# Handreichung zur Nutzung von Smartphones und Tablet-Computer in Behörden und Unternehmen

## 1. Einleitung

Nach aktuellen Marktdaten wird der Smartphone- und Tablet-Computer-Markt nahezu ausschließlich von Geräten mit den Betriebsystemen iOS und Android OS dominiert. Beide Plattformen wurden für den Privatkunden-Markt entwickelt. Sie werden aber mit steigender Tendenz auch im Unternehmensumfeld eingesetzt, obwohl sie im Gegensatz zu den BlackBerry und Windows Mobile Systemen nicht für den Unternehmenseinsatz konzipiert wurden (siehe Kapitel 2 Ausgangslage und historische Entwicklung).

Mit den konzeptionellen Unterschieden beider Systeme beschäftigt sich Kapitel 3.

Das vierte Kapitel behandelt Fragestellungen, ob und wie diese Systeme trotzdem im beruflichen Umfeld eingesetzt werden können. Dabei ist es unumgänglich, die entsprechenden konzeptionellen Vorarbeiten zu machen. Nur weil neue Gerätetypen eingesetzt werden, dürfen Datenschutz und Datensicherheitsanforderungen nicht gesenkt werden. Bei allen denkbaren Problemen im Detail lässt sich außerdem feststellen, dass der Einsatz eines Mobile Device Management Systems (MDM) zwingend ist. Nur dadurch können einige gebotene Anforderungen an den Einsatz technisch durchgesetzt werden.

Gustav-Stresemann-Ring 1 • 65189 Wiesbaden • Telefon 0611 1408 0 • Telefax 0611 1408 900

E-Mail poststelle@datenschutz.hessen.de • Internet http://www.datenschutz.hessen.de

# 2. Ausgangslage und historische Entwicklung

## 2.1. Symbian OS

Die erste Generation von Smartphones wurde bereits 1996 mit dem Nokia Communicator eingeführt. Ab dem Jahr 2001 wurde dieser bereits mit Betriebssystem Symbian OS betrieben, welches sich in den Folgejahren auch bei anderen Herstellern (u. a. Nokia, Sony Ericcson) für Smartphone-Modelle etablierte. Dabei existierten zwei unterschiedliche Varianten: Die eine wurde mit den üblichen Tasten eines Mobiltelefons bedient, die andere mit einem Stift auf einem berührungsempfindlichen Bildschirm. Nach einer Statistik von ABI Research erreichte Symbian OS 2006 mit einem Markanteil von 73% seinen Höhepunkt im Smartphone-Bereich. Größere Sicherheitslücken wurden in der Anfangszeit geschlossen und bestehende Gefahren konnten durch den Einsatz von Lösungen bekannter Hersteller von Sicherheits-Software abgewehrt werden. Diese Plattform war besonders erfolgreich bei Privat-Kunden. Nach einem größeren Einbruch der Absatzzahlen entschloss sich Nokia im Frühjahr 2011 keine neuen Geräte mit Symbian OS zu produzieren. Dies führte dazu, dass diese Plattform heute keine Relevanz im Smartphone-Markt mehr hat.

## 2.2. Windows Mobile/Phone

2002 stieg Microsoft mit Windows Mobile erfolgreich in den Markt für Smartphones ein. Das Aussehen und die Handhabung (Look & Feel) entsprach dem der jeweils aktuellen Windows-Version für den Desktop. Die Software wurde als nicht besonders bedienerfreundlich empfunden, da sie nicht für kleine Bildschirme ausgelegt und für die Bedienung des berührungsempfindlichen Bildschirms ein Stift nötig war. Dafür konnten die Windows Mobile Geräte sehr gut in eine Microsoft-Infrastruktur integriert werden, weil für sie eine abgespeckte Version von Microsoft Office existierte (Pocket Word, -Excel, -PowerPoint, -Outlook). Mit Pocket Outlook war eine zuverlässige Anbindung an den Microsoft Exchange Server (E-Mails, Termine, Adressbuch u. v. m.) möglich. Deshalb war Windows Mobile nicht nur auf dem Privatkunden-Markt, sondern auch im Unternehmensumfeld relativ erfolgreich. Absatzprobleme führten später dazu, dass Microsoft als Nachfolgesystem Windows Phone neu entwickelte, und dabei besonderen Wert auf eine gute Bedienbarkeit legte. Diese Plattform wird von einer Vielzahl von Geräteherstellern unterstützt (Samsung, HTC, u. v. m.). Seit Februar 2011 gibt es eine Allianz zwischen Microsoft und Nokia mit dem Ziel, Windows Phone zum bevorzugten Betriebssystem auf Nokia Smartphones zu machen.

Microsoft brachte im Oktober 2012 unter dem Namen Surface den ersten Tablet-Computer mit dem neuen Betriebsystem Windows 8 RT auf den Markt. Weitere Tablet-Computer mit Windows 8 RT folgten von verschiedenen Herstellern.

Weder Windows Phone noch Windows RT konnten bis zum Beginn des 1. Quartals 2013 nennenswerte Marktanteile erreichen.

## 2.3. Blackberry

Mit dem Blackberry führte die Firma Research In Motion (RIM) 1999 ein Smartphone ein, welches vor allem im Unternehmensumfeld erfolgreich war. Die Grundlage für den Erfolg war ein Push-Dienst zur Synchronisierung von E-Mails, Kalendereinträgen, Notizen und Adressbucheinträgen. Das bedeutet, dass die Daten auf dem Smartphone immer auf dem aktuellen Stand sind. Beispielsweise werden damit E-Mails sofort zugestellt. Darüber hinaus ermöglichte die Blackberry-Infrastruktur eine sichere Anbindung an Firmennetze, Unternehmensressourcenplanungs–Systeme (ERP) und Datenbanken. Der Datenspeicher des Gerätes und die Verbindungen zu den Blackberry Servern sind verschlüsselt. Ferner existiert die Möglichkeit eines zentralen Gerätemanagements. Trotzdem sind die Absatzzahlen in den vergangen 2 Jahr stark eingebrochen. Ursache war neben der Vernachlässigung der Privatkunden als Zielgruppe auch die von vielen Benutzern als nicht mehr zeitgemäß empfunden Benutzeroberfläche. Im Januar 2013 wechselte RIM seinen Unternehmensnamen zu BlackBerry. Im März 2013 erschien der BlackBerry Z10 mit dem völlig neu entwickelten Betriebsystem BlackBerry 10. Dieses Gerät orientiert sich von der Benutzung bis zur Optik an den führenden Geräten mit iOS und Android OS, allerdings mit starker Ausrichtung auf das Unternehmensumfeld und der Option der Trennung von privaten und geschäftlichen Daten.

## 2.4. iOS und Android OS

Einen Wendepunkt im Smartphone-Markt markierte die Einführung des iPhone (iPhone OS, heute iOS) im Herbst 2007 und Smartphones mit Android OS ein Jahr später. iOS wird von Apple entwickelt und Android OS vom Konsortium Open Handset Alliance (OHA) unter Führung von Google. Grundlage für den Erfolg war die einfache, intuitive Bedienung mit einem oder mehreren Fingern. Hinzu kamen neue Funktionalitäten wie Mediaplayer (Musik, Film, Podcasts) und Dienste in Verbindung mit Ortungsdiensten (Karten, Navigation u. v. m.), die vorher von eigenständigen Geräteklassen abgedeckt wurden. Außerdem sind diese Systeme nahezu wartungsfrei nutzbar. Eine ähnlich zunehmende Bedeutung haben die Tablet-Computer beider Plattformen. Sie lösen teilweise Systeme mit Desktop-Betriebsystem ab. Der Absatz von Tablet-Computern steigt etwa in dem Maße an, wie der Absatz für Desktop-Computer und Notebooks sinkt. Die Verkaufszahlen für Tablet-Computer stiegen im Weihnachtsgeschäft 2012 auf über 52 Millionen an. Das bedeutet eine Steigerung von fast 74 Prozent gegenüber dem Vorjahr.

# 3. Unterschiede zwischen iOS und Android OS

Zum jetzigen Zeitpunkt gibt es zwei relevante Systeme auf dem Markt der Smartphones und Tablet-Computer: die Geräte von Apple mit der Betriebssystemfamilie iOS einerseits und die auf den Android-Betriebssystemen aufbauenden Geräte, die von einer großen Anzahl Hersteller angeboten werden, andererseits. Trotz der auf den ersten Blick vorhandenen Ähnlichkeit gibt es eine Reihe von konzeptionellen und technischen Unterschieden, auf die im Folgenden kurz eingegangen wird. Beachten Sie dazu bitte auch das „Infoblatt zum Umgang mit iOS- und Android-Geräten“[1].

## 3.1. iOS

Apple hat ein in sich geschlossenes System konzipiert, bei dem Hardware, Software (sogenannte „Apps“) und Daten so miteinander verbunden sind, dass insbesondere Software und Daten vermarktet werden können. Dreh- und Angelpunkt für den Kauf von Software, Musik und anderer Artikel ist der iTunes Store, bei dem sich ein Nutzer registrieren muss, um die Geräte sinnvoll nutzen zu können. Es gibt keine Alternative von anderen Herstellern zu dieser herstellerspezifischen Variante. Je nach Konfiguration der Geräte und den genutzten Apps werden an Apple außerdem unterschiedlich viele Daten übermittelt. Da Apple den Eigentümer des Gerätes (i. d. R.) kennt, besitzt die Firma Informationen über das Benutzerverhalten vieler Millionen Kunden.

Was die zunehmende Nutzung von Clouds – insbesondere, aber nicht nur im betrieblichen Umfeld – angeht, gibt es hier die sogenannte „iCloud“, einen von Apple zur Verfügung gestellten Speicher im Internet, in dem Nutzer von Apple-Geräten ihre Daten speichern können.

### 3.1.1. Software

Die Apps für iOS können im Appstore, einem Teil des iTunes-Store gekauft werden. Die Apps können ohne eine weitere Datenübertragung funktionieren, aber in den meisten Fällen werden Daten aus dem Internet heruntergeladen oder auf Server im Internet übertragen. Dabei kann es zu vom Nutzer ungewollten Datenübertragungen persönlicher Daten kommen. Damit erhalten die Betreiber von Servern personenbezogene Daten.

Dies gilt bspw. für die Spracherkennungskomponente Siri, bei der die Erkennung auf Servern von Apple erfolgt, die auch im außereuropäischen Ausland, z. B. in den USA, stehen können, d.h. in Ländern ohne oder nicht ausreichend schützenden Datenschutzgesetzen.

[1] http://www.datenschutz.hessen.de/tf016.htm

### 3.1.2. Updates

Apps werden über den Appstore installiert und aktualisiert. Apple unterzieht alle Apps einer Überprüfung auf ein Mindestmaß an Qualität, Einhaltung des Jugendschutzes und Malware-Bestandteile. Die Kombination aus zentraler Stelle für Software Installationen/Aktualisierungen und App-Überprüfung erhöht die Sicherheit des Gesamtsystems. Deshalb ist im Gegensatz zu PC Systemen auf Tablet- und Smartphone-Systemen die von Apple installierte Software auf einem relativ aktuellen Versionsstand.

Gleiches gilt auch für das Betriebssystem iOS, das schon seit längerer Zeit Over-the-air (OTA), d.h. per mobiles Netz (GSM, GPRS, EDGE, UMTS, HSDPA, LTE oder WLAN) aktualisiert wird. Ein weiteres Gerät, wie z. B. ein PC, ist nicht notwendig. Die Erfahrung zeigt, dass die Benutzer nach einer Update-Benachrichtigung dieses auch ausführen.

### 3.1.3. Sicherheit

Das Grundkonzept von iOS sieht vor, dass die verschiedenen Apps einen eigenen, gegen andere Apps abgeschotteten Datenspeicher haben (Sandbox). Es gibt einige wenige Daten, die allen Apps zur Verfügung stehen können (s. Berechtigungen). Ein Datenaustausch zwischen Apps muss über Speicherdienste im Internet oder den privaten Desktop-Computer mit Hilfe von iTunes geschehen.

Durch die Abschottung der Speicherbereiche und Apps ist die Infektion durch Schadsoftware unwahrscheinlicher als bei den üblichen Desktop- Computern.

Der Flash-Speicher des Gerätes kann seit iOS 6 mit einen Passwort (Einstellungen > Allgemein > Code-Sperre) verschlüsselt werden. Dabei ist die Wahl eines sicheren Passwortes obligatorisch. Auf keinen Fall darf es sich um ein leicht zu erratendes Wort handeln. Baut ein Angreifer den Speicher zum Auslesen aus, liegen die Daten somit verschlüsselt vor. Erlangt er jedoch Zugriff auf ein laufendes System sind diese im Klartext sichtbar.

In alten Versionen von iOS können Schlüssel ausgelesen werden, so dass eine ausreichende Sicherheit nicht gegeben ist.

### 3.1.4. Berechtigungen

Mit der aktuellen Version 6 von iOS gibt es eine entscheidende Verbesserung für den Schutz der Benutzerdaten. Der Benutzer muss für jede App seine Zustimmung auf den Zugriff von Daten außerhalb der Sandbox erteilen. Diese Einstellungen sind auch nachträglich änderbar.

Unter Einstellungen -> Datenschutz können Zugriffe auf folgende Daten konfiguriert werden:

- Ortungsdienste
- Kontakte
- Kalender
- Erinnerungen
- Fotos
- Bluetooth
- Accounts sozialer Netzwerke (Facebook, Twitter etc.)

## 3.2. Android OS

Android-Geräte sind prinzipiell ohne irgendeine Registrierung bei einem Anbieter nutzbar. Dies gilt insbesondere für alle vorinstallierten Apps (Anwendungsprogramme mobiler Endgeräte) z. B. Google Maps (Kartendienst und Navigation), Browser, Youtube (Videoportal), Kontakte, Kalender, Notizen, Musik, Video, UKW Radio u. v. m. Zur Nutzung der vorinstallierten E-Mail-App kann jeder E-Mail-Provider verwendet werden.

Wird das Gerät hingegen mit einem oder mehreren Google-Konten betrieben, verbindet sich das Gerät mit einem Google-Server, der mittels Google Cloud Messaging (GCM)-Protokoll ohne Einwilligung des Benutzers Aktionen auf dem Gerät auslösen kann (z. B. Apps löschen oder reset auf Werkseinstellung u. v. m.).

Die Google-Dienste werden nicht zuletzt wegen ihrer Funktionalität gern genutzt und stehen kostenpflichtige Varianten der Konkurrenz nicht nach. Hier eine Auswahl der bekannteren:

- Google Suche
- Google Maps
- Google Mail
- Google Kontakte
- Google Kalender
- Google News
- Google Reader
- Picassa
- Google+
- U. v. m..

### 3.2.1. Software

Unter Android bestehen mehrere Möglichkeiten Software zu installieren. Neben Google Play (vormals Android Market) gibt es noch den AndroidPIT App Center und die Amazon Apps. Manche Telekommunikationsanbieter installieren noch einen eigenen Android App Store.

Das Angebot an Apps ist überwiegend dasselbe wie für iOS. Unterschiede existieren bei den Preisen, bei den Bezahlmöglichkeiten und bei den Allgemeinen Geschäftsbedingungen. Für den Benutzer hat AndroidPIT den Vorteil, dass die deutschen Datenschutzgesetze gelten, da es sich um ein Unternehmen mit Sitz in Berlin handelt. Für Amazon Apps mit Sitz in Luxemburg gilt der europäische Rechtsrahmen. Als US-amerikanisches Unternehmen gelten für Google (und Apple) weder die deutschen noch die europäischen Datenschutzgesetze, zum Nachteil der Nutzer. Darüber hinaus können unter Android – analog zu Linux – auch Installations-Dateien (Android Packages mit der Endung APK) manuell installiert werden. Mobile Device Management Systeme (MDM) ermöglichen auch die Einrichtung eines firmenspezifischen App-Stores (siehe Kapitel 4.2.1).

### 3.2.2. Updates

App-Aktualisierungen funktionieren über die verfügbare Android App Stores prinzipiell genauso, wie bei iOS. Allerdings prüfen diese den Inhalt nicht so konsequent wie Apple, sodass auch malware-behaftete Apps in den Android App Stores angeboten werden. Manuell installierte Apps müssen auch manuell aktualisiert werden.

Updates des Betriebssystems für Android sind häufig ein Problem. Google entwickelt Android OS i. d. R. für Referenzgeräte. Diese werden zusammen mit wechselnden Herstellern entwickelt und tragen den Teilnamen Nexus. Für Android 4.0 (Ice Cream Sandwich) und 4.1 (Jelly Bean) ist dies das Smartphone Galaxy Nexus von Samsung und der Tablet-PC Nexus 7 von ASUS. Nachdem Google den Quellcode der aktuellen Version veröffentlicht hat, müssen die Hersteller diese Version auf die Hardware ihrer Geräte anpassen. Nahezu alle relevanten Hersteller haben noch eigene Benutzeroberflächen, um sich von einander abzugrenzen (z. B. Samsung TouchWiz, HTC Sense, Motorola MotoBlur, etc.). Diese müssen natürlich ebenfalls aufwendig angepasst werden. Dies hat zur Folge, dass es häufig nur für ein Jahr Betriebssystem-Updates für die führende Geräte gibt. Zur Erhöhung der Sicherheit sollten aber alle Apps und das Betriebssystem auf dem aktuellen Versionsstand sein.

### 3.2.3. Sicherheit

Android ist ein Linux-basiertes Betriebsystem. Die meisten Sicherheitskonzepte wurden von Linux übernommen und bauen wie folgt aufeinander auf. Auf oberster Ebene existiert das Benutzerkonzept. Pro installierter App wird automatisch ein (Linux-)Benutzer und ein Ordner im Gerätespeicher angelegt. Der Besitzer des Ordners ist der (Linux-) Benutzer, d. h. die App. Dies hat zur Folge, dass nur die App ihre Daten in diesem Ordner ablegen kann. Anderen Apps wird dadurch der Zugriff verwehrt. Umgekehrt kann die App nicht auf Systemdienste zugreifen, dies kann erst einmal nur der Superuser (root).

Damit dies funktioniert, nutzt Android ein Linux-Dateisystem, welches in der Lage ist, das Durchsetzen solcher Ordner und dateibasierter Rechte zu garantieren. Änderungen am System darf nur ein Superuser (root) durchführen. Das System schützt sich somit gegen Manipulationen der Geräte Benutzer und der installierten Apps.

Oft besitzen Android-Geräte wechselbare Flash-Speicher, die nicht mit einem Linux-Dateisystem formatiert sind. Dies hat zur Folge, dass diese Inhalte von allen Apps lesbar und veränderbar sind. Zudem ist bei vielen Geräten dieser Steckplatz von außen zugänglich. Daten unverschlüsselter Speicherkarten können leicht entfernt und von Fremden gelesen werden.

Native Android Apps werden in der Programmiersprache Java entwickelt. Deshalb laufen diese nicht direkt auf der Hardware, sondern in einer virtuellen Maschine, jeweils in einem eigenen Prozess. Virtuelle Maschinen steigern ebenfalls die Sicherheit eines Systems, da laufende Programme von Ihnen überwacht werden.

Die Summe aller Maßnahmen stellt sicher, dass Apps in einem eigenen abgeschotteten Bereich laufen. Diesen nennt man allgemein Sandbox. Im Gegensatz zum Sandboxing unter iOS bildet dieses Verfahren einen geringeren Schutz gegen Malware, da ein direkter Zugriff gewährt wird. In iOS werden Daten zwischen den Apps als Kopie ausgetauscht.

Apps brauchen in der Regel – je nach Zweck – aber Zugriff auf bestimmte Daten und Systemdienste. Bspw. benötigt eine Navigations-App Zugriff auf den GPS-Sensor und die Twitter-App Zugriff auf das Internet. Deshalb existieren unter Android zum Austausch und zur Kommunikation der Sandbox nach außen Berechtigungen (s. Berechtigungen).

Um das unberechtigte Auslesen von Flashs-Speicher zu verhindern, gibt es seit Android 4 die Möglichkeit, interne und externe Flash-Speicher des Gerätes zu verschlüsseln. So sind die Daten bspw. von einen anderen Gerät nur lesbar, wenn man einen gültigen Schlüssel besitzt.

### 3.2.4. Berechtigungen

Während des Installationsvorgangs wird angezeigt, welche Rechte eine App verlangt. Ob die App alle aufgelisteten Rechte wirklich benötigt, muss der Benutzer selbst entscheiden, indem der Installationsvorgang abgeschlossen wird oder nicht. Es besteht also nicht die Möglichkeit, einzelne Rechte zu vergeben. Oft verlangen Apps nach Rechten, die sie zur Funktionserfüllung nicht brauchen. Dann besteht die Gefahr, dass Daten unberechtigt als Ware gehandelt werden sollen.

Momentan gibt es lediglich die Möglichkeit durch AppGuard[2], eine App zu installieren und den Zugriff trotzdem einzuschränken. AppGuard analysiert den Bytecode, deinstalliert die App und installiert diese mit Veränderungen neu. Die Veränderungen bestehen darin, dass Zugriffe auf Bytecode-Ebene entfernt werden. Es existieren Alternativen, die ein rooten des Gerätes voraussetzen. Davon ist allerdings dringend abzuraten. Da dadurch das Betriebsystem manipuliert wird und Sicherheitsmaßnahmen teilweises außer Kraft gesetzt werden.

Welche Rechte einzelne Apps nutzen, zeigen nicht nur die Apps der Security Software Anbieter, sondern auch Android OS. Dazu startet man den sog. App Drawer, er listet alle installierten Apps. Nahezu alle Geräte haben eine entsprechende Verknüpfung auf ihrem Startbildschirm. Ab Android OS 4 zieht man per drag & drop das Symbol der App im App-Drawer auf den Bereich App-Info im oberen Bildschirmbereich.

Alternativ werden die Berechtigungen auch im Google Play Store angezeigt. Dazu wählt man die entsprechende App aus und wechselt auf den Reiter Berechtigungen. So lassen sich auch nach Installation noch alle Berechtigungen ablesen.

Leider sind viele Benutzer von der Vielzahl an Rechten überfordert oder sogar genervt von den Hinweisen Berechtigungen zu prüfen. Dies hat zur Folge, dass Benutzer gedankenlos fragwürdige Apps installieren.

[2] http://www.backes-srt.de/produkte/srt-appguard/

# 4. Berufliche Nutzung

## 4.1. Anforderungen

Neben den Anforderungen an Geräte gibt es auch Rahmenbedingungen für die Nutzung als solche.

Wenn Smartphones für berufliche Zwecke eingesetzt werden sollen, müssen vorher eine Reihe von Festlegungen getroffen sein.

- Für welche Zwecke werden sie benötigt?
- Welche Apps werden für die Zwecke benötigt?
- Wie wird eine ausreichende Datensicherheit gewährleistet, d. h. wie werden die Datensicherheits-Standards für andere vom Arbeitgeber zur Verfügung gestellte Geräte bei den Smartphones analog durchgesetzt?
- Ist die Art und Weise der Nutzung geregelt?

Ausgangspunkt der Betrachtungen müssen die Daten sein. Wegen der rechtlichen Anforderungen an eine Auftragsdatenverarbeitung ist derzeit die Speicherung beruflicher Daten in einer Cloud nur dann möglich, wenn entsprechende Verträge vorliegen. Dies muss der für die Datenverarbeitung Verantwortliche prüfen. So dürfte in aller Regel das Speichern in der iCloud unzulässig sein.

Exkurs: Speichern verschlüsselter Daten in der Cloud
Es gibt auf dem Markt eine Reihe von Programmen, die Daten verschlüsselt speichern. Bei einigen Verfahren besitzt der Anbieter einen „Generalschlüssel“, mit dem er Daten entschlüsseln kann. In diesen Fällen müssen die Anforderungen an eine Datenverarbeitung im Auftrag erfüllt werden. Falls der Schlüssel nur auf Dienstgeräten, also bspw. dem Smartphone oder Tablet-PC, gespeichert wird, kann eine Speicherung in einer Cloud eventuell möglich sein. Dazu muss man sich aber vor Augen halten, dass das Verschlüsseln seine Aufgabe, Unbefugte an der Kenntnisnahme zu hindern, nur solange erfüllt, wie es keine Hintertüren gibt oder der Schlüssel nicht bekannt wird. Nur wenn diese Anforderungen erfüllt sind, kann davon ausgegangen werden, dass die Daten für den Anbieter nicht personenbezogen sind. Wenn also wegen technischer und organisatorischer Mängel die Verschlüsselung ihre Aufgabe nicht mehr erfüllen kann, muss die verantwortliche Stelle einen Zustand herstellen können, in dem keine Daten mehr beim Anbieter vorliegen; sie muss die ganze Zeit die Herrschaft über die Daten haben. Sie muss bei Zweifeln an der Güte der Maßnahme den Zugriff auf die verschlüsselten Daten kontrollieren können. D. h. es muss vertraglich sichergestellt sein, dass auf ihre Anforderung hin alle Daten, auch Kopien auf Sicherungsbändern, gelöscht werden. Ferner muss der Zugriff so reglementiert sein, dass es keine unbefugten Zugriffe, bspw. durch Dritte, auf die verschlüsselten Daten gibt. Nur so kann für die Dauer der Speicherung erreicht werden, dass die ergriffenen Maßnahmen ihre Wirkung entfalten.

Auch die Frage der Datensicherheit wirft eine Reihe von Problemen auf. Da Smartphones sehr oft außerhalb der Büros genutzt werden, ist das Risiko eines Verlusts oder Diebstahls auch sehr hoch. Die Geräte sind jedoch nicht so konstruiert, dass sie standardmäßig eine hohe Hürde gegen Angriffe von Hackern bieten. Daten auf verlorenen Geräten können relativ ausgelesen werden. Ferner müssen unbefugte Zugriffe über bösartige Apps oder andere Zugriffe aus dem Internet als Schwachstelle bei der Erstellung eines Sicherheitsheitskonzeptes betrachtet werden.

Es ist daher unbedingt erforderlich, ein Sicherheitskonzept zu erstellen. Dabei ist zu beachten.

- Es dürfen keine besonders schutzwürdigen Daten verarbeitet oder gespeichert werden.
- Die Datensicherheitsstandards der Behörde / des Unternehmens müssen auch bei Smartphones und Tablet-PCs eingehalten werden.
- Die Schnittstellen müssen kontrolliert werden.
- Daten müssen verschlüsselt gespeichert werden.
- Falls das Gerät verloren geht, muss es die Möglichkeit geben, die gespeicherten Daten aus der Ferne zu löschen.

## 4.2. Realisierung

Um eine große Zahl von Smartphones und Tablet-Computern sicher zu verwalten, ist es unbedingt notwendig ein Mobile Device Management System (MDM) einzusetzen. Mit ihm können bestimmte Sicherheitseinstellungen erzwungen werden. Dies betrifft bspw. die Länge und Komplexität von Passwörtern. Es kann auch erkannt werden, ob das Gerät sich in einem definierten Zustand befindet: kein Jailbreak / nicht gerootet, nur bestimmte Apps (s. u.). Wenn gegen diese Vorgaben verstoßen wird, kann das Gerät gesperrt werden oder sogar die Daten gelöscht werden. Diese Systeme nutzen spezielle APIs um bestimmte Sicherheitseinstellungen auf den Geräten zu erzwingen und zu überwachen. Android und iOS bieten erst seit der Version 4 eine vernünftige MDM-API. Die MDM API des nativen Android ohne Hersteller-Erweiterungen (Vanilla Android genannt), bietet nicht so viele Funktionen wie beispielsweise die API von iOS. Deshalb hat Samsung -der Hersteller mit dem größten Marktanteil im Androidmarkt- eine eigene MDM-Schnittstlelle entwickelt. Ein Mobile Device Management (MDM) benötigt einen sogenannten Agenten auf den jeweiligen Geräten, dessen Privilegien höher sein müssen, als die des Benutzers. Sonst können Sicherheitseinstellungen nicht erzwungen oder vorgeschrieben werden.

Auf Basis eines Sicherheitskonzeptes sind die Ziele für das MDM festzulegen. Folgende Punkte können eine Rolle spielen:

- Einheitliche Konfiguration für den gesicherten Zugang auf berufliche E-Mail, Kalender und Kontakte.
- Vollständige Verschlüsselung der Geräte.
- Zugang zum Firmen-/Behördeninternen Netzwerk nur mit gesichertem Zugang.
- Verschiedene Passwort-Richtlinien.
- Überwachung welche Geräte sich nicht in einem definierten Zustand befinden (Geräteklasse, Betriebsystem Version, Jailbreak, rooting, nicht erlaubte Apps usw.).
- Anwender Unterstützung bei Problemen.
- Definieren eines Maßnahmenkataloges, für den Fall, dass Anwender gegen Sicherheitsrichtlinien verstoßen.
- Fernlöschung bei Diebstahl, Verlust.
- Geregelte Software-(App)Verteilung (s.u.).
- Sicherheitsrichtlinien unveränderbar für Anwender.

#### 4.2.1. Software-Verteilung

Eine wichtige Funktion ist die Möglichkeit zu kontrollieren, welche Apps vorhanden sind. Nicht nur aus Gründen des Urheberschutzes greift eine Blacklist, bei der die installierten Apps gegen eine Liste verbotener Apps geprüft werden, zu kurz. Es gibt mehrere 100.000 Apps die installiert werden könnten. Zu keinem Zeitpunkt gibt es einen annähernd zuverlässigen Überblick, welche der Apps Schadroutinen haben; die Gefahr ist daher relativ groß. Außerdem sind nur wenige, vorgegebenen Zwecke zu erfüllen und somit auch eine überschaubare Anzahl geeigneter Apps. Es ist daher besser eine, eventuell großzügige, Liste erlaubter Apps vorzuhalten (whitelist). Aus dieser kann dann eine App installiert werden.

Bei der Software Verteilung gibt es einige Unterschiede zwischen iOS und Android.

Die Verteilung unternehmensinterner Software über den iTunes App-Store lässt Apple nicht zu. Um selbst Software über einen eigenen Webserver zu Verteilen, müssen Deployment Profile generiert und mit MDM auf den Geräten verteilt werden. Diese Profile erlauben die eigene Software Verteilung, sogar eine über MDM automatisierte Installation und Deinstallation. Dafür muss der Betreiber einen Enterprise Developer Account besitzen. Apple lässt aus Sicherheitsgründen nur registrierte Unternehmen zu diesem Programm zu.

Für Apps aus dem öffentlichen iTunes App-Store ist dies aber nicht möglich, da die Deployment Profile dieser Apps an die Benutzereigene Apple-ID gebunden sind. Somit wird eine zentrale Verteilung verhindert. Deshalb müssen Anwender solche Apps manuell installieren. In einigen MDM Systemen lässt sich ein App Katalog definieren mit Apps, die der Anwender dann individuell installieren kann. Der öffentliche iTunes App-Store kann aber nicht entfernt werden. So behält der Anwender weiterhin die Kontrolle über die App-Installationen. Eine echte Beschränkung durch MDM ist mit White-/Blacklisting nicht möglich, da durch MDM nur festgestellt werden kann, dass nicht erlaubte Apps installiert wurden. Eine entsprechende Reaktion im o.g. Maßnahmenkatalog ist unerlässlich.

Unter Android OS hingegen ist es mit MDM möglich, die Nutzung von Google Play durch den Benutzer zu unterbinden. Über die Einrichtung eines firmenspezifischen App Stores über MDM ist es möglich, dem Benutzer eine Whitelist von Apps anzubieten. Zusätzlich können Apps automatisiert installiert und deinstalliert werden.

#### 4.2.2. private Nutzung beruflicher Geräte

In diesem Punkt gibt es rechtlich keine wesentlichen Unterschiede zur bisherigen Praxis. Von der technischen Seite her gibt es keine Möglichkeit mehrere Benutzerkennungen anzulegen (mit Ausnahme von Tablet-Computern mit Android OS 4.2).

Viele MDM Anbieter versuchen dieses Problem mit sicheren Containern (Behälter) zu lösen. Das bedeutet, dass die beruflichen Daten (z.B. E-Mails, Kontakte, Kalender usw.) nicht mit den Standard-Apps des Gerätes verarbeitet werden. Dieser Container ist selbst eine App, die eine Anmeldung mit Passwort erfordert, alle Daten verschlüsselt abspeichert und vom MDM kontrolliert wird. So können berufliche Daten bei Bedarf gelöscht werden, ohne dass die privaten Daten betroffen sind.

In der Praxis entstehen bei den Anwendern Aktzeptanz-Probleme. Ist die Container-App nicht geöffnet, werden keine beruflichen E-Mails empfangen. Berufliche Termine mit Erinnerungen werden nicht gemeldet und Namen aus dem beruflichen Adressbuch von Anrufern werden nicht angezeigt. Anwender begreifen dieses Anwendungsverhalten als Fehler und sind nicht bereit – besonders wenn sie in der Hierarchie höher gestellt sind – zu akzeptieren, dass es sich um ein Leistungsmerkmal handelt und nicht um einen Fehler.

Es existieren auch Ansätze mit Virtualisierung zwei Systeme – ein privates und ein berufliches – auf einem Gerät zu betreiben. Dafür sind Änderungen am Betriebsystem notwendig. Deshalb existieren keine Lösungen für iOS aber für Android Systeme, da es sich um ein Open Source Betriebssystem handelt. Marktreife Produkte für Android sind in naher Zukunft zu erwarten. Diesen Lösungsansatz verwendet auch das Betriebsystem Blackberry 10.

Außerdem ist die Installation auf handelsüblichen Smartphones mit Problemen verbunden, weil Hersteller technische Hürden aufbauen, um zu verhindern, dass fremde Systeme aufgespielt werden.

Deshalb ist eine private Nutzung beruflicher Geräte ohne Container oder Virtualisierung nur mit einem umfassend durch MDM verwalteten Gerät möglich. Daher wird eine Kontrolle der beruflichen Nutzung zwangsläufig auch die private Nutzung tangieren. Dies muss in den Vereinbarungen berücksichtigt werden.

#### 4.2.3. Berufliche Nutzung privater Rechner (BYOD)

Unter dem Schlagwort BYOD (Bring your own device, Bringen Sie Ihr eigenes Gerät) wird derzeit diskutiert, ob und unter welchen Rahmenbedingungen private Rechner beruflich genutzt werden können. Der Schub kam durch die Verfügbarkeit von „schicken" Smartphones und Tablet-Computer im Privatkunden-Markt, die in der Bedienung einfacher waren als die vom Arbeitgeber zur Verfügung gestellten Geräte und die gerade in den oberen Führungsetagen viel Anklang finden. Dadurch lastet ein hoher Druck auf IT-Abteilungen, in kurzer Zeit diese Privatgeräte in das berufliche Umfeld einzubinden. Für die Nutzung dieser Geräte, die für die private Nutzung optimiert sind, wurde auch der Begriff „Consumerization" gewählt. BYOD steht demgegenüber für eine bewusste strategische Entscheidung, private Geräte für eine berufliche Nutzung zuzulassen.

Die dabei anstehenden Fragenkomplexe lassen sich nicht auf das Thema Datenschutz reduzieren, auch wenn sie zum großen Teil damit zusammenhängen. Es gibt eine Reihe von Anforderungen denen sich der Arbeitgeber stellen muss, damit er auch nur ansatzweise die ihm nach dem Datenschutzrecht und anderen Bereichen obliegende Verantwortung wahrnehmen kann. Hier sind beispielhaft zu nennen:

- Datenschutz, Datensicherheit, IT-Compliance
- Arbeitsrecht
- Urheberrecht
- Strafrechtliche Aspekte
- Allgemeine Haftungsfragen
- Ggf. Handels- und Steuerrecht

Allein schon die Themen Datenschutz und Datensicherheit bieten reichlich Zündstoff. So muss der Arbeitgeber einige Forderungen an den Arbeitnehmer richten. Dazu gehören u. a.

- Er muss sich verpflichten, sein Smartphone keinem Dritten zur Verfügung zu stellen.
- Die vorgegeben Sicherheitseinstellungen dürfen nicht geändert werden. Dies muss trotz der privaten Natur des Geräts durch eine technische Lösung erreicht werden.
- Die installierten Apps müssten ggf. vom Arbeitgeber abgesegnet werden.
- Es müssten ev. bestimmte Apps installiert werden.
- Der Arbeitgeber muss die Möglichkeit haben, seine Daten - auch aus der Ferne - zu löschen.

Der Arbeitnehmer muss diese Einschränkungen seiner Verfügungsgewalt über das eigene Smartphone / den Tablet-PC akzeptieren.

Es gibt derzeit Versuche, eine Trennung der privaten und der beruflichen Nutzung durch technische Maßnahmen zu erreichen, da dieser Anwendungsfall von iOS und Android nicht vorgesehen ist. Die oben genannten Ansätze mit Containern oder Virtualisierung existieren. Das Angebot an Lösungen ist so schnelllebig wie der Markt der Mobilen Geräte selbst.

Um die Problematik mit Virtuallisierung zu lösen, müsste ein neues Betriebsystem auf den Privatgeräten installiert werden. Dieser Eingriff kann den Besitzern nicht zugemutet werden. Wird für die nicht private Nutzung eine Lösung mit einem Container gewält, wird die Funktionalität des Endgerätes auf die Leistungsfähigkeit des Containers begrenzt. D.h., hat der Container keinen Viewer für E-Mail Anhänge, können diese nicht betrachtet werden. Lässt der Container zu, dass berufliche Daten ihn verlassen, um beispielsweise einen Anhang anzuzeigen, ist er nicht geeignet. Private und berufliche Daten müssen getrennt bleiben. Eben diese strikte Trennung ist als 3. Alternative mit einem durch MDM umfassend verwalteten Gerät ebenfalls nur schwer zu realisieren.

Ob die verfügbaren Produkte und technischen Ansätze geeignet sind, die Trennung wirksam sicherzustellen, muss durch unabhängige Stellen geprüft werden. Dies steht noch aus.

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) befasst sich ebenfalls mit dieser Thematik. Ein Überblickspapier zu Consumerisation und BYOD wurde Anfang 2013 veröffentlicht. Darin sind eine Reihe von Szenarien betrachtet und Anforderungen formuliert, die unbedingt umgesetzt sein müssten. Es wäre wünschenswert, wenn die Überlegungen in Maßnahmenempfehlungen im Grundschutzkatalog des BSI einfließen.

Vor dem Hintergrund der rechtlichen und technischen Probleme ist ein datenschutzkonformer Einsatz wohl – noch – nicht möglich. Lediglich Daten die zwangsläufig in den privaten Bereich ausstrahlen, hier sind beispielhaft Termine zu nennen, können auch jetzt schon mit den vorhandenen Lösungen für BYOD auf dem privaten Gerät verarbeitet werden. Der Datenumfang muss dann soweit wie möglich reduziert sein und bei einer unbefugten Kenntnisnahme dürfen keine Beeinträchtigungen der gesellschaftlichen Stellung oder wirtschaftlichen Verhältnisse der Betroffenen zu erwarten sein.