschutz, sowie Geräteverlust sind wichtige Themen, mit denen sich Anwender auseinandersetzen müssen.

Bei Verwendung privater Geräte für betriebliche Zwecke kommen zudem zahlreiche rechtliche Risiken hinzu, die sich im Kern um das Thema Datenschutz drehen. Eine Missachtung der Datenschutzanforderungen, die sich aus der Anlage zu §9 BDSG ergeben, so wie Konflikte bei unsauberer Trennung zwischen betrieblichen und privaten Daten sind bei fehlenden Betriebsrichtlinien und -vereinbarungen nicht nur zu befürchten, sondern sehr wahrscheinlich. Für Datenschutzverstöße als Folge fehlender Datenschutzmaßnahmen können Unternehmen voll haftbar gemacht werden – dies gilt auch für Verstöße, die die Mitarbeiter auf ihren Privatgeräten verursachen.

Den zuvor genannten Risiken sollten Betriebe auf drei Ebenen entgegnen: auf der Geräteebene, der Mitarbeiterebene und der Verwaltungsebene. Nachfolgend sollen für alle drei konkrete Schutzmaßnahmen genannt werden.

**Notizen**

# 3. Schutzmaßnahmen auf der Geräteebene – Basisschutz

Ein ausreichender Grundschutz der Geräte bildet das Fundament der betrieblichen IT-Sicherheit, ohne den elektronische Geschäftsprozesse nicht durchgeführt werden sollten. Erfüllt die IT eines Handwerksbetriebs nicht diese Voraussetzungen, stehen die Ressourcen des Unternehmensnetzwerks praktisch schutzlos den digitalen Bedrohungen gegenüber. Konflikte mit dem Bundesdatenschutzgesetz sind sehr wahrscheinlich, sodass Unternehmen für unsichere Erhebung, Verarbeitung oder Speicherung personenbezogener (Kunden-)Daten haftbar gemacht werden können (siehe Kapitel *2.10.3 Datenschutzanforderungen*).

***Bei Verwendung von Geräten ohne ausreichenden Basisschutz sind Verstöße gegen das BDSG wahrscheinlich.***

Nachfolgend sollen Schutzmaßnahmen auf der Ebene einzelner Geräte erläutert werden. Das heißt, es geht um Gerätekonfiguration und zu installierende Sicherheitssoftware.

## 3.1 Basisschutz für Netbooks und Notebooks

Basisschutz-Maßnahmen für Laptops können analog zu den Vorkehrungen bei klassischen Desktop-PCs getroffen werden.

### 3.1.1 Zugriffssperre

***Die Authentisierung und Authentifizierung dient zur Überprüfung der Identität. Für das Gegenüber muss ein Beweis geliefert werden. Dieser kann über den Besitz (zum Beispiel eine Smartcard), das Wissen (zum Beispiel ein Passwort) oder biometrische Merkmale wie die Iris festgestellt werden.***

Die Überprüfung der Nutzeridentität erfolgt durch eine Authentifizierung zwecks Zugangskontrolle. Hierbei ist zwischen den Begriffen Authentisierung und Authentifizierung zu unterscheiden: Authentisierung ist der Vorgang des Nachweises der eigenen Identität. Authentifizierung meint die Überprüfung der Echtheit einer behaupteten Identität, beispielsweise einer Person.

Die Authentisierung und Authentifizierung ist ein zweigeteilter Vorgang, um die Identität eines Subjektes, zum Beispiel einer Person oder eines IT-Systems, festzustellen. Dazu muss das Subjekt den Besitz eines Objektes, das Wissen um ein Geheimnis nachweisen oder den Besitz bestimmter, bei Personen zum Beispiel biometrischer Merkmale aufweisen und sich anhand dieser authentisieren. Das Gegenüber authentifiziert das Subjekt anhand dieser Eigenschaften, indem es diese mit ihm bereits vorliegenden Informationen vergleicht. Das Objekt könnte eine Smartcard oder ein USB-Token mit einem gespeicherten Schlüssel sein. Geeignete biometrische Merkmale können beispielsweise die Stimme, das Tippverhalten, die Handvenen oder die Iris sein. Das Geheimnis kann das Wissen um vorab definierte Paare von Fragen und Antworten sowie ein Passwort sein. Für sicherheitskritische Funktionen ist eine sogenannte Multi-Faktor-Authentifizierung mittels mehrerer Authentisierungsmerkmale optimal: Bei der Online-Authentisierung mittels neuem Personalausweis im Internet ist neben dem Besitz der Karte die Kenntnis der PIN als Beweis der Identität notwendig. Die Gefahr des Missbrauches ist somit geringer als bei alleiniger Überprüfung des Besitzes.[25]

[25] *https://www.internet-sicherheit.de/service/glossar/eintrag/eintrag-detail/authentisierung-und-authentifizierung/?no_cache=1*

Bei einem Computer-Nutzerkonto erfolgt die Authentifizierung häufig über den Nachweis des "Wissens": Der Benutzer kennt ein geheimes Passwort, welches in Kombination mit seinem Benutzernamen den Zugriff ermöglicht. Ein Benutzerkonto sollte mit einem sicheren Passwort geschützt werden (siehe hierzu: Kapitel *4.2 Passwortsicherheit und -tools*). Mitarbeiter sollten das Passwort regelmäßig, mindestens vierteljährlich ändern. Eine entsprechende Richtlinie sollte in den Unternehmensrichtlinien festgelegt sein (siehe Kapitel *5.3 Auflagen und Richtlinien für die Mitarbeiter*). Bei Verdacht auf Passwortklau sollten Beschäftigte ihr Passwort umgehend ändern.

***Die Zugriffssperre aktivieren Windows-Nutzer mit der Tastenkombination Windows-Taste + L.***

Grundsätzlich sollten alle Mitarbeiter ihr System sperren, sobald sie ihren Arbeitsplatz verlassen – und sei es nur für den Toilettengang. Angreifern reichen wenige Sekunden, um sensible Daten abzugreifen oder das System mit Schadsoftware zu infizieren. Dieses Risiko erhöht sich exponentiell, wenn Mitarbeiter in einer unsicheren Arbeitsumgebung arbeiten.

Zusätzlich zur Zugangskontrolle bei Systemstart sollte eine Zugriffssperre bei Inaktivität sprich nach dem Start des Bildschirmschoners erfolgen. Auf diese Weise schützen Anwender ihre Daten, sollten sie einmal beim Verlassen ihres Platzes die Zugriffssperre vergessen haben.

***Schützen Sie Ihr System mit einem sicheren Passwort, bestehend aus mindestens zehn Zeichen, inklusive Zahlen und Sonderzeichen. Ein im Wörterbuch zu findendes Wort oder ein Name ist leicht angreifbar und damit ungeeignet. Sperren Sie Ihr System beim Verlassen des Arbeitsplatzes. Aktivieren Sie die automatische Zugriffssperre bei Bildschirmschoneraktivität.***

### 3.1.2 Virenschutz

***Virenscanner durchsuchen Dateien im Hintergrund fortlaufend nach Schädlingsbefall.***

IT-Nutzer ohne aktuelles Virenschutzprogramm laufen Gefahr, ihr System durch Malware zu kontaminieren. Dies könnte unter Umständen erhebliche Schäden für das Unternehmensnetzwerk nach sich ziehen (siehe Kapitel *2.2 Viren, Würmer, Trojaner*). Ein Virenscanner durchsucht alle auf dem Gerät gespeicherten Dateien in Echtzeit nach Auffälligkeiten, die auf einen Schädlingsbefall hinweisen. Beim ersten Start einer Antivirensoftware erfolgt eine Antivirenprüfung des gesamten Systems. Eine solche vollständige Überprüfung des Systems sollte regelmäßig durchgeführt werden. Bei der Identifizierung einer infizierten Datei können mithilfe weiterer Programmfunktionen entsprechende Maßnahmen eingeleitet werden. Das betreffende Gerät ist in diesem Fall umgehend vom Unternehmensnetzwerk zu entfernen, um den weiteren Schädlingsbefall anderer Geräte einzudämmen. Mithilfe der Schutzsoftware können Schädlinge in Quarantäne versetzt oder gelöscht werden. Im Unternehmenskontext ist die Neuinstallation des Betriebssystems bei Kontamination zwingend erforderlich. Nur so können Manipulationen am produktiven System ausgeschlossen werden. Betroffene sollten sich an den Administrator – bei Handwerksbetrieben meist ein Systemhaus – wenden.

#### Auswahl der geeigneten Software

***Die Überprüfung des Softwareherstellers auf Seriosität sollte bei jedem Softwareprodukt und erst recht bei Antivirensoftware erfolgen.***

Vor dem Kauf einer Software sollten sich Unternehmen über den gewünschten Funktionsumfang im Klaren sein. Ein Abgleich der beschriebenen Produktfeatures mit den hier vorgestellten Mindestanforderungen an einen Geräte-Basisschutz kann bei der Kaufentscheidung helfen. Unternehmer sollten kostenlose Produkte kritisch hinterfragen. Welche Intention verfolgt der Hersteller? Gegebenenfalls müssen Nutzer kostenloser Angebote Spam oder Schlimmeres in Kauf nehmen. Eine Kontrolle der Seriosität eines Herstellers sollte in jedem Fall erfolgen – egal, ob es sich um ein kostenpflichti-

ges oder kostenloses Produkt handelt. Die Website des Herstellers, insbesondere die im Impressum angegebenen Informationen, kann für eine Einschätzung weiterhelfen. Verantwortliche sollten sich zudem vor dem Erwerb eines Produkts Testberichte seriöser Medien und Nutzerbewertungen ansehen. Meistens ist die Installation mehrerer Schutzsoftware-Produkte nicht möglich, da sie sich in ihrer Funktionalität durch die Aktivitäten des jeweils anderen Programmes gestört fühlen.

#### Software-Aktualität als Voraussetzung für gute Analyseergebnisse

***Das Einspielen von Antivirensoftware-Updates sollte die erste Maßnahme nach Systemstart sein.***

Sämtliche Dateien (Programme, Dokumente, Fotos etc.), die auf den Geräten abgespeichert werden, sollten zunächst mithilfe des Virenschutzprogramms auf Schädlingsbefall geprüft werden. Wichtig ist, dass das Virenschutzprogramm auf den Geräten immer aktuell ist. Wie im Kapitel 3.1.4 und 3.2.8 (*Aktualitätsprinzip*) dargestellt, ist Software-Aktualität einer der entscheidenden Faktoren für die betriebliche IT-Sicherheit. Virenschutzprogramme können nur neueste Schadsoftware als solche identifizieren, wenn sie auf dem neuesten Informationsstand sind. Die meisten Programme führen automatisch regelmäßige Updates ihrer Virensignaturen durch, beispielsweise beim Systemstart. Sollte das Programm mehrere Tage lang nicht aktualisiert worden sein – zum Beispiel bei der Wiederinbetriebnahme nach dem Wochenende oder Urlaub – sollten sich Anwender von der Aktualität der Software genau überzeugen. Sie können den Update-Vorgang auch manuell starten (meist durch einen Rechtsklick auf das Programmsymbol, das sich oft unten rechts am Bildschirm befindet).

***Installieren Sie ein Virenschutzprogramm, halten sie es stets auf dem neuesten Stand und führen Sie regelmäßig eine Antivirenprüfung des gesamten Systems durch. Prüfen Sie darüber hinaus auch alle Dateien, insbesondere Software, vor der Ausführung/Installation auf Schädlingsbefall.***

### 3.1.3 Personal Firewall

***Eine Personal Firewall arbeitet wie ein Türsteher, der Datenverkehr zwischen Laptop und dem Netzwerk regelt.***

Eine Personal Firewall überwacht den Datenverkehr zwischen dem Laptop und dem Netzwerk, mit dem es verbunden ist (beispielsweise das Internet). Sie arbeitet wie ein Türsteher, der aufgrund eines definierten Reglements entscheidet, welche Programme Daten über das Internet senden und empfangen dürfen. Einer Reihe von Programmen wie der Update-Funktion des Betriebssystems und dem E-Mail-Programm kann eine Kommunikation mit dem Internet permanent gestattet werden. Möchten unbekannte Anwendungen Daten übertragen, blockiert die Personal Firewall diesen Kontakt erst einmal. Daraufhin erscheint ein Dialog, indem der Nutzer entscheiden muss, ob er bestimmten Anwendungen Datenverkehr gewährt oder nicht. So hilft die Firewall zum Schutz vor Trojanern, die sensible Daten vom Anwender-Gerät zu einem entfernten Server übersenden wollen. Der Härtegrad des Reglements zur Unterbindung von unbekannten Verbindungen lässt sich durch die Software variieren.
Üblicherweise bringen aktuelle Betriebssysteme eine Firewall von Haus aus mit (beispielsweise die Windows-Firewall unter Windows oder die Internet Protocol Firewall unter iOS X). Diese informieren Nutzer ebenfalls über den Datensendewunsch bestimmter Anwendungen. Windows-Nutzer werden oft bei Programmstarts über Zugriffswünsche informiert, die sie infolge zulassen oder ablehnen können. Hier haben Anwender die Möglichkeit, nochmal die Seriosität der Anwendung zu überprüfen, bevor sie ihre Zustimmung zur Datenübertragung geben.

Die bei Betriebssystemen mitgelieferten Firewalls sind allerdings recht rudimentär gehalten. Daher ist es ratsam, eine zusätzliche Software zu verwenden. Es gibt auch kostenlose Personal- Firewall-Lösungen im Internet, zum Beispiel ZoneAlarm oder Comodo[26] – beide für Windows. Außerdem sind in den meisten Security Suiten Firewalls bereits enthalten.

***Installieren Sie sich eine Personal Firewall und halten Sie diese analog zum Virenschutzprogramm stets auf dem neuesten Stand.***
***Bei Firewall-Meldungen, die Sie nicht einschätzen können oder bei plötzlichen Meldungen ohne eine vorherige Aktion von Ihnen, sollten Sie den Zugriff verweigern.***
***Anfragen, die Sie einem von Ihnen verwendeten Programm zuordnen können, sind in der Regel unproblematisch. Diese erscheinen oft in dem Moment, in dem Sie das entsprechende Programm starten, wie beispielsweise den Browser oder das E-Mail-Programm.***

### 3.1.4 Aktualitätsprinzip – Sicherheitsupdates und -tools

***Das Risiko einer Malware-Infektion wird durch das zeitnahe Einspielen von Softwareupdates drastisch reduziert.***

Wie in Kapitel *2.2. Viren, Würmer, Trojaner* dargestellt, ist das Zeitfenster zwischen Bekanntgabe und Installation von Sicherheitsupdates von entscheidender Bedeutung für die betriebliche IT-Sicherheit des Unternehmensnetzwerks. IT-Anwender können das Risiko einer Malware-Infektion dadurch minimieren, dass sie Sicherheitsupdates ihrer genutzten Programme unmittelbar nach dem Erscheinen einspielen[27]. Dadurch bleibt Angreifern weniger Zeit, um Software-Schwachstellen für ihre Zwecke auszunutzen.

Es gibt hilfreiche Anwendungen, die das zeitnahe Einspielen aktueller Sicherheitsupdates unterstützen. Das Institut für Internet-Sicherheit bietet mit der Anwendung securityNews einen Service, der auf aktuelle Updates hinweist und Sicherheitsempfehlungen gibt. Zudem zeigt securityNews ein aktuelles Bild der Sicherheits- und Schwachstellenlage, so wie sie von IT-Sicherheitsexperten eingeschätzt wird. Die integrierte BSI-Schwachstellenampel gibt einen schnellen Überblick über die Anzahl und Schwere offener Schwachstellen in der gängigsten Standardsoftware und zeigt sichere Alternativen. securityNews gibt es als mobile Variante, als App für Smartphones und Tablets und als E-Mail-Dienst für Mac und PC. Siehe: https://www.it-sicherheit.de/securitynews/.

***Aktivieren Sie die automatischen Update-Routinen in den Einstellungen Ihrer genutzten Programme sowie die automatische Update-Funktion Ihres Betriebssystems. Halten Sie sämtliche installierte Software stets auf dem neuesten Stand und prüfen Sie regelmäßig die Aktualität der Software – aktualisieren Sie gegebenenfalls manuell über die Herstellerseite des betreffenden Programms. Installieren Sie sich die Anwendung securityNews, um auf dem Laufenden zu bleiben.***

---

[26] *https://www.internet-sicherheit.de/institut/buch-sicher-im-internet/workshops-und-themen/konfigurationen/programme-zum-basisschutz/*
[27] *Es ist ratsam, im Vorfeld einer Software-Aktualisierung ein Datenbackup durchzuführen, um eventuellen Inkompatibilitäten der neuen Software-Version vorzubeugen. Updates an essentiellen Dienstanwendungen sollten zunächst auf einem Testsystem erprobt werden, sodass es bei Software-Ausfall nicht zu Verdiensteinbrüchen kommt.*

### 3.1.5 Datensicherung – Backups

Je häufiger Mitarbeiter die lokal gespeicherten Daten auf den Geräten und die zentral gespeicherten Server-Daten durch Sicherungskopien (Backups) archivieren, desto kleiner ist der Schaden bei Daten- und Geräteverlust. Die langfristige Speicherung von Geschäftsbriefen, E-Mails und Rechnungen ist für Unternehmen sogar gesetzlich vorgeschrieben[28]. Deshalb sollte die Häufigkeit der Datensicherung in den Unternehmensrichtlinien innerhalb eines Datensicherungskonzeptes verankert sein (siehe Kapitel *5.3 Auflagen und Richtlinien für die Mitarbeiter*).
Die Daten sollten auf separaten Speichermedien kopiert und mithilfe einer Verschlüsselungssoftware (siehe nachfolgendes Kapitel) vor dem Zugriff Unbefugter geschützt sein.
Neben der Sicherung einzelner Datenpakete sollten Mitarbeiter regelmäßig eine Sicherungskopie des gesamten Systems vornehmen. So kann bei Ausfall der gesamten Festplatte schnell das neue System inklusive aller Daten in wenigen Stunden neu aufgespielt werden. Als Datenträger eignen sich HDD-Festplatten. Zu beachten ist, dass Datenträger nicht immer fehlerfrei sind und die Kopien daher am besten auf verschiedenen Datenträgern redundant gespeichert und regelmäßig kontrolliert werden sollten. Eine Möglichkeit zur Absicherung vor hardwareseitigem Datenverlust ist der Einsatz von RAID- Systemen, bei dem parallel mindestens zwei Festplatten gleichzeitig eingesetzt werden. Redundant Array of Independent Disks (RAID) ersetzt jedoch nicht zusätzliche Backup-Routinen.
Als Lagerungsorte für die Datenträger eignen sich trockene Räume, die keine Feuchtigkeit oder starke Temperaturschwankungen aufweisen. Direkte Sonneneinstrahlungen und die Nähe zu magnetischen Komponenten, beispielsweise in Lautsprechern, sind zu vermeiden. Im besten Fall lagern die Backup-Dateien an verschiedenen Orten, um einer Zerstörung von Daten beispielsweise durch einen Brand vorzubeugen.

***Für Backups eignen sich externe HDD-Festplatten. Nach Möglichkeit sollten mehrere Sicherungskopien redundant angelegt und die Festplatten an verschiedenen Orten aufbewahrt werden.***

***Legen Sie regelmäßig Sicherungskopien Ihres gesamten Systems auf mehreren externen HDD-Festplatten an. Lagern Sie die Backup-Festplatten trocken und geschützt vor dem Zugriff Unbefugter, möglichst an verschiedenen Orten.***

### 3.1.6 Datenverschlüsselung

Neben der Möglichkeit, einzelne Ordner oder Verzeichnisse zu verschlüsseln, bietet die Festplatten-Vollverschlüsselung den größten Komfort bei gleichzeitig größtem Schutz vor Datenklau. Ist die gesamte Festplatte des Anwenders verschlüsselt, braucht er lediglich einmal bei Systemstart zu entschlüsseln und nicht – wie bei der Teilverschlüsselung – jedes Mal, wenn er auf das betreffende Verzeichnis oder den betreffenden Ordner zugreifen möchte. Darüber hinaus haben Diebe bei vollverschlüsselter Festplatte geringe Chancen, innerhalb einer zumutbaren Zeit auch nur an einen einzigen Datensatz zu kommen. Sind dazu im Unterschied nur bestimmte Bereiche geschützt, liegen die übrigen offen für die Einsicht Krimineller. Für beide Wege eignet sich das kostenlose Verschlüsselungstool TrueCrypt, das mittels Advanced Encryption Standard (AES) verschlüsselt. In Verbindung mit einem sicheren Passwort können Anwender einen starken Schutz vor unbefugter Dateneinsicht erreichen. Die

***Eine Festplatten-Vollverschlüsselung ist die effizienteste Präventivmaßnahme vor Datenverlust bei verlorenen oder gestohlenen Geräten.***

[28] *Unternehmen sind verpflichtet, diese Daten über mindestens zehn Jahre zu speichern.*

verschlüsselten Daten liegen hier nur in chiffrierter Form auf der Festplatte – ein Angreifer findet ohne Einsatz des passenden Schlüssels nur kryptischen Datenmüll vor. Weitere Hinweise zur Verschlüsselung der Kommunikationswege in den Kapiteln *4.3 Sicherheit bei drahtloser Kommunikation via WLAN, Bluetooth und Co* und *4.4 Sichere Datenübertragung*.

### 3.1.7 Physischer Diebstahlschutz

***Portable Schlösser für Laptops schützen vor Gelegenheitsdieben, beispielsweise auf Messen.***

Einen leichten physischen Diebstahlschutz bieten portable Schlösser, die Netbooks und Notebooks an ein größeres Objekt wie zum Beispiel einen Tisch binden. So können zumindest Gelegenheitsdiebe abgeschreckt werden, die beispielsweise auf Produktmessen ihr Glück versuchen.

*Abbildung 7: Portables Schloss am Laptop („Kensington-lock-slot“, o. A.)*

Den größten Schutz vor Datenklau im Fall des Geräteverlusts bietet eine im vorigen Kapitel vorgestellte Festplatten-Vollverschlüsselung. Die sensiblen Daten auf der Festplatte sind so gegen die allermeisten Angriffe für längere Zeit geschützt. Da Anwender nach einem Diebstahl keinen Zugriff mehr auf die lokal gespeicherten Daten mehr haben, sollten als Präventivmaßnahme geeignete Datensicherungsroutinen eingerichtet werden (siehe *Kapitel 3.1.5 Datensicherung – Backups*).

### 3.1.8 Sichtschutz

***Sichtschutzfilter sind beim Geräteeinsatz in unsicheren Arbeitsumgebungen zu verwenden.***

Arbeiten Mitarbeiter nicht alleine im Büroraum, sondern in einem Raum, der auch von Kunden und Kollegen anderer Firmen frequentiert wird, sollten sie ihren Laptop mithilfe einer speziellen Sichtschutzfolie vor allzu neugierigen Blicken schützen. Die Folie schränkt den Sichtwinkel des Displays soweit ein, dass er nur frontal betrachtet lesbar ist. Die Empfehlung zum Einsatz einer solchen Folie betrifft im Besonderen diejenigen Mitarbeiter, die ihr Gerät in unsicheren Arbeitsumgebungen, beispielsweise bei Außendienstterminen oder unterwegs im Zug, beruflich nutzen.


*Abbildung 8: Laptopdisplay mit und ohne Sichtschutzfilter (Sebastian Wacowski, 2014)*

Darüber hinaus sollten die in den Netbooks und Notebooks integrierten Kameras außerhalb ihrer Nutzung überklebt werden. Angreifern ist es möglich, mithilfe von Malware Zugriff auf die Kamera eines Nutzers zu bekommen. Auf diese Weise können sie pikante Details über Büroräume, Arbeitsabläufe et cetera in Erfahrung bringen, die sie für Social-Engineering-Angriffe nutzen können.

***Sollten Sie Ihren Laptop in unsicheren Arbeitsumgebungen (z.B. im Zug oder im Café) nutzen, dann verwenden Sie einen Sichtschutzfilter. Überkleben Sie die eingebaute Kamera Ihres Geräts, die sich im Regelfall am oberen Rand des Displaygehäuses befindet.***

## 3.2 Basisschutz für Smartphones und Tablets

***Beim Basisschutz für Smartphones und Tablets kommen weitere Schutzmaßnahmen hinzu.***

Grundlegende Sicherheitsvorkehrungen für Smartphones und Tablets gleichen den zuvor vorgestellten für Laptops. Allerdings sollten sich Anwender der Multifunktionalität der kleinen Alleskönner bewusst sein und dem Schutz gerätespezifischer Funktionen, die sie vom Desktop-PC unterscheiden, besondere Aufmerksamkeit schenken. Nachfolgend sollen sicherheitsrelevante Gerätekonfigurationen sowie Sicherheitstools und -Softwarefunktionen vorgestellt werden.

### 3.2.1 Zugriffssperre

Die SIM-Karten in Smartphones und Tablets sind standardmäßig durch PIN-Abfragen vor unbefugtem Zugriff zu schützen. Schaltet der Gerätebesitzer sein Smartphone oder Tablet ein, muss er zunächst eine mindestens vierstellige Zahlenkombination eingegeben, um Zugriff auf seine SIM-Karte zu erhalten. Darüber hinaus kommen die Geräte von Werk aus meist mit einer automatischen Bildschirmsperre daher, die sich aktiviert, sobald der Anwender sein Gerät mehrere Sekunden oder Minuten nicht bedient. Die automatische Tastensperre ist in puncto Gerätesicherheit zu vernachlässigen, kann sie doch durch eine einfache Tastenkombination oder einen Fingerwisch gelöst werden.

***PIN-Abfrage und Bildschirmsperre allein sind hinsichtlich der IT-Sicherheit ungenügend.***

PIN-Abfrage und Bildschirmsperre allein bieten keinen ausreichenden Schutz vor unbefugten Gerätezugriff. Ein Dieb braucht lediglich die SIM-Karte des gestohlenen Geräts durch eine andere auszutauschen, um vollen Zugriff auf das System und die gespeicherten Daten zu erlangen. Trotz des hohen Sicherheitsrisikos verzichten laut BITKOM zwei Drittel aller Handy-Besitzer auf weitere Sicherheitsabfragen (vgl. BITKOM, 2012a). Anwender sollten gerade im Firmenumfeld bei ihrem Smartphone und/oder Tablet eine echte Zugriffssperre einrichten. Diese sollte nach dem Lösen der automatischen Bildschirmsperre einhaken, sodass das Gerät erst nach Eingabe einer Sicherheitsabfrage genutzt werden kann. Je nach System stehen Smartphone-Anwendern mit der Code- oder Wischmuster-Abfrage zwei verschiedene Sicherheitsmechanismen zur Verfügung, wobei die populäre Wischmusterabfrage die unsicherere ist.

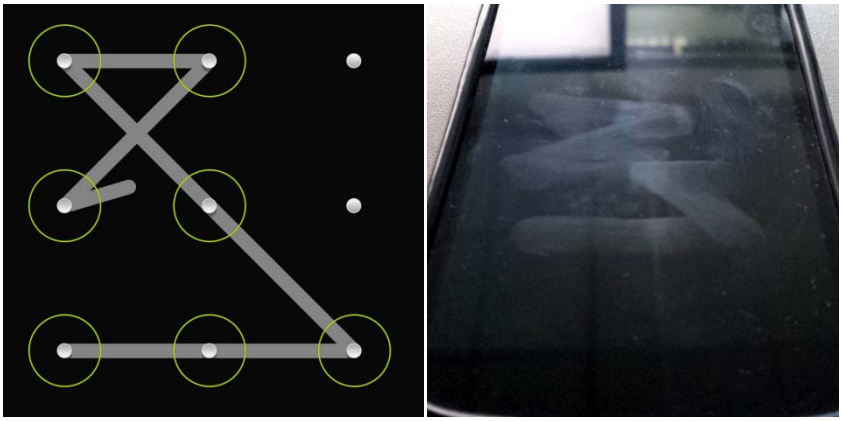


*Abbildung 9: Wischmusterabfrage (links) und die hinterlassenen Fingerspuren auf dem Gerätedisplay (rechts) (Falk Gaentzsch, 2013)*

Wie die Abbildung 9 zeigt, hinterlässt die Wischmuster-Abfrage Spuren auf dem Display des Gerätes, die ein Angreifer nachvollziehen kann. Außerdem können Muster vom aufmerksamen Beobachter leichter erkannt werden als Tastenkombinationen.

Darüber hinaus stehen bisweilen noch andere Sperrmechanismen wie der Gesichtserkennung zur Verfügung – diese sind jedoch manipulierbar und bieten keinen ausreichenden Schutz.

***Zugriffssperren mit sn Passwörtern (Tablets) oder langen Zeichenkombinationen (Smartphones) bieten den größten Schutz.***

Allen Besitzern von Smartphones und Tablets ist zu raten, ihre Geräte nach Möglichkeit durch sichere Passwörter (bei Tablets) oder lange Zahlenkombinationen (bei Smartphones) vor fremden Zugriff zu schützen. Wie in Kapitel *4.2 Passwortsicherheit und -tools* dargestellt, korreliert die Stärke des Passwortes mit der Zeichenanzahl des verwendeten Zeichensystems und der Länge des Kennwortes in hohem Maße. Großen Schutz bietet also eine zehnstellige Kombination aus Klein- und Großbuchstaben, Zahlen und Sonderzeichen. Die Eingabe letzterer über Touchdisplays kann gegebenenfalls sehr umständlich sein, sodass aus Gründen der Praktikabilität nur eine Kombination aus Klein- und Großbuchstaben angewandt wird. Hiermit sei aber ausdrücklich auf den Sicherheitsvorteil der erst genannten Variante hingewiesen. Klar sollte sein, dass neben der Zugriffssperre noch Datenverschlüsselungsmaßnahmen (siehe Kapitel *3.2.6 Datenverschlüsselungsmechanismen*) eingesetzt werden müssen. Knackt ein Angreifer die Zugriffssperre des Geräts, hat er ansonsten freien Zugriff auf sämtliche sensible Daten.

***Schützen Sie Ihr Smartphone und/oder Tablet mit einer eingerichteten Zugriffsperre, in Form einer Passwortabfrage nach dem Lösen der Tastensperre. Verwenden Sie hierzu nach Möglichkeit ein sicheres Passwort, bestehend aus mindestens zehn Zeichen, inklusive Klein- und Großbuchstaben, Zahlen und Sonderzeichen. Vermeiden Sie Daten wie Telefonnummern und Geburtsdaten, die auf Sie und Ihr Umfeld zurückzuführen sind.***

***Zugriffssperre bei iOS:***
***Einstellungen -> Allgemein -> Code-Sperre***

***Zugriffssperre bei Android:***
***Einstellungen -> Sicherheit -> Display-Sperre einrichten***

***Zugriffssperre bei Windows Phone:***
***Einstellungen -> Sperre & Hintergrund***

***Zugriffssperre bei RIM bzw. Blackberry:***
***Einstellungen -> Sicherheitsoptionen -> Allgemeine Optionen***
***bzw. Einstellungen -> Kennwort***

### 3.2.2 Mobile Security Suites – Kosten und Funktionsumfang

***Mindestfunktionsumfang einer MSS-Lösung: Virenschutz, Personal Firewall, Anruf- und SMS-Filter, Datenverschlüsselungsfunktion, Diebstahlschutz-Funktionen.***

In einem von acht Handwerksbetrieben wissen Mitarbeiter nicht darüber Bescheid, ob und wie regelmäßig Sicherheitssoftware zum Schutz des Unternehmensnetzwerkes eingesetzt wird (vgl. IT-Sicherheit im Handwerk, 2013). Ein alarmierender Befund, sollte doch die Inanspruchnahme einer Schutzsoftware Grundvoraussetzung für berufliche wie auch private IT-Nutzung sein.
Mobile Security Suites (MSS) sind Sicherheits-Apps für Smartphones und Tablets, die einige Schutzfunktionen in einem Produkt bündeln. Ihr Umfang unterscheidet sich dabei je nach Hersteller. Anwender sollten beim Kauf einer Mobile Security Suite darauf achten, dass die Software mindestens mit allen grundlegenden Funktionen, die in den folgenden Kapiteln *3.2.3 Virenschutz* bis *3.2.7 Diebstahlschutz* vorgestellt werden, ausgestattet ist. Darüber hinaus sind weitere Programmfeatures vonnöten, sollten auf den Geräten besonders sensible Daten wie Geschäftsgeheimnisse gespeichert sein oder sie sich in permanentem Austausch mit dem Unternehmensserver befinden (Stichwort: Enterprise Apps). Bei der Auswahl einer geeigneten Software sollten Anwender die Produkte kritisch hinterfragen – insbesondere dann, wenn es sich um kostenlose Software handelt. Als Faustregel gilt: Kostenlose Angebote kommen meist mit geringerem Funktionsumfang und weniger Serviceleistungen daher und/oder beinhalten unter Umständen viel Werbung. Manchmal setzen Hersteller kostenloser Software auch ein höheres technisches Grundverständnis voraus, damit Anwender ein Sicherheitsniveau erreichen können, das kostenpflichtiger Software gleicht. Außerdem ist zu klären, ob die kostenlosen Produkte überhaupt für gewerbliche Zwecke genutzt werden dürfen. Eventuell kann es zu lizenzrechtlichen Problemen kommen.

#### Produkthersteller auf Seriosität prüfen

***Nur Herstellern, die auf Seriosität überprüft wurden, sollte Vertrauen entgegengebracht werden. Produkten aus anderen Quellen als den offiziellen Markets sollten misstraut werden.***

Die Installation einer Mobile Security Suite kommt einem großen Vertrauensbeweis des Anwenders gegenüber dem Software-Hersteller gleich, denn meist fordern solche Produkte umfangreiche Zugriffsrechte auf verschiedene, zum Teil sehr sensible Geräteressourcen ein. In jedem Fall sollten Anwender den Produkthersteller daher auf Seriosität überprüfen, ganz gleich ob es sich um kostenlose oder kostenpflichtige Software handelt. Hinter jedem Produkt könnte sich prinzipiell eine schadhafte Anwendung verstecken – der Wolf im Schafspelz. Anwender sollten die Herstellerwebsite, insbesondere die Angaben im Impressum und die Allgemeinen Geschäftsbedingungen (AGB) überprüfen. Ein beliebter Trick von Kriminellen ist es, kostenlose Pseudo-Duplikate gängiger Softwareprodukte anzubieten, die in ihrer Beschreibung und Optik den Originalen gleichen. Sicherheitsapps aus anderen Quellen als den offiziellen App Markets sollten Anwender prinzipiell misstrauisch gegenübertreten (siehe Kapitel *2.3.1 Bezugsquellen*). Vor dem Download einer Software sollten Nutzerbewertungen sowie Testberichte seriöser Fachmedien zu Rate gezogen werden. Sollten Anwender bei der Auswahl eines geeigneten Produkts unsicher sein, können meist kostenlose Software-Testversionen, die zeitlich beschränkt nutzbar sind, bei der Produktentscheidung weiterhelfen. Unter keinen Umständen darf einer AppRoot-Zugriffsrechte gewährt werden, auch wenn der Softwarehersteller dies empfiehlt[30].

[30] *In diesem Fall ist die Seriosität des Herstellers fraglich.*

### Mobile Security Suites im Test

Nachfolgend sollen Testergebnisse von Mobile Security Suites dargestellt werden, die im August 2013 von zwei unabhängigen Instituten publiziert wurden. Diese können bei der Auswahl eines geeigneten Produkts als Anhaltspunkt dienen – es sollte aber im Hinterkopf behalten werden, dass es sich hierbei um Momentaufnahmen der jeweiligen Produktversionen handelt. Anwender sollten sich nicht nur auf die Ergebnisse verlassen, sondern zusätzliche Informationen über die Produkte einholen.

AV-Comparatives ist eine nicht-kommerzielle Organisation, die laut eigenen Angaben unabhängige Vergleichstests von Security-Produkten durchführt. Im „Mobile Security Review“ vom August 2013 hat die Organisation 16 Mobile Security Suites für Android in puncto Malwareschutz (Erkennung von Android-Schädlingen), Diebstahlsicherung und Batterieverbrauch untersucht (vgl. hier und im Folgenden: AV-Comparatives, 2013).
Die Malware-Erkennungsleistung wurde durch die Installation bösartiger Applikationen gemessen – das Testset bestand aus 2947 bösartigen Apps, die im Juli 2013 gesammelt wurden. Die fünf deutsch- und englischsprachigen Produkte mit den höchsten Erkennungsraten waren laut AV-Comparatives: AhnLab V3 Mobile mit 99,9 Prozent erkannter Malware, Kaspersky Mobile Security mit 99,7 Prozent Erkennungsleistung, ESET Mobile Security mit 99,6 Prozent, Bitdefender Mobile Security Premium (99,4 Prozent) sowie avast! Mobile Security (99,0 Prozent). Insgesamt war die Erkennungsleistung sehr hoch: Kein Produkt erkannte laut AV-Comparitives weniger als 91 Prozent der installierten Schädlinge. Einen Fehlalarm bei Installation einer App, die als nicht bösartig gilt, sei nicht gemeldet worden. Für alle Produkte gibt es im Bericht eine Detailübersicht, in der die enthaltenen Sicherheitsfeatures aufgelistet sowie ein knappes Qualitätsurteil getroffen wird. Was den Mythos angeht, MSS-Produkte steigerten den Batterieverbrauch enorm, so brauchten sich Anwender keine Sorgen zu machen: Lediglich zwei Produkte (Qihoo 360 Mobile Security und Webroot SecureAnywhere Mobile) zeigten laut AV-Comparitive einen Batterieverbrauch von drei oder mehr Prozent, die übrigen lagen darunter. Eine Vergleichstabelle im Anhang des Berichts kann Anwendern schlussendlich bei der Wahl eines geeigneten Produkts weiterhelfen.

AV Test ist ebenfalls eine laut eigenen Angaben unabhängige Test-Institution, die sich auf IT-Sicherheitsprodukte spezialisiert hat. Im September und Oktober 2013 wurden 28 MSS-Produkte für Android unter den Gesichtspunkten Schutzwirkung, Benutzbarkeit und Features untersucht (vgl. hier und im Folgenden AV-Test, 2013). Vergleicht man die separaten Testergebnisse für jedes Produkt, stechen besonders avast! Mobile Security, ESET Mobile Security und Kaspersky Mobile Security hervor: Die Erkennungsrate von Malware aus den vier Testwochen im oben genannten Zeitraum liegt hier laut AV Test bei über 99 Prozent erkannter Malware aus einer Stichprobe von 1.460 bösartigen Anwendungen. Ein Fehlalarm sei nicht gemeldet worden. Wird ihnen in Sachen Benutzbarkeit ein einwandfreies Handling bescheinigt, so unterscheiden sie sich laut AV Test in ihrem Funktionsumfang. Alle drei Produkte verfügten über drei Anti-Diebstahlfunktionen (Fern-Ortungs, -Sperr-, und -Lösch-Funktion), einen Anruf-, E-Mail und SMS-Filter und eine Browserschutz-Funktion, so AV Test. Leider fehle bei allen drei Produkten eine Backup- und Dateiverschlüsselungsoption. Während avast! Mobile Security im Funktionsumfang zusätzlich mit Firewall, Network Meter und Application Management aufwartet, kommt ESET Mobile Security mit Security Audit und Anti-Phishing-Funktion daher. Kaspersky Mobile Security wirbt mit der zusätzlichen Option Privacy Protection.

Was diese Schutzfunktionen im Einzelnen bewirken, soll in den nachfolgenden Kapiteln erläutert werden.

***Für die Auswahl eines geeigneten Produkts beachten Sie aktuelle Testberichte seriöser Medien und Nutzerbewertungen sowie den vom Hersteller angegebenen Funktionsumfang. Überprüfen Sie die Herstellerwebsite, AGB und etwaige Zertifikate kritisch vor der Installation der Anwendung. Beziehen Sie das Produkt ausschließlich über einen der offiziellen App Markets.***

### 3.2.3 Virenschutz

***Virenschutz bei Smartphones/Tablets hat im Vergleich zum Virenschutz bei Laptops/Desktop-PCs weitaus weniger Funktionstiefe. Eine Mitarbeitersensibilisierung bietet daher meistens größeren Schutz als es Softwareprodukte für Smartphones und Tablets könnten.***

Zunächst soll verdeutlicht werden, dass Antivirus-Apps für Smartphones und Tablets in ihrer Funktionsweise nicht gleichzusetzen sind mit bewährten Virenschutz-Lösungen für herkömmliche Desktop-PCs und Laptops. Im Unterschied zu letzteren sind Antiviren-Apps aufgrund der Rechtevergabe stärker eingeschränkt im Zugriff auf bestimmte Ressourcen und Daten anderer auf dem Gerät installierter Anwendungen. Für viele Funktionen, die eine Virenschutzlösung beim Desktop-PC realisieren kann, bräuchten Virenschutz-Apps mehr Zugriffsrechte, als sie tatsächlich bekommen können und sollten. Unter Android laufen Anwendungen beispielsweise in eigenen Umgebungen, sodass sie sich gegenseitig voneinander abschirmen. Jeder Anwendung wird bei diesem Sandboxing-Prinzip eine UserID zugewiesen, die sie auf den Zugriff bestimmter Systembereiche und Daten beschränkt. Auch bei Apple behindert die Rechtevergabe eine tiefergehende Funktionalität der Virenschutz-Apps, mit dem Unterschied, dass es hier von vornherein nur sehr wenige solcher Apps in den App Store schaffen. Grund hierfür dürfte die Forderung nach weitreichenden Zugriffsrechten sein, die den App-Prüfmechanismen von Apple widersprechen.

***Auch wenn Rooting die Funktionalität der Virenschutz-App theoretisch erhöhen könnte, sollten Anwender dies unter keinen Umständen tun.***

Demzufolge sind die Versprechungen der Hersteller dieser Anwendungen mit Vorsicht zu genießen; Virenschutz-Apps können nur in geringem Maße vor Malware schützen, die aufgrund von fahrlässigem Verhalten den Weg auf die Firmengeräte findet. Beispielsweise ist es nicht möglich, mithilfe von Mobile Security Apps E-Mail-Anhänge auf Viren zu überprüfen.

Auch hier sei noch einmal erwähnt, dass Anwender ihre Geräte unter keinen Umständen rooten sollten (siehe Kapitel *2.7 Risiko Jailbreaking und Rooting*), auch wenn Hersteller von Virenschutzlösungen dies mit dem Verweis auf die Möglichkeit der erweiterten Zugriffsrechte und der daraus resultierenden höheren Effizienz des Produkts empfehlen sollten. Eine Mitarbeitersensibilisierung bietet daher meistens größeren Schutz als es Softwareprodukte für Smartphones zurzeit könnten.

Virenschutzlösungen für Smartphones und Tablets erfüllen drei übergeordnete Aufgaben:

#### Echtzeit-Virenscan

Ein Echtzeit-Virenscanner startet sich bei Systemstart und ist im Arbeitsspeicher des Geräts ständig geladen. Er überprüft fortwährend einige Dateien auf Schädlingsbefall, die der Anwender speichern, öffnen oder – im Fall von Anwendungen – starten möchte. Wie oben beschrieben, bleibt der Zugriff auf die Dateien allerdings sehr limitiert, da die für einen ganzheitlichen Scan erforderlichen Rechte fehlen. Lediglich die Dateien, die auf der SD-Karte des Geräts liegen, können beim Ausführen vollständig auf Virenbefall Wie oben beschrieben, bleibt der Zugriff auf die Dateien allerdings sehr limitiert, da die für einen ganzheitlichen Scan erforderlichen Rechte fehlen. Lediglich die Datei-

en, die auf der SD-Karte des Geräts liegen, können beim Ausführen vollständig auf Virenbefall geprüft werden.
Im Echtzeit-Scan werden die betreffenden Dateien in Sekundenbruchteilen analysiert und mit der Datenbank der Virenschutz-Lösung abgeglichen, bevor der Anwender Zugriff auf die Dateien erhält beziehungsweise diese ausführen kann. Sind die Dateien unauffällig im Sinne des Datenbank-Vergleichs, erhält der Anwender sofortigen Zugriff. Auffälligkeiten werden dem Anwender in einem Dialog gemeldet, der Zugriff auf die betreffende Datei bleibt gesperrt. Wie auch beim Virenschutz für Laptops ist Software-Aktualität Bedingung für bestmögliche Analyseergebnisse und Echtzeit-Schutz.

***Der Echtzeit-Virenscanner prüft Dateien, die ein Anwender speichern, öffnen oder – im Falle von Apps – starten möchte, auf Schädlinge. Diese Dateianalyse ist allerdings aufgrund der Rechtebeschränkung nur sehr begrenzt möglich.***

### Partielle Systemprüfung

Eine partielle Prüfung des Systems muss vom Anwender initialisiert werden. Neben der manuellen Aktivierung ist auch die automatische Aktivierung mithilfe eines Zeitplans möglich. Auf schadhafte Elemente werden der Speicher des Geräts, inklusive der gespeicherten Nachrichten (SMS), integrierte Speicherkarten (z.B. SD Memory Cards) sowie einige Betriebssystemdateien überprüft, sofern die Zugriffsrechte der Virenschutz-App dies erlauben. Grundlage hierfür ist ebenfalls ein Abgleich mit der Datenbank der Virenschutz-Software. Eine vollständige Prüfung des gesamten Systems ist aufgrund der unzureichenden Zugriffsrechte (Stichwort: Sandboxing) in der Regel nicht möglich beziehungsweise ineffizient.

***Der Speicher des Gerätes, inklusive integrierter Speicherkarten, wird in der partiellen Systemprüfung auf Schädlinge überprüft. Hierbei werden nur die Bereiche analysiert, auf die via Berechtigungssystem zugegriffen werden kann.***

### Anwendungscheck

Im Anwendungscheck, einer erweiterten Komponente der Systemprüfung, werden installierte Apps unter die Lupe genommen, sofern möglich. Hierbei werden Anwendungen nicht nur auf verseuchte Elemente hin überprüft, sondern auch auf Art und Umfang der von ihnen eingeforderten Zugriffsberechtigungen (siehe Kapitel *2.3.2 App-Zugriffsrechte*). Haben bestimmte Apps besonders weitreichende Zugriffsrechte, wird der Anwender benachrichtigt. Er hat nun die Wahl, diesen Apps die erteilten Zugriffrechte nachträglich wieder zu entziehen – was meist die Deinstallation der betreffenden Anwendung bedeutet. Apps können sogar vor der Installation durch den Anwendungscheck auf Unbedenklichkeit hin geprüft werden. Sollten aufgrund von gesammelten Erfahrungswerten und Dateianalyse Auffälligkeiten festgestellt werden, blockiert die Schutzsoftware die App-Installation. Anzumerken ist hierbei, dass die Erfahrungswerte, die die Grundlage für den Abgleich darstellen, von Hersteller zu Hersteller variieren und unterschiedliche Aktualität aufweisen. Gewiefte Entwickler von schadhaften Anwendungen könnten den Prüfmechanismus sehr leicht aushebeln, indem sie ständig neue Versionen ihrer Anwendungen mit veränderten Funktionen veröffentlichen. Der Anwendungs-Check kann also die menschliche Komponente, die kritische Überprüfung der gewünschten Anwendungen, nicht ersetzen. Sollte eine Anwendung zur Installation Root-Rechte benötigen, ist von der Installation dieser Software grundsätzlich abzusehen.

***Der Anwendungscheck ist wichtiger Bestandteil jeder Virenschutz-App. Er überprüft auf Schädlingsbefall und meldet Apps mit auffällig vielen Zugriffsrechten.***

***Installieren Sie auf Smartphones und Tablets eine Virenschutz-Lösung mit angemessenem Funktionsumfang, inklusive der Möglichkeit zum Echtzeit-Virenscan, zur Systemprüfung und zum Anwendungscheck. Halten Sie Ihre Virenschutz-Software stets auf dem neuesten Stand. Verlassen Sie sich nicht allein auf die Virenschutz-Software, sondern nutzen Sie Ihre Smart Mobile Devices mit Bedacht. Gewähren Sie keiner Anwendung Root-Rechte.***

### 3.2.4 Personal Firewall

***Die Personal Firewall auf dem Smartphone kann nur sehr bedingt Datenabfluss verhindern. Mehr Schutz bietet die sichere Handhabung der Geräte. Nutzer sollten sich umfassend über Apps informieren, bevor sie diese installieren.***

Die Personal Firewall einer Mobile Security Suite gleicht einer Personal Firewall bei Laptops nur bedingt. Sie analysiert – soweit es ihr möglich ist – die Netzwerkverbindungen des betreffenden Smartphones oder Tablets. Je nach eingestellter Sicherheitsstufe entscheidet sie entsprechend eines Reglements, ob der ein- und ausgehende Datenverkehr zwischen einer Anwendung und einem Netzwerk, beispielsweise dem Internet, geblockt wird oder nicht. Der Nutzer kann in einem Dialog entscheiden, ob einer App beispielsweise der Internetzugriff erlaubt wird oder nicht. So entsteht nach und nach ein Verbindungsfilter, der unbemerkten Datenabfluss verhindern kann. Sicherheitsexperten warnen allerdings davor, die Blockade-Funktion der Personal Firewall Apps zu überschätzen. Ohne erweiterte Zugriffsrechte, dem Root-Zugriff, kann nicht ausgeschlossen werden, dass trotz angeblich blockierter Kommunikation zwischen einer bestimmten App und einem Internetserver Datenpakete abfließen. Viele Personal Firewall Apps können also nur scheinbar Verbindungen kappen. Anwender sollten sich daher auf den gesunden Menschenverstand verlassen und diese Funktionen ihrer App eher als Entscheidungshilfe sehen.

#### Zusätzliche Funktion: URL-Filter

Neben der oben genannten Funktion warnen viele Personal Firewalls vor gefährlichen URLs, sobald diese durch den Nutzer oder eine Anwendung aufgerufen werden. Soll eine URL aufgerufen werden, die aufgrund von gesammelten Erfahrungswerten, oft Website-Reputation genannt, und formalen Auffälligkeiten als gefährlich eingestuft wird, verhindert die Personal Firewall das Aufrufen der Seite im Browser noch vor Verbindungsaufbau. Da der jeweilige Hersteller einer Mobile Security Suite die Website-Reputationen festlegt, gibt es hierbei herstellerspezifische Unterschiede. Es kann passieren, dass eine MSS-Lösung vor einer gefährlichen (Phishing-)Website warnt, während ein anderes Produkt dieselbe Website als ungefährlich einstuft. Eine formale Auffälligkeit kann beispielsweise durch die Länge der Internetadresse begründet werden: Sogenannte Short-URLs sind stark verkürzte Internetadressen, die aufgrund ihrer Praktikabilität oft in sozialen Netzwerken wie Twitter zum Einsatz kommen. Beispielsweise führt die Short-URL „http://bit.ly/16Meh7Q“ auf die Internetseite des Projekts IT-Sicherheit im Handwerk (www.it-sicherheit-handwerk.de). Da der Nutzer aufgrund der kryptischen Zeichenfolge einer Short-URL aber nicht mehr die tatsächliche Zieladresse eines Links erkennen kann, muss er blind darauf vertrauen, nach Aktivierung des Links auf die gewünschte Seite umgeleitet zu werden. Ein Vertrauen, das von Kriminellen ausgenutzt werden kann, um auf schadhafte Webseiten zu lotsen. Es ist ratsam, die Personal Firewall sensibel einzustellen, sodass sie vor Short-URLs warnt, Zieladressen der verkürzten Links anzeigt und gegebenenfalls den Verbindungsaufbau blockiert.

***Auf der Internet-Seite http://unshort.me/ können Short-URLs aufgelöst werden.***

### Schutz vor USSD-Manipulation

Der Besuch einer präparierten Seite kann dazu führen, sämtliche auf dem Gerät gespeicherten Daten zu verlieren. Auch eine Sperrung der SIM-Karte ist möglich. Android-Geräte vor Version 4.1.1 sind anfällig für Manipulation über USSD-Steuercodes, die beim Aufruf einer präparierten Seite bestimmte Funktionen auslösen können. QR-codierte URLs, die mit den Buchstaben „TEL“ beginnen, können beispielsweise einen bestimmten USSD-Steuercode automatisch auslösen, der mehrmals hintereinander einen bestimmten PIN und nachfolgend eine bestimmte PUK an das Telefonmodul des Gerätes übermittelt, sodass sich die SIM-Karte durch die mehrmalige Falscheingabe der PIN automatisch sperrt. Anwender können mithilfe des USSD-Checks vom Heise-Verlag[31] testen, ob ihr Gerät anfällig ist für USSD-Manipulation Sofern es anfällig ist, kann die App NoTelURL[32] Schutz bieten. Hiermit kann der Nutzer einstellen, dass beim Aufruf einer URL, in der sich ein versteckter USSD-Steuercode befindet, statt der Telefonanwendung standardmäßig die NoTelURL-Anwendung ausgeführt werden soll. Diese analysiert den „TEL:“-Befehl und blockiert die Ausführung bei einem Angriffsversuch. Harmlose Befehle kann der Nutzer auf Wunsch in einem Dialog zulassen.

***Installieren Sie eine Personal Firewall auf Ihrem Smartphone und/oder Tablet. Halten Sie diese stets auf dem neuesten Stand und wählen Sie eine angemessene Sicherheitsstufe. Sind Sie Android-Nutzer, sollten Sie überprüfen, ob Ihr Gerät anfällig ist für USSD-Manipulation und gegebenenfalls die kostenlose App NoTelURL installieren.***

## 3.2.5 Anruf- und SMS-Filter

Die meisten Geräte bieten von Werk aus die Möglichkeit, bestimmte Kontakte zu sperren, sodass Anrufe und SMS blockiert werden. Die entsprechende Funktion findet sich meist in einem Auswahlmenü bei den Kontaktdetails. Alternativ erfüllen diesen Zweck viele MSS-Produkte sowie kostenlose Apps wie Schwarze Liste (Blacklist)[34] für Android. Der Anruf- und SMS-Filter filtert auf dem Smartphone unerwünschte Text-Nachrichten und Anrufe auf Basis einer Schwarzen und einer Weißen Liste. Beide enthalten Telefonnummern und Kontaktdaten von Personen, deren Kommunikationsversuche entweder erwünscht sind (Weiße Liste) oder unerwünscht sind (Schwarze Liste).

***Der Anruf- und SMS-Filter selektiert anhand der weißen Liste (erwünschte Kontakte) und der schwarzen Liste (unerwünschte Kontakte).***

Die Schwarze Liste beinhaltet in Bezug auf Antispam bei MSS-Produkten typischerweise E-Mail-Adressen und E-Mail-Domains, die durch Spamversand auffällig geworden sind. In Bezug auf Anruffilter sind dies üblicherweise Telefonnummern. Wird bei einem Anruf oder einer SMS eine Übereinstimmung ausschließlich mit der Schwarzen Liste festgestellt, so wird der Anruf oder die SMS blockiert und dem Nutzer nicht angezeigt. Die blockierten Kommunikationsversuche von Telefonnummern und Kontakten der Schwarzen Liste werden protokolliert und so für den Nutzer dokumentiert. Er hat zudem die Möglichkeit, manuell bestimmte Rufnummern der Schwarzen oder Weißen Liste hinzuzufügen und weitere Einstellungen des Anruf- und SMS-Filters

[31] *Siehe hierzu: http://www.heise.de/security/dienste/USSD-Check-1717811.html*
[32] *http://fotovossblog.peggy-forum.com*
[34] *http://anttek.com/support/blacklist-for-android-user-guide*

vorzunehmen. Nachteil bei der Verwendung einer MSS oder App zur Filterung der Anrufe und SMS ist, dass der Nutzer oft nicht darüber Bescheid weiß, welche seiner Kommunikationsdaten auf den Servern des jeweiligen App-Herstellers landen.

### Sperrung der Premium-SMS-Dienste

Um sich vor der Abzocke durch teure Premium-SMS-Dienste[35] zu schützen (siehe Kapitel *2.2 Viren, Würmer, Trojaner*), sollten Nutzer auf Nummer sicher gehen: durch eine Sperrung der Drittanbieter-Dienste beim Mobilfunk-Provider. Je nach Provider können einzelne Rufnummern und Services oder sämtliche Drittanbieter-Dienste, sogenannte Mehrwertdienste, zur Abrechnung gesperrt werden. Die Möglichkeit zur Sperrung dieser Dienste ist eindeutig im Telekommunikationsgesetz (TKG) seit 2012 geregelt:

***Schutz vor Kosten durch Premium-SMS, welche durch unbemerkt installierte Schadsoftware verschickt werden, bietet die providerseitige Sperre aller Drittanbieterdienste.***

*„Der Teilnehmer kann von dem Anbieter öffentlich zugänglicher Mobilfunkdienste und von dem Anbieter des Anschlusses an das öffentliche Mobilfunknetz verlangen, dass die Identifizierung seines Mobilfunkanschlusses zur Inanspruchnahme und Abrechnung einer neben der Verbindung erbrachten Leistung unentgeltlich netzseitig gesperrt wird.“* (§ 45d, TKG)

Im Gegensatz zum Anruf- und SMS-Filter auf dem jeweiligen Gerät setzt die providerseitige Sperre auf einer höheren Ebene an und bietet somit größeren Schutz.

T-Mobile-Kunden können hierzu die Service-Kurzwahl 2202 wählen, um folgende Dienste kostenlos sperren zu lassen:

- „Sperre von Business-Diensten: Börsenkurse, Nachrichten aller Art, Wetter, Sport, Ticketing Programme“
- „Sperre von Consumer-Diensten: Spiele, Chats“
- „Sperre von 16+ bzw. Adult-Inhalten, beispielsweise erotische Angebote“
- (Telekom Deutschland, o. J.)

O2-Kunden können über die O2-Hotline 0800 33 999 33 drei verschiedene Sperrprofile wählen:

- *„Komplettsperre aller Drittanbieter inkl. O2 Dienste*
- *Alle Drittanbieterdienste und alle O2 Dienste werden gesperrt.“*
- *„Nur Drittanbietersperre exkl. O2 Dienste*
- *Es werden alle Drittanbieterdienste gesperrt, O2 Dienste bleiben weiterhin verfügbar.“*
- *„Nur Drittanbietersperre exkl. O2 Dienste und exkl. Mpass*
  *Es werden alle Drittanbieterdienste gesperrt. Alle mpass Dienste und alle O2 Dienste bleiben weiterhin verfügbar.“*
- (Telefónica Germany, o. J.)

Vodafone-Kunden haben die Wahl, Einzelverkäufe oder Einzelverkäufe und Abos von Drittanbietern sperren zu lassen. Dazu wählen sie im Kundenbereich „MeinVodafone“ unter „Mobiles Bezahlen“ einfach selbst die gewünschte Sperre aus.

[35] *http://www.heise.de/ct/artikel/Abzocke-per-Premium-SMS-1940221.html*

E-Plus-Kunden können eine globale Drittanbietersperre beispielsweise über die Kurzwahl-Rufnummer 1000 einrichten lassen.

***Nutzen Sie einen Anruf- und SMS-Filter auf Ihrem Smartphone. Bevorzugen Sie die systemeigene Filterfunktion – sofern vorhanden. Lassen Sie Premium-SMS-Dienste beziehungsweise sämtliche Drittanbieter-Dienste bei Ihrem Mobilfunk-Betreiber sperren.***

### 3.2.6 Datenverschlüsselungsmechanismen

Nachfolgend einige Datenverschlüsselungsmechanismen.

#### Vollverschlüsselung

***Eine Vollverschlüsselung schützt den gesamten Gerätespeicher vor unbefugtem Zugriff. Falls möglich sollte zusätzlich eine SD-Kartenverschlüsselung eingerichtet werden.***

Eine Vollverschlüsselung schützt das gesamte Dateisystem des Smartphones vor fremden Zugriffen. Sofern in der Betriebssystem-Version angeboten, sollte diese eingerichtet werden. Bei neueren iOS-Geräten wird der Speicher automatisch vollverschlüsselt, sobald eine Code-Sperre eingerichtet wurde. Nutzer von Android (ab Version 4.0) und BlackBerry müssen diese in einem gesonderten Menü einrichten. Der zu wählende Entschlüsselungscode entspricht entweder dem PIN-Code der Zugriffssperre oder kann neu gewählt werden (gegebenenfalls ist die Vergabe eines neuen PIN-Codes oder eines Passwortes möglich). Oft werden SD-Karten nicht mit-verschlüsselt – diese Funktion ist herstellerabhängig. Sofern ein Gerät neben der Vollverschlüsselung auch die SD-Kartenverschlüsselung ermöglicht, findet sich letztere meist im selben Einstellungsmenü wie die Vollverschlüsselung.
Da prinzipiell jede installierte Anwendung auf dem Gerät Zugriff auf die SD-Karte hat, ohne weitere Berichtigungen einfordern zu müssen, empfiehlt es sich, keine sensiblen Daten auf der SD-Karte zu speichern. Auch bei einer verschlüsselten SD-Karte sollten Anwender immer im Hinterkopf behalten, dass die SD-Karte leicht und schnell aus dem Gerät entfernt werden kann. Hat ein Angreifer die SD-Karte in seinen Besitz gebracht, kann er beliebig viel Zeit dafür investieren, die Verschlüsselung zu überwinden.

***Eine Vollverschlüsselung des Gerätes ist ratsam. Unbedingte Maßnahme vor der Einrichtung einer Vollverschlüsselung sollte eine Datensicherung des Gerätespeichers sein – kommt es im Verschlüsselungsvorgang zu einem Fehler, sind die Daten andernfalls verloren.***

#### Container-Verschlüsselung für Ordner

Eine Container-Verschlüsselung schützt Daten auf den Systemen und erlaubt es, diese Daten zusätzlich verschlüsselt mit dem Unternehmensserver zu synchronisieren.

Realisiert werden kann dies mittels einer Mobile Security Suite, einem Mobile-Device-Management-Produkt (siehe Kapitel *5.4 Zentralisierte Verwaltung der Geräte – Mobile Device Management*) oder einer kostenlose Verschlüsselungs-Apps wie „EDS Lite“[36],

[36] *http://sovworks.com*

die auch mit gängiger Verschlüsselungs-Software für Laptops wie TrueCrypt kompatibel ist.

***Zu verschlüsselnde Daten können in einen passwortgeschützten Ordner abgelegt werden. Dieser kann infolge für den Datenaustausch mit dem Unternehmensnetzwerk genutzt werden.***

Zur Verschlüsselung wählen Nutzer die gewünschten Ordner aus und vergeben ein sicheres Masterpasswort zum Entschlüsseln der Ordnerinhalte (Hinweise zur Vergabe sicheren Passwörter: siehe Kapitel *4.2 Passwortsicherheit und -tools*). Infolge liegen die Daten chiffriert auf dem Speicher des jeweiligen Geräts bis zu dem Zeitpunkt der Entschlüsselung via Passwort. Personen, die sich unbefugt Zugriff zu den verschlüsselten Daten verschaffen wollen, finden ohne das entsprechende Passwort nur unlesbare Daten vor. Alle Dateien, die in die verschlüsselten Ordner, auch Container genannt, kopiert werden, stehen danach ebenfalls unter dem Schutz der Verschlüsselung.

Weitere Hinweise hierzu im Kapitel *5.4.3. Trennung zwischen Unternehmens- und Privatbereich auf den Geräten.*

Einen erhöhten Schutz bietet die Konfigurationsmöglichkeit, den Datenzugriff, der durch Passworteingabe gewährt wird, nach Ablauf einer festgelegten Zeitspanne und Inaktivität wieder zu verwehren. Mit dieser Einstellung wird der Zugriff gesperrt, wenn das Programm oder der Ordner eine bestimmte Zeit nicht genutzt wurde, sodass der Nutzer erneut zur Eingabe des Passwortes aufgefordert wird.

### Verschlüsselung der Kommunikation

Neben der Möglichkeit, einzelne Ordner zu verschlüsseln, können Smartphone-Nutzer verschiedene Möglichkeiten nutzen, Textnachrichten oder E-Mails verschlüsselt auszutauschen. Diese können vom Empfänger nur dann gelesen werden, wenn er das entsprechende Passwort kennt. So können Mitarbeiter die IT-Sicherheit erhöhen, wenn sie sensible Informationen nur mittels echter Ende-zu-Ende-Verschlüsselung austauschen.

***PGP benötigt einen entsprechenden PGP-Schlüssel, während S/MIME typischerweise ein sogenanntes X.509v3-Zertifikat zur Verschlüsselung erfordert.***

Wie bei Laptops könnten auch Smartphone- und Tablet-Nutzer ihre E-Mails mittels PGP-Verschlüsselung schützen, eine Alternative stellt S/MIME dar. Der Vollständigkeit halber sei erwähnt, dass S/MIME auch zusammen mit PGP verwendet werden kann. Die Verfahren unterscheiden sich vor allem durch die Art des vertrauenswürdigen Austausches von öffentlichen Schlüsseln. PGP benötigt einen entsprechenden PGP-Schlüssel, während S/MIME typischerweise ein sogenanntes X.509v3-Zertifikat erfordert. S/MIME wird von den meisten E-Mail-Clients standardmäßig unterstützt, für PGP ist dagegen häufig eine Erweiterung notwendig.

Beide sind auch kostenlos einsetzbar, wobei es für S/MIME nur sehr wenige kostenlose und sinnvoll nutzbare Zertifikate gibt. Einen PGP-Schlüssel können Sie mithilfe verschiedener Programme erzeugen, die den OpenPGP-Standard umsetzen.

Das kann zum Beispiel über das freie PGP-Programm des Projekts GnuPG geschehen oder auch über kommerzielle Angebote.

Durch den Einsatz dieser Technologien können E-Mails nicht nur verschlüsselt und somit für Fremde unleserlich gemacht werden, sondern auch digital signiert, also unterschrieben werden. Damit kann der Empfänger sicher sein, dass der Absender tatsächlich der ist, für den er sich ausgibt. So wird gleichzeitig das Problem des gefälschten Absenders gelöst.

Für den privaten Gebrauch ist es am einfachsten, PGP einzusetzen. Dabei ist wichtig zu wissen, dass der Kommunikationspartner natürlich über die gleiche Verschlüsselungsmethode verfügen muss. Bei PGP benötigen die Partner jeweils die öffentlichen Schlüssel voneinander. Ist die Verschlüsselung jedoch erst einmal eingerichtet, genügt ein Mausklick, um eine E-Mail zu verschlüsseln. Wie eine solche PGP-Verschlüsselung installiert und verwendet werden kann, zeigt ein Onlineworkshop[37] oder eine Schritt-für-Schritt-Anleitung[38] des Instituts für Internet-Sicherheit. Mehr zum Thema Verschlüsselung im Onlineartikel «Kryptographie» [39].

***Threema ist eine sichere Alternative zu WhatsApp.***

PGP und S/MIME sollte grundsätzlich nur auf vertrauenswürdigen Geräten eingerichtet werden, da der private Schlüssel auf dem Speicher des Geräts liegt und somit leichter entwendet werden kann.
Ist Mitarbeitern die Verwendung eines Instant Messengers zur Kommunikation mit den Kollegen gestattet, sollte eine Software gewählt werden, die Gespräche automatisch verschlüsselt (vgl. Kapitel *2.3.3 Fokus WhatsApp – Instant Messenger mit Tücken*). Beispiel für solch einen Messenger ist die App Threema[40] für Android und iOS (Preis: rund 2 Euro). Threema ist ein Beispiel für eine App, die laut Hersteller eine Ende-zu-Ende-Verschlüsselung realisiert, bei der nur die Gesprächspartner den Gesprächsverlauf lesen können[41].
Eine effiziente Gesprächsverschlüsselung ist auch ratsam. Immer mehr Lösungen werden als App kostenlos oder preisgünstig angeboten.

***Richten Sie falls möglich eine Vollverschlüsselung für den gesamten Gerätespeicher und Ihre Speichererweiterungskarten (z.B. SD Memory Cards) ein. Schützen Sie sensible Dateien auf den Geräten in passwortgeschützten verschlüsselten Daten-Containern. Verschlüsseln Sie Ihre Kommunikation mithilfe geeigneter Software, achten Sie hierbei auf eine echte Ende-zu-Ende-Verschlüsselung.***

***Vollverschlüsselung und SD-Kartenverschlüsselung unter Android: Einstellungen -> Sicherheit -> Verschlüsselung [Speicher und SD-Karten auswählen]***

***Vollverschlüsselung und SD-Kartenverschlüsselung unter BlackBerry: Optionen -> Sicherheit -> Verschlüsselung [Speicher und Medienkarte auswählen]***

### 3.2.7 Logischer Diebstahlschutz

Wie in Kapitel *2.8 Geräteverlust und -diebstahl* schon beschrieben, hat laut BITKOM jeder zehnte Deutsche schon einmal sein Mobiltelefon verloren; die Hälfte der verlorenen Geräte fiel Dieben in die Hände (vgl. BITKOM, 2012b). Was passiert, wenn das

[37] *http://www.internet-sicherheit.de/institut/buch-sicher-im-internet/videos/screenvideos/?tx_bddbflvvideogallery_pi1%5Bvideo%5D=3*
[38] *http://www.internet-sicherheit.de/fileadmin/docs/pgp-zi/Anleitung_PGP-Schluessel.pdf*
[39] *http://www.internet-sicherheit.de/institut/buch-sicher-im-internet/workshops-und-themen/verschluesselung-und-identitaeten/kryptographie/grundlagen-der-kryptographie/*
[40] *https://threema.ch/de/*
[41] *Stand 12/13*

verlorene Smartphone von Fremden gefunden wird? Diese Frage stellte sich das Sicherheitsunternehmen Symantec und entwickelte ein Experiment: Die Sicherheitsexperten verteilten 50 Smartphones, auf denen Apps installiert wurden, die scheinbar Zugriff auf sensible persönliche und berufliche Daten ermöglichen (vgl. Symantec, 2012). In Wahrheit erfüllten die einschlägig betitelten Apps für Online-Banking, Soziale Netzwerke, E-Mail-Konten, Kalender, Kontakte, Dokumente und Passwörter keine echte Funktion, sondern dienten nur als Lockmittel. Versuchte Zugriffe auf diese Apps wurden protokolliert. Das Ergebnis: Über 80 Prozent der Finder versuchten, auf berufliche Apps und Daten zuzugreifen, 90 Prozent versuchten an persönliche Daten zu gelangen und 70 Prozent versuchten sogar beides (ebenda).
Diese Zahlen sprechen eine deutliche Sprache: Das Risiko, (Daten-)Dieben zum Opfer zu fallen, ist groß. Selbst, wenn ein Finder eines Smartphones lediglich versucht, einen Kontakt zum Besitzer herzustellen, kommt es zu unbefugtem Datenzugriff. Anwender sollten daher die Vielzahl sensibler Daten auf den Geräten schützen – diese sind meist wertvoller als das Gerät selbst.
Ein guter Diebstahlschutz für Smartphones und Tablets kombiniert mehrere Schutzmaßnahmen aus den zuvor genannten Kapiteln. Das Gerät des Anwenders sollte eine sichere Zugriffssperre aufweisen, gespeicherte Daten sollten durch Verschlüsselungsmechanismen geschützt sein und regelmäßig auf externen Datenträgern als Sicherungskopien abgelegt werden.

## IMEI – der Geräte-Fingerabdruck

***Die IMEI-Nummer dient zur Identifikation jedes Smartphones.***

Smartphone-Anwender sollten sich die International Mobile Station Equipment Identity (IMEI) ihres Gerätes separat notieren. Diese 15-stellige Seriennummer dient zur eindeutigen Identifikation des Smartphones und ist hilfreich, sobald ein Anwender sein Gerät beim Mobilfunkanbieter oder bei der Polizei als gestohlen melden möchte. Stellt die Polizei Diebesgut sicher, können über den Abgleich der IMEI-Nummern schnell die Besitzer der Geräte ausfindig gemacht werden. Die IMEI findet sich gedruckt auf einem Etikett unter dem Geräteakku, manchmal auch auf der Originalrechnung oder -verpackung des Geräts. Alternativ kann die Nummer technisch über die Eingabe des Codes „*#06#“ (ohne Anführungszeichen) im Eingabefeld des Smartphones abgefragt werden.

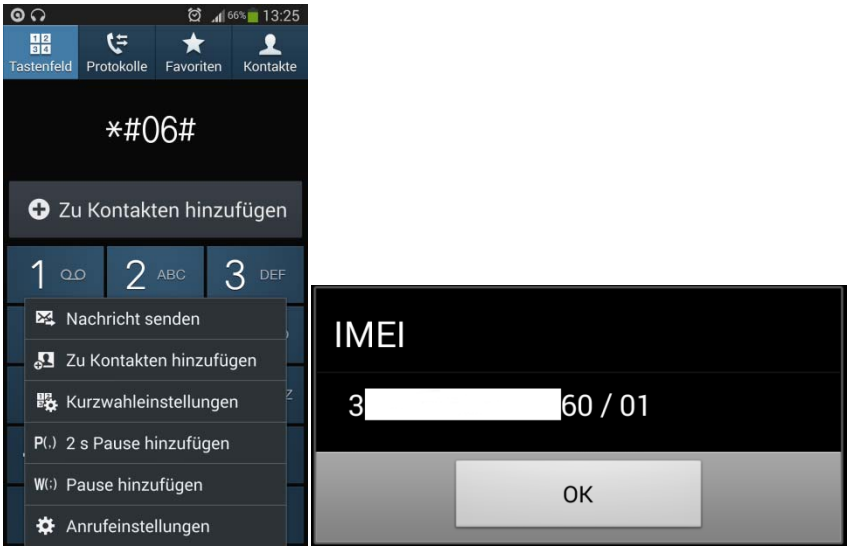



*Abbildung 10: IMEI-Abfrage über das Smartphone-Eingabefeld*

Die installierte Mobile Security Suite des Anwenders sollte über Fern-Ortungs-, Sperr- und Lösch-Funktionen verfügen, die je nach Software unterschiedlich effektiv sind. Anwender sollten bei der Auswahl eines Softwareprodukts darauf achten, ob tatsächlich alle gespeicherten Daten, also auch diejenigen auf den externen SD-Karten, mittels Fern-Löschung gelöscht werden können.

***Fernortungs-, Sperr- und Lösch-Funktion haben neuere Geräte ab Werk. Ansonsten muss auf die MSS-Lösung zurückgegriffen werden.***

**Physische Schutzmaßnahmen**

Besitzer mobiler Endgeräte sollten ihre Smartphones und Tablets stets im Auge behalten, nie verleihen oder aus der Hand geben. Auch der Arbeitsplatz im Büro sollte nie ohne das mobile Endgerät verlassen werden, gerade dann, wenn das Büro von Kunden und Reinigungskräften frequentiert wird. Auf Messen und Tagungen können portable Schlösser an Schutzhüllen befestigt werden, sodass sie einen kleinen Schutz vor Gelegenheitsdieben bieten. Die Schlösser binden die kleinen Geräte an größere Objekte wie beispielsweise einen Messetisch, sodass sie nicht einfach mit einem Griff entwendet werden können.

***Stellen Sie sicher, dass die installierte Mobile Security Suite Fern-Ortungs-, Sperr- und Löschfunktionen im Funktionsumfang beinhaltet. Geben Sie ihr mobiles Endgerät niemals aus der Hand. Verlassen Sie Ihren Arbeitsplatz nicht ohne Ihr Smartphone und/oder Tablet. Nutzen Sie – wenn möglich – portable Schlösser zum Schutz vor Gelegenheitsdieben, die beispielsweise auf Messen sehr aktiv sind. Notieren Sie sich die IMEI Ihres Smartphones.***

### 3.2.8 Aktualitätsprinzip – Sicherheitsupdates und -tools

Wie zuvor dargestellt, spielt die Aktualität der genutzten Mobile Security Suite eine entscheidende Rolle für die Analyseergebnisse und Abwehr von Schädlingen. Analog zum Aktualitätsprinzip bei Laptops (siehe Kapitel *3.1.4 Aktualitätsprinzip – Sicherheitsupdates und -tools*) kann die Notwendigkeit der Software-Aktualität sämtlicher installierter Anwendungen und insbesondere des Betriebssystems von Smartphones und Tablets gar nicht oft genug betont werden.

***Aktualität von Betriebssystem und installierter Software muss zur Bedingung in jedem Unternehmen werden.***

Dem gegenüber steht der leichtfertige Habitus vieler Smartphone-Nutzer: Nur ein Viertel der Anwender aktualisiert das Betriebssystem umgehend nach Erscheinen eines neuen Updates (vgl. hier und im Folgenden: Tomorrow Focus Media, 2013). Der Rest wartet, bis ihn das Gerät selbst an das Update erinnert (35 Prozent), bis andere Nutzer Feedback zum Update geben (11,7 Prozent) oder bis es ihm zeitlich passt (7,3 Prozent). Rund ein Fünftel aller Smartphone-Nutzer weiß nicht, ob sein System aktuell ist oder aktualisiert grundsätzlich nicht. Daher ist es ratsam, automatische Updates nach Möglichkeit zu aktivieren und Updates zentral zu steuern. Für Handwerksbetriebe ist es empfehlenswert, einen IT-Dienstleister zu Rate zu ziehen. Anwender sollten ein Bewusstsein für die Notwendigkeit aktueller Software entwickeln. Neigen Mitarbeiter in puncto Software-Aktualisierung zur Vergesslichkeit, sollten sie häufiger vom Sicherheitsbeauftragten daran erinnert werden, zu updaten. Software-Aktualität sollte zudem als festgelegte Norm Teil der Unternehmensrichtlinien sein (siehe Kapitel *5.3 Auflagen und Richtlinien für die Mitarbeiter*).

Android-Nutzer können in den Einstellungen des Play Stores die automatische Update-Funktion aktivieren, sodass installierte Apps bei Erscheinen einer neueren Softwareversion automatisch aktualisiert werden.
Alle Nutzer von Smartphones sollten regelmäßig prüfen, ob sie alle installierten Apps noch benötigen. Nicht mehr verwendete Apps sollten sofort deinstalliert werden.

### Heterogene Android-Landschaft

Neben der anwenderbedingten Trägheit in Sachen System-Updates, gibt es im Fall von Android auch Gerätehersteller-bedingte Verzögerungen. Hat Google ein neues Update seines Betriebssystems Android entwickelt, wird es zunächst an die Gerätehersteller verteilt und dort an die spezifische Hardware der hauseigenen Geräte angepasst. Die Anpassung (im Fachjargon: Portierung) des bereitgestellten Android-Programmcodes durch die Geräte-Hersteller nahm in der Vergangenheit einige Zeit in Anspruch (vgl. Lamberty, 2012).


*Abbildung 11: Verspätete Android-Updates in Monaten nach Hersteller (heise online nach Lamberty, 2012)*

Je nach Hersteller ergaben sich enorme Verzögerungen bis eine neue Android-Version für die Nutzer bereitstand – ein einladender Spielraum für Angreifer, die Schwachstellen alter Versionen für ihre Zwecke auszunutzen. Die Konsequenz der unterschiedlich langen Veröffentlichungswege ist eine große Fragmentierung unterschiedlicher Android-Versionen, die derzeit in Umlauf sind.

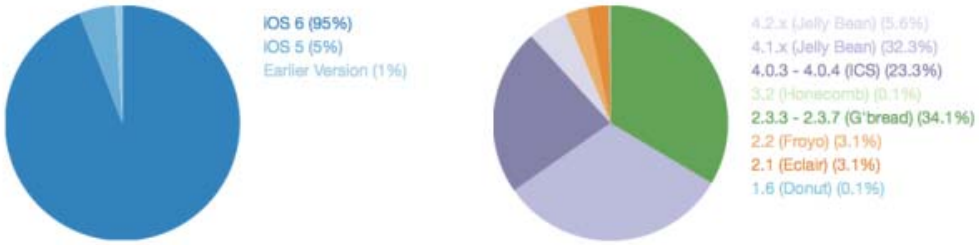



*Abbildung 12: Fragmentierung iOS- und Android-Betriebssystem im Vergleich (Open Signal nach Beiersmann 2013)*

Einige ältere Android-Geräte sind hardwareseitig überhaupt nicht mit den neueren Android-Versionen kompatibel. Andere werden durch den jeweiligen Gerätehersteller nicht mehr mit Updates versorgt. Diese Problematik ist eine Herausforderung für die

Unternehmensführung und die Sicherheitsbeauftragten in Unternehmen, da ältere Android-Versionen anfälliger sind für Schädlinge. Gegebenenfalls sollte über den Ausschluss bestimmter Geräte vom Unternehmensnetzwerk entschieden werden (siehe Kapitel *5.2 Auflagen und Richtlinien für die Mitarbeiter*). Beim Kauf neuer Geräte sollte darauf geachtet werden, welcher Hersteller guten Service auch für ältere Geräte bietet, indem er sie laufend mit neuen Updates versorgt. Bei Smartphones der Typenreihe Nexus gibt es kürzere herstellerbedingte Verzögerungen in Sachen Betriebssystem-Updates – hier erfolgt der Vertrieb durch Google selbst, eine Portierung der Android-Updates entfällt.

Wie in Kapitel *3.1.4 Aktualitätsprinzip Sicherheitsupdates und -tools* beschrieben, gibt es nützliche Apps, die dabei helfen, Software auf dem neuesten Stand zu halten. Apps wie securityNews[43] informieren über das Erscheinen von Sicherheitsupdates sowie über aktuelle Sicherheitshinweise.

***SecurityNews für iOS, Android und Windows 8 liefert nützliche Hinweise zu Sicherheitsupdates und -meldungen.***

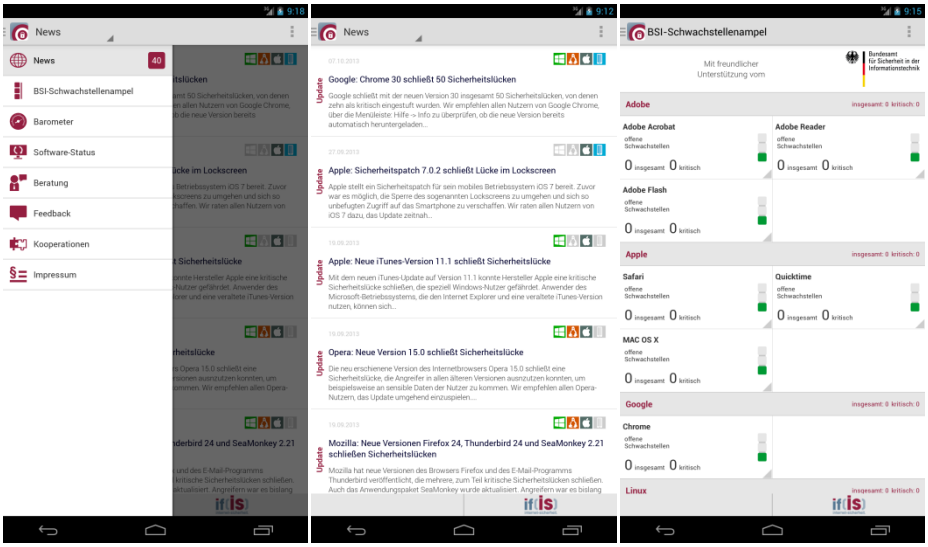



*Abbildung 13: App securityNews für iOS, Android und Windows 8. Von links: Navigation, Newsfeed, BSI-Schwachstellenampel*

***Halten Sie das Betriebssystem Ihres mobilen Endgerätes, die Mobile Security Suite und sämtliche installierte Anwendungen stets auf dem neuesten Stand. Installieren Sie Apps wie securityNews für iOS, Android oder Windows 8, um über aktuelle Sicherheitsmeldungen informiert zu werden. Deinstallieren Sie Apps, die Sie nicht mehr benötigen.***

### 3.2.9 Datensicherung – Backup-Tools für Smartphones und Tablets

Smartphone- und Tablet-Speicher beherbergen eine Vielzahl Daten: Kalender-, Adress- und Telefonbuch-Daten,Fotos, Videos, Dokumente, E-Mails und SMS mit sensiblen Inhalten. Bei beruflicher Nutzung können neben geschäftlicher E-Mail-Korrespondenz auch Kunden-Stammdaten und andere hochsensible Datensätze ihren

[43] *https://www.it-sicherheit.de/securitynews/*

Weg auf die Geräte finden. Grund hierfür kann der Gebrauch von Enterprise Apps sein, die beispielsweise Datenerfassung direkt beim Kunden vor Ort ermöglichen. Meist ist es eine Frage der Software-Einstellung, ob erfasste Daten lokal auf dem Eingabegerät oder auf dem Unternehmensserver abgelegt werden. Bei Geräteverlust kann ein enormer Schaden entstehen. Kurzum: Regelmäßige Datensicherungsmaßnahmen müssen bei Smartphones und Tablets analog zu Laptops und Desktop-PCs getroffen werden. Es gibt bei Smartphones und Tablets verschiedene Möglichkeiten, Datensicherungskopien (Backups) anzulegen.

### Synchronisation mit dem Laptop oder Desktop-PC

***Die gespeicherten Daten auf den Geräten sollten regelmäßig auf separaten Speichermedien gesichert werden.***

Den meisten Geräten wird von Haus aus eine Software bereitgestellt, mit der Anwender ihr Gerät mit einem Desktop-PC oder einem Laptop verbinden und Inhalte austauschen können. Diese Software ist meist in Form einer CD-ROM Teil des Produktumfangs beim Kauf des Geräts. Alternativ können Anwender diese Software aus dem Internet beziehen – dann können sie sicher sein, dass sie sich eine aktuelle Programmversion installieren. Verwaltungsprogramme unterscheiden sich je nach Betriebssystem und Hersteller erheblich in ihrem Funktionsumfang, sodass sich einige Programme nur bedingt oder gar nicht zur Datensicherung eignen.
In jedem Fall sollten Anwender regelmäßig sämtliche auf den Geräten gespeicherten Daten – also auch Einstellungsdaten, Anruflisten und Apps – sichern. Sofern die Software dies nicht ermöglicht, sollte eine alternative Software zur Erstellung der Backups genutzt werden (siehe auch: *3.1.5 Datensicherung – Backups*).
Nachfolgend ein kurzer Überblick über gängige Software-Produkte:

Apples iTunes legt automatisch ein Backup der auf dem jeweiligen Gerät gespeicherten Daten an, sobald das iPhone oder iPad mit dem Computer verbunden wird. Zur Verschlüsselung des angelegten Backups sollten Anwender in der Navigationsleiste unter dem Punkt „Übersicht“ die Option „iPhone-Backup verschlüsseln“ beziehungsweise „iPad-Backup verschlüsseln“ wählen. iTunes ermöglicht es Anwendern beispielsweise bei Geräteverlust, sämtliche gespeicherte Daten des letzten Backups auf ein neues Gerät zu übertragen.

Android-Geräte kommen je nach Geräte-Hersteller mit unterschiedlichen Software-Produkten daher. Samsung-Smartphones (mit Android-Betriebssystem) werden üblicherweise mit der Software Kies ausgeliefert. Hiermit können Daten ausgewählt werden, die auf der Festplatte des PCs gesichert werden sollen. Kies ermöglicht es, auch Dateien fremder Smartphones auf das Samsung-Gerät zu übertragen.

HTC-Geräte, auf denen das Betriebssystem Android installiert ist, kommen mit dem HTC Sync Manager daher, der die Synchronisation von Multimedia-Dateien (Fotos, Audio- und Videodateien), Kontaktdaten sowie Browsereinstellungen anbietet.

Die Software Windows Phone Anwendung für Windows-Geräte ab Version 8 bietet lediglich die Möglichkeit, Multimedia-Dateien zwischen Smartphone oder Tablet und PC zu verschieben.

Nutzer von BlackBerry-Geräten haben mit dem Programmpaket BlackBerry Desktop erweiterte Speicherungsmöglichkeiten und können beispielsweise via BlackBerry Media Synch Fotos, Videos und Audiodateien kopieren. Daneben wird auch die Synchronisation von Kalenderdaten und E-Mail-Konten bereitgestellt. Auch die Übertragung der gespeicherten Daten auf ein neues Gerät ist möglich.

### Backup-Apps

Apps (ohne Root-Rechte) sind in der Regel nicht in der Lage, komplette System-Backups sämtlicher auf den Geräten befindlicher Daten anzufertigen. Dies ist darin begründet – wie in *Kapitel 3.3.2 App-Zugriffsrechte* schon erwähnt – dass beispielsweise einige Anwendungsdateien auf einem geschützten Bereich des Geräte-Speichers liegen, der für Apps nicht zugänglich ist. Eine Kopie der meisten Daten gelingt normalerweise nur in Verbindung mit einer Software für PC oder Laptop, wie beispielsweise dem kostenlosen My Phone Explorer[44] für Android-Geräte. Dieser ermöglicht es unabhängig vom Geräte-Hersteller in Verbindung mit der zugehörigen App MyPhoneExplorer Client, alle Daten zur Übertragung auf den PC oder Laptop auszuwählen. Dabei fungiert die App lediglich als Schnittstelle, das eigentliche Systemabbild wird durch die PC-Anwendung realisiert. Ein ähnliches Paar bilden das Programm Helium[45] und die zugehörige App Helium - App Sync and Backup. Hier gibt es allerdings zwei unterschiedliche Software-Versionen, eine kostenlose und eine kostenpflichtige. Erstere beschränkt die möglichen Speicherorte des Backups auf die SD-Karte im Smartphone (sofern vorhanden) und einen Cloud Service. Aufgrund der begrenzten Auswahl der Backup-Speicherorte (und wegen eventueller Lizenzkonflikte) ist die kostenpflichtige Version von Helium somit vorzuziehen.

***Backup-Apps können in der Regel nur in Verbindung mit einer Software für Laptop/Desktop-PC die meisten Daten des Gerätespeichers sichern.***

### Synchronisation mit der Cloud

Prinzipiell ist es möglich, Sicherungskopien der gespeicherten Daten in einer Cloud abzulegen. Dem Vorteil der ständigen Zugriffsmöglichkeit über das Internet stehen einige wichtige Sicherheitsbedenken gegenüber. So sollten sich Anwender unbedingt gut überlegen, welchen Cloud-Dienstleister sie nutzen wollen – stehen die Server des Anbieters außerhalb der EU, liegt häufig ein geringeres Datenschutzniveau vor. Als Konsequenz könnten die Daten des Anwenders weniger gut vor staatlichem Zugriff geschützt sein, wie es beispielsweise in den USA der Fall ist.

***Von der Synchronisation mit der Cloud eines US-amerikanischen Anbieters ist abzuraten – hier hat der Staat die Möglichkeit, gespeicherte Daten einzusehen.***

Im Vorfeld sollten zudem die Sicherheitsvorkehrungen des Cloud-Dienstleisters und dessen Seriosität überprüft werden (siehe Handbuch *Cloud Computing*, Abschnitt *Auswahl Cloud-Anbieter*). Personenbezogene Daten sollten prinzipiell nur verschlüsselt in der Cloud gespeichert werden – es sei denn, ein Unternehmen betreibt seine eigene Cloud, beispielsweise via OwnCloud[46] (siehe Handbuch *Cloud Computing*). Der Übertragungsweg der Daten vom Gerät in die Cloud sollte stets ein sicherer sein. Apps zur Synchronisation mit der Cloud sollten daher SSL/TLS-Übertragungsverschlüsselung nutzen (siehe Kapitel *4.4.1 HTTPS*). Anwender sollten die voreingestellten Synchronisations-Routinen ihres Gerätes mit der Cloud überprüfen und gegebenenfalls anpassen (siehe dazu die nachfolgende Abbildung 14).

[44] *http://www.fjsoft.at/de*
[45] *http://clockworkmod.com*
[46] *http://owncloud.org*

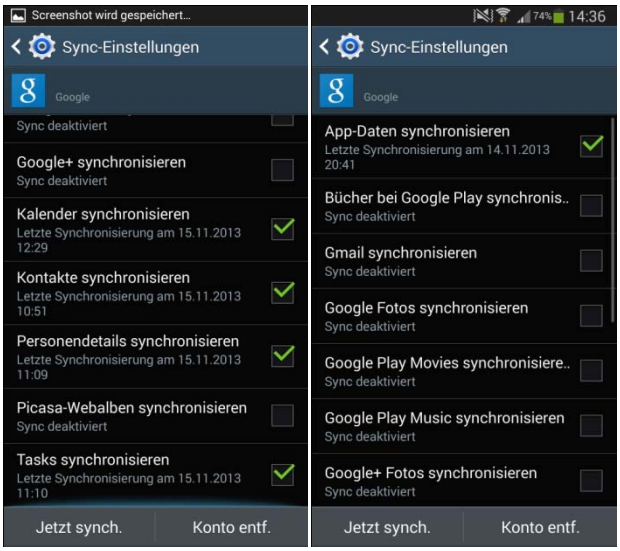



*Abbildung 14: Synchronisations-Einstellungen unter Android*

Ist das Sicherheitsniveau des jeweiligen Backup-Verfahrens via Cloud ungeklärt oder ungenügend im Sinne der Unternehmensrichtlinien (siehe Kapitel *5.2 Auflagen und Richtlinien für die Mitarbeiter*), sollte grundsätzlich keine Geräte-Synchronisation mit einer Cloud erfolgen. Die herstellereigene Synchronisationssoftware ist stets vorzuziehen und es ist anzuraten, einen Dienst mit Serverstandort in Deutschland zu wählen.

### Weitere Datensicherungsmöglichkeiten und -einstellungen

***Die E-Mail-Konten des Anwenders sollten bevorzugt IMAPS nutzen, da E-Mails hier zentral auf dem Mailserver verbleiben und von dort aus verwaltet werden.***

Grundsätzlich ist es ratsam, so wenige Daten wie möglich lokal auf dem Smartphone oder Tablet zu speichern und so wenige wie möglich in öffentlichen Clouds. So können Anwender den Schaden im Falle des Geräteverlusts eingrenzen.
Die auf dem mobilen Gerät verwalteten E-Mail-Konten sollten grundsätzlich so konfiguriert werden, dass abgerufene E-Mails weiterhin auf dem Server vorliegen und nur eine Kopie auf das Gerät gesendet wird. Verliert ein Mitarbeiter sein dienstlich genutztes Smartphone, kann er noch von einem anderen Gerät auf sein E-Mail-Konto zugreifen.
Zur Übertragung von E-Mails dienen die Protokolle IMAP(S) und POP3(S), wobei am „S“ jeweils die durch SSL/TLS verschlüsselte Verbindung erkennbar ist.
Das Netzwerkprotokoll IMAPS (Interactive Mail Access Protocol Secure) sollte bevorzugt genutzt werden, da es unter anderem Vorteile für den Fernzugriff bietet. Bei IMAPS bleiben E-Mails auf dem Mailserver und werden von dort aus verwaltet.
Bei dem alternative Verfahren POP3S (Post Office Protocol Version 3 Secure) werden E-Mails standardmäßig nach dem Abholen vom Server gelöscht, sofern im E-Mail-Programm nicht manuell eingestellt wurde, dass eine Kopie auf der Server verbleibt.
POP3S ist somit wenig komfortabel, wenn E-Mails auf verschiedenen Geräten bearbeitet werden sollen, was beim mobilen Arbeiten eine wichtige Voraussetzung ist.

Zahlreiche Apps erlauben es zudem, gespeicherte SMS- und MMS-Nachrichten automatisch sichern zu lassen, indem sie sie regelmäßig vom mobilen Gerät zu einem vom Anwender genutzten Mail-Konto hinüber kopieren. Auch die Kontakte können oft mit einem Online-Dienst synchronisiert werden, sodass sie nicht nur lokal auf dem Gerät gespeichert liegen. Android-Nutzer könnten beispielsweise in den Kontakt-Einstellungen ihre gespeicherten Kontakte mit ihrem Google-Konto verknüpfen, Windows-Phone-Nutzer nutzen hierfür ihr Microsoft-Konto. Hierbei sollten allerdings

wieder die oben genannten Sicherheitsaspekte bezüglich Synchronisation mit der Cloud bedacht werden.

***Die Regelmäßigkeit von Backup-Routinen variiert von Unternehmen zu Unternehmen. Eine tägliche Sicherung der Daten ist nach Ansicht vieler Sicherheitsexperten ein guter Richtwert. Backups sollten verschlüsselt, redundant abgespeichert und auf fehlerfreie Wiederherstellbarkeit geprüft werden.***

Welche Backup-Methode auch gewählt wird: Ein Testlauf für das Auffinden und Widerherstellen gespeicherter Daten sollte in jedem Unternehmen in festen Zeiträumen durchgespielt werden, um zu überprüfen, ob alles so funktioniert wie es soll. Welche Periodizität die Backup-Routinen aufweisen sollten, lässt sich nicht pauschal beantworten. Meist hilft es weiter, sich die Frage zu stellen: Welcher Schaden entstünde, wenn (Unternehmens-)Daten von einer Arbeitsstunde, einem Arbeitstag oder einer Arbeitswoche verloren gingen? Die Beantwortung der Frage hat eine finanzielle (bezahlte Arbeitszeit) sowie pragmatische (investierte Zeit) Ebene. Außerdem spielt es eine Rolle, welche Tätigkeitsfelder ein Unternehmen bearbeitet und welcher Branche es zugehörig ist. Oft gibt es gesetzliche Vorschriften für die Speicherung bestimmter Daten (siehe Kapitel *2.10 Rechtliche Risiken*). Ein guter Richtwert ist es, eine tägliche Datensicherung durchzuführen. Diese Sicherung sollte verschlüsselt und redundant abgespeichert werden und regelmäßig auf fehlerfreie Wiederherstellbarkeit überprüft werden.

***Sichern Sie sämtliche lokal gespeicherte Daten auf den Geräten regelmäßig redundant und verschlüsselt auf externen Speichermedien wie SSD-Festplatten. Verwenden Sie dazu Gerätehersteller-eigene Software, sofern diese die Synchronisation sämtlicher Daten ermöglicht. Beachten Sie die Sicherheitsrisiken bei Nutzung von Cloud-Diensten zur Synchronisation und wählen Sie einen Dienst mit Serverstandort in Deutschland. Entscheiden Sie sich im Zweifelsfall nach Absprache mit der Unternehmensführung für oder gegen die Nutzung eines solchen Dienstes. Prüfen Sie die gewählte Backup-Methode durch regelmäßige Testläufe.***

### 3.2.10 Sicheres Akku-Laden

***Datenabfluss vom mobilen Endgerät ist durch kompromittierte Ladegeräte, beispielsweise an öffentlichen Plätzen, möglich.***

Der Begriff Juice Jacking bezeichnet Datenklau bei Smartphones und Tablets, während die Geräte ihren Akku aufladen. Möglich wird das durch kompromittierte Ladestationen, die sich beispielsweise auf Flughäfen oder Messen befinden können. Auch bei Geräten, die sich zwecks Aufladung mit einem PC oder Laptop verbinden, ist Datenabfluss denkbar. Sogar ein schlichtes Ladekabel, das Anwender in eine Steckdose stecken, kann kompromittiert sein. Bei allen oben genannten Gefährdungsszenarios erfährt der Gerätebesitzer nichts vom Angriff auf seine Daten.
Anwender sollten sich vor Datenabfluss während des Ladevorgangs schützen, indem sie prinzipiell nur ihre eigene Hardware und hier im Speziellen nur ihre eigenen Ladegeräte benutzen. Werbegeschenke und Angebote öffentlicher Ladestationen sollten freundlich abgelehnt werden.

***Nutzen Sie stets nur Ihre eigenen Ladegeräte zum Aufladen Ihrer Geräte. Meiden Sie öffentliche Ladestationen und verbinden Sie Ihre Geräte niemals mit fremden Computern.***

### 3.2.11 Sicheres Entsorgen alter Geräte

Werden private oder firmeneigene Geräte nicht mehr benötigt, müssen sie verantwortungsvoll entsorgt werden. Landen sie nach Benutzung ohne entsprechende Sicherheitsvorkehrungen einfach auf dem Müll oder bei einer Auktionsplattform, besteht die Gefahr, dass persönliche Daten in falsche Hände geraten. Denn oft sind sensible Daten, die auf den Geräten speicherten, nicht richtig gelöscht worden. Löscht ein Nutzer die entsprechenden Ordner oder Apps manuell über ein Kontextmenü, werden die Dateien lediglich als gelöscht markiert. Sie bleiben weiterhin auf dem Speicher des Geräts, bis der vermeintlich freie Speicherplatz neu überschrieben wird. Bei oberflächlichem Löschen der Daten haben Datendiebe leichtes Spiel. Sie können die Daten des Gerätespeichers und auch gelöschte SMS mithilfe spezieller Recovery-Tools wiederherstellen.

Im ersten Schritt sollten Anwender sämtliche gespeicherten Daten auf dem Gerät auf einem externen Datenträger verschlüsselt speichern (siehe Kapitel *3.2.9 Datensicherung – Backup-Tools für Smartphones und Tablets*), die gespeicherten Kontakte auf die SIM-Karte exportieren und diese anschließend aus dem Gerät entfernen. Zu beachten ist, dass meist nur wenige Kontaktinformationen wie der Name und nur eine Nummer des jeweiligen Kontakts auf der SIM-Karte gespeichert werden können. Anwender sollten also mithilfe geeigneter Backup-Verfahren sicherstellen, dass auch die restlichen Kontaktinformationen gesichert werden.

#### Einsatz der Wipe-Funkton

***Vor dem Entsorgen alter Geräte sollte die Wipe-Funktion in Anspruch genommen werden.***

Unbedingte Maßnahme vor dem Entsorgen des jeweiligen Gerätes sollte sein, das System über das Konfigurationsmenü auf den Auslieferungszustand zurückzusetzen. Durch die sogenannte Wipe-Funktion werden sämtliche Daten des internen Speichers, inklusive Dateien, Kontaktdaten, SMS, lokal gespeicherten E-Mails, installierten Apps und Systemeinstellungen, gelöscht. Ausgenommen sind hier die Daten, die auf externen Speichern lagern, beispielsweise auf der SD-Karte im Kartenslot des Geräts. Anwender sollten ihre SD-Karte aus dem Gerät entfernen – sie kann im nächsten Gerät wiederverwendet werden. Eine Wiederherstellung der Daten, die mittels Wipe-Funktion gelöscht wurden, gestaltet sich für Angreifer schwieriger.

#### Speicher-Vollverschlüsselung als Präventivmaßnahme

Auf Nummer sicher können Anwender gehen, wenn Sie vor Nutzung der Wipe-Funktion den Speicher ihres Gerätes vollständig verschlüsseln. Selbst wenn es Angreifern gelingt, die via Wipe-Funktion gelöschten Daten wiederherzustellen, finden sie dann nur noch kryptischen Datenmüll vor. Soll im Unternehmen eine größere Zahl alter IT-Geräte entsorgt werden, beispielsweise um der nächsten Geräte-Generation Platz zu machen, kann ein spezieller Dienstleister für die professionelle Entsorgung hilfreich sein. Verantwortliche sollten sich im Vorfeld von der Seriosität des Dienstleisters überzeugen und die Website des Dienstleisters, Kundenkommentare, Testberichte, Zertifikate und unternehmensbetreffende Presseberichte umfassend prüfen bevor sie einen Vertrag abschließen.

Sind alle sensiblen Daten vom Gerätespeicher gelöscht, sollte überlegt werden, ob sich der Erlös, der sich durch den Weiterverkauf des nicht mehr benötigten Gerätes ergibt, in einem Verhältnis zum Risiko steht, dass doch noch Daten vom Gerät wiederhergestellt werden könnten. Im Zweifelsfall sollte sich immer für die Vernichtung des Gerätes entschieden werden.

***Ein Weiterverkauf alter Geräte steht meist in keinem Verhältnis zum Risiko, dass doch noch vermeintlich gelöschte Daten wiederhergestellt werden könnten.***

***Löschen Sie sämtliche gespeicherten Daten, Anwendungen und Einstellungen bevor Sie Ihr Smartphone oder Tablet entsorgen. Nutzen Sie dazu die Wipe-Funktion Ihres Geräts sowie eine vorherige Verschlüsselung des gesamten Gerätespeichers. Beauftragen Sie gegebenenfalls ein seriöses Dienstleistungsunternehmen zum Entsorgen mehrerer Geräte, auf denen besonders sensible Daten abgelegt wurden. Ziehen Sie die Vernichtung des Gerätes dem Weiterverkauf vor, sollten Sie sich nicht ganz sicher sein, dass wirklich keine Daten wiederherstellbar sind.***

***Wipe-Funktion bei iOS:***
***Einstellungen -> Allgemein -> Zurücksetzen -> Inhalte & Einstellungen löschen***

***Wipe-Funktion bei Android:***
***Einstellungen -> Speicher -> Auf Werkszustand zurück***

***Wipe-Funktion bei Windowsphone:***
***Einstellungen -> Info -> Handy zurücksetzen***

***Wipe-Funktion bei RIM/Blackberry:***
***Einstellungen -> Sicherheitsoptionen -> Allgemeine Einstellungen -> Blackberry-Menütaste -> Gerät löschen***
***bzw. Einstellungen -> Sicherheitsoptionen -> Sicherheitslöschung***

### 3.2.12 Sichtschutz

Analog zum Sichtschutz bei Netbooks und Notebooks (siehe Kapitel *3.1.8 Sichtschutz*) sollte auch bei Smartphones und Tablets ein Sichtschutzfilter zum Einsatz kommen, sofern Mitarbeiter diese Geräte für berufliche Zwecke in unsicheren Arbeitsumgebungen nutzen. Zu den unsicheren Arbeitsumgebungen zählen die öffentlichen Nahverkehrsmittel, Wartehallen im Bahnhof und im Flughafen, Cafés, Restaurants, Aufenthaltsräume in Hotels, das Ausstellungsgelände auf Messen, Baustellen und andere öffentliche Orte, die für den schnellen E-Mail-Check in Betracht kommen.

***Ein Sichtschutz für Smartphones und Tablets sollte bei unsicheren Umgebungen stets zum Einsatz kommen.***

Spezielle Sichtschutzfolien können direkt auf das Display des Gerätes geklebt werden und verringern den Blickwinkel so, dass die Anzeige des Bildschirms nur noch frontal betrachtet lesbar ist. Sichtschutzfolien gibt es schon ab vier Euro in Elektrofachgeschäften oder online zu kaufen.

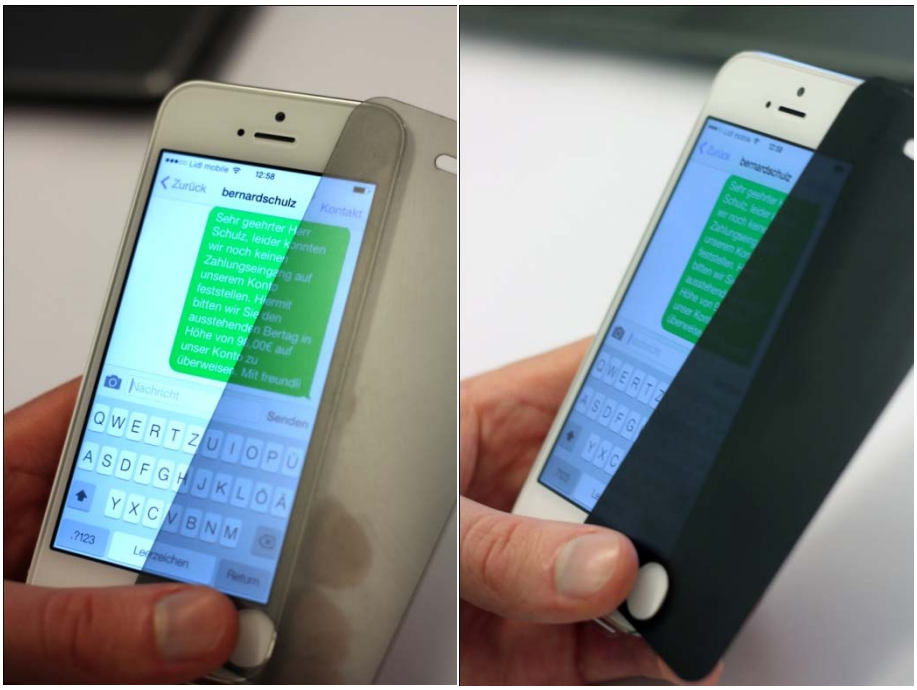



*Abbildung 15: Smartphone-Sichtschutzfolie mit verändertem Blickwinkel (Sebastian Wacowski, 2014)*

***Wenn Sie ihr Smartphone in unsicheren Arbeitsumgebungen für berufliche Zwecke nutzen wollen, dann schützen Sie die Bildschirmanzeige via Sichtschutzfolie vor neugierigen Blicken.***

### 3.2.13 Weitere betriebssystemspezifische Sicherheitseinstellungen

Je nach Betriebssystem können Nutzer weitere relevante Sicherheitseinstellungen vornehmen, um ihren Basisschutz zu erhöhen.

#### Ad-Tracking unter iOS und Android beschränken

***Ad-Tracking dient zur Sendung von Informationen an bestimmte Werbefirmen.***

Standardmäßig übermitteln einige Apps bei iPhone, iPad und Android-Geräten eine sogenannte Werbungs-ID temporär an bestimmte Werbenetzwerke, die diese persönliche Geräteidentifizierung nutzen, um dem jeweiligen Nutzer personenspezifische Werbung zu schalten (Ad-Tracking). Ab der iOS-Version 6 können Apple-Nutzer das Ad-Tracking beschränken, sodass Werbefirmen weniger Informationen über das Gerät und den Nutzer sammeln können. Auch Android-Nutzer können die „interessensbezogenen Anzeigen“ in den Einstellungen Ihres Google-Kontos deaktivieren.

***Deaktivieren Sie als iOS-Nutzer die Ad-Tracking-Funktion, wenn Sie keine gerä- te- und personenbezogenen Informationen an Werbefirmen übersenden wollen, unter:***
***Einstellungen -> Datenschutz -> Werbung -> kein Ad-Tracking***

***Ad-Tracking unter Android deaktivieren:***
***Einstellungen -> Google Einstellungen --> Anzeigen -> [Häkchen setzen bei „Interessensbezogene Anzeigen deaktivieren“]***

### Deaktivierung der cloudbasierten Sprachassistenten

Apples Sprachassistentin Siri ist trotz aktiver Zugriffssperre sehr redselig und führt Befehle aus. Voraussetzung ist, dass das Gerät in den Händen eines Dritten ist. Sie gibt jedem, der fragt, Auskunft über gespeicherte Telefonnummern, E-Mail-Adressen, Termine, Tweets und SMS. Aus Sicherheitsgründen sollten Anwender auf cloudbasierte Sprachassistenten wie Siri verzichten.

***Deaktivieren Sie cloudbasierte Sprachassistenten bei Ihrem Smartphone. Insbesondere dann, wenn Sie Besitzer eines iPhones (ab iPhone 4S) sind:***

***Einstellungen -> Allgemein -> [Schieberegler bei „Siri“ nach links wischen]***

### App-Bestätigung unter Android

Die App-Bestätigung (App Verifying) von Google dient zur Vorbeuge vor Installation schadhafter Anwendungen, die aus anderen Quellen als dem Google Play Store heruntergeladen werden (siehe Kapitel *2.3.1 Bezugsquellen* und *4.1 Sichere Handhabung der Geräte*). Grund hierfür sind vor allem fehlende Kontroll- und Sicherheitsmechanismen alternativer Plattformen. Wollen sich Nutzer nicht auf den offiziellen Google-Market beschränken lassen, kann die Funktion „App-Bestätigung“ hilfreich sein. Mit dieser Funktion wird im Vorfeld einer App-Installation von Google überprüft, ob es sich bei der gewünschten Anwendung um eine schädliche handelt. Dazu werden Daten über das Nutzergerät wie die Protokollinformationen, Geräte-ID, Version des Betriebssystems und die IP-Adresse sowie Informationen über die App, beispielsweise die mit der App verbundenen URLs, an Google zur Kontrolle übersandt. Stuft Google die App als schädlich ein, erhält der Nutzer einen Hinweis und die Installation der App wird geblockt.

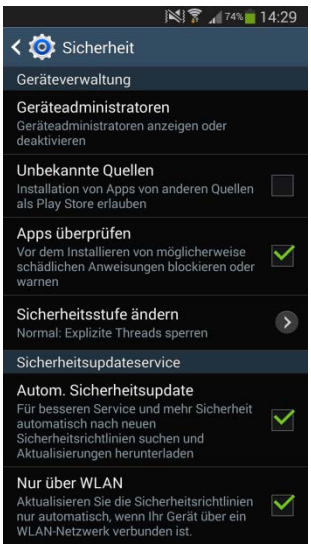



*Abbildung 16: App-Bestätigung via „App überprüfen" unter Android*

***Wollen Sie sich trotz Sicherheitsbedenken nicht auf den offiziellen App Market Google Play beschränken lassen, sollten Sie die App-Bestätigungsfunktion aktivieren:***

***Einstellungen -> Sicherheit -> Apps bestätigen***

***Die bessere Alternative ist der Verzicht auf die App-Installation aus alternativen Quellen:***

***Einstellungen -> Sicherheit -> [Häkchen entfernen bei: Unbekannte Quellen]***

## 3.3 Zusammenfassung

**Schutzmaßnahmen auf der Geräteebene – Basisschutz**

In diesem Kapitel wurden Basisschutzmaßnahmen zur technischen Sicherung mobiler Geräte vorgestellt. Grundsätzliche Dinge, die den Basisschutz bei Laptops betreffen, gelten auch für Smartphones und Tablets. Geräte-Zugriffssperren, Datenverschlüsselungsmechanismen, Backup-Routinen, Sichtschutz bei Verwendung in unsicheren Arbeitsumgebungen und die Norm der Software-Aktualität sollten bei allen mobilen Endgeräten hochgehalten werden.

Unterschiede betreffen vor allem die zu installierende Schutzsoftware und den Diebstahlschutz. Aufgrund der Systemarchitektur von Smartphones und Tablets arbeiten Virenschutz- und Personal-Firewall-Apps nicht so effizient wie die Virenschutz- und Firewall-Software bei Laptops. So können Virenscanner bei Smartphones beispielsweise nur diejenigen Systembereiche scannen, auf die sie über das Berechtigungssystem Zugriff erhalten haben. Eine effiziente vollständige Systemprüfung ist nicht möglich. Daher sollten sich Smartphone- und Tablet-Nutzer keinesfalls nur auf diese Funktionen verlassen – ein verantwortungsvoller Umgang mit den Geräten bietet weitaus größeren Schutz (siehe Kapitel *Schutzmaßnahmen auf der Mitarbeiterebene – Mitarbeitersensibilisierung*).

Diebstahlschutz kommt bei den Smart Mobile Devices eine sehr große Bedeutung zu, bündeln doch Smartphones und Tablets eine Fülle von sensiblen (personenbezogenen und betrieblichen) Daten. Geeignete Präventivmaßnahmen sollten schon im Vorfeld getroffen werden, bevor es überhaupt zur Inanspruchnahme der Diebstahlschutz-Funktionen (Fern-Ortungs-, Lösch- und Sperr-Funktion) kommt.

Aufgrund der technischen Eigenheiten von Smartphone und Tablet kommen gegenüber dem Laptop weitere relevante Schutzmaßnahmen hinzu, wie die providerseitige Sperre von Drittanbieter-Diensten zum Schutz vor Premium-SMS-Diensten sowie der Schutz vor Phishing und Gerätemanipulation.

Übergeordnetes Ziel für Arbeitgeber ist es, die Datenschutzanforderungen, die sich aus der Anlage zu §9 BDSG ergeben, bei mobilen Endgeräten wirksam umzusetzen.

**Notizen**

# 4. Schutzmaßnahmen auf der Mitarbeiterebene – Sensibilisierung

Befragungen von Verantwortlichen in Unternehmen bestätigen immer wieder: Das größte Gefahrenpotenzial für die betriebliche IT-Sicherheit ist die Unachtsamkeit der Mitarbeiter. In der aktuellen Sicherheitsstudie der Zeitschrift <kes>, die in Zusammenarbeit mit Microsoft durchgeführt wurde, belegt der Gefahrenbereich „Irrtum und Nachlässigkeit eigener Mitarbeiter“ den ersten Rang (vgl. SecuMedia, 2012).

Wurde im vorigen Kapitel gezeigt, wie Mitarbeiter mithilfe von Software und Geräte-Einstellungen den Grundstein für IT-Sicherheit im Unternehmen legen können, folgen nun die wichtigsten Handlungsanweisungen für den sicheren Einsatz mobiler Endgeräte im Betriebsalltag. Verantwortlichen in Unternehmen sollte klar sein: Technische Sicherheitsvorkehrungen nutzen wenig, wenn Mitarbeiter nicht für die digitalen Gefahren sensibilisiert werden.

## 4.1 Sichere Handhabung der Geräte

Die sichere Handhabung der Geräte meint sowohl den vorausschauenden physischen Umgang mit den Geräten als auch den verantwortungsbewussten Einsatz dieser im dienstlichen Kontext.

### Keine Chance für spontane Angreifer

Wie in Kapitel *3.1.1 Zugriffsperre* dargestellt, sollten Anwender die Zugriffssperre ihres Laptops sofort beim Verlassen des Arbeitsplatzes aktivieren. Kleinere mobile Endgeräte wie Smartphones und Tablets sollten nicht am Arbeitsplatz liegengelassen werden, um Gelegenheitsdiebstahl und Gerätemanipulation vorzubeugen. Leere Büroräume sollten beim Verlassen abgeschlossen werden.

***Zugriffssperren sollten stets beim Verlassen des Arbeitsplatzes aktiviert werden.***

Arbeiten von unterwegs aus, auf der Baustelle, beim Kunden vor Ort, im Zug, im Café, im Hotel oder in Wartehallen sollten prinzipiell mit nur großer Vorsicht durchgeführt werden. Trotz Sichtschutzfilter (siehe Kapitel *3.1.8* und *3.2.12 Sichtschutz*) können Nutzer mobiler Endgeräte nie sicher sein, wer die dienstlichen E-Mails und Dokumente mitliest. Es sollte vermieden werden, auf besonders sensible Daten von unterwegs aus zuzugreifen.

Unbedingte Regel für mobiles Arbeiten lautet: Keine Geräte aus der Hand geben. Freundliche Anfragen, ob kurz das Handy für ein Telefonat ausgeliehen werden könne, müssen entschuldigend abgelehnt werden. Angreifer können beispielsweise innerhalb weniger Sekunden Kontaktdaten auslesen oder Schädlingsprogramme auf das Gerät des Anwenders schleusen.

***Mobile Endgeräte sollten grundsätzlich nie aus der Hand gegeben (bzw. verliehen) werden.***

***Beaufsichtigen Sie stets Ihre mobilen Endgeräte. Sperren Sie Ihren Laptop, sobald sie den Arbeitsplatz verlassen. Verschließen Sie leere Büroräume. Bearbeiten und lesen Sie keine besonders sensiblen Dokumente von unterwegs aus. Geben Sie Ihr Smartphone oder Tablet niemals aus der Hand.***

### Die verantwortungsvolle Nutzung von Apps bei Smartphones und Tablets

Kapitel *2.3 Programme und Apps als Sicherheitsrisiken* beschreibt ausführlich die Gefahren, die mit der Installation von Apps einhergehen. Erlauben Verantwortliche in Unternehmen den Mitarbeitern die Installation von Apps auf Dienstgeräten oder dienstlich genutzten Privatgeräten, muss dies mit der Bedingung einhergehen, Apps stets nur aus den offiziellen App Markets herunterzuladen. Jailbreaking beziehungsweise Rooting der Geräte sollte Mitarbeitern aufgrund der in Kapitel *2.7 Risiko Jailbreaking und Rooting* genannten Sicherheitsrisiken untersagt sein.

Sind den Mitarbeitern seitens der Unternehmensführung keine Einschränkungen hinsichtlich der Software-Auswahl und Erweiterbarkeit der Geräte gegeben, liegt die Verantwortung beim Mitarbeiter, ein hohes Sicherheitsniveau seiner mobilen Endgeräte zu gewährleisten (vgl. Kapitel *2.10 Rechtliche Risiken* und *5.2 Auflagen und Richtlinien für Mitarbeiter*). Interessieren sich Mitarbeiter für eine Anwendung, sollten sie die Nutzerbewertungen im jeweiligen App Market lesen und Test- und Medienberichte zu Rate ziehen. Vor der Installation einer App sollten Anwender die Hersteller-Website auf Seriosität hin prüfen. Impressum, AGB und Zertifikate geben erste Hinweise.

***Auf Anwendungen, die weitreichende oder für ihre Funktionalität ungewöhnliche Zugriffsrechte einfordern, ist zu verzichten.***

Am wichtigsten ist die Kontrolle der Zugriffsberechtigungen, die eine App zur Installation einfordert. Art und Umfang der Berechtigungen sollten stets mit dem beschriebenen Funktionsumfang der Anwendung verglichen werden. Können Zugriffsberechtigungen nicht logisch durch Funktionalitäten der App begründet werden, ist Misstrauen angebracht. Eine Quiz-App sollte beispielsweise keinen Zugriff auf die GPS-Ortung des Geräts benötigen, um zu funktionieren. Es ist eine vorsichtige Tendenz dahingehend erkennbar, dass kostenlose Anwendungen durchschnittlich mehr Zugriffsrechte einfordern als kostenpflichtige. Verlangt eine Anwendung – egal ob kostenlos oder kostenpflichtig – ungewöhnlich viele Zugriffsrechte zu sensiblen Bereichen wie zum Beispiel Kontaktdaten, Kamera und Kommunikationsdiensten, ist von der Installation abzuraten. Eine Übersicht über die einzelnen Berechtigungen nach Betriebssystem findet sich in Kapitel *2.3.2 App-Zugriffsrechte*.

### Zugriffssperre für Anwendungen

Es ist von Apps abzuraten, welche weitreichende Zugriffsrechte auf andere Applikationen fordern, da diese zu Datenschutzproblemen führen können. Die Folge wäre ein Abfließen von persönlichen Informationen zum App-Hersteller. Vor der Installation einer App sollten Nutzer sich über diese umfassend informieren und die geforderten Rechte genau dahingehend prüfen, welche Funktionen der App tatsächlich benötigt werden.

### Bereits erteilte Zugriffsrechte prüfen und nachträglich entziehen

Anwender sollten sich regelmäßig einen Überblick darüber verschaffen, welche Zugriffsrechte bereits installierte Apps haben. Manchmal fordern installierte Apps beim Einspielen eines Updates weitere Zugriffsrechte ein.

Sind sie mit dem Zugriff einzelner Apps auf bestimmte System- und Software-Ressourcen nicht mehr einverstanden, sollten sie Zugriffsrechte nach Möglichkeit nachträglich wieder entziehen. Dies kann je nach Betriebssystem des Geräts entweder direkt in den Geräte-Einstellungen erfolgen (so bei Android 4.3, iOS ab Version 6 und bei Blackberry) oder muss über den Umweg einer anderen Software beziehungsweise Mobile Security Suite umgesetzt werden. Lässt sich auch durch die Mithilfe

einer Software die Berechtigung nicht entziehen, bleibt Nutzern nur noch die Option zur Deinstallation der betreffenden Anwendung.

***Laden Sie Apps nur aus den offiziellen Markets herunter. Verzichten Sie auf Jailbreaking beziehungsweise Rooting Ihres Geräts. Prüfen Sie vor der Installation Nutzerkommentare, Test- und Medienberichte sowie die Liste der geforderten Zugriffsberechtigungen. Entscheiden Sie sich nach dem Abgleich der Berechtigungen mit dem Funktionsumfang der App für oder gegen die Installation dieser. Kontrollieren Sie die erteilten Zugriffsrechte der bereits installierten Apps regelmäßig und entziehen Sie gegebenenfalls einzelne Berechtigungen nachträglich. Falls dies nicht möglich ist, deinstallieren Sie die betreffenden Anwendungen.***

***Deinstallation einzelner Apps bei iOS:***
***[auf betreffende Anwendungen auf dem Homescreen tippen und gedrückt halten] -> [auf das kleine“„X“-Symbol tippen]***

***Deinstallation einzelner Apps bei Android:***
***Einstellungen -> Anwendungen -> Anwendungen verwalten -> [Name der Anwendung] -> Deinstallieren***

***Deinstallation einzelner Apps bei Windowsphone:***
***Anwendungsliste -> [auf betreffende Anwendung tippen und gedrückt halten] -> Deinstallieren***

***Deinstallation einzelner Apps bei BlackBerry:***
***My World -> Apps und Spiele -> [unter der betreffenden App auf „Deinstallieren klicken“]***

## 4.2 Passwortsicherheit und -tools

Weniger als Hälfte aller Betriebe mit unter zehn Mitarbeitern nutzt sichere Passwörter und vergibt diese regelmäßig (vgl. IT-Sicherheit im Handwerk, 2013). Um zu verstehen, warum die Vergabe sicherer Passwörter überhaupt so wichtig ist, werden nachfolgend die Angriffsmethoden krimineller Datendiebe erläutert.

### Angriff auf Grundlage von Wahrscheinlichkeiten

***Angreifer haben sehr gute Chancen, ein Nutzerpasswort zu erraten, indem sie einfach die meist genutzten Passwörter ausprobieren.***

In regelmäßigen Abständen veröffentlichen Sicherheitsexperten und -unternehmen Ranglisten der meistgenutzten Passwörter. Diese Listen erstellen sie auf Basis bekanntgewordener Passwörter, die durch Datenpannen großer Unternehmen ans Licht der Öffentlichkeit gelangen. Als Beispiel kann die Twitter-Datenpanne im Mai 2012 aufgeführt werden, bei der auf einen Schlag 35.000 Zugangsdaten von Twitter-Nutzer öffentlich wurden.
Sicherheitsexperte Mark Burnett wertete über einen längeren Zeitraum sechs Millionen dieser bekanntgewordenen Passwörter aus und erstellte eine Hitliste der zehntausend meistgenutzten Passwörter für den amerikanischen Raum (vgl. Burnett, 2011). Die Plätze Eins bis Drei belegen: „password“, „123456“ und „12345678“. Knapp fünf Prozent aller Nutzer hatten das Passwort „password“ für verschiedene Dienste

und Nutzerkonten gewählt, über neunzig Prozent der Nutzer vergaben Passwörter, die unter den ersten hundert Plätzen zu finden waren (ebenda). Es ist davon auszugehen, dass die von Burnett ermittelte Häufigkeitsverteilung in ähnlicher Form auf sämtliche Passwörter, also auch die unbekannten, zutrifft. Das bedeutet, dass sich ein Angreifer in neun von zehn Fällen Zugang zu einem fremden Nutzerkonto verschaffen kann, wenn er zu einem Benutzernamen die ersten hundert Plätze der meistgenutzten Passwörter ausprobiert. Würde Burnetts Untersuchung auf den deutschsprachigen Raum übertragen, kämen höchstwahrscheinlich ähnliche Ergebnisse heraus.

Anwender sind nicht gut beraten, wenn sie zur Passwortvergabe bestimmte Tastaturmuster wie „qwertz“ verwenden – solche Kombinationen sind zwar leicht zu merken, sie finden sich aber garantiert unter den oberen Plätzen der Passwort-Ranglisten und werden somit auch häufig von Angreifern ausprobiert.

### Gezielter Angriff durch Beschaffung personenbezogener Daten

***Viele Nutzer wählen ein Passwort, das in Zusammenhang mit ihren persönlichen Daten steht. Der Name des Haustiers ist beispielsweise ein unsicheres Passwort.***

Eine weitere Angriffsmethode, die ebenfalls auf Wahrscheinlichkeiten beruht, kombiniert typische Passwort-Vergabemuster mit personenbezogenen Kenntnissen über das Opfer. Bei gezielten Angriffen auf Personen versucht ein Angreifer im Vorfeld, so viele Informationen über sein Opfer zu beschaffen wie möglich. Dazu sucht er beispielsweise in sozialen Netzen wie Facebook nach öffentlich zugänglichen Informationen über das Opfer. Von besonders großem Interesse sind dabei beispielsweise der Name des Partners, des Haustiers oder das Geburtsdatum des Opfers. Viele IT-Anwender gebrauchen diese Kombinationen als Passwörter. Ein Angreifer kann seine Erfolgschancen durch persönliche Kontaktaufnahme mit dem Opfer vergrößern (Stichwort: Social Engineering, s. Kapitel *2.5 Phishing und Social Engineering*).

### Angriff durch die Wörterbuch-Methode

***Namen und Wörter sind in Verzeichnissen zu finden, die Angreifer automatisiert durchtesten können.***

Bei dieser Angriffsmethode braucht der Angreifer keine Informationen über das Opfer in Erfahrung zu bringen. Zahlreiche Angreifer machen sich digitale Wörterbücher und Namensverzeichnisse zunutze, um beispielsweise Passwörter zu E-Mailkonten, Webshop-Benutzerkonten oder Unternehmensnetzwerken zu knacken. Dabei testen sie automatisiert die in den Lexika enthaltenen Namen, Wörter und Wortgruppen aus – vorwärts und rückwärts, in Kombinationen mit Zahlen und Sonderzeichen (z.B.: sebastian, naitsabes, sebastian!, bello! usw.).

### Angriff durch die Brute-Force-Methode

***Die Brute-Force-Methode führt mathematisch gesehen, immer zum Ziel. Daher sind Passwortlänge und verwendete Zeichenkombination so wichtig.***

Bei der Brute-Force-Methode (im Deutschen: „Methode der rohen Gewalt“) handelt es sich um eine erschöpfende Suche nach dem korrekten Passwort. Automatisiert werden alle möglichen Kombinationen aus Buchstaben und Zahlen durchprobiert (a, b, aa, bb, ab, ba, ab1, ba1 usw.). Mathematisch gesehen, führt diese Methode früher oder später in jedem Fall zum Erfolg – die Frage ist nur: Wie viel Zeit wird vergehen, bis ein Angreifer erfolgreich ist. In Abhängigkeit von der Leistungsstärke des Angreifer-Computers und der Länge der gesuchten Zahlen- und Buchstabenkombination kann diese Attacke bei kurzen Passwörtern innerhalb weniger Sekunden zum Ziel führen oder bei sehr langen variationsreichen Passwörtern Wochen oder Jahre dauern. Die mathematische Regel für die Gesamtzahl möglicher Kombination lautet:

**Anzahl möglicher Kombinationen = Zeichenanzahl des verwendeten Zeichensystems hoch Länge des Passwortes.**

Werden für ein siebenstelliges Passwort beispielsweise nur Kleinbuchstaben des Alphabets, ohne die Umlaute „ä“, “ö“, “ü“ und „ß“ verwendet, gibt es 26 hoch sieben, also insgesamt etwa acht Milliarden mögliche Kombinationen. Ein sehr schneller Rechner hat diese Anzahl an Kombinationen in unter zehn Sekunden durchgespielt (vgl. Schröder, o. J.). Zum Vergleich: Bei einem zehnstelligen Passwort, das sich aus Groß- und Kleinbuchstaben sowie Zahlen und Sonderzeichen zusammensetzt, benötigt ein Angreifer mit schnellem Rechner 12,7 Jahre zum Erproben aller 62 hoch zehn Kombinationsmöglichkeiten (ebenda).

## Regeln zur Vergabe sicherer Passwörter

Um die Erfolgswahrscheinlichkeiten oben genannter Angriffsmethoden zu verringern, sollten IT-Anwender grundlegende Regeln zur Passwortvergabe einhalten. Passwörter sollten sich aus mindestens zehn Zeichen, inklusive Klein- und Großbuchstaben, Zahlen und Sonderzeichen (z.B.: „< > ( ) [ ] { }? ! $ % & / = * + ~ , . ; : < > - _“) sinnfrei zusammensetzen. Sinnfrei bedeutet, dass das zusammengesetzte Passwort keiner erkennbaren Systematik folgt und keine Daten wie Geburtsdaten oder Telefonnummern enthält, die auf den Anwender zurückzuführen sind. Das Passwort und seine Bestandteile sollten nicht in Wörterbüchern oder Namensverzeichnissen auffindbar sein.

Beispiel für ein sicheres Passwort ist: IkjTa1s>-@wv.

***Eselsbrücken helfen dabei, sich sichere Passwörter ins Gedächtnis einzuprägen.***

Einfache Eselsbrücken können dem Anwender dabei helfen, sich ein solches Passwort einzuprägen. So könnte ein Akronym einer ausgedachten Geschichte als Basis dienen: „Ich komme jeden Tag an einer schönen Blumenwiese vorbei“. Das Wort „einer“ kann durch die Ziffer „1“ ersetzt werden und „Blume“ durch eine Zeichenkombination, die aussieht wie eine Blume („>-@“).

***Für jeden Dienst ist ein anderes sicheres Passwort zu wählen.***

Für jeden Dienst und jedes Konto sollte ein anderes sicheres Passwort verwendet werden, sodass Angreifer, die beispielsweise aufgrund einer Datenpanne in den Besitz von Passwörtern gekommen sind, sich nicht auf einen Schlag Zugang zu mehreren Nutzerkonten eines Anwenders verschaffen können. Um die Wahrscheinlichkeit eines Passwort-Diebstahls weiter zu verringern, sollten Anwender ihre Passwörter regelmäßig ändern. Das zu wählende Änderungsintervall steht in Abhängigkeit davon, wie sensibel die passwortgeschützten Inhalte oder Nutzerkonten sind. Im besten Fall vergeben Anwender alle drei Monate neue sichere Passwörter. Bei dem kleinsten Verdacht, dass ein Passwort nicht mehr sicher ist, sollten Anwender dieses umgehend ändern. Einige Dienste und Software-Produkte weisen Neukunden voreingestellte Passwörter zu (z.B. „admin“). Diesen Umstand machen sich Datendiebe zunutze und testen zunächst, ob ein voreingestelltes Passwort noch nicht individualisiert wurde. Das bedeutet, dass Anwender ihr voreingestelltes Passwort nach Erhalt umgehend ändern sollten, um Hackern keine Angriffsfläche zu bieten.

## Sichere Aufbewahrungsorte für Passwörter

IT-Anwender verwalten heute eine Vielzahl verschiedener Nutzerkonten. Alle Passwörter im Gedächtnis behalten zu wollen, erscheint unmöglich. Post-It-Zettel an den Monitorrand oder auf den Schreibtisch zu kleben, ist eine denkbar schlechte Alternative zum Auswendiglernen. Jeder Bürobesucher kann sich so Zugriff zu sensiblen Unternehmensdaten verschaffen – Datendiebe haben leichtes Spiel.

Nutzer sollten ihre Passwörter nicht auf Zettel notieren, sofern sie diese nicht in einem Tresor verschließen können.

Zum Aufbewahren und Verwalten vieler Passwörter eignet sich ein digitaler Passwort-Manager. Software-Produkte wie KeePass[48] oder Password Safe[49] sind kostenlos und ermöglichen es, sämtliche Nutzernamen und Passwörter verschlüsselt abzuspeichern. Zum Entschlüsseln und Lesen der gespeicherten Zugangsdaten benötigen Anwender nur noch ein einziges Passwort, das sogenannte Masterpasswort. Hat der Anwender nach Systemstart seinen Passwort-Safe mit dem Masterpasswort entriegelt, kann er sämtliche gespeicherten Passwörter einfach bei Bedarf herauskopieren, um sich beim entsprechenden Dienst anzumelden. Das Masterpasswort sollte selbstverständlich ein besonders sicheres Passwort sein, das Anwender nicht notieren, sondern auswendig lernen. Die gespeicherten Zugangsdaten können innerhalb der Software nach Kategorien wie „E-Mail-Konten“ und „Online-Banking“ sortiert werden. Auch ist es möglich, neue sichere Passwörter für Dienste mit dem Passwort-Manager automatisch zu generieren. Das angewandte Verschlüsselungsverfahren zum Speichern der Zugangsdaten, Advanced Encryption Standard (AES), wird höchsten Sicherheitsansprüchen gerecht und dient Regierungen sogar zum Verschlüsseln von Dokumenten mit höchster Geheimhaltungsstufe.

***Digitale Passwort-Safes helfen bei der Verwaltung der sicheren Passwörter. Anwender brauchen sich hier lediglich ein einziges, das Masterpasswort zu merken.***


*Abbildung 17: Eingabefeld des Master-Passwortes bei KeePass*

## Risiko: Eingabe der Zugangsdaten auf fremden Systemen

***Zugangsdaten sollten niemals an Systemen eingegeben werden, die nicht vertrauensvoll sind.***

Die besten Passwörter schützen nicht, wenn das System auf dem sie eingegeben werden, durch Schädlingsbefall kontaminiert ist. Sogenannte Keylogger (im Deutschen: „Tastenrekorder“) sind Schadprogramme, die sämtliche Tastatureingaben des Anwenders aufzeichnen und an einen Angreifer senden. So gelangen Kriminelle schnell an die erforderlichen Zugangsdaten für E-Mail-Konto und Online-Banking-Account. Anwender sollten Zugangsdaten generell nur an ihren eigenen oder den zur Verfügung gestellten Arbeitsplatzgeräten eingeben. Die Nutzung fremder Geräte, beispielsweise in Internet-Cafés oder beim Kunden vor Ort, ist nicht zu empfehlen. Sie können sich hier nicht sicher sein, wer nach der Benutzung im Besitz ihrer Zugangsdaten ist.

[48] *http://keepass.info*
[49] *http://www.passwordsafe.de*

***Vergeben Sie für jeden Dienst stets nur sichere Passwörter, bestehend aus mindestens zehn Zeichen, inklusive Klein- und Großbuchstaben, Zahlen und Sonderzeichen. Wählen Sie für jeden Dienst und jede Anwendung ein neues Passwort. Ändern Sie Ihre Passwörter regelmäßig je nach Sicherheitsniveau der schützenswerten Inhalte. Geben Sie Zugangsdaten nur an vertrauenswürdigen Rechnern ein. Bewahren Sie Ihre Passwörter an sicheren Orten, im Safe oder im digitalen Passwort-Manager auf. Nutzen Sie für letzteren ein sicheres Passwort. Merken Sie sich besonders wichtige Passwörter (wie das Masterpasswort für den Safe) mittels einfacher Eselsbrücken. Notieren Sie sich keine Passwörter und heben Sie diese nicht an Monitor, Schreibtisch oder im Portemonnaie auf.***

## 4.3 Sicherheit bei drahtloser Kommunikation via WLAN, Bluetooth und Co

Einfachste Maßnahme, um Hackern weniger Angriffsfläche zu bieten, lautet, drahtlose Schnittstellen bei Nicht-Gebrauch deaktivieren und nur bei Bedarf im Einstellungsmenü aktivieren. Dies betrifft insbesondere Bluetooth und WLAN. Gerade bei letzterem sind Angriffe populär und besonders gefährlich für die Datensicherheit (siehe Kapitel *2.1.1 Wireless Lan (WLAN) und Hotspots*).

***Eine Deaktivierung der drahtlosen Schnittstellen bei Nicht-Gebrauch bietet Angreifern weniger Angriffsfläche.***

Bei Gebrauch eines öffentlichen WLAN-Netzes wird eine Verschlüsselung erforderlich, die beispielsweise via VPN oder SSL/TLS zu realisieren ist (siehe Kapitel *4.4.2 VPN*). Falls dies nicht möglich sein sollte, muss auf die Nutzung des WLANs verzichtet beziehungsweise auf das mobile Internet ausgewichen werden.

### Schutz vor unsicheren QR-Codes

QR-Codes können mithilfe der Gerätekamera von Smartphone oder Tablet und einer geeigneten App (QR-Code Scanner) interpretiert werden, sodass beispielsweise codierte Internetadressen aufrufen werden können. Wie in Kapitel *2.1.8 Quick Response Codes* dargestellt, besteht hier ein Sicherheitsrisiko: Angreifer können beispielsweise Original-QR-Codes auf Werbeplakaten mit ihren eigenen überkleben, um unvorsichtige Nutzer auf präparierte Websites zu lenken.

Der Besuch einer präparierten Seite kann dazu führen, sämtliche auf dem Gerät gespeicherten Daten zu verlieren (siehe Kapitel *2.1.6 Quick-Response-Codes*). QR-Codes sollten nur in Verbindung mit einem sicheren Scanner genutzt werden, welcher die Zieladresse im Vorfeld anzeigt. Dieser ist entweder Teil der Mobile Security Suite oder sollte separat als App heruntergeladen werden. Beispiel für einen kostenlosen Scanner ist die App Norton Snap[50] für Android und iOS. Wird hiermit ein QR-Code gescannt, erfährt der Nutzer noch vor Verbindungsaufbau zu welcher Zieladresse der Code führt und ob die jeweilige Website als vertrauenswürdig eingestuft wird oder nicht.

***Der Scan eines gefälschten QR-Codes kann eine Sperrung der SIM-Karte nach sich ziehen. Anwender sollten auf die Zieladresse achten, die ein empfehlenswerter QR-Code-Scanner anzeigt.***

***Nutzen Sie den sicheren QR-Code Scanner Ihrer Mobile Security Suite oder alternativ eine separate App wie Norton Snap, wenn Sie QR-Codes scannen möchten.***

[50] *http://community.norton.com/t5/Other-Mobile-Products/bd-p/Other_Mobile*

## 4.4 Sichere Datenübertragung

***Eine WPA2-Verschlüsselung genügt nicht bei der Übertragung sensibler Daten, beispielsweise wenn sich Angreifer im selben Netzwerk befinden.***

Vertrauliche Daten sollten auf einem sicheren Weg über das Internet übertragen werden. Die grundsätzliche Verschlüsselung des Netzwerks, beispielsweise durch WPA2-Verschlüsselung bei WLAN-Nutzung (siehe voriges Kapitel), genügt hier nicht. Diese schützt nur davor, dass sich unberechtigte Nutzer einfach mit dem drahtlosen Netz verbinden können. Im verschlüsselten WLAN selbst können alle Nutzer unverschlüsselten (nicht via z.B. SSL/TLS geschützten) Netzwerkverkehr untereinander mithören. Gleiches gilt auch auf dem weiteren kabelgebundenen Übertragungsweg hinter dem Router. Möglichkeiten zur Online-Übertragung vertraulicher Daten sind vielfältig. Neben Login-Daten, die zur Nutzung verschiedener Internetdienste wie dem Online-Banking-Portal im Browser eingegeben werden müssen, kommen Filehosting- und Cloud-Computing-Dienste, Instant Messenger, E-Mail-Verkehr, soziale Netzwerke oder Firmenanwendungen für den Austausch sensibler Daten in Betracht (siehe auch Handbuch *Cloud Computing*).

### Browsersicherheit

Grundlage für eine sichere Nutzung von Internetdiensten sind verschärfte Sicherheitseinstellungen des genutzten Webbrowsers.

Dieser Abschnitt erläutert die sicherheitsrelevanten Aspekte bei der Nutzung im Internet anhand zwei weit verbreiterer Browser: dem Open-Source-Browsers Firefox der Mozilla Foundation und dem Internet Explorers von Microsoft.

Mozilla Firefox
Der Browser Firefox selbst lässt sich sicherheitstechnisch optimieren und bringt bereits einige Sicherheitsfunktionen von Haus aus mit. Die entsprechenden Einstellungen können Sie beim Firefox im Menü «Extras» im Reiter «Sicherheit» vornehmen.


Abb.: Sicherheitseinstellungen im Firefox Browser

Basis-Einstellungen

Wie in Abbildung X zu sehen ist, sollten hier bestimmte Haken gesetzt sein. Der zweite und dritte Haken erklären sich von selbst und sollten auf jeden Fall aktiviert werden, um nicht auf Webseiten zuzugreifen, die nachweislich problematisch
sind. Ist der erste Haken zusätzlich gesetzt, werden sogenannte Add-ons geblockt, die automatisch installiert werden sollen, also ohne vorherige Interaktion mit dem Anwender.

Add-ons sind kleine Zusatzprogramme, mit denen der Browser erweitert werden kann, ähnlich der Sonderausstattung im Auto. Im Normalfall können diese, wie noch beschrieben wird, sehr nützlich sein. Aber es könnten auch Add-ons installiert werden, welche die Sicherheit bedrohen, daher die Warnung. Der sich anschließende Bereich «Passwörter» bezieht sich auf die Speicherung von eingegebenen Passwörtern. Der Browser merkt sich nach der ersten Eingabe auf Wunsch die Zugangsdaten und füllt die entsprechenden Felder beim nächsten Besuch automatisch aus. Diese Komfortfunktion kann nicht als ausreichend sicher betrachtet werden und sollte daher nicht genutzt werden.

Werbung und aktive Inhalte blocken

Blinkende Werbebanner sind oftmals ein Hilfsmittel für kriminelle Machenschaften. Um diese Art Werbung zu blocken, sollten Sie Ihren Browser ausrüsten, indem Sie ein entsprechendes Add-on installieren – beim Firefox zum Beispiel Adblock Plus. Dazu rufen Sie die Mozilla-Add-on-Webseite auf und geben in das Suchfeld
«Adblock Plus» ein. Zur Installation drücken Sie lediglich den Button "Zu Firefox hinzufügen" und wählen im folgenden Dialog «Jetzt installieren» aus.

Nachdem das Add-on installiert wurde, müssen Sie den Browser neu starten, und es öffnet sich eine Webseite, auf der Sie aufgefordert werden, eine der angegebenen Listen auszuwählen. Für Deutschland, Österreich und die Schweiz ist es sinnvoll, die vorgewählte «Easy List Germany + Easy List» auszuwählen.

und die Eingabe zu bestätigen. Fortan bleiben Sie größtenteils von lästiger und manchmal auch gefährlicher Werbung verschont.

Aktive Inhalte können, wie bereits erläutert, ebenfalls eine Gefahr darstellen. Deshalb besitzen die meisten Browser bereits einen eingebauten Warnmechanismus, wenn aktive Inhalte zur Ausführung kommen sollen. Dieser ist aber nicht sehr flexibel und reicht kaum aus. Eine deutlich bessere und komfortablere Kontrolle bietet da das Firefox-Add-on NoScript. Die Installation folgt dem Beispiel von Adblock Plus.
Danach blockt NoScript zunächst alle Skripte (aktive Inhalte) auf einer Webseite und teilt Ihnen dies mit. Sie können nun entscheiden, welche Skripte Sie – temporär oder immer – zulassen wollen und welche nicht. Der gelbe Balken am unteren Bildrand signalisiert Ihnen, dass Skripte vorhanden sind, und mit einem Klick auf den Einstel lungen- Button beziehungsweise auf das -Symbol rechts unten in der Statusleiste gelangen Sie in das entsprechende Menü (siehe Abbildung X #TODO). Das Symbol zeigt gleichzeitig an, welche Skripte geblockt werden und welche nicht.

NoScript ist einfach aufgebaut und damit auch für unerfahrene Internetnutzer empfehlenswert. Der tägliche Surfaufwand erhöht sich minimal, doch Sicherheit benötigt eben auch Zeit und Aufmerksamkeit.

Eine andere Möglichkeit ist, JavaScript über die Grundeinstellung des Browsers vollständig zu blocken (beim Firefox über das Menü «Extras» und dann im Reiter «Inhalt»).
Allerdings führt das im Zeitalter von Web 2.0 dazu, dass sehr viele Webseiten nicht mehr richtig nutzbar sind. Darum ist es sinnvoller, mit Add-ons wie NoScript flexibel zu bleiben.

Beispielsweise können Anwender in Microsofts Internet Explorer unter mehreren Sicherheitsstufen eine geeignete wählen. Hier kann beispielweise festgelegt werden, dass vom Nutzer eingegebene Passwörter niemals gespeichert werden oder diese erst durch die Eingabe eines Master-Passwortes zu Beginn einer Browsersitzung freigegeben werden. Außerdem kann der Zugriff auf Websites gesperrt werden, die als unseriös eingestuft werden. Für mehr Transparenz über Hintergrundprozesse, die automatisch und oft unbemerkt vom Anwender ablaufen, wie beispielsweise die verschlüsselte oder unverschlüsselte Datenübertragung oder die Installation bestimmter Add-Ons, sollten sämtliche Warnmeldungen und -hinweise aktiviert werden.

Auf die praktische aber unsichere Passwort-Speicher-Funktion des Browsers (ohne die Eingabe eines Master-Passworts) und das Auto-Vervollständigen, beispielsweise bei Google-Suchen, sollte verzichtet werden. Verschafft sich ein Angreifer erfolgreich Zugriff auf das System des Anwenders, hat er nämlich aufgrund des Passwort-Speichers sonst gleich auch Zugriff auf sämtliche genutzte Online-Dienste.

***Die Deaktivierung der aktiven Inhalte erhöht die Browsersicherheit maßgeblich, führt aber zum Komfortverlust beim Surfen.***

Eine der wichtigsten Entscheidungen betrifft die Darstellung sogenannter aktiver Inhalte auf Websites. Aktive Inhalte wie beispielsweise Videos können durch Browser-Plug-Ins wiedergegeben werden. Ihnen ist gemein, dass sie nach dem Laden einer aufgerufenen Website lokal auf dem System des Anwenders temporär gespeichert und ausgeführt werden. Genau hier besteht ein großes Sicherheitsrisiko, da aktive Inhalte als Träger von Schädlingen eine unmittelbare Gefahr für das Anwendersystem darstellen können. Java und Flash sind – wie in Kapitel 2 schon erwähnt – besonders populäre Anwendungen und damit Zielscheibe krimineller Bemühungen. Leider werden gerade die Sicherheitsupdates dieser Plug-Ins oft erst mit großer Verzögerung von Nutzern eingespielt.

Entscheidet sich ein Anwender des Internet Explorers für die höchste Sicherheitseinstellung im Browser, wird die Ausführung der aktiven Inhalte auf Websites unterbunden und somit auch nicht lokal zwischengespeichert. Dieses höhere Sicherheitsniveau geht allerdings mit Komfortverlust beim Surfen einher, das witzige Video vom Kollegen kann gegebenenfalls nicht wiedergegeben werden.

### Clickjacking-Gefahr

Clickjacking ist eine Angriffsmethode, bei der sichtbare Webinhalte von unsichtbaren Schaltflächen überlagert werden, die sich beim Mausklick des Nutzers unbemerkt aktivieren und bestimmte Prozesse auslösen. Clickjacking ist besonders in sozialen Netzwerken verbreitet – hier betätigen Nutzer beispielsweise mit dem Klick auf ein harmlos wirkendes Video einen unsichtbaren Like-Button und verbreiten einen betrügerischen Link in ihrem Freundeskreis.
Zum Schutz vor Clickjacking ist die Nutzung des Browser-Plug-Ins NoScript[51] empfehlenswert. Hiermit werden alle unsichtbar ausgeführten Skripte auf Internetseiten sichtbar und können wahlweise gestoppt werden.

### Sensible Daten vor der Übertragung schützen

Sollen sensible Dateien und Dokumente wie Firmeninterna, Strategiepapiere oder Kunden-Stammdaten online verschickt werden, wird es wichtig, sowohl die Dateien an sich als auch ihren Versandweg vor fremden Zugriff abzusichern. Dazu sollte zunächst ein geeigneter Datenverschlüsselungsmechanismus gewählt werden, wie ihn beispielsweise das Programm TrueCrypt bietet (siehe Kapitel *3.1.6 Datenverschlüsselung* und *3.2.6 Datenverschlüsselungsmechanismen*). Wird nun auch der Übertragungskanal verschlüsselt, auf dem Dateien zum Adressaten übersandt werden, sind die Dateien doppelt abgesichert. Große Sicherheit bietet hier beispielsweise ein PGP- oder S/MIME-verschlüsselter E-Mailversand oder spezielle Firmensoftware.

***Sensible Daten sollten vor der Übertragung verschlüsselt werden. Tools wie TrueCrypt bieten eine sichere Verschlüsselungstechnik.***

### Sicheres Chatten

Selbst wenn sich die Gesprächspartner eines Chats im selben WLAN aufhalten, sollten alle Gesprächsdaten über das Chatprogramm verschlüsselt übertragen werden. Bei der Wahl eines Chatprogramms sollten Anwender darauf achten, ob Gesprächsdaten standardmäßig verschlüsselt übertragen werden.
Kostenlose Programme sollten auf ihre Nutzungsbedingungen und Schutzmaßnahmen hin überprüft werden. Auch hier kann der Besuch der Hersteller-Website erste Anhaltspunkte auf die Seriosität liefern. Ein Beispiel hierfür sind Messanger wie Pidgin[52], die den sogenannten XMPP[53]-Standard nutzen. Anwender können mit der Erweiterung „Off-the-Record“ (OTR) verschlüsselt chatten – vorausgesetzt, der Kommunikationspartner nutzt ebenfalls XMPP [54]und OTR.
Chatfunktionen sozialer Netze wie Facebook eignen sich in der Regel nicht zum Austausch sensibler Daten, da sie meist unzureichend vor fremden Zugriff geschützt sind.

***Für Chats sind Instant Messenger mit Verschlüsselungsfunktion und keinesfalls die Chatfunktion sozialer Netzwerke wie Facebook zu nutzen.***

[51] *http://noscript.net*
[52] *https://www.pidgin.im/*
[53] *Extensible Messaging and Presence Protocol (XMPP), früher „Jabber“*
[54] *http://www.heise.de/ct/hotline/FAQ-Instant-Messaging-2055987.html*

***Wählen Sie geeignete Sicherheitseinstellungen für Ihren Webbrowser und blockieren Sie gegebenenfalls die Wiedergabe aktiver Inhalte auf Websites. Nutzen Sie Add-Ons wie „NoScript“. Deaktivieren Sie bei akuten Gefahren bestimmte Plug-Ins wie Java oder Flash in den Einstellungen des Browsers. Verzichten Sie auf die Passwort-Speicher-Funktion des Browsers und das Auto-Vervollständigen. Aktivieren Sie alle Warnmeldungen und -hinweise. Schützen Sie sensible Dateien vor dem Versand durch eine Datenverschlüsselungssoftware und verschlüsseln Sie zudem den Kommunikationskanal, auf dem sie versandt werden. Nutzen Sie zum Chatten ausschließlich einen Instant Messenger, der Gesprächsdaten standardmäßig verschlüsselt. Meiden Sie die Chatfunktion sozialer Netzwerke zum Austausch sensibler Informationen.***

### 4.4.1 HTTPS

Sensible Daten, die etwa für Online-Shopping und -banking oder für Ticketreservierung von Bahn- und Flugreisen erforderlich werden, sollten auf gesichertem Weg vom Webbrowser zum Zielserver übertragen werden. Hierfür ist eine Verschlüsselung via SSL/TLS (Secure Sockets Layer/ Transport Layer Security) gebräuchlich. Diese erfüllt hauptsächlich zwei Funktionen: Erstens wird überprüft, ob tatsächlich eine Verbindung mit dem gewünschten Internetserver aufgebaut wurde, der sich hinter einer Internet-Adresse verbirgt (Authentifikation der Kommunikationspartner). Dazu fordert der Browser ein SSL-Domänen-Zertifikat vom Zielserver an, das dem Betreiber des jeweiligen Internetdienstes von einem der wenigen Zertifizierungsstellen bereitgestellt worden ist. Hat der Browser ein geprüftes Domänen-Zertifikat erhalten, entsteht nach weiteren kleinen Kommunikationstests der Verbindungsaufbau innerhalb weniger Sekundenbruchteile. Zweitens wird ein gesicherter Kommunikationsweg über einen verschlüsselten Kanal aufgebaut (Verschlüsselungsverfahren unter Nutzung eines gemeinsamen Sicherheitsschlüssels).

Erkennbar ist die SSL/TLS-verschlüsselte Verbindung an dem zusätzlichen „s“ hinter dem „http“ der aufgerufenen Internetadresse („https“). In der Browser-Adresszeile könnte also beispielsweise stehen: „https://www.it-sicherheit-handwerk.de“. Oft erscheint zusätzlich ein kleines Schlosssymbol in der Statusleiste des Browsers. Die Stärke der Verschlüsselung kann durch einen Doppelklick auf dieses Symbol in Erfahrung gebracht werden. Der verwendete Schlüssel sollte mindestens 128bit lang sein und als Verschlüsselungsalgorithmus soll z.B. RSA-, AES- oder Camellia verwendet werden.

***Bei Eingabe/Übertragung sensibler Daten in/an Online-Dienste, ist auf eine SSL/TLS-Verschlüsselung zu achten. Erkennbar ist diese am zusätzlichen „s“ in „https“.***

Online-Dienste, die vertrauliche Daten vom Nutzer einfordern, ohne eine solche https-Verschlüsselung bereitzustellen, sollten kritisch auf Seriosität hin überprüft werden. Oft können Anwender so präparierte und schadhafte Websites, die bekannten Internetseiten in ihrer Optik nachempfunden wurden, als Schwarze Schafe enttarnen, da Kriminelle dieses Sicherheitsmerkmal nicht so leicht vortäuschen können (siehe Kapitel *2.5 Phishing und Social Engineering*). Auch kleinere und mittelständische Unternehmen, die Online-Dienste zur Verfügung stellen, bei denen Kunden sensible Daten austauschen, kommen um eine SSL/TLS-Verschlüsselung nicht umher. So sollte beispielsweise die Kaufabwicklung im Online-Shop der Firma nur auf gesichertem Wege erfolgen. Soll der Online-Shop durch einen externen Dienstleister bereitgestellt werden, ist dieser im Vorfeld auf Seriosität und Sicherheitsmechanismen hin zu überprüfen.

## Browser-Plug-Ins für mehr Sicherheit

Um von der SSL-Verschlüsselung profitieren zu können, ist Software-Aktualität des genutzten Browsers wichtig. Ältere Browser und Browserversionen unterstützen bisweilen keine gängigen Verschlüsselungsverfahren.

***Browser-Plug-Ins wie HTTPS Everywhere helfen dabei, von der SSL/TLS-Verschlüsselung überall da zu profitieren, wo sie angeboten wird.***

Einige Erweiterungen für gängige Browsertypen verhelfen Anwendern dazu, stets verschlüsselte Verbindungen zwischen Browser und Server automatisch aufzubauen, sofern der jeweilige Online-Dienst-Betreiber SSL-Zertifikate für seinen Dienst bereitstellt. Beispiele hierfür sind KB SSL Enforcer[55] für Google Chrome, Redirect to HTTPS[56] für Opera und HTTPS Everywhere für Mozilla Firefox[57]. Wird eine http-Adresse im Browser aufgerufen, leiten die Plug-Ins automatisch auf die https-Version der Internetseite um, sofern möglich.

***Achten Sie bei Eingabe sensibler Daten in den Browser stets auf eine SSL/TLS-verschlüsselte Verbindung (erkennbar am „https“ der Adresszeile). Als Betreiber von Online-Diensten, die einen Austausch vertraulicher Daten mit Kunden zur Nutzung voraussetzen, sollten Sie ebenfalls einen gesicherten Übertragungsweg bereitstellen. Nutzen Sie stets eine aktuelle Browserversion und installieren Sie Browser-Plug-Ins wie HTTPS Everywhere für mehr Sicherheit im Netz.***

[55] *https://chrome.google.com/webstore/detail/kb-ssl-enforcer/flcpelgcagfhfoegekianiofphddckof/details*
[56] *https://addons.opera.com/en/extensions/details/redirect-to-https/?display=en*
[57] *https://www.eff.org/Https-everywhere*

### 4.4.2 VPN

***VPN-Tunnel sollten in jedem WLAN-Netz außerhalb des Firmennetzes verwendet werden, egal ob es WPA2-verschlüsselt oder öffentlich ist.***

Zur sicheren Kommunikation mit dem Unternehmensnetzwerk von unterwegs aus eignet sich das sogenannte Virtual Private Network (VPN). Vereinfacht gesagt, können sich Anwender, die in einem öffentlichen Netzwerk surfen, mithilfe eines VPN-Tunnels so mit ihrem Unternehmensnetzwerk verbinden, als wären sie tatsächlich vor Ort in den Büroräumen des Unternehmens. Das öffentliche Netz stellt somit im übertragenen Sinn einen sicheren Tunnel zum Unternehmensnetzwerk dar. Die so hergestellte Verbindung ist verschlüsselt und kann von Angreifern nicht direkt angegriffen werden. Wenn also Daten mit dem Unternehmensserver ausgetauscht werden sollen, wird die Verwendung einer VPN-verschlüsselten Verbindung notwendig – gerade dann, wenn sich Mitarbeiter in einem öffentlichen Netz aufhalten. Neben dem verschlüsselten Außenzugriff ist zudem eine interne Netzwerk-Verschlüsselung ratsam, damit es im Fall eines kontaminierten Netzwerkteilnehmers trotz externer Netzwerkverschlüsselung nicht zu einem Datenabfluss kommt.

***Nutzen Sie das Handbuch Netzwerksicherheit oder andere Fachliteratur für detailliertere Informationen zum Thema VPN.***

***Nutzen Sie die betriebliche VPN-Verbindungen, sobald Sie von unterwegs aus mit dem Unternehmensserver oder anderen Online-Diensten kommunizieren wollen. Hinweise zu VPN und zur Erstellung eines betrieblichen VPN-Tunnels finden Sie auf der Internetseite des Bundesamts für Sicherheit in der Informationstechnik[58].***

## 4.5 Sicheres Speichern und Löschen von sensiblen Daten

Speicherorte für sensible Daten sollten entsprechend des in den Unternehmensrichtlinien festgelegten Reglements ausgewählt werden. Gibt es hier Zweifel, ist der Sicherheitsbeauftragte im Unternehmen oder die Unternehmensleitung zu kontaktieren. Wie schon im Kapitel *3. Maßnahmen auf der Geräteebene – Basisschutz* beschrieben, sollten möglichst wenige Kunden- und Unternehmensdaten lokal auf den mobilen Endgeräten gespeichert werden. In vielen Fällen ist der Unternehmensserver oder die unternehmenseigene Cloud der passende Speicherort.

#### Sicheres Löschen von sensiblen Daten

Das sichere Löschen von sensiblen Daten wird vor allem dann relevant, wenn Altgeräte aus dem Bestand entsorgt werden sollen. Auch hier können sich Mitarbeiter an den dokumentierten Unternehmensrichtlinien orientieren. Wie zuvor schon erwähnt, erfüllt das einfache Löschen höhere Sicherheitsanforderungen meist nicht. Angreifer haben dann große Chancen, die vermeintlich gelöschten Daten wiederherzustellen, sollte ihnen ein entsorgtes Gerät in die Hände fallen.

[58] *https://www.bsi.bund.de*

***Programme zum sicheren löschen für Windows sind beispielsweise „Secure Eraser[59]“ (ca. 20 € für die kommerzielle Version) oder „Eraser[60]“ (nur auf Englisch verfügbar).***

## 4.6 Sicheres Bezahlen mit mobilen Endgeräten

***Online-Banking ausschließlich über das Smartphone ist gefährlich, da hier das Risiko nicht auf zwei Geräte verteilt wird.***

Bei dem sogenannten mTan-Verfahren (mobile Tan) werden zum Online-Banking zwei Geräte genutzt: Laptop oder Desktop-PC plus Handy oder Smartphone. Erfolgt das Online-Banking ausschließlich via Smartphone, verteilt sich das Risiko, Opfer eines Datendiebes zu werden, nicht auf zwei verschiedene Geräte. Ist ein Smartphone beispielsweise mit Schädlingen kontaminiert, könnten sowohl Zugangspasswörter zum Banking-Account als auch mTans mitgelesen werden. Diese Informationen werden bei Nutzung zweier Geräte getrennt voneinander vorgehalten. Das Smartphone allein eignet sich also nicht für Online-Banking.

Bei Geräten, die zum E-Payment oder auch Mobile Banking genutzt werden, sind nicht nur angewandte Verschlüsselungsmechanismen zwischen E-Payment-Gerät und Smartphone entscheidend. Wird zur betrieblichen Finanzbuchhaltung der Dienst eines Cloud-Service Providers in Anspruch genommen, sollten auch hier Kommunikationswege sowie Serverstandorte kritisch überprüft werden. Amerikanische Dienstleister haben beispielsweise andere Datenschutzauflagen als deutsche.

Hinweise für das Micro-Payment via NFC-Chip im Kapitel *2.1.5 Near Field Communication*.

[59] *https://www.ascomp.de/de/products/show/product/secureeraser*
[60] *http://eraser.heidi.ie/download.php*

## 4.7 Zusammenfassung

**Schutzmaßnahmen auf der Mitarbeiterebene – Sensibilisierung**

Technische Schutzmaßnahmen, die von Arbeitgeberseite aus getroffen werden, sollten stets einhergehen mit einer umfassenden Mitarbeitersensibilisierung. Eine sichere Handhabung der Geräte ist Voraussetzung für den Einsatz mobiler Endgeräte. Diese umfasst physische Schutzmaßnahmen wie den Diebstahlschutz aber auch die verantwortungsvolle Nutzung von Apps (Stichwort: Zugriffsrechte).

Passwortsicherheit sollte in Unternehmen ohnehin schon ein großes Thema sein und ist auch in Zusammenhang mit mobilem Arbeiten  an von großer Relevanz. So sollten alle genutzten Dienste, verschlüsselte Festplatten und Ordner in jedem Fall mit sicheren Passwörtern versehen sein und nach Möglichkeit auch der Geräte-Zugriff.

Kommunikationswege zwischen Außendienstmitarbeitern und Unternehmensserver sollten stets sichere sein, hier sind Verschlüsselungsmaßnahmen via VPN und HTTPS notwendig.

Datenspeicherorte sind ausdrücklich durch den Arbeitgeber festzulegen und auch das sichere Löschen sensibler Daten beziehungsweise die Geräteentsorgung sollten Themen bei Mitarbeiterschulungen sein, damit ist nicht zu bösen Überraschungen kommt.

**Notizen**

# 5. Schutzmaßnahmen auf der Verwaltungsebene – Organisation

Dieses Kapitel soll den Verantwortlichen in Unternehmen helfen, den Handlungsspielraum für Mitarbeiter im Umgang mit mobilen Endgeräten festzulegen. Es gibt Verantwortlichen die Möglichkeit, das Sicherheitsniveau für die Firma anhand dieser Leitlinie selber zu definieren. Falls noch nicht geschehen, sollte die Unternehmensführung in Absprache mit den Mitarbeitern zunächst eine Person als IT-Sicherheitsbeauftragten festlegen[61]. Der Sicherheitsbeauftragte setzt sich infolge mit IT-sicherheitsrelevanten Themen auseinander, um seinen Kollegen mit Rat und Tat zur Seite zu stehen. Im Idealfall ist er besonders IT-affin und bereits zuständig für die betriebliche IT. Kommt es zu einem Sicherheitsvorfall, ist er die erste Anlaufstelle und informiert die Unternehmensführung.

***Übertragen Sie einem Mitarbeiter den Verantwortungsbereich „IT-Sicherheitsbeauftragter des Unternehmens“.***

## 5.1 Klassifizierung sensibler Daten – Speicherorte, Kommunikationswege und Zugriffsrechte

Jeder dritte Handwerksbetrieb mit weniger als zehn Mitarbeitern gewährt allen Mitarbeitern Zugriff auf sämtliche, zum Teil besonders sensible Unternehmensdaten. Knapp 20 Prozent der mittelgroßen Betriebe mit bis zu 49 Mitarbeitern verzichten ebenfalls auf die Beschränkung von Zugriffsrechten zu vertraulichen Unternehmensdaten (vgl. IT-Sicherheit im Handwerk, 2013). Sicherheitsexperten gehen davon aus, dass diese empirisch erhobenen Zahlen sogar positiver ausfallen als in der Realität. Die Beschränkung der Zugriffsrechte auf sensible Ressourcen ist sinnvoll, um die Anzahl möglicher Angriffsvektoren zu reduzieren. Je mehr Mitarbeiter vollen Zugriff auf sämtliche Unternehmensdaten haben, desto größer ist die Chance für Angreifer, sich Zugriff auf diese zu verschaffen – beispielsweise durch Social-Engineering-Angriffe (*siehe Kapitel 2.5 Phishing und Social Engineering*).

### Vertraulichkeitsstufen definieren Speicherorte und Kommunikationswege

***Es sind mindestens vier Vertraulichkeitsstufen für Daten zu definieren, aus denen Speicherorte und Kommunikationswege resultieren.***

Zunächst sollten sich Verantwortliche darüber klar werden, welche Daten in der Informationstechnologie und speziell in ihrem Unternehmen als vertraulich gelten sollten. Personenbezogene Daten sind qua Gesetz schutzbedürftig und demnach vertraulich zu behandeln (siehe Kapitel *2.10 Rechtliche Risiken*). Dies betrifft insbesondere Kranken- und Rentenversicherungsnummern, Finanzdaten, Personaldaten und Kundendaten. Darüber hinaus gelten auch Betriebs- und Geschäftsdaten (z.B. Zugangsdaten für bereitgestellte Online-Dienste) als besonders sensibel und schützenswert. Je nach Verwendungszweck der gespeicherten Daten muss diese Liste um weitere Positionen ergänzt werden. Für einen sicherheitsbewussten Umgang mit der Flut an sensiblen

[61] *Oft eignet sich der Datenschutzbeauftragte (nach BDSG) für diese Position.*

Daten sollten Verantwortliche im Vorfeld eine Klassifizierung aller betrieblichen Informationen vornehmen. Dazu sind Vertraulichkeitsstufen der unterschiedlichen Datensätze anhand einer simplen Fragestellung festzulegen: Welchen Nutzen haben Dritte, wenn ihnen speziell diese Daten in die Hände fallen? Die Antwort auf diese Frage gibt einen Hinweis auf die Schwere des Verlusts dieser Daten. Auf diese Weise können Informationen unterschiedlichen Vertraulichkeitsstufen zugeteilt werden. Die Anzahl der Stufen ist variabel, mindestens sind jedoch vier Stufen empfehlenswert, um Speicherorte und Kommunikationswege genauer definieren zu können.
Beispielsweise:

- Öffentlich: Daten sind für die Öffentlichkeit bestimmt
- Normal: Die Schadensauswirkungen sind begrenzt und überschaubar.
- Hoch: Die Schadensauswirkungen können beträchtlich sein.
- Sehr hoch: Die Schadensauswirkungen können ein existenziell bedrohliches, katastrophales Ausmaß erreichen.

Je nach Vertraulichkeitsstufe sind unterschiedliche Speicherorte für sensible Daten zu wählen. Mit steigernder Vertraulichkeitsstufe wachsen auch die Sicherheitsanforderungen an den zu wählenden Speicherort. Gleiches gilt für die Kommunikationswege bei Übermittlung vertraulicher Informationen an einen Kunden oder Kollegen. Ein Passwort zu einem gemeinsam genutzten Online-Dienst (hohe Vertraulichkeitsstufe) sollte beispielsweise nur mündlich oder mittels PGP-verschlüsselter E-Mail an den Kollegen übermittelt werden. Sensible Kundendaten sollten dem Kunden nur postalisch und nicht via E-Mail mitgeteilt werden.

**Daten-Zugriffsbeschränkungen**

***Die Klassifizierung der Daten geht einher mit dem Einsatz eines Berechtigungssystems, das anhand von Berechtigungsprofilen Zugriffsrechte der Mitarbeiter reglementiert.***

Es gilt die Regel: Ein Mitarbeiter erhält Zugriff auf diejenigen Daten, die er aufgrund seines Tätigkeitsbereichs zum Arbeiten benötigt. Es sollte im Unternehmen also ein Berechtigungssystem geben, das mit der Authentifizierung des Mitarbeiters zum Unternehmensnetzwerk gekoppelt ist. Jedem Mitarbeiter wird eine Berechtigungsrolle zugewiesen, die ihn für den Zugriff auf bestimmte Daten autorisiert. Der Zugriff auf personenbezogene Unternehmensdaten wie beispielsweise Kunden-Daten ist qua Bundesdatenschutzgesetz Unbefugten zu verwehren („Zugriffskontrolle“ in der Anlage des BDSG, siehe Kapitel *2.10.3 Datenschutzanforderungen*), sodass in diesem Fall ein Berechtigungssystem unumgänglich wird.
Zugriff auf Daten der höchsten Vertraulichkeitsstufe (z.B. nicht angemeldete Patentdokumente) sollte der Unternehmensführung vorbehalten sein.

### 5.1.1 Umgang mit hochsensiblen Bereichen

Hochsensible Daten wie beispielsweise Unterlagen, die für eine Patentanmeldung gedacht sind, sollten nicht auf die Speicher von Smartphones und Tablets gelangen. Gleiches gilt auch für Bank- und Kreditkartendaten.

## 5.2 Auflagen und Richtlinien für Mitarbeiter

Die Verantwortlichen im Unternehmen sollten gemeinsam mit dem Sicherheitsbeauftragten und gegebenenfalls externen Sicherheitsexperten einen Katalog von Anforderungen und Richtlinien anfertigen, der den Mitarbeitern im Unternehmen eine Orientierungshilfe für Fragen der IT-Sicherheit sein soll. Auf die „IT-Sicherheitsrichtlinien der Firma XY“ können sich infolge sowohl die Mitarbeiter als auch die Unternehmensfüh-

rung im Zweifel oder im Streitfall berufen. Sie gelten nach Meinung des IT-Rechtsexperten Wilfried Reiners jedoch nicht als Rechtsgrundlage, sofern der Arbeitgeber den erforderlichen Zugriff auf das private Gerät begründen wolle („Auftragskontrolle“, siehe Kapitel *2.10.2 Datenschutzbestimmungen*). Zur Ausarbeitung der darin enthaltenen Auflagen für die Mitarbeiter ist ein kontinuierlicher Austausch mit diesen essentiell, um späteren Konfliktsituationen vorzubeugen. Verbindlichkeitscharakter erhalten die Unternehmensrichtlinien durch die Unterschriften der Mitarbeiter. Verstöße gegen die vereinbarten Regelungen sollten Konsequenzen nach sich ziehen. An dieser Stelle können keine konkreten Auflagen vorgegeben werden – das Ausmaß und die Strenge der Auflagen hängen von der jeweiligen Unternehmenspolitik ab.
Nachfolgend also lediglich eine Übersicht über die Fragen, die in den Unternehmensrichtlinien geklärt werden sollten.

***Die Strenge der Auflagen für die Mitarbeiter ist individuell für jedes Unternehmen zu treffen.***

### 5.2.1 Trennung von Privatem und Geschäftlichem

- Soll Mitarbeitern die Nutzung von privaten Geräten für dienstliche Zwecke (BYOD) gestattet oder untersagt werden?
- Mit welchen (technischen) Mitteln sollen bei BYOD die Unternehmensdaten von den privaten Daten auf den Gerätespeichern separiert werden?
- Für welche Unternehmenssoftware-Produkte bestehen erweiterte Lizenzen, die auch private Nutzung beinhalten und für welche nicht?
- Wer haftet bei Geräteverlust oder -beschädigung, sofern durch Mitarbeiter verschuldet?
    - Auf welche Art und Weise erfolgt der Hinweis auf den vertrauensvollen Umgang mit Firmendaten?
- Wie werden die Kontroll- und Zugriffsrechte des Arbeitgebers unter Beachtung des Fernmeldegeheimnisses sichergestellt?
- Welche Schritte sind bei Beschäftigungsende neben der Löschung der Unternehmensdaten vom Privatgerät des Mitarbeiters nötig?
    - Soll eine Kontrolle der Löschung durch den Arbeitgeber erfolgen?

### 5.2.2 Richtlinien für den Umgang mit den Geräten

- Durch welche technischen Mittel werden die Datenschutzauflagen, die sich aus dem BDSG §9 ergeben, praktisch umgesetzt?
- Sind neben dem Geräte-Basisschutz weitere Sicherheitsanforderungen Voraussetzung zur dienstlichen Nutzung der Geräte?
    - Sollten nur bestimmte Gerätetypen Zugang zum Unternehmensnetzwerk erhalten?
    - Sollte der Unternehmensführung vorbehalten sein, zu alte Geräte (bzw. Geräte mit veralteter Software) oder unsichere Geräte (Stichwort: Jailbreaking/Rooting) aus dem Unternehmensnetzwerk auszuschließen?
    - Sollte die Installation ganz bestimmter IT-Sicherheitsprodukte für alle Mitarbeiter verpflichtend sein (betrifft: Security Suite, Sicherheitstools, Verschlüsselungssoftware, Browser-Plug-Ins)?
- Wie sind die privaten Geräte zu warten und wer ist verantwortlich für den Geräte-Support?
- Welche Anforderungen gibt es hinsichtlich der zu wählenden Passwörter für genutzte Dienste?

- Ist es Mitarbeitern gestattet, nicht-dienstliche Anwendungen/Programme auf den Geräten zu installieren?
- Welche Schritte sind im Fall des Geräteverlusts zu tun?
    - Besteht die Zustimmung des Mitarbeiters, dass im Fall des Geräteverlusts mittels Fernlösch-Funktion auch private Daten gelöscht werden können (unter Beachtung der rechtlichen Risiken für den Arbeitgeber)?
    - Können gezielt nur die Unternehmensdaten mithilfe einer Mobile-Device-Management-Lösung gelöscht werden (siehe Kapitel *5.4 Zentralisierte Verwaltung der Geräte*)?

### 5.2.3 Kommunikation mit dem Unternehmensserver

- Welche Software wird für die Zuweisung digitaler Zertifikate für einen sicheren Zugang zum Unternehmensnetzwerk verwendet?
- Welchen Verschlüsselungsstandard muss ein unterwegs genutztes Netzwerk (z.B. WLAN) aufweisen?
- Ist die Nutzung eines VPN-Tunnels zur Kommunikation mit dem Unternehmensnetzwerk Pflicht?
- Ist die Nutzung von verschlüsselter E-Mail-Kommunikation Pflicht?

### 5.2.4 Datenspeicherungsroutinen und -orte

- Welcher Speicherort ist für welchen Datentyp entsprechend seiner Vetraulichkeitsstufe zu wählen, wie in Kapitel 5.1 dargestellt?
- Welche sensiblen Daten dürfen auf den mobilen Endgeräten gespeichert werden?
- Wie lautet der zu wählende Verschlüsselungsmechanismus für sensible Daten, die auf den Geräten abgelegt werden?
- Wie sehen die Backup-Routinen aus?
    - Welche Backup-Regelmäßigkeiten sollen gelten?
    - Wo und wie sind die Backups anzulegen?
    - Wie werden die gesicherten Daten verschlüsselt?

## 5.3 Notfallplan: Was im Fall des Geräteverlusts zu tun ist

Hat ein Anwender den Verlust seines Gerätes festgestellt, hat er verschiedene Handlungsoptionen, die er unmittelbar mit dem Sicherheitsbeauftragten des Unternehmens oder der Betriebsleitung besprechen sollte. Bestenfalls ist die Vorgehensweise bei Geräteverlust in den Richtlinien des Betriebs vorgeschrieben. In jedem Fall sollten schnellstmöglich sämtliche Passwörter zu genutzten Diensten geändert werden. Falls möglich, sollte umgehend vom Arbeitgeber der Zugriff des vermissten Geräts zum Unternehmensnetzwerk mittels Mobile Device Management (siehe nachfolgendes Kapitel) gesperrt werden. Im Folgenden soll eine mögliche Vorgehensweise für den Verlust eines Smartphones beschrieben werden. Diese kann in Teilen auch für den Verlust eines Tablets gelten.

### Verlust des Smartphones

Im ersten Schritt ist es sinnvoll, die Fern-Ortungsfunktion in Anspruch zu nehmen. Sofern das Smartphone nach dem Verlust nicht manipuliert wurde, erhält ein Anwender per SMS oder E-Mail die geografischen Koordinaten seines Gerätes. Gegebenenfalls löst der Ortungsversuch einen Warnton aus, der von Passanten in der Nähe oder sogar vom Anwender selbst wahrgenommen werden kann, sollte sich das Gerät noch in der Nähe befinden. So lassen sich auch liegengelassene Smartphones wiederfinden, die nicht gestohlen wurden.
Auch ein Anruf der eigenen Rufnummer kann unter Umständen hilfreich sein – vielleicht hört der Gerätebesitzer seinen Klingelton in der Nähe oder ein ehrlicher Finder nimmt ab. Natürlich wird hier im Fall eines Diebstahls auch der Dieb darüber informiert, dass ein Besitzer den Verlust seines Gerätes festgestellt hat – er wird dementsprechend reagieren, sodass für den Anwender der Handlungsspielraum zum Schutz der gespeicherten Daten eventuell kleiner wird.

***Vorgehensweise nach dem Verlust eines Smartphones:***

Bleibt das Gerät unauffindbar, kommen Smartphone-Nutzer, die ihre privaten Geräte beruflich einsetzen oder sogar ein firmeneigenes Gerät nutzen, nicht umher, die auf dem Gerät gespeicherten Daten (z.B. Kalendereintrage, Kontakte, Fotos, SMS, E-Mails, Einstellungen, Apps) via Fern-Löschungsfunktion unwiderruflich zu löschen. Selbst, wenn sämtliche Daten auf dem Gerätespeicher durch eine Verschlüsselung geschützt sind, ist die Löschung der Daten die sicherste Option. Daneben sollten SIM-Lock-Funktionen der Mobile Security Suite zum Einsatz kommen, die die SIM-Karte des gestohlenen Gerätes sperren. Die Sperre sollte in jedem Fall auch zusätzlich über den jeweiligen Mobilfunkanbieter erfolgen. Nachfolgend einige Anbieter-Hotlines für die SIM-Sperre:

***1. Schritt: Ortung;***
***2. Schritt: Anruf;***
***3. Schritt: Daten löschen;***
***4. Schritt: Sperrung der SIM-Karte;***
***5. Schritt: Anzeige bei der Polizei***

**T-Mobile: 0800-3302202**
**Vodafone: 0172-1212**
**E-plus: 0177-1771000**
**O2: 01804-055222**
**Bundesnetzagentur (für sonstige Anbieter): 116 116**
(vgl. Pursche, 2013)

Einige Mobile Security Suites bieten neben der regulären SIM-Sperre auch weitere automatische Geräte-Sperren. Diese werden beispielsweise dann aktiv, wenn die SIM-Karte aus dem gestohlenen Gerät gewechselt oder das Gerät ohne SIM-Karte eingeschaltet wurde. Anschließend ist es ratsam, Passwörter zu E-Mail-Konten, Unternehmensnetzwerk, Firmen-Anwendungen und anderen Online-Diensten zu ändern – viele (Enterprise-)Apps speichern Passwörter, sodass sie unter Umständen nun im Besitz des Diebes sind.
Sind die Daten auf dem Gerät gelöscht, ist die SIM-Karte gesperrt und sind alle Kennwörter geändert, sollten Diebstahl-Opfer unter Angabe der IMEI Anzeige bei der Polizei erstatten. Eventuell gelangt das verlorene Gerät über Umwege wie zum Beispiel Fundstellen doch noch zurück zum Gerätebesitzer.

***Lassen Sie den Zugriff des verlorenen Geräts auf das Unternehmensnetzwerk sperren. Versuchen Sie, bei Geräteverlust das verlorene Smartphone zu orten. Ist es weiterhin nicht auffindbar, löschen Sie sämtliche gespeicherten Daten via Fernlösch-Funktion. Sperren Sie die SIM-Karte des Gerätes mithilfe der MSS-Software oder Ihrem Mobilfunkanbieter. Ändern Sie sämtliche Passwörter zu allen genutzten E-Mail-Konten, Firmenanwendungen und Online-Diensten. Erstatten Sie Anzeige bei der Polizei unter Angabe der IMEI.***

## 5.4 Zentralisierte Verwaltung der Geräte – Mobile Device Management (MDM)

***Mobile Device Management dient der zentralen Verwaltung von Smartphones und Tablets von einem Arbeitsplatz aus.***

Die IT-Landschaft deutscher Handwerksbetriebe ist sehr heterogen, auch innerhalb eines einzelnen Betriebs. Im täglichen Einsatz sind Geräte unterschiedlicher Typen und Hersteller mit unterschiedlicher Systemausstattung. So liegen beispielsweise auf dem Schreibtisch neben Laptop mit Windows-Betriebssystem ein Smartphone mit Android-Betriebssystem sowie ein Apple iPad. Kaum ein Betrieb, der seine Mitarbeiter flächendeckend mit Geräten derselben Marke, geschweige denn desselben Modells ausstattet. Das Konzept BYOD fördert die Gerätevielfalt, sofern in den Richtlinien zur Einbindung neuer Geräte in das Unternehmensnetzwerk keine spezifischen Geräteklassen vorgeschrieben sind (siehe Kapitel *5.3 Auflagen und Richtlinien für Mitarbeiter*). Die Vielfalt der unterschiedlichen mobilen Endgeräte im Betrieb hat aus einer organisatorischen Perspektive einen Kontrollverlust zur Folge. Verantwortliche sind voll und ganz auf den sicherheitsbewussten Umgang durch die Mitarbeiter angewiesen – in Bezug auf die Systemkonfiguration und Nutzung der Geräte, vor allem aber auch in Bezug auf das Einspielen von Sicherheitsupdates. Für sie ist es unmöglich, einen Überblick darüber zu bekommen, welche installierte Software auf dem neuesten Stand ist und welche nicht. Genügt das Vertrauen in die Sensibilität der Mitarbeiter nicht (siehe Kapitel *3.2.6. Aktualitätsprinzip*), sollte eine Softwarelösung gefunden werden, die eine zentralisierte Verwaltung der mit dem Unternehmensnetzwerk verbundenen mobilen Endgeräte ermöglicht.

### Funktionsumfang und Sicherheitsvorteile von MDM

***Der Funktionsumfang eines MDM-Produkts sollte beinhalten: (Fern-)Konfiguration, Wartung, Überwachung und Inventarisierung der Geräte***

Software aus dem Bereich des Mobile Device Managements (MDM) dient zur Verwaltung von Smartphones und Tablets und beinhaltet unter anderem Funktionen wie (Fern-)Konfiguration, Wartung, Überwachung und Inventarisierung aller Geräte in Echtzeit von einem Arbeitsplatz aus. Dazu greift die jeweilige MDM-Software aus der Ferne auf verschiedene Schnittstellen im Betriebssystem der Geräte zu, um diese konfigurieren, verwalten und kontrollieren zu können. Je nach Software variiert der Funktionsumfang von MDM-Anwendungen, da in manchen Fällen Kooperationen zwischen Software- und Geräte-Herstellern Zugriffe auf erweiterte Schnittstellen möglich machen, sodass mit der jeweiligen Software tiefergehende Konfigurationen an den Geräten umsetzbar sind.

Der Sicherheitsvorteil liegt auf der Hand: Werden Smartphones und Tablets zentral verwaltet, können Verantwortliche sicher sein, dass Unternehmensrichtlinien in puncto Gerätekonfiguration eingehalten und wichtige Sicherheitsupdates zeitnah installiert werden. Nutzen Mitarbeiter allerdings Privatgeräte für dienstliche Zwecke, ist die Bereitschaft der Mitarbeiter, ihre privaten Geräte in die MDM-Lösung integrieren zu lassen, Voraussetzung für die erfolgreiche Umsetzung einer zentralen Geräteverwaltung. Grundsätzlich sollten bei Verwendung einer MDM-Lösung nur registrierte und kontrollierte Geräte Zugang zum Unternehmensnetzwerk erhalten.

### Software-Beispiel: AirWatch

AirWatch[62] ist eine MDM-Software, die die plattformübergreifende zentrale Verwaltung von Smartphones und Tablets mit den Betriebssystemen iOS, Android, Windows, Blackberry und Symbian über eine Cloud oder eine lokale Anwendung ermöglicht. Der Funktionsumfang von AirWatch variiert dabei aufgrund der unterschiedlichen Geräte-Schnittstellen.

Dieser beinhaltet laut Hersteller unter anderem:

- Geräte-Fernkonfiguration: Beschränkung der Gerätefunktionen (z.B. Deaktivierung der Kamera-App, des cloudbasierten Sprachassistenten oder der GPS-Ortungsfunktion), Eingrenzung der Erweiterbarkeit (Installationsverbot von Apps der schwarzen Liste, Datei-Download-Verbot), Zwang zur Verwendung sicherer Passwörter
- Umsetzung eines Berechtigungssystems (Authentifikation bestimmter Benutzergruppen zur Nutzung bestimmter Dienste; Registrierungsbeschränkungen und Zugriffssperren bei Verwendung zu alter Software/Geräte)
- Durchführung automatischer Aktionen (z.B.: Software-Aktualisierung)
- Datei-Verschlüsselung
- Einrichtung eines firmeneigenen App Markets
- Umsetzung der Betriebsrichtlinien mithilfe der Konformitätsrichtlinien
- Einrichtung eines sicheren E-Mail-Kontos
- Sicherer Zugriff auf Unternehmensdaten und -verzeichnisse mithilfe des „Secure Content Lockers“ und des „Cloud Connectors“; sichere Dateiübertragung (AES- und SSL-verschlüsselt)
- Sicherer Zugang zu Firmenanwendungen und -apps mithilfe des „Mobile Access Gateways“)
- Identifikation gefährdeter Geräte (z.B. gejailbreakte/gerootete Geräte)
- Fernortungs- und Sperr- und Löschfunktion (Löschung sämtlicher Daten oder nur der Daten im Unternehmenscontainer)
- Sperrung unbekannter Geräten, die auf das Unternehmensnetzwerk zugreifen

Die zentrale Geräteverwaltung erfolgt über den Internetbrowser. Unerfahrene Nutzer werden mit einem Tutorial („Erste Schritte“) durch die AirWatch-Umgebung geleitet.

[62] *http://www.air-watch.com/de/*

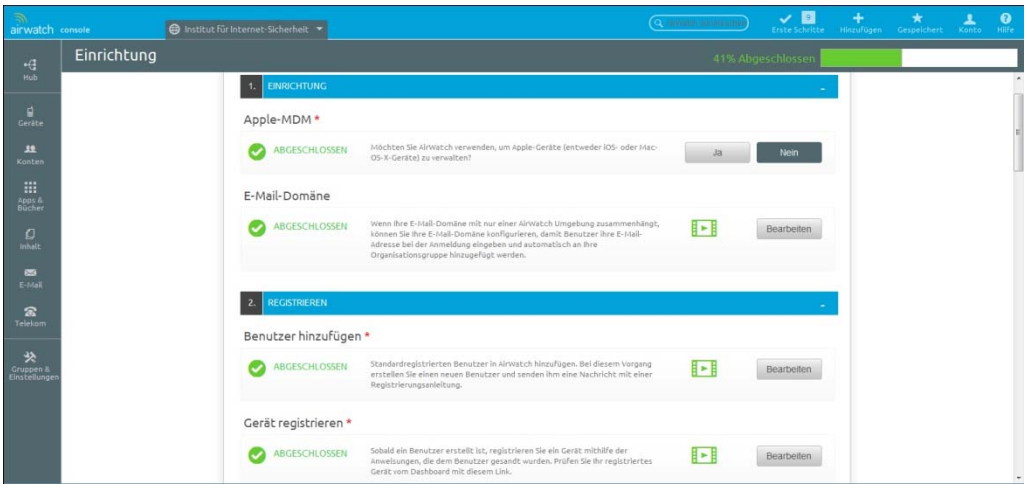



*Abbildung 18: Tutorial „Erste Schritte" in der AirWatch-Umgebung*

Daneben steht dem Nutzer ein Service-Portal („myAirWatch“), das Zugriff auf über 500 Anleitungen und Erfahrungsberichte („AirWatch Ressources“), Webinare und Zertifizierungsprogramme für Mitarbeiter („AirWatch Acadamy“), Nutzungsstatistiken („AirWatch Analytics“) und Support-Forum gewährt.
Zu beachten: Mit Ausnahme vom Service-Telefon und einigen Menütexten ist AirWatch englischsprachig.

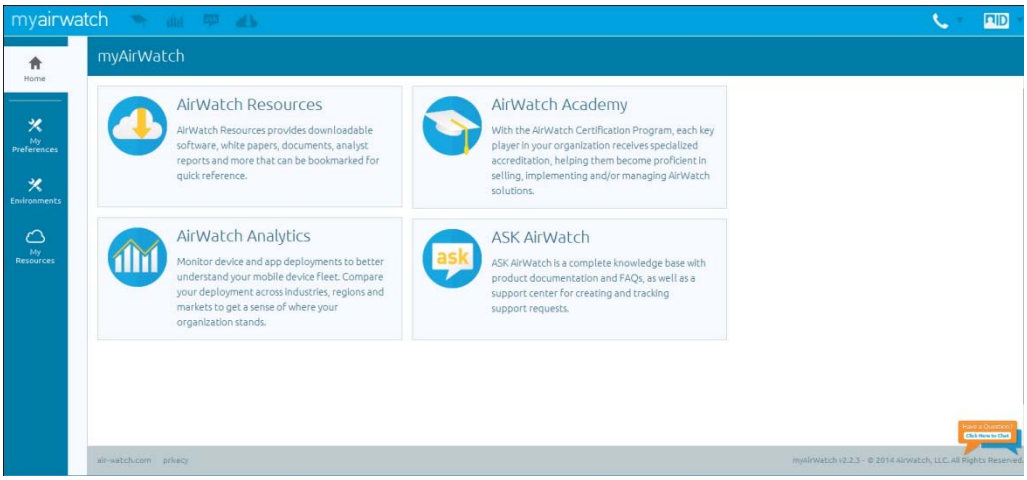



*Abbildung 19: Service-Portal „myAirWatch"*

Nachfolgend sollen grundlegende Funktionen vorgestellt werden, die im Funktionsumfang einer MDM-Lösung enthalten sein sollten. Zur Illustration werden einige Abbildungen der AirWatch-Software aufgeführt. Die im Text vorgestellten Themen und Funktionen beziehen sich allerdings nicht unbedingt auf diese Beispielsoftware.

### 5.4.1 Einbindung neuer Geräte

Die Einbindung neuer Geräte in das Unternehmensnetzwerk und somit in den MDM-Verbund erfolgt üblicherweise durch ein User-Self-Service-Portal, mit dem der Mitarbeiter selbstständig sein Gerät mithilfe seiner Zugangsdaten in das zentrale Verwaltungssystem integrieren kann. Diese Benutzeroberfläche bietet ihm je nach Konfiguration die Möglichkeit, sein Gerät zu orten, Gerätedetails einzusehen, das Gerät komplett zu verschlüsseln, zu sperren oder aus dem System zu löschen. Gegebenenfalls können die Mitarbeiter auch vertrauenswürdige Anwendungen über das Portal installieren (siehe Kapitel *5.5.5 Verwaltung der Anwendungen und Patch-Management*).

***Über das User-Self-Service-Portal erfolgt die Authentifikation des Mitarbeiters. Hier hat er gegebenenfalls die Möglichkeit, sein Gerät zu sperren oder zu löschen und Apps zu installieren.***

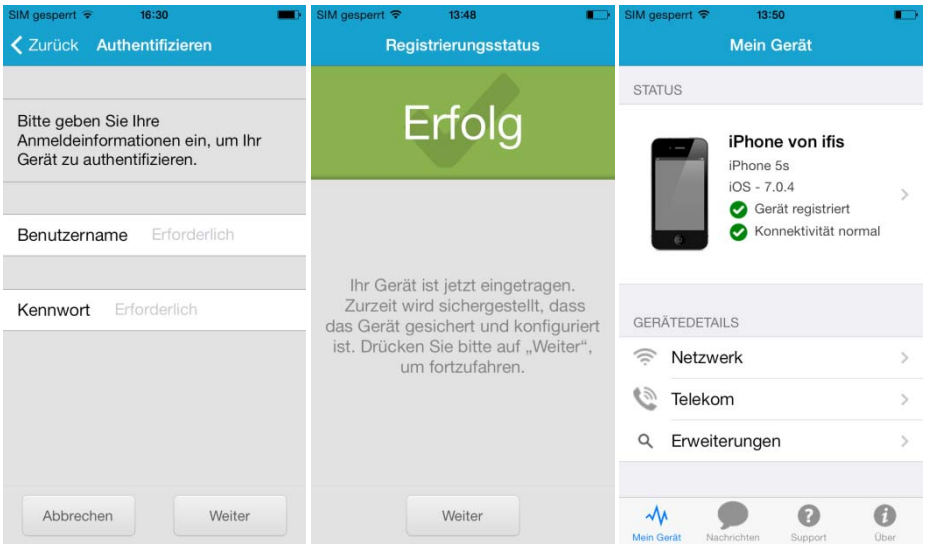



*Abbildung 20: Einbindung eines iOS-Gerätes in den AirWatch-MDM-Verbund*

### 5.4.2 Zugangsrechte für verschiedene Benutzergruppen

Ist allen Mitarbeitern eines Betriebs der uneingeschränkte Zugriff auf sämtliche im Unternehmensnetzwerk verfügbaren Ressourcen erlaubt, stellt dies ein sehr großes Sicherheitsrisiko dar. Oft ist ein weitreichender Zugriff insbesondere dann gegeben, wenn Mitarbeiter auf ihren Geräten firmenspezifische Anwendungen, die sogenannten Enterprise Apps nutzen, um mit dem Unternehmensnetzwerk in Informations- und Datenaustausch zu treten. Ein von Schadsoftware infiziertes Smartphone, das mit dem Unternehmensnetzwerk verbunden ist, könnte Kriminellen dann schon genügen, um sensible Informationen wie Kunden- und Geschäftsdaten abzugreifen. Im schlimmsten Fall können sie sämtliche Daten stehlen, auf die der Benutzer des Gerätes zugreifen kann.

***Der MDM-Verbund eignet sich für ein effizientes Rechte-Management. Zugriffsrechte und Gerätekonfigurationen werden für verschiedene Benutzerprofile zentral festgelegt und in Echtzeit umgesetzt.***

Es gilt, das große Risiko mithilfe eines Berechtigungskonzepts (Information Rights Management) einzugrenzen. Hier sollten Zugangsrechte für bestimmte Bereiche des Unternehmensnetzwerks an verschiedene Benutzergruppen verteilt werden. Ein Mitarbeiter sollte aufgrund seines individuellen Berichtigungsprofils mit seinem mobilen Gerät nur Zugriff auf diejenigen Ressourcen, sprich Daten und Software, haben, die er bei seiner Arbeit auch wirklich benötigt. Wird das Gerät durch Malware kompromittiert, kann der Schaden auf die Bereiche eingegrenzt werden, zu denen der Mitarbeiter Zugang hatte. Die entsprechenden digitalen Berechtigungszertifikate für Softwarenutzung werden den Mitarbeitern über das MDM-System zur Verfügung gestellt und sind

an die Authentifizierung (Zugangskontrolle) des eingangs erwähnten User-Self-Service-Portals gekoppelt.

### 5.4.3 Trennung zwischen Unternehmens- und Privatbereich auf den Geräten

Neben den Einschränkungen in Konfigurier- und Erweiterbarkeit der Geräte, die mit der Einbindung in das MDM-System einhergehen, sollte besonderes Augenmerk auf die Datenspeicherorte privater und beruflicher Daten (Verbindungsdaten, Dateien, Adressverzeichnisse, E-Mails, Kalenderdaten, Fotos etc.) gelegt werden. Eine Trennung ist schon allein deshalb wichtig, da beim Entfernen des Gerätes aus dem MDM-Verbund eine gründliche Datenlöschung aller gespeicherten Firmendaten durchgeführt werden sollte, die durch eine Vermischung beider Bereiche umständlicher ist. Zudem kann es im Falle des Geräteverlusts oder -diebstahls zu einem Interessenskonflikt zwischen Unternehmen und Mitarbeiter kommen, sobald eine Fernlöschung der Daten notwendig wird. In diesem Fall drohen private Daten verloren zu gehen. Die Rechte des Mitarbeiters überwiegen hier meist, sodass er eine Löschung verhindern kann.

***Eine MDM-Lösung kann hilfreich dabei sein, private von Unternehmensdaten auf den Gerätespeichern zu separieren.***

Daneben gibt es noch weitere sicherheitsrelevante Gründe, die die Bereiche Datenverfügbarkeit und -schutz tangieren. Die Vertraulichkeit privater E-Mails sollte durch die Nutzung zwei verschiedener Mail-Konten gewährleistet werden, steht doch das geschäftliche E-Mail-Konto in ständiger Verbindung mit dem Unternehmensnetzwerk. Auch in Hinblick auf automatische Backup-Routinen (siehe nachfolgendes Kapitel) muss sichergestellt sein, dass sich private und berufliche Daten in verschiedenen Ordnern befinden, damit nicht unbeabsichtigt private Daten auf dem Unternehmensserver landen. Als privat eingestufte Verbindungsdaten (GPS-Daten, Roaming-Status etc.) sollten nicht in der MDM-Umgebung protokolliert werden.

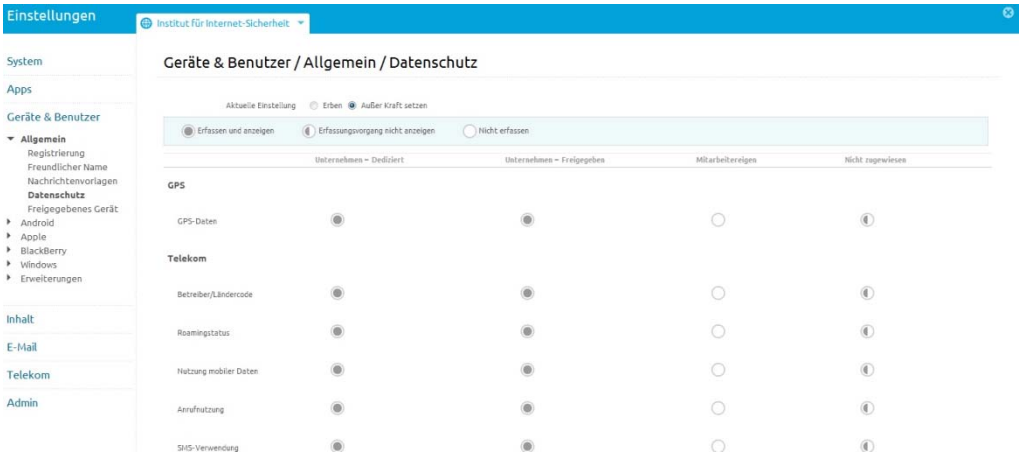



*Abbildung 21: Übersicht über die Erfassung und Anzeige von Daten, die als privat oder geschäftlich eingestuft werden in der AirWatch-Umgebung*

Es gibt verschiedene Techniken, Privates von Beruflichem auf den Geräten zu separieren.

## Containerisierung

Die Methode Containerisierung ist sehr populär in Zusammenhang mit MDM. Hier können Mitarbeiter auf den Geräten mithilfe spezieller Software einen verschlüsselten Container anlegen, in den alle dienstlichen Daten und Anwendungen abgelegt werden. Dieser ist von den übrigen (privaten) Daten auf dem Gerät abgeschirmt, eine Verbindung aus Container-Daten und privaten Daten, beispielsweise innerhalb eines gemeinsamen Terminkalenders, ist nicht möglich. Die Kommunikation zwischen Daten-Container und Unternehmensserver erfolgt verschlüsselt. Nachteil dieser Methode ist, dass die präzise Trennung zwischen Container und den übrigen Anwendungen auf dem Gerät betriebssystemabhängig ist. Infolge kann sie nur als bedingt sicher beziehungsweise eher oberflächlich eingestuft werden.

***Bei der Containerlösung werden Unternehmensdaten in einen isolierten verschlüsselten Container abgelegt. Dieser steht in Verbindung mit dem Unternehmensserver.***

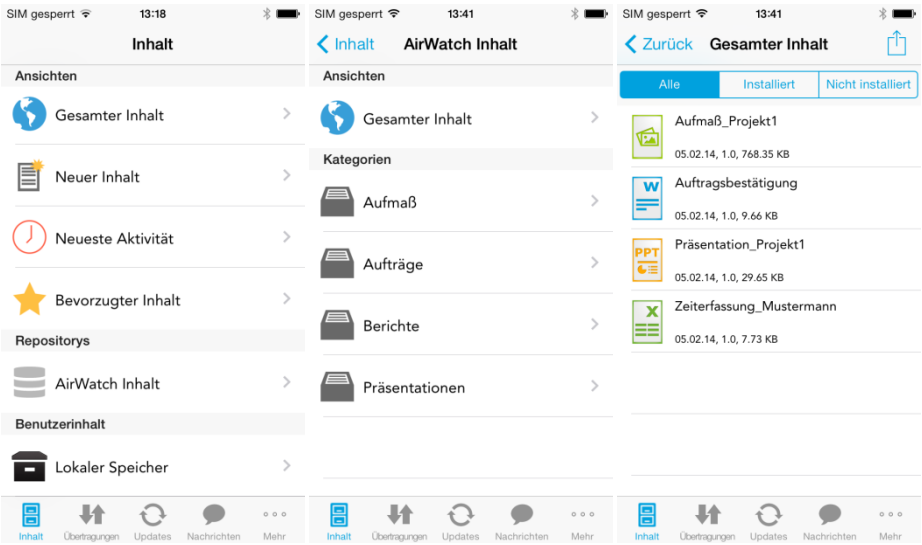



*Abbildung 22: Von links: Inhaltsübersicht im „Secure Content Locker“ von AirWatch, Kategorien der geteilten Unternehmensdaten, AES-geschützte Dateien im Container*

## Dual-Sim-Verfahren

Dual-Sim-Technologie ermöglicht bei Smartphones den Einsatz zweier SIM-Karten in einem Gerät. Auf diese Weise erhält der Benutzer zwei Rufnummern, eine für den geschäftlichen, eine für den beruflichen Bereich. So lassen sich bestimmte Dienste, die sich auf die Rufnummer beziehen, voneinander separieren. Allerdings bietet dieses Verfahren keine Sicherheit für die gespeicherten Unternehmensdaten beziehungsweise es verhindert nicht die Vermischung von Beruflichem und Privatem.

## Sicherheitskern und Virtualisierung

Ein neuer Trend, um eine höhere Sicherheit bei mobilen Geräten zu gewährleisten, ist die Nutzung von sogenannten Sicherheitskernen mit Virtualisierungs- und Isolierungslösungen, bei denen auf einem mobilen Gerät zwei Instanzen des Betriebssystems parallel, aber durch starke Isolation getrennt ausgeführt werden; sozusagen zwei „Smartphones“ auf einem mobilen Gerät. Der Vorteil ist, dass eine Instanz für den privaten Gebrauch verwendet werden kann, in welche auch unsichere Apps wie Spiele installiert werden können. Die andere Instanz ist die „Business-Instanz“, in der sicherheitsrelevante Apps und Daten, wie z.B. geschäftliche E-Mails und Firmenanwendungen residieren. Diese Trennung schützt vor Angriffen auf Firmendaten und –infrastrukturen aus einer unsicheren App heraus. Die Kommunikation in das Firmen-

netz ist nur aus der sicheren Business-Instanz heraus und über ein VPN möglich. Zusätzlich sind in diesen Isolations-Lösungen auch die Mobile Device Management-Funktionen integriert. Solche Lösungen werden z.B. von T-Systems unter dem Namen „SiMKo 3[63]“ oder von der Sirrix AG unter „BizztrusT[64]“ angeboten und bieten eine sehr gute Sicherheit.

### Terminal Service

***Ein Terminal Service bietet eine effiziente Trennung der Daten, benötigt aber eine stabile Internetverbindung.***

Eine weitere sichere aber wenig praktikable Möglichkeit ist, einen sogenannten Terminal Service zu nutzen. Hierbei handelt es sich um eine dem Cloud-Computing ähnliche Anwendung, die Mitarbeiter auf ihren mobilen Geräten installieren, um mithilfe einer verschlüsselten Verbindung zum Unternehmensserver dort befindliche Firmenanwendungen nutzen zu können. Es handelt sich also um eine Art Fenster, eine Benutzeroberfläche. Die eigentliche Firmensoftware ist nicht auf den Endgeräten installiert, sondern liegt auf dem Unternehmensserver. Es werden keine Unternehmensdaten auf den Geräten abgespeichert und eine Datensicherung entfällt somit. Voraussetzung hierfür ist eine ausreichend leistungsfähige und stabile Internetverbindung sowie ein ausreichend großes Display der mobilen Geräte. Kommt es zu einem Verbindungsabbruch, kann die Firmensoftware nicht genutzt werden.

Neueste Entwicklungen auf dem Smartphone-Markt deuten darauf hin, dass in Zukunft vermehrt Geräte mit höheren Sicherheitsanforderungen für die Business-Nutzung veröffentlicht werden könnten, als dies bisher der Fall ist. Seit Anfang 2013 sind beispielsweise Geräte des Herstellers Blackberry auf dem Markt, die eine strenge Isolation beider Bereiche ermöglichen. Es bleibt abzuwarten, wie bald die übrigen Smartphone-Hersteller nachziehen.

## 5.4.4 Fern-Konfiguration und –Wartung

***Fern-Konfiguration ist ein Kernelement einer MDM-Lösung. Je nach Software können unterschiedliche Konfigurationen und Einschränkungen getroffen werden.***

Zu kontrollieren, ob sich die Mitarbeiter an die in den unternehmensinternen Richtlinien vereinbarten Gerätekonfigurationen auch wirklich halten, kann mit einer zentralen Geräteverwaltung erleichtert werden. Sicherheitsrelevante Gerätekonfigurationen können bequem von einem Arbeitsplatz aus per Fernsteuerung bei allen Geräten einheitlich umgesetzt werden. So ist es beispielsweise möglich, Kriterien für sichere Passwörter fest vorzugeben oder für die Datenablage auf den Geräten einen verpflichtenden Verschlüsselungsmechanismus festzulegen. Sichere Kommunikation mit dem Unternehmensserver kann durch einen Nutzungszwang einer VPN-Verbindung bei Übertragung sensibler Daten gewährleistet werden. Um die Datensicherheit weiter zu erhöhen, lassen sich automatische Datensicherungsroutinen festlegen, bei denen die lokal gespeicherten Daten auf den mobilen Endgeräten regelmäßig auf dem Unternehmensserver abgelegt werden. Im Fall von Geräteverlust und -diebstahl kann die Geolokalisierung (Ortung) hilfreich sein. Bevor es zu einem Geräteverlust kommt, sollte bereits festgelegt sein, welche Schritte hier einzuleiten sind (siehe Kapitel *3.2.7 Diebstahlschutz* und *5.3 Was im Fall des Geräteverlusts zu tun ist*). Unter Umständen sollten Verantwortliche dann von der Fernsperrung und der Fernlöschung der auf dem Gerät gespeicherten Daten Gebrauch machen, sofern es sich um hochsensible Daten handelt. Neben diesen Basisfunktionen gibt es – je nach Software – weitere Konfigu-

[63] *http://security.t-systems.de/loesungen/mobile-simko*
[64] *https://www.sirrix.de/content/pages/63769.htm*

rationsmöglichkeiten, die beispielsweise die Überwachung und Steuerung der drahtlosen Kommunikation via WLAN, Bluetooth und NFC betreffen.

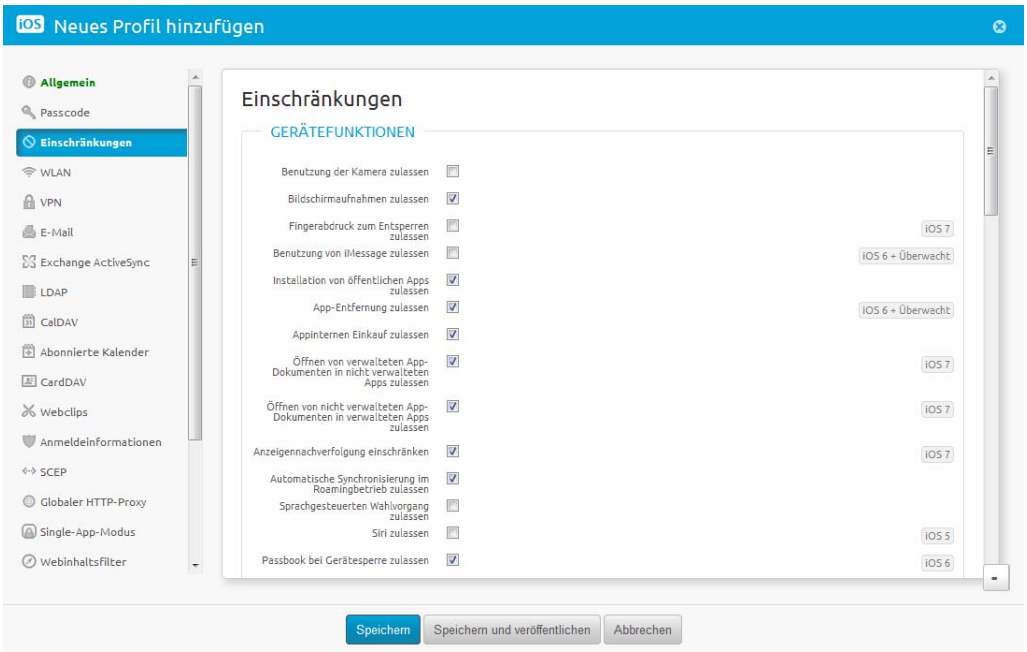



*Abbildung 23: Einschränkung der Geräte-Funktionen bestimmter Benutzergruppen in der AirWatch-Umgebung*

Außerdem können bei Geräten im MDM-Verbund bestimmte Funktionen wie die der Fotokamera bei Smartphones und Tablets deaktiviert werden, um die Sicherheit weiter zu erhöhen. Verantwortliche in den Betrieben sind also mithilfe von Mobile Device Management in der Lage, der Handhabung der Geräte in puncto Konfigurier- und Erweiterbarkeit (siehe nachfolgendes Kapitel) klar definierte Grenzen zu setzen.


*Abbildung 24: Von links: iOS-Startdisplay ohne Einschränkungen, Übersicht über aktive Einschränkungen, iOS-Startbildschirm mit Einschränkungen (keine Kamera, kein „iTunes Store“, kein „FaceTime“, kein „Safari“)*

### 5.4.5 Verwaltung der Anwendungen und Patch Management

Die über das MDM-System zur Verfügung gestellten Berechtigungszertifikate für die Nutzung von Firmensoftware unterscheiden sich auf zweierlei Weise. Zum einen gibt es Unternehmenszertifikate, die den Nutzern eine allumfassende Nutzung aller Funktionen der betreffenden Software einräumen. Das bedeutet, dass auf sämtliche Daten, die mit der Software eingesehen und bearbeitet werden können, mit dem Gerät des Anwenders zugegriffen werden kann. Daneben gibt es unterschiedliche Benutzerzertifikate, die die Nutzung einer Software auf bestimmte Bereiche einschränkt. Letztere sollten an diejenigen Mitarbeiter verteilt werden, die nicht den gesamten Funktionsumfang einer Software bei der täglichen Arbeit benötigen. Neben bestimmten Zertifikaten zur Softwarenutzung können über das MDM-System auch Zertifikate für E-Mail-verschlüsselung und VPN-Verbindungen ausgegeben werden.

Einige MDM-Produkte bieten die Möglichkeit, vertrauensvolle Software (Firmenanwendungen und Apps) über das User-Self-Service-Portal den Mitarbeitern zur Verfügung zu stellen oder die Anwendungen direkt auf den Endgeräten zu installieren, ohne Zutun der Mitarbeiter. Mit einem solchen firmeneigenen App Market geben die Verantwortlichen einen Spielraum für die Erweiterbarkeit der auf den Geräten installierten Software vor und erhöhen dadurch maßgeblich die Softwaresicherheit.

***Das Problem der fehlenden Software-Aktualität ist in einem MDM-Verbund praktisch gelöst.***

Mittels MDM kann die Aktualität der Software und der Betriebssysteme aller mobilen Endgeräte sichergestellt werden. Dieses sogenannte Patch-Management lässt entweder dadurch realisieren, dass relevante Updates direkt nach Erscheinen via MDM-Verbund auf den Geräten automatisch installiert werden. Die andere Variante ist, das Patch-Management den Mitarbeitern zu überlassen und über ein Nachrichtensystem lediglich auf die Veröffentlichung sicherheitsrelevanter Updates hinzuweisen. Bedingung hierfür sollte allerdings sein, dass sich der Arbeitgeber die Möglichkeit qua Unternehmensrichtlinie (siehe Kapitel 5.2 *Auflagen und Richtlinien für Mitarbeiter*) vorbehält, bestimmte Geräte aus dem Unternehmensnetzwerk auszuschließen, sollten diese aufgrund veralteter Software die IT-Sicherheit des Betriebs gefährden.

### 5.4.6 Nutzerüberwachung

Innerhalb des MDM-Systems erfolgt eine Kontrolle aller verbundenen mobilen Geräte in Echtzeit. Mithilfe der sogenannten Data Loss Prevention (DLP), die jedoch einen hohen technischen Aufwand erfordert, werden fortlaufend Protokolle aller Datenabrufe des Unternehmensnetzwerks durch die mobilen Endgeräte erstellt und diese auf Auffälligkeiten untersucht. Kommt es zu ungewöhnlichen Datenabrufen wird der Administrator informiert – er kann infolge über den Ausschluss des jeweiligen Geräts entscheiden.

### 5.4.7 Schutz vor Softwaremanipulation, Rooting/Jailbreak

Zum Sicherheitskonzept einer MDM-Anwendung gehört neben der Nutzerüberwachung und der Überwachung der Gerätekonfigurationen auch eine fortlaufende Prüfung der Geräte hinsichtlich möglicher Softwaremanipulation, die durch Schadsoftware verursacht wurde, und hinsichtlich Modifikationen am jeweiligen Betriebssystem der

Geräte, die eine Umgehung bestimmter Nutzungsrechte verursacht (z.B. Rooting bei Andriod oder Jailbreaking bei iOS). Software-Missbrauch oder eine mehrmalige falsche Eingabe des Kennworts führen innerhalb des MDM-Systems zur Isolation oder sogar zur Fernlöschung des betreffenden Gerätespeichers, der Zugriff auf das Unternehmensnetzwerk wird verweigert. Einige MDM-Anwendungen unterscheiden zwischen Privatgeräten und firmeneigenen Geräten, sodass die Meldung von Auffälligkeiten in Software und Nutzung (siehe vorheriges Kapitel) unterschiedlich empfindlich sein kann. Auch die sich daraus ergebenden Konsequenzen können dementsprechend unterschiedlich drastisch ausfallen.

### 5.4.8 Entfernung der Geräte aus dem MDM-System

Mit der Entfernung eines mobilen Endgeräts aus dem MDM-Verbund geht die Löschung der lokal gespeicherten Firmendaten einher, damit unter anderem Datenschutzbestimmungen eingehalten werden können. Im Vorfeld sollte sämtliche installierte Firmensoftware auf dem Gerät deinstalliert werden, auch deshalb, um Lizenzbedingungen einhalten zu können. Beim Löschen der Daten wird bei Geräten im Privatbesitz zwischen partieller und vollständiger Löschung aller auf dem Gerät gespeicherten Daten unterschieden. Bei ersterer werden nur die Firmendaten gelöscht und die privaten Daten beibehalten. Eine vollständige Löschung aller Daten auf dem Gerät ist die sicherere Alternative. Zu beachten ist hierbei, dass das Zurückstellen des Gerätes auf den Werkzustand bei Android-Geräten keine rückstandslose Löschung bedeutet. Um auf Nummer sicher zu gehen, sollte spezielle Software genutzt oder ein seriöses Dienstleistungsunternehmen beauftragt werden.

***Manche MDM-Produkte bieten die Möglichkeit einer partiellen Löschung, bei der nur die Unternehmensdaten (beispielsweise im Container) gelöscht werden können.***

## 5.5 Zusammenfassung

**Schutzmaßnahmen auf der Verwaltungsebene – Organisation**

Durch klare Auflagen und Richtlinien legen Arbeitgeber den Grundstein für die betriebliche IT-Sicherheit. Ergebnis von Analysen und Beratungen sollte ein Katalog von Anforderungen sein, der Arbeitgebern und Arbeitnehmern als Orientierungshilfe dient. Welche Maßnahmen konkret für welches Unternehmen zu treffen sind, kann nicht generalisiert beantwortet werden. Lediglich die Themen, die verhandelt werden müssen, sind klar.

Mit dem Mobile Device Management kann Unternehmen eine starke Software-Lösung an die Hand gegeben werden, die die betriebliche Sicherheit erhöht sowie die Organisation der zumeist heterogenen IT-Landschaft deutlich vereinfachen kann. Typische Funktionen einer MDM-Software sind Fern-Konfiguration und -Wartung mobiler Endgeräte, Rechtemanagement, Patch-Management, Schutz vor Softwaremanipulation sowie Nutzer- und Anwendungskontrolle.

**Notizen**

# 6. Praxisbeispiel

Nachfolgend sollen vorangegangene Risiken und Schutzempfehlungen an zwei Beispielen illustriert werden, die sich jeweils auf dieselbe Ausgangssituation der fiktiven Firma Melzing Landschaftsbau beziehen.

Die Firma Melzing Landschaftsbau hat 40 Mitarbeiter, zehn arbeiten im Büro und koordinieren die Kolonne der dreißig Baustellenarbeiter. Die Angestellten im Büro verwalten die Aufträge und kümmern sich um die Kundenkommunikation mit den Architekten, die per Telefon, Post und E-Mail erfolgt. Ihnen stehen arbeitgeberseitig Desktop-PCs sowie Tablet-PCs zur Verfügung – letztere nutzen sie für Präsentationen bei Außer-Haus-Terminen in den Architektenbüros oder auf Baustellen.

## 6.1 Negativbeispiel

Hin und wieder nutzen die Büromitarbeiter das Telefon und das berufliche E-Mail-Konto, beispielsweise um mit Familienangehörigen über anstehende Termien und Urlaubsplanungzu sprechen. Die Tablets liegen oft ungenutzt auf dem Schreibtisch. Zwei Mitarbeiter sind deshalb auf die Idee gekommen, sie mit nach Hause zu nehmen, damit wenigstens die Kinder Freude an ihnen finden. Neben der Präsentations- und Raumplanungs-App finden sich jetzt auch einige Spiele, ein Fotobearbeitungsprogramm und ein Instant-Messenger auf dem Gerätespeicher – die Dialoge mit den Zugriffsrechten wurde bei der Installation schnell weitergeklickt. Zum Test der eingebauten Kamera haben die Kinder Fotos von sich aufgenommen, die jetzt im Fotoordner neben den Baustellenaufnahmen und fotografierten Aufmaß-Zeichnungen zu finden sind. Hin und wieder werden die gespeicherten Fotos und Dateien vom Tablet auf die lokale Festplatte eines Bürorechners übertragen. Die meisten Unternehmensdaten liegen allerdings im Netzwerk-Ordner, auf den alle voll zugreifen können, die mit dem WLAN des Unternehmens (Melzing_Fritzbox“) verbunden sind. Praktischerweise sind das Netzwerkpasswort und die Zugangspasswörter zu genutzten Diensten (Firmensoftware und amerikanischer Cloud-Dienstleister) kurz, sodass man es sich nach ein paar Monaten gut merken kann. Da auf diese Daten ohnehin zentral zugegriffen werden kann, brauchen Sicherungskopien auch nicht so oft angelegt werden. Eine Regelung gibt es hier ohnehin nicht.

Die Mitarbeiter der Kolonne sind vom Arbeitgeber bislang nur mit herkömmlichen Handys ohne Kamera ausgestattet, um mit den Büromitarbeitern in Verbindung zu bleiben. Bei kleineren Baustellen übernehmen sie die Aufmaß-Papierzeichnungen. Wenn es schnell gehen soll, fotografieren sie diese mit ihren eigenen Smartphones, um sie kostenlos per Instant-Messenger an die Mitarbeiter im Büro zu senden. Selten übersenden sie so auch die abfotografierten Berichte bei Fertigstellung eines Projekts, um sich den Umweg über Firma zu sparen, wenn es schnell weiter zur nächsten Baustelle gehen soll. Die Berichte, die üblicherweise abends im Büro abgegeben werden, enthalten die Namen der Arbeiter, die Zeiterfassung sowie verwendete Ressourcen wie genutzte Geräte und Materialien. Wenn die Internetverbindung unterwegs schlecht ist, senden sie die Berichte auch mal in der Mittagspause vom nahegelegenen Imbiss aus – heutzutage besitzen die meisten Restaurants und Cafés glücklicherweise eigene WLAN-Hotspots, die frei und von jedermann genutzt werden können.

Der Chef hat sich bislang noch nicht darüber beklagt, dass viele Mitarbeiter ihre privaten Geräte zum Übersenden der Unterlagen verwenden, ihm kann der Geschwindigkeitsvorteil nur Recht sein. Wie viele Mitarbeiter das so handhaben, weiß er nicht so genau. Über Regeln zur Nutzung der Privatgeräte hat er noch nicht nachgedacht, hier fehlte einfach bislang die Zeit. Natürlich hält er aber seine Mitarbeiter dazu an, beim Weiterverkauf alter Geräte vorher die gespeicherten Unternehmensdaten über das Kontextmenü zu löschen.

Sicherheitsapps sind auf den Privatgeräten selten installiert, da sie die Performance der Geräte schmälern und ohnehin unpraktisch sind. Automatische App-Updates sind deaktiviert, da sie nur unnötig das Traffic-Volumen belasten würden. Auch die Betriebssystemversion ist schon in die Tage gekommen, eine neuere Version kann nur auf neueren Geräten installiert werden. Eine Vollverschlüsselung des Gerätespeichers oder die Verschlüsselung einzelner Dateien scheint unnötig: Was sollte ein Dieb schon mit ein paar Telefonnummern anfangen können? Außerdem kämen dann noch mehr Passwörter hinzu, die man sich merken müsste. In der Mittagspause surfen einige Büromitarbeiter mit ihrem privaten Smartphone im Firmen-WLAN, um von der schnellen und kostenlosen Internetverbindung zu profitieren. Die Geräte verbinden sich hier praktischerweise automatisch. Einige jüngere Mitarbeiter nutzen gejailbreakte bzw. gerootete Smartphones, um auch Apps aus inoffiziellen Markets herunterladen zu können.
Wenn nach 18 Uhr noch eine Kunden-E-Mail eintrifft, wird diese auch schon mal auf dem Nachhauseweg im Bus von den privaten Smartphones der Büromitarbeiter beantwortet; auch dann, wenn es voll ist im Bus und die Mitreisenden auf das Display schauen können – wen sollte das schon interessieren? Neulich wurde ein Mitarbeiter in der Bahn gefragt, ob er sein Smartphone kurz für ein Telefonat entbehren könne – da hilft man natürlich gerne weiter.

**Fazit: Die Datensicherheit ist in diesem Beispiel auf einem gefährlich niedrigen Niveau.**

## 6.2 Positivbeispiel

Melzing Landschaftsbau ist eine moderne Firma, in der die Digitalisierung als Chance wahrgenommen wird, Arbeitsabläufe und Kommunikationswege zu optimieren. Ziel ist, auf lange Sicht jedem Mitarbeiter ein mobiles Endgerät zur Verfügung zu stellen, das er für betriebliche Anwendungen nutzen kann. Bis dahin wird ein BYOD-Konzept als Übergangslösung eingesetzt, das Sicherheitsrisiken auf ein Minimum reduzieren soll. Erste Investition war eine geeignete Mobile-Device-Management-Lösung, mit der sich alle mobilen IT-Geräte der Firma Melzing zentral verwalten lassen. Die anfänglichen Bedenken der Angestellten konnten nach einer Mitarbeitersensibilisierung ausgeräumt werden, bei der die Gefahrenpotenziale von mobilem Arbeiten offengelegt wurden.

Aufmaß und Zeiterfassung können die Mitarbeiter der Kolonne mithilfe einer Enterprise App erledigen, die in einer sicheren isolierten Umgebung innerhalb der MDM-Lösung ausgeführt wird. Die erfassten Daten werden sofort an den Unternehmensserver gesandt, ohne dass sie lokal auf den Geräten gespeichert würden. Die Mitarbeiter sind einverstanden damit, dass ihre Geräte mithilfe der Enterprise App geortet werden, sodass die Büromitarbeiter die Flotten bequem kontrollieren können. Ein Administrator kann per Fernzugriff mithilfe der MDM-Lösung die betrieblichen Sicherheits-

richtlinien umsetzen, auf die sich Mitarbeiter und Geschäftsführung im Vorfeld geeinigt hatten. Mit dem Einsatz einer MDM-Lösung ist die Einführung eines Berechtigungssystems einhergegangen, das den Zugriff auf das Unternehmensnetzwerk beziehungsweise den Datenzugriff beschränkt. Entsprechend seines Berechtigungsprofils hat ein angemeldeter Mitarbeiter nur Zugang zu den Daten und Diensten, die er für seine Arbeit benötigt.

Der MDM-Administrator sorgt dafür, dass verwendete Software wie die Enterprise-App, die genutzte Mobile Security Suite und das Betriebssystem stets auf dem neuesten Stand sind und kann bei Geräteverlust gezielt Unternehmensdaten wie Adressdaten und E-Mails löschen, da sich diese in einem separierten verschlüsselten Container auf den Geräten befinden. Als zusätzlichen Diebstahlschutz haben die Mitarbeiter die Gerätespeicher vollverschlüsselt. Apps installieren sie über den betriebseigenen App Market, der ebenfalls über die MDM-Plattform realisiert wurde. Die App securityNews liefert ihnen zusätzliche Sicherheitshinweise speziell für ihre Betriebssysteme. Alle genutzten Dienste sind mit sicheren Passwörtern geschützt, die mit einem Passwort-Manager vom jeweiligen Mitarbeiter verwaltet werden. Sicherheitsbackups der Gerätespeicher erfolgen in einem eingestellten Intervall automatisch über das MDM-System. Allen im Unternehmen ist klar, dass private Daten von Unternehmensdaten separiert werden müssen und auch, dass Telefone und berufliche E-Mailkonten nicht für Privates genutzt werden dürfen. Bei Verwendung öffentlicher WLAN-Netze verschlüsseln sie ihre Kommunikation via VPN standardmäßig, und achten auf „HTTPS“ beim Surfen. Sie geben ihr Smartphone nicht aus der Hand und schützen es vor dem Zugriff Dritter – auch vor Familienangehörigen, Freunden und Bekannten.

**Fazit: Die Datensicherheit ist in diesem Beispiel auf einem vorbildlichen Niveau.**

# 7. Umgang mit BYOD im Betrieb

***Ein Argument für BYOD ist, dass Arbeitgeber hier mehr Transparenz darüber haben, welche Privatgeräte der Mitarbeiter tatsächlich dienstlich genutzt werden.***

Wie in Kapitel *2.10 Rechtliche Risiken* beschrieben, raten einige Juristen vom Konzept BYOD grundsätzlich ab. Es kommt jedoch vor, dass Mitarbeiter trotz eines Arbeitgeberverbotes ihre Privatgeräte für betriebliche Zwecke nutzen[65] – mit dem Ergebnis, dass Arbeitgeber das Sicherheitsniveau sensibler Daten falsch einschätzen und unbewusst einen großen Kontrollverlust erleiden. Ein Argument, BYOD im Unternehmen doch zu gestatten, ist, dass Gefahrenpotenziale sichtbarer werden.

Entscheiden sich Unternehmer nach Abwägung der Vor- und Nachteile (siehe nachfolgendes Kapitel) tatsächlich für die Einführung eines BYOD-Konzeptes, sollte ein genauer Analyseprozess vorausgehen. Zu klärende Fragen: Welche Software-Produkte kommen im Betrieb zum Einsatz und welche Lizenzen liegen für diese vor? Welche Mitarbeiter sollen von welchen Standorten aus auf welche Daten und Dienste außerhalb der Büroräume zugreifen können?
Damit einhergehen zahlreiche Entscheidungen, beispielsweise für oder gegen die zentrale Geräteverwaltung oder für oder gegen die Nutzung virtualisierter Software.

Nicht verhandelbare Voraussetzungen von BYOD sollten jedoch sein:

- die Möglichkeit zur technischen Trennung von privaten und Unternehmensdaten auf den gewünschten Geräten
- die Kompatibilität der Geräte mit aktuellen Verschlüsselungstechniken
- die Unversehrtheit der Geräte in Hinblick auf mögliche Software-Manipulationen (siehe Kapitel *2.7 Risiko Jailbreaking und Rooting*)
- die Bereitschaft des Mitarbeiters, die zu vereinbarenden Auflagen einzuhalten und eventuelle Nutzungseinschränkungen zu akzeptieren

Ergebnis der Planungsphase, die in großen Teilen gemeinsam von Arbeitgeber und Arbeitnehmer durchgeführt werden sollte, ist ein Auflagenkatalog, der für die Mitarbeiter Bedingung für die betriebliche Nutzung ihrer Privatgeräte ist (siehe Kapitel *5.2 Auflagen und Richtlinien für die Mitarbeiter*).

## 7.1 Vor- und Nachteile von BYOD aus Arbeitgeber- und Mitarbeitersicht

Die generellen Vorteile von mobilem Arbeiten liegen auf der Hand: Das ortsunabhängige Arbeiten bringt mehr Flexibilität für Arbeitgeber und Arbeitnehmer, Kundenanfragen können schneller beantwortet werden, Mitarbeiter haben bei Vor-Ort-Terminen Zugang zu aktuellen Datenbeständen, Aufgaben können gemeinsam über größere Entfernungen hinweg bearbeitet werden.
Arbeitgeber stellen sich heute meist nicht mehr die Frage, ob mobile Geräte zum Einsatz kommen sollen, sondern ob sich die Geräte in Unternehmens- oder Mitarbeiterbesitz befinden dürfen. Hier sei nochmal ausdrücklich darauf hingewiesen, dass einige Juristen aufgrund der hohen rechtlichen Risiken vom Einsatz privater Geräte abraten. Der nachfolgende Pro-Contra-Vergleich dient daher nur der Übersicht.

[65] *Dieses Verhalten ist arbeitsrechtlich verboten.*

| BYOD aus Arbeitgebersicht | |
|---|---|
| Vorteile | Nachteile |
| Kosteneinsparungen (es müssen keine Geräte angeschafft werden) | Ggf. Kosten durch Beteiligung am Kauf neuer Privatgeräte der Arbeitnehmer und aufgrund zusätzlicher Sicherheitsmaßnahmen |
| Hohe Akzeptanz für BYOD beim Arbeitnehmer | Verlust an (Datenschutz-)Kontrollmöglichkeiten bei vollem Haftungsrisiko; Risiko der Vermischung von privaten und Unternehmensdaten |
| Höhere Effizienz der Mitarbeitern, da die Bedienung der Geräte bekannt ist | Potenziell mehr Gefahren für die betriebliche IT-Sicherheit aufgrund zusätzlicher Angriffsvektoren (z.B. Schädlinge auf den Geräten) |
| Bessere Identifikation der Mitarbeiter mit ihrem Arbeitsgerät und dem Unternehmen (Verzahnung von Beruf und Privatleben in einem Gerät) | Gerätevielfalt (heterogene IT-Landschaft) erschwert Organisation; ggf. kommt es auch zu Hard- und Software-Inkompatibilitäten |
| Mitarbeiter sind achtsamer im physischen Umgang mit den Privatgeräten, sodass weniger Reparaturen notwendig werden | Aufwändigere Planungsphase, da mehr Mitarbeitervereinbarungen notwendig werden als bei Nutzung unternehmenseigener Geräte |
| Höhere Transparenz darüber, wie viele Geräte tatsächlich für dienstliche Zwecke genutzt werden | Großer Vertrauensvorschub notwendig |

*Tabelle 6: Vor- und Nachteile BYOD aus Arbeitgebersicht*

| BYOD aus Mitarbeitersicht | |
|---|---|
| Vorteile | Nachteile |
| Größere Praktikabilität, da weniger Geräte genutzt werden | Konflikte bei Trennung von privaten und Unternehmensdaten (z.B. bei Inanspruchnahme der Fernlösch-Funktion) |
| Größere Freiheiten in der Geräteauswahl und Benutzung als bei unternehmenseigenen Geräten | Große Sorgfaltspflicht; Einschränkungen aufgrund der getroffenen Vereinbarungen und Auflagen |
| Evtl. Kostenbeteiligung des Arbeitgebers | Ggf. Gefühl der Überwachung aufgrund der möglichen Kontrollen durch den Arbeitgeber |
| | Technische Organisation schwieriger als bei unternehmenseigenen Geräten |

*Tabelle 7: Vor- und Nachteile BYOD aus Mitarbeitersicht*

## BYOD – ein populäres Konzept

Der BYOD-Trend ist nicht zu übersehen. Nach Schätzungen des Instituts für Internet-Sicherheit befinden sich heute 80 Prozent der betrieblich genutzten Smartphones im Privatbesitz der Mitarbeiter. Arbeitgeber sollten sich – falls noch nicht geschehen – frühzeitig mit diesem Thema auseinandersetzen, um zukünftigen Schäden und Konfliktfällen vorzubeugen.

***Ob es Arbeitgeber wollen oder nicht: BYOD ist im Trend.***

Eine Alternative zu BYOD ist das Konzept CYOD (Chose Your Own Device). Hierbei verbleibt das Gerät in Unternehmensbesitz, der Arbeitgeber hat die volle Kontrolle über den Datenschutz – dem Mitarbeiter wird jedoch die Freiheit gegeben, ein von ihm gewünschtes Gerät auszuwählen.

## 7.2 Zentrale oder dezentrale Verwaltung der Geräte?

Die zentrale Verwaltung der mobilen Endgeräte mittels Mobile Device Management bietet große organisatorische Vorteile sowie erweiterte Kontrollmöglichkeiten für Arbeitgeber, um die Datenschutzanforderungen entsprechend §9 BDSG zu erfüllen: Geräte im MDM-Verbund können automatisiert aktualisiert werden, Zugriffsrechte für benötigte Dienste können für verschiedene Benutzergruppen individuell zugewiesen werden, Softwaremanipulationen werden erkannt und Geräteeinstellungen können von der Ferne aus, in Hinblick auf Sicherheit, optimiert werden. Als Konsequenz kann eine höhere IT-Sicherheit konstatiert werden.

Aufgrund der hohen Kontrollmöglichkeit des Arbeitgebers kann sich beim Mitarbeiter ein Gefühl der Überwachung einstellen. Arbeitnehmer können sich in puncto Einstell- und Erweiterbarkeit bisweilen derart eingeschränkt sehen, dass ihre Akzeptanz zur Einbindung des Privatgeräts in den MDM-Verbund stark sinkt. Damit Arbeitgeber die oben beschriebenen Vorteile von BYOD (z.B. Steigerung der Effizienz) in Verbindung mit einer MDM-Lösung tatsächlich nutzen können, müssen dann Kompromisse gefunden werden, die beide Seiten zufrieden stellen können.

***Oft kommen MDM-Produkte bei größeren Unternehmen zum Einsatz.***

Es ist zu beobachten, dass Mobile Device Management gerade bei Unternehmen mit mehr als 30 Mitarbeitern bevorzugt zum Einsatz kommt, um die große Heterogenität der IT-Landschaft in den Griff zu bekommen.

## 7.3 Virtualisierung oder nativer Gerätebetrieb?

Anwendungen und Dienste im nicht-virtuellen (nativen) Betrieb verarbeiten und speichern genutzte Daten auf dem lokalen Speicher des verwendeten Geräts. Oft stehen sie in direktem Austausch mit Datenbanken des Unternehmensservers. Im Unterschied dazu werden Software-Produkte und Dienste im virtualisierten Modus von einem zentralen Ort aus verwaltet. Daten werden hierbei lediglich über eine Benutzeroberfläche (Virtual Desktop Infrastructure-Client) verarbeitet und liegen dabei auf dem Unternehmensserver beziehungsweise dem Server des Cloud-Dienstleisters. Es werden also keine Daten lokal auf den Mobilgeräten gespeichert.

***Der virtuelle Modus bietet viele Sicherheitsvorteile, benötigt jedoch eine permanent stabile Internetverbindung.***

Während der native Betrieb eine deutlich höhere Arbeitsgeschwindigkeit der Anwendungen ermöglicht, besticht der virtualisierte Betrieb durch weitaus höhere Datensicherheit (beispielsweise im Fall des Geräteverlusts). Nachteil des letzteren ist jedoch, dass zur Nutzung virtualisierter Anwendungen eine gute und permanente Internetverbindung erforderlich ist. Dieser Umstand beschränkt Standorte und Flexibilität des Nutzers.

## 7.4 Zusammenfassung

**Umgang mit BYOD im Betrieb**

Es gibt einige Vor- und viele Nachteile von BYOD, die Arbeitgeber zunächst gründlich abwägen sollten. Nur weil die Nutzung privater Geräte für betriebliche Zwecke im Trend liegt, ist sie nicht gleich geeignet für jeden Betrieb.

Hat sich der Arbeitgeber dafür entschieden, bedingt die Einführung eines BYOD-Konzeptes ein intensiver Planungsprozess, in dem zu nutzende Software und Geräte identifiziert und Mitarbeitervereinbarungen getroffen werden.

Nicht-verhandelbare Voraussetzungen sind die Möglichkeit zur technischen Trennung von privaten und Unternehmensdaten, die Kompatibilität der Geräte mit aktuellen Verschlüsselungstechniken, die Unversehrtheit der Geräte in Hinblick auf Manipulationen (z.B. Rooting/Jailbreaking) und die Bereitschaft des Mitarbeiters, vereinbarte Auflagen einzuhalten.

Inwieweit die Ausgestaltungsmöglichkeit der Geräte durch den Arbeitgeber beschränkt wird, ist im Einzelfall zu entscheiden. Ist die Belegschaft bereit, eine zentrale Geräteverwaltung zu akzeptieren, bietet dieses Konzept einige organisatorische und sicherheitstechnische Vorteile.

Die Virtualisierung der genutzten Software ist aus Datenschutzsicht wünschenswert, macht jedoch eine permanente und gute Internetverbindung erforderlich.

**Notizen**

# 8. Checkliste „Mobiles Arbeiten (BYOD)“

IT-Sicherheit im Handwerk

Checkliste IT-Sicherheit

Gefördert durch:

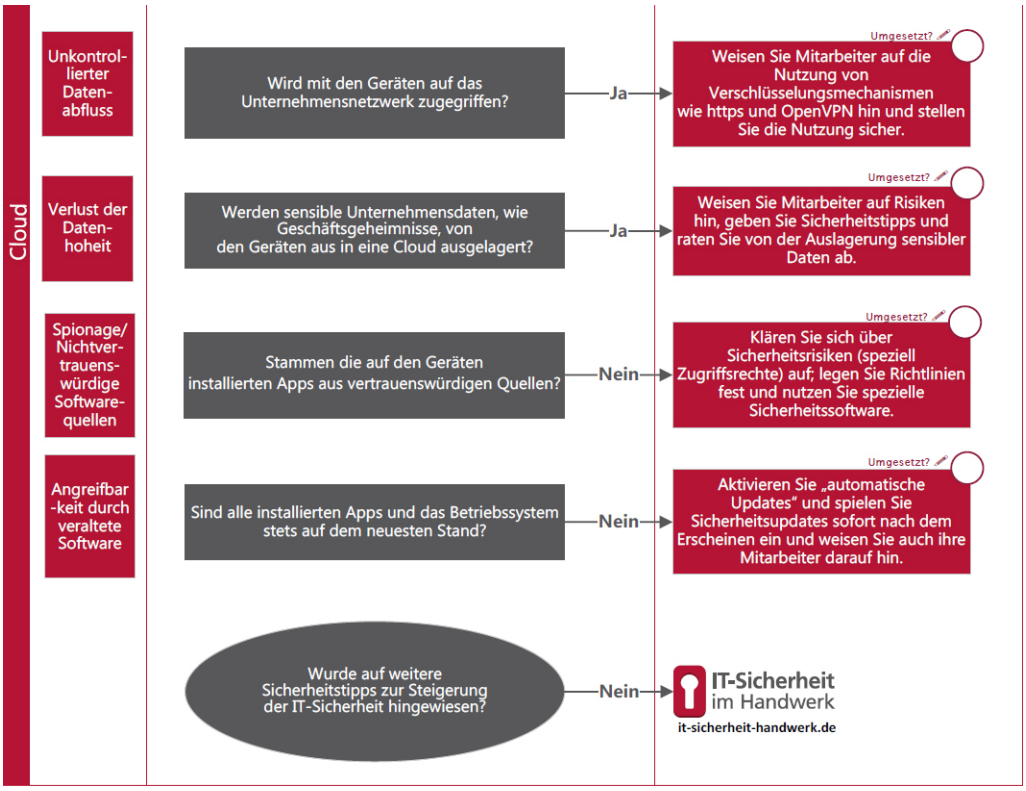
Bundesministerium für Wirtschaft und Energie

TASK FORCE IT-SICHERHEIT IN DER WIRTSCHAFT
Mehrwert und Schutz für Rechner.

aufgrund eines Beschlusses des Deutschen Bundestages

## Mobile Sicherheit für Smartphones und Tablets im Unternehmen

| | Gefahr/ Risiko | Überprüfung des Ist-Zustands | | Maßnahme |
|---|---|---|---|---|
| Datensicherheit | Verlust vertrau-licher Daten | Nutzen Mitarbeiter private Geräte (Smartphones, Tablets, Notebooks etc.) für berufliche Zwecke? | Ja | Klären Sie Mitarbeiter über Rechtsrisiken auf und kommunizieren Sie Nutzungsrichtlinien. (Umgesetzt?) |
| | | Sind die mobilen Geräte ausreichend geschützt? | Nein | Den Schutz mit Hilfe der „Checkliste Basisschutz” überprüfen. (Umgesetzt?) |
| | | Werden regelmäßig Backups der auf den Geräten gespeicherten Daten durch systemeigene Programme durchgeführt? | Nein | Installieren Sie nach Möglichkeit systemeigene Backup-Software (z.B „Kies“ oder „iTunes“)auf allen mobilen Geräten; falls keine Software von Werk aus vorhanden ist, sollte auf alternative Tools zurückgegriffen werden. Lassen Sie Backups regelmäßig durch alle Nutzer mobiler Geräte vornehmen. Sichern Sie die Daten nicht ausschließlich in der Cloud. (Umgesetzt?) |
| | Unberech-tigte Speiche-rung vertrau-licher Daten | Wird vermieden, vertrauliche Daten wie E-Mails und Geschäftsgeheimnisse auf den Geräten zu speichern? | Nein | Sie sollten alle sensiblen Daten ausschließlich auf dem Unternehmensserver ablegen und nur ausnahmsweise via VPN auf mobilen Geräten bearbeiten. (Umgesetzt?) |
| | Verlust von Geräten und Daten | Haben Sie folgende Vorkehrungen für einen möglichen Geräteverlust getroffen? 1. Registrierung der Geräte beim Hersteller 2. Dokumentation von Serien-Nr. und IMEI 3. Hinweis auf Kontaktdaten und Finderlohn im Gerät 4. Anti-Theft-Tool und Fernlösch-Funktion installiert | Nein | Führen Sie die dargestellten Präventivmaßnahmen für den Fall des Verlusts durch. (Umgesetzt?) |
| | Angriffe durch Schadpro-gramme | Ist auf den Geräten eine Mobile Security Suite installiert? | Nein | Installieren Sie eine Mobile Security Suite mit geeignetem Funktionsumfang (Virenscanner, Virenschutz, Personal-Firewall, auto-matische Updatefunktion, Fernlösch-ungsfunktion, SIM-Lock-Funktion und weitere Schutz-Tools ) auf allen Geräten. (Umgesetzt?) |
| | Mitlesen, Abhören und Manipu-lation | Sind Sicherheits-Apps installiert? | Nein | Laden Sie die App auf it-sicherheit-handwerk.de herunter. (Umgesetzt?) |
| WLAN | | Sind die drahtlosen Schnittstellen der Geräte wie WLAN, Bluetooth und Infrarot standardmäßig deaktiviert? | Nein | Weisen Sie ihre Mitarbeiter auf Risiken hin und bewegen diese dazu die Einstellungen zu ändern. (Umgesetzt?) |
| | | Nutzen die Mitarbeiter öffentliche WLAN-Netze? | Ja | Klären Sie ihre Mitarbeiter über Risiken der Nutzung öffentlicher WLAN-Netze auf und halten Sie diese zur ausschließlichen Nutzung von WLAN-Netzen mit Verschlüsselungsmechanismen wie aktuell WPA2 an. (Umgesetzt?) |




TASK FORCE
IT-SICHERHEIT IN DER WIRTSCHAFT
Mehrwert und Schutz für Rechner.

**Task Force „IT-Sicherheit in der Wirtschaft“**
Die Task-Force „IT-Sicherheit in der Wirtschaft“ ist eine Initiative des Bundesministeriums für Wirtschaft und Energie, die gemeinsam mit IT-Sicherheitsexperten aus Wissenschaft, Wirtschaft und Verwaltung vor allem kleine und mittelständische Unternehmen für IT-Sicherheit sensibilisieren und dabei unterstützen will, die Sicherheit der IKT-Systeme zu verbessern. Weitere Informationen zur Task-Force und ihren Angeboten sind unter:

www.it-sicherheit-in-der-wirtschaft.de abrufbar

www.it-sicherheit-handwerk.de

itb- Institut für Technik der Betriebsführung im Deutschen Handwerksinstitut e.V.

Heinz-Piest-Institut für Handwerkstechnik an der Leibniz Universität Hannover

Handwerkskammer Rheinhessen, Kompetenzzentrum für IT-Sicherheit und qualifizierte digitale Signatur

if(is)- Institut für Internet-Sicherheit der Westfälischen Hochschule

# 9. Weblinks

- https://www.it-sicherheit-handwerk.de
- https://www.it-sicherheit.de
- https://www.internet-sicherheit.de
- https://www.bsi.bund.de
- https://www.bsi-fuer-buerger.de
- https://www.sicher-im-netz.de
- http://www.heise.de/security
- http://www.datakontext.com
- http://www.zdnet.de
- http://www.golem.de/specials/security

# 10. Literaturverzeichnis

Aschermann, Tim (2013): iOS-Berechtigungen und Ihre Bedeutung. Herausgegeben von Chip Online. Online verfügbar unter http://praxistipps.chip.de/ios-berechtigungen-und-ihre-bedeutung_9866, zuletzt geprüft am 13.02.2014.

AV-Comparatives (2013): Mobile Security Review. AV-Comparatives. Online verfügbar unter http://www.av-comparatives.org/wp-content/uploads/2013/08/avc_-mob_201308_de.pdf, zuletzt geprüft am 13.02.2014.

AV-Test (2013): Detaillierte Testberichte – Android. September/Oktober 2013. AV-Test. Online verfügbar unter http://www.av-test.org/tests/mobilgeraete/-android/sep-2013/, zuletzt geprüft am 13.02.2014.

Baden-Württembergischer Handwerkstag – BWHT (2012): Umfrage zur IT in Handwerksbetrieben. 1. Quartal 2012. Baden-Württembergischer Handwerkstag – BWHT. Online verfügbar unter http://www.handwerk-bw.de/uploads/media/-bwht-umfrage-it-im-handwerk.pdf, zuletzt geprüft am 20.08.2013.

Barchnicki, Sebastian; Pohlmann, Norbert (2012): „Bezahlen“ mit dem guten Namen. Facebook als Angriffstool für Cybercrime. In: IT-SICHERHEIT, H. 6, S. 53–57.

Beiersmann, Stefan (2013): Studie: Android-Fragmentierung nimmt weiter zu. Herausgegeben von ZDNet. Online verfügbar unter http://www.zdnet.de/-88164000/studie-android-fragmentierung-nimmt-weiter-zu/, zuletzt geprüft am 13.02.2014.

BITKOM – Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e. V. (2014): Smartphone-Boom setzt sich 2014 ungebrochen fort. Pressemitteilung vom 12.02.2014. Online verfügbar unter http://www.bitkom.org/78651_78640.aspx, zuletzt geprüft am 14.03.2014

BITKOM – Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e. V. (2013a): Bring Your Own Device. Unter Mitarbeit von Susanne Dehmel. Berlin. Online verfügbar unter http://www.bitkom.org/files/documents/20130404_LF_BYOD_2013_v2.pdf, zuletzt geprüft am 20.08.2013.

BITKOM – Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e. V. (2013b): Schub fürs mobile Breitband. Pressemitteilung vom 23.07.2013. Berlin. Online verfügbar unter http://www.bitkom.org/de/presse/8477_76810.aspx, zuletzt geprüft am 20.08.2013.

BITKOM – Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e. V. (2013c): Smartphones sorgen für 96 Prozent des Handy-Umsatzes. Pressemitteilung vom 13.02.2013. Berlin. Online verfügbar unter http://www.bitkom.org/de/presse/8477_75052.aspx, zuletzt geprüft am 20.08.2013.

BITKOM – Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e. V. (2013d): Tablet Computer drängen in die Berufswelt. Pressemitteilung vom 19.04.2013. Berlin. Online verfügbar unter http://www.bitkom.org/de/presse/8477_75913.aspx, zuletzt geprüft am 20.08.2013.

BITKOM – Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e. V. (2012a): Handysicherheit: Tastensperre allein reicht nicht. Pressemitteilung vom 04.09.2012. Berlin. Online verfügbar unter http://www.bitkom.org/de/markt_statistik/64022_73298.aspx, zuletzt geprüft am 13.02.2014.

BITKOM – Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e. V. (2012b): Verlorene Handys sind keine Seltenheit. Pressemitteilung vom 02.07.2012. Berlin. Online verfügbar unter http://www.bitkom.org/de/presse/74532_72651.aspx, zuletzt geprüft am 20.08.2013.

BITKOM – Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e. V. (2012c): Vertrauen und Sicherheit im Netz. Online verfügbar unter http://www.bitkom.org/de/publikationen/38338_72966.aspx, zuletzt geprüft am 20.08.2013.

Bundesministeriums für Wirtschaft und Technologie (BMWi) (2012): IT-Sicherheitsniveau in kleinen und mittleren Unternehmen. Studie im Auftrag des Bundesministeriums für Wirtschaft und Technologie (BMWi). Bundesministeriums für Wirtschaft und Technologie (BMWi). Online verfügbar unter http://www.bmwi.de/DE/Mediathek/publikationen,did=525400.html, zuletzt geprüft am 23.08.2013.

Burnett, Mark (2011): 10,000 Top Passwords. Online verfügbar unter https://xato.net/passwords/more-top-worst-passwords/#more-269, zuletzt geprüft am 13.02.2014.

Check Point Software Technologies Ltd (2013): THE IMPACT OF MOBILE DEVICES ON INFORMATION SECURITY. A SURVEY OF IT PROFESSIONALS. Check Point Software Technologies Ltd. Online verfügbar unter http://www.checkpoint.com/downloads/products/check-point-mobile-security-survey-report2013.pdf, zuletzt geprüft am 20.08.2013.

Cisco Systems, Inc. (2013): Cisco Jahresbericht zum Thema Sicherheit 2013. Cisco Systems, Inc. Online verfügbar unter http://www.cisco.com/web/DE/products/security/index.html, zuletzt geprüft am 20.08.2013.

DATEV und Deutschland sicher im Netz e.V. (2013): Sicheres Arbeiten von unterwegs. Leitfaden zum Umgang mit mobilen Medien für Unternehmen. DATEV und Deutschland sicher im Netz e.V. Online verfügbar unter https://www.sicher-im-netz.de/unternehmen/2246.aspx, zuletzt geprüft am 23.08.2013.

Dell (Hg.) (2012): Dell und TNS Infratest Studie IT-Consumerization. Online verfügbar unter http://www.pressebox.de/pressemitteilung/dell-gmbh/Dell-Umfrage-Nutzung-privater-IT-Geraete-ist-in-deutschen-Unternehmen-kaum-geregelt/boxid/485463, zuletzt geprüft am 20.08.2013.

Deutschland sicher im Netz e.V. (2013a): Bring Your Own Device. Regeln für KMU und Nutzer. Deutschland sicher im Netz e.V. Online verfügbar unter https://www.sicher-im-netz.de/unternehmen/2246.aspx, zuletzt geprüft am 23.08.2013.

Deutschland sicher im Netz e.V. (o. J.): Sicheres Arbeiten von unterwegs. Leitfaden zum Umgang mit mobilen Medien für Unternehmen. DATEV und Deutschland sicher im Netz e.V. Online verfügbar unter http://www.datev.de/portal/ShowContent.do?pid=dpi&cid=212583, zuletzt geprüft am 13.02.2014.

Deutschland sicher im Netz e.V. (2013b): IT-Sicherheitslage im Mittelstand 2013. Eine Studie von Deutschland sicher im Netz. Update zur Studie von Deutschland sicher im Netz aus dem Jahr 2012. Deutschland sicher im Netz e.V. Online verfügbar unter https://www.sicher-im-netz.de/unternehmen/sicherheitslage_-mittelstand_2013.aspx, zuletzt geprüft am 23.08.2013.

Duscha, Andreas (Hg.) (2011): Praxishandbuch IT- und Informationssicherheit. Sammelband des BMWi/NEG-Verbundprojekts „Sichere E-Geschäftsprozesse in KMU und Handwerk". E-Commere-Center Handel. Köln. Online verfügbar unter http://www.mittelstand-digital.de/MD/Redaktion/DE/PDF/praxishandbuch-it-und-informationssicherheit,property=pdf,bereich=md,sprache=de,rwb=true.pdf, zuletzt geprüft am 13.02.2014.

Eikenberg, Ronald (2012): Erneut Account-Klau bei WhatsApp möglich. Herausgegeben von heise online. Online verfügbar unter http://www.heise.de/security/meldung/Erneut-Account-Klau-bei-WhatsApp-moeglich-1756224.html, zuletzt geprüft am 13.02.2014.

Eikenberg, Ronald (2013): WhatsApp-Zahlungen manipulierbar. Herausgegeben von heise online. Online verfügbar unter http://www.heise.de/security/meldung/WhatsApp-Zahlungen-manipulierbar-1924703.html, zuletzt geprüft am 13.02.2014.

Fischermann, Thomas (2012): Smartphones. "Es gibt immer Schwachstellen". In: DIE ZEIT, Jg. 66, Ausgabe 39, 2012. Online verfügbar unter http://www.zeit.de/2012/39/Sicherheit-Smartphone-Norbert-Pohlmann, zuletzt geprüft am 13.02.2014.

Gartner (2014): Gartner Says Annual Smartphone Sales Surpassed Sales of Feature Phones for the First Time in 2013. Pressemitteilung vom 13.02.2014. Online verfügbar unter https://www.gartner.com/newsroom/id/2665715, zuletzt geprüft am 06.03.2014.

Hamada, Joji (2011): New Android Threat Gives Phone a Root Canal. Herausgegeben von Symantec. Online verfügbar unter

http://www.symantec.com/connect/blogs/new-android-threat-gives-phone-root-canal, zuletzt aktualisiert am 23.01.2014, zuletzt geprüft am 14.02.2014.

Heidisch, Maik (2013): SMARTPHONE SECURITY FOR TOMORROW BUSINESS. Unveröffentlichter Projektbericht. Institut für Internet-Sicherheit.

Heinemeyer, Dennis (2013): »Bring Your Own Device« (BYOD). Rechtliche Aspekte und praktische Tipps. Tagung der Working Group 2. Institut für Rechtsinformatik Leibniz Universität Hannover. Online verfügbar unter http://www.eicar.org/files/eicar_wg2_2013_-_iri_-_byod.pdf, zuletzt geprüft am 13.02.2014.

heise online (Hg.) (2012): Google will das Android-Update-Problem entschärfen. Online verfügbar unter http://www.heise.de/newsticker/meldung/Google-will-das-Android-Update-Problem-entschaerfen-1628129.html, zuletzt geprüft am 13.02.2014.

Heister, Nico (2012): App-Berechtigungen und was sie bedeuten. Herausgegeben von AndroidPit. Online verfügbar unter http://www.androidpit.de/app-berechtigungen-android-erklaerung, zuletzt aktualisiert am 2013, zuletzt geprüft am 13.02.2014.

Institut für IT-Recht (2010): Beschäftigten-Datenschutz: Private Arbeitnehmer-E-Mails und die Reichweite des Fernmeldegeheimnisses. Online verfügbar unter http://www.iitr.de/index.php?option=com_content&view=article&id=230:beschaeftigten-datenschutz-private-arbeitnehmer-e-mails-und-die-reichweite-des-fernmeldegeheimnisses&catid=28&Itemid=61, zuletzt geprüft am 13.02.2014.

IT-Sicherheit im Handwerk (2013): IT -Sicherheitsniveau im Handwerk.

Juniper networks Mobile Threat Center (2013): Third Annual Mobile Threats Report. March 2012 through March 2013. Abstract. Herausgegeben von Juniper Networks Inc. Online verfügbar unter http://www.juniper.net/us/en/local/pdf/additional-resources/3rd-jnpr-mobile-threats-report-exec-summary.pdf, zuletzt geprüft am 23.08.2013.

Kalus, Georg (2013): Überblick: Die Fähigkeiten und Zugriffsrechte von Windows Phone Apps. Herausgegeben von WParea.de – Das Windows Phone Magazin. Online verfügbar unter http://wparea.de/2013/04/uberblick-die-fahigkeiten-und-zugriffsrechte-von-windows-phone-apps/, zuletzt geprüft am 13.02.2014.

Karpf, Achim (2006): Datenschutz für mobile Daten durch Verschlüsselung.Täglich bleiben tausende mobile Endgeräte in Taxis liegen. Herausgegeben von Security Insider. Online verfügbar unter http://www.security-insider.de/themenbereiche/identity-und-access-management/zugangskontrolle/articles/49472, zuletzt geprüft am 13.02.2014.

Klemm, Markus (2014): Was macht Facebook mit den WhatsApp-Daten?. Herausgegeben von DIE WELT. Online verfügbar unter http://www.welt.de/regionales/hamburg/article125046086/Was-macht-Facebook-mit-den-WhatsApp-Daten.html, zuletzt geprüft am 06.03.2014.

Kwasniewski, Nicolai (2014): Übernahme durch Facebook: Datenschützer ruft zu Boykott von WhatsApp auf. Herausgegeben von SPIEGEL ONLINE. Online verfügbar unter http://www.spiegel.de/wirtschaft/unternehmen/facebook-kauft-whatsapp-datenschuetzer-weichert-empfiehlt-boykott-a-954783.html, zuletzt geprüft am 06.03.2014.

Lamberty, Michael (30.08.2012): Sie haben kein Recht zu schweigen. Kritische Betrachtung des Sicherheitskonzepts von Android. Unveröffentlichte Bachelorarbeit. Betreut von Georg Rock. Trier. Fachhochschule Trier.

Lamberty, Michael; Pohlmann, Norbert (2013): Sicherheitsrisiko Smartphone. Die Kehrseiten unbegrenzter Mobility. In: IT-SICHERHEIT, H. 3, S. 56–59.

McAfee (Hg.) (2013): McAfee Threat-Report. Erstes Quartal 2013. Kurzfassung. Online verfügbar unter http://www.mcafee.com/apps/view-all/publications.aspx?region=de&tf=mcafee_labs, zuletzt geprüft am 23.08.2013.

Münsterländer Kompetenzzentrum für elektronischen Geschäftsverkehr (MÜKE) (Hg.) (2011): Mit Hammer, Säge und Smartphone. Mobiles Arbeiten im Handwerk. Netzwerk Elektronischer Geschäftsverkehr (NEG). Online verfügbar unter http://www.ebusiness-lotse-berlin.de/data/files/vortraege/Mit_Hammer__-Säge_und_Smartphone.pdf, zuletzt geprüft am 23.08.2013.

Open Signal (2013): Android Fragmentation Visualized. Open Signal. Online verfügbar unter http://opensignal.com/reports/fragmentation-2013/, zuletzt geprüft am 13.02.2014.

Pohlmann, Norbert; Linnemann, Markus (2010): Sicher im Internet. Tipps und Tricks für das digitale Leben. Zürich: Orell Füssli Verlag.

Ponemon Institute (2012): Global Study on Mobility Risks. Survey of IT & IT Security Practitioners. Research Report. Ponemon Institute. Online verfügbar unter http://www.ponemon.org/local/upload/file/Websense_Mobility_US_Final.pdf, zuletzt geprüft am 23.08.2013.

Pursche, Olaf (2013): Das sollten Sie nach einem Smartphone-Diebstahl tun. Unter Mitarbeit von DIE WELT. Online verfügbar unter http://www.welt.de/wirtschaft/webwelt/article118768360/Das-sollten-Sie-nach-einem-Smartphone-Diebstahl-tun.html, zuletzt geprüft am 13.02.2014.

Schieb, Jörg (2013): Deeplink: WhatsApp. Herausgegeben von DasErste.de – Ratgeber Internet. Online verfügbar unter http://www.daserste.de/information/ratgeber-service/internet/sendung/wdr/2013/sendung-vom-17082013-110.html, zuletzt aktualisiert am 28.11.2013, zuletzt geprüft am 13.02.2014.

Schmidt, Malte G.; Spooren, Sebastian (2011): Kriminelle Dienstleistung. Neue Gefahren im Web 2.0. In: iX Magazin für professionelle Informationstechnik, H. 11, S. V–IX.

Schmidt, Malte G.; Spooren, Sebastian (2012): Zielscheibe Smartphone – Gefahren und Risiken. In: IT business, H. 2, S. 2–4.

Schröder, Heiko (o. J.): Zusammenhang von Brute-Force-Attacken und Passwortlängen. Herausgegeben von 1PW. Online verfügbar unter http://www.1pw.de/brute-force.html, zuletzt geprüft am 13.02.2014.

Schüler, Jürgen (2013): Unveröffentlichte Präsentationsfolien zum Thema Mobile Security. Herausgegeben von Kompetenzzentrum IT-Sicherheit und Signatur. Handwerkskammer Rheinhessen.

SecuMedia (Hg.) (2013a): <kes> Microsoft Sicherheitsstudie. Lagebericht zur Informationssicherheit. Sonderdruck aus <kes> 2012#4/6. In: <kes> Die Zeitschrift für Informations-Sicherheit, Jg. 4, 6. Ingelheim: SecuMedia Verlags-GmbH.

SecuMedia (Hg.) (2013b): Mobile Security. special. In: <kes> Die Zeitschrift für Informations-Sicherheit, Juli. Ingelheim: SecuMedia Verlags-GmbH.

Spogahn, Nikolai; Pohlmann, Norbert (2011): In der Cloud, aber nicht anonym! Googles Cloud-Angebot – Wie wertvoll ist uns der Datenschutz? (Teil 1). In: IT-SICHERHEIT, H. 2, S. 50–53.

Statista (Hg.) (2013): Anzahl der angebotenen Apps in den Top App-Stores im Juli 2013. Online verfügbar unter http://de.statista.com/statistik/daten/studie/208599/umfrage/anzahl-der-apps-in-den-top-app-stores/, zuletzt geprüft am 12.02.2014.

Süddeutsche.de (Hg.) (2012): Path schnappt sich Adressbuchdaten. Online verfügbar unter http://www.sueddeutsche.de/digital/soziales-netzwerk-path-schnappt-sich-adressbuchdaten-1.1279229, zuletzt geprüft am 13.02.2014.

Symantec (2012): The Symantec Smartphone Honey Stick Project. Symantec. Online verfügbar unter http://www.symantec.com/content/en/us/about/presskits/b-symantec-smartphone-honey-stick-project.en-us.pdf, zuletzt geprüft am 13.02.2014.

Telefónica Germany (o. J.): Drittanbietersperre. Mit der Drittanbietersperre teure Premiumdienste einfach sperren. Online verfügbar unter http://www.o2online.de/business/service/extra/handy/drittanbietersperre/, zuletzt geprüft am 13.02.2014.

Telekom Deutschland (o. J.): Häufige Fragen zum Thema Drittanbieter. Online verfügbar unter http://www.t-mobile.de/faq/1,1951,18-_,00.html?c=699, zuletzt geprüft am 13.02.2014.

Tomorrow Focus Media (2013): Mobile Effects 2013-2. Immer näher dran – der neue Trend zum Second Screen. Tomorrow Focus Media. Online verfügbar unter http://www.slideshare.net/tomorrowfocus/mobile-effects-2013-2, zuletzt geprüft am 23.08.2013.

Trend Labs (Hg.) (2013): Evolved Threats In A "Post-PC" World. 2012 ANNUAL SECURITY ROUNDUP. Trend Micro. Online verfügbar unter: http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/reports/rpt-evolved-threats-in-a-post-pc-world.pdf, zuletzt geprüft am 23.08.2013.

Whittome, Chris (2013): Security Alert! A Factory Reset is not enough when selling your cell phone. Herausgegeben von trade2safe Blog. Online verfügbar unter https://www.trade2save.com/blog/2013/04/security-alert-a-factory-reset-is-not-enough-when-selling-your-cell-phone/, zuletzt geprüft am 13.02.2014.

**Gesetzestexte:**

Bundesdatenschutzgesetz. (BDSG), vom 14.8.2009. Online verfügbar unter http://www.gesetze-im-internet.de/bundesrecht/bdsg_1990/gesamt.pdf, zuletzt geprüft am 13.02.2014.

Telekommunikationsgesetz in der konsolidierten, nicht amtlichen Fassung. (TKG), vom 9. Mai 2012. Online verfügbar unter: http://www.bmwi.de/BMWi/Redaktion/PDF/Gesetz/tkg-nicht-kosolidierte-fassung-2012,property=pdf,bereich=bmwi2012,sprache=de,rwb=true.pdf, zuletzt geprüft am 13.02.2014.

# 11. Stichwortverzeichnis

# 12. Abbildungsverzeichnis

# 13. Tabellenverzeichnis

9 783944 916132