Lehrstuhl Managementinformationssysteme (MIS) der
Fakultät für Informatik (FIN) der
Otto-von-Guericke Universität Magdeburg

Masterarbeit

Mobile Endgeräte und deren nachhaltiger Umgang am Ende ihrer Lebenszeit unter Berücksichtigung von Sicherheitsrichtlinien in Organisationen

Autor: Artur Borodatyy

Studiengang: Wirtschaftsinformatik (M.Sc.)

Gutachter: 1. Prof. Dr. Hans-Knud Arndt
2. Prof. Dr. Jana Dittmann

Datum: 01.07.2014

Borodatyy, Artur:

Mobile Endgeräte und deren nachhaltiger Umgang am Ende ihrer Lebenszeit unter Berücksichtigung von Sicherheitsrichtlinien in Organisationen

Masterarbeit, Otto von Guericke Universität Magdeburg, 2014.

Selbständigkeitserklärung

Hiermit erkläre ich, dass ich die vorliegende Masterarbeit selbstständig verfasst und keine anderen als die angegebenen Quellen und erlaubten Hilfsmittel benutzt habe. Weiter erkläre ich, die Masterarbeit in gleicher oder ähnlicher Form keiner anderen Prüfungsbehörde vorgelegt zu haben.

Kaufbeuren, den 01.07.2014 Artur Borodatyy

Abstract

Immer mehr Beschäftigte der Organisationen nutzen mobile Endgeräte im geschäftlichen Alltag. Dies geschieht entweder mit Organisationseigenen oder mitgebrachten (BYOD) Geräten. Doch irgendwann erreichen sie die Ende der Nutzungszeit und müssen ausgemustert werden. Ein Überblick zeigt, wie in Organisationen mit mobilen (Alt-)Geräten am Ende ihrer Nutzungszeit verfahren wird: die mobile Endgeräte werden entweder weitergenutzt (Zweitnutzung) oder endgültig stillgelegt. Dabei existieren mehrere Szenarien. Bei Weiternutzung können Organisationen die Geräte Verkaufen, Spenden oder als Not-Gerät behalten. Bei Außerbetriebssetzung können Geräte noch für Teile gelagert oder endgültig Entsorgt werden. Nach einer Untersuchung und Analyse werden folgende Nachhaltige schritte empfohlen: gekaufte mobile Endgeräte möglichst lange nutzen, Geräte mit geringer elektromagnetischer Strahlung (SAR-Wert kleiner 0,6 W/kg) nutzen, mobile (Alt)Geräte sachgerecht bei der kommunalen Sammelstelle entsorgen und wenn möglich Aufrüsten statt neu kaufen. Zur Sicherheit wird folgendes empfohlen: Sicherheitsrichtlinien einführen, Festplatten sicher formatieren und evtl. verschlüsseln, Netzwerkverbindungen verschlüsseln (z.B. mit WPA2), Backup regelmäßig durchführen, nur sichere Apps installieren, Geräte durch Passwort sperren, MDM-Lösung einführen und BSI-Empfehlungen zu beachten.

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

Abkürzungsverzeichnis

APP	Applikation
BSI	Bundesamt für Sicherheit in der Informationstechnik
BYOD	Bring Your Own Device
DMZ	Demilitarized Zone
ERP	Enterprise-Resource-Planning
ISO	International Organization for Standardization
LTE	Long Term Evolution
MDM	Mobile Device Management
OMA	Open Mobile Alliance
SaaS	Software as a Service
SAR	Spezifische Absorptionsrate
SSL	Secure Sockets Layer
TK	Telekommunikationstechnologie
UMPC	Ultra-Mobile PC
VoIP	Voice over IP
VPN	Virtual Private Network
WPA	Wi-Fi Protected Access

1. Einleitung

1.1. Hintergrund

Die mobilen Endgeräte wie Smartphones, Tablets und Notebooks gehören immer mehr selbstverständlich zu unserem Alltag.[1] Dies lässt sich anhand von Kennzahlen zur Entwicklung der mobilen Datenvolumen darlegen. Die Abbildung 1 zeigt eine Statistik zum mobilen Datenverkehr weltweit in den Jahren 2011 bis 2014 und eine Prognose bis 2016.[2] Laut dieser Statistik steigt der jährliche mobiler Internettrafik signifikant von Jahr zu Jahr.

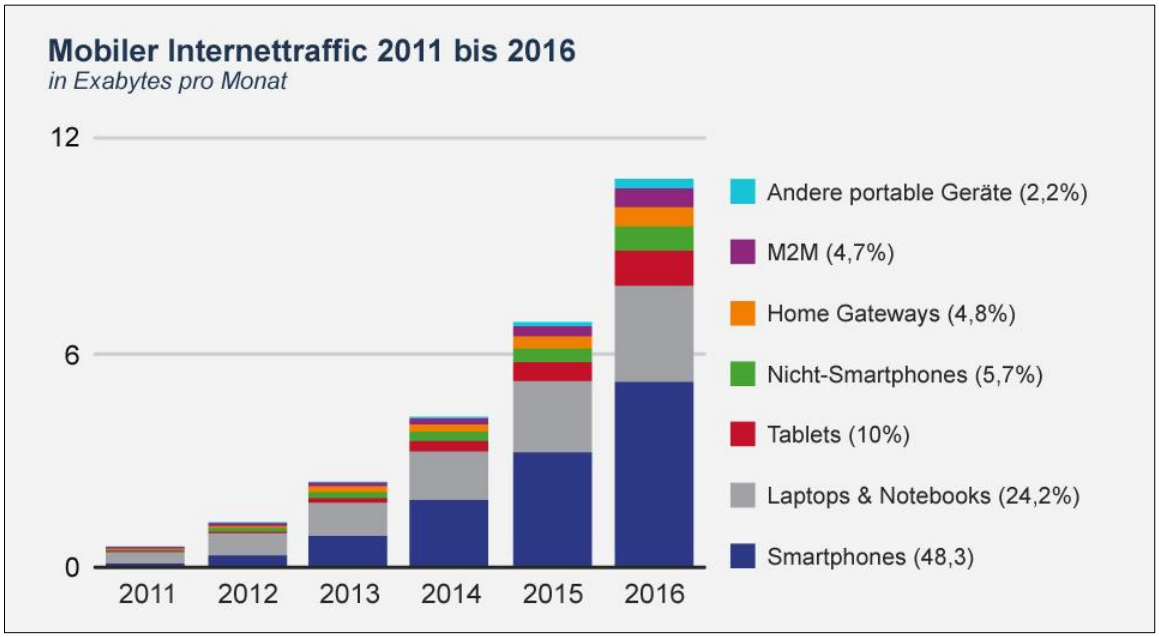


Abbildung 1: Kennzahlen zur Entwicklung des mobilen Datenvolumens bis 2016[3]

Auch die Funktionsnutzung z.B. der Smartphone-Nutzer hat sich verändert (siehe Abbildung 2). So ist der Zugang zum Internet für die meisten Smartphone-Nutzer inzwischen die wichtigste Funktion - knapp vor dem Telefonieren. Die mobilen Endgeräte begleiten uns täglich. Durch die Nutzung von einfachen und praktischen Diensten, wie zum Beispiel der Navigation, den Nachrichten- oder Kommunikationsdiensten, sind die mobile Endgeräte endgültig im Alltag des Menschen angekommen.[4]

[1] J. Dahms (2014)
[2] statista (2014)
[3] statista (2014)
[4] mobile zeitgeist (2010)

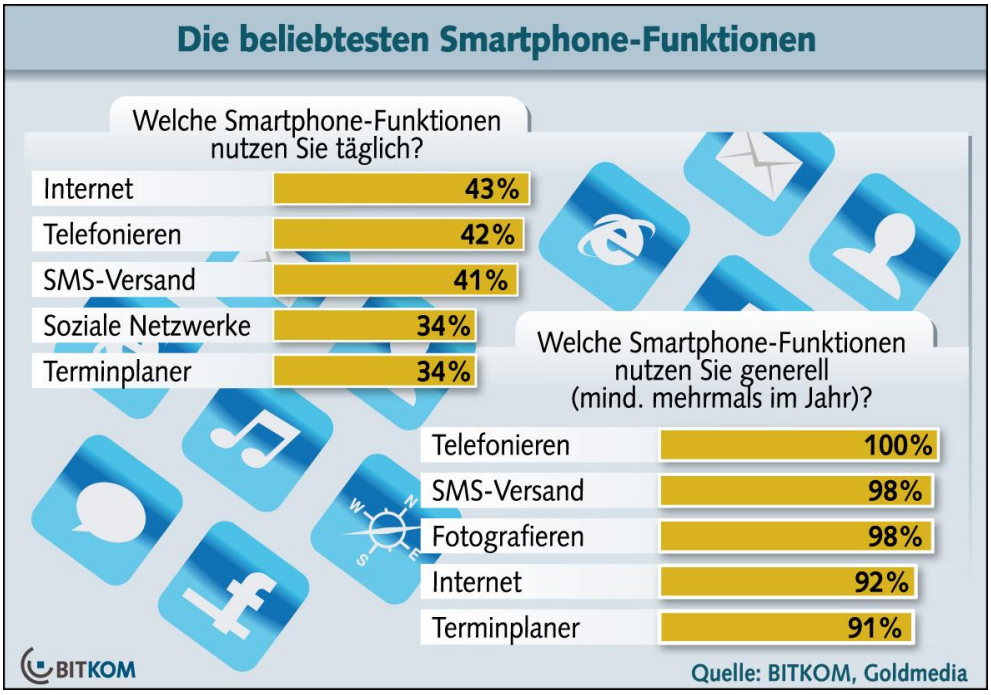


Abbildung 2: Die beliebtesten Smartphone-Funktionen[5]

Ebenso ist die Verfügbarkeit des Mediums Internet heutzutage annähernd flächendeckend gegeben. Damit steigt die Bedeutung des Internets als zentraler Kanal der Organisationskommunikation. Das Internet wird intensiv auch von Organisationen und ihren Zielgruppen als Informations- und Kommunikationsplattform genutzt.[6] Immer mehr Organisationen bieten ihren Mitarbeitern für die Kommunikation Smartphones oder Tablets an. Vor allem größere Organisationen mit mehr als 250 Beschäftigten stellen tragbare Geräte zur Verfügung (91%). In kleinen Unternehmen mit weniger als 50 Angestellten ist es immerhin noch knapp die Hälfte (48%). Bei weniger als zehn Angestellten sind es dagegen erst 31%. Dabei wird ihnen neben dem Zugriff auf das öffentliche Internet auch der Zugang zum unternehmenseigenen E-Mail-System (72%), auf interne Dokumente (44%) und Firmen interner Software gewährt.[7]

Durch vielseitigen Funktionsumfang der heutigen mobilen Endgeräte können diese für viele Organisationen mit verschiedenen Aufgaben nutzbar sein und eingesetzt werden. Die verschiedenen Endgeräte (z.B. Smartphones, Tablets, Notebooks etc.)

[5] BITKOM (2012a)
[6] H. Duschinski (2007, S. 7)
[7] Haufe Online Redaktion (2012)

können zum Beispiel für folgende Zwecke und Funktionen bei einer Organisation eingesetzt werden:

- unterwegs abrufen der Firmen E-Mails
- arbeiten außerhalb vom Büro, wo Mobilität gefragt ist
- Hilfe von individuellen Programmen an bestimmten Orten.

1.2. Motivation

Durch häufige und vielseitige Nutzung der Datendienste von mobilen Endgeräten entstehen in der Regel große Mengen von Daten an, wobei auch vertrauliche Daten von Privatpersonen oder Organisationen gespeichert werden. Bei den vielen Vorzügen und Funktionen der mobilen Geräte muss man aber auch an die sichere Verwaltung der Geräte denken, um beispielsweise Unternehmen vor Manipulation oder Industriespionage zu schützen.[8] Ebenso sollen die Sicherheitsrichtlinien der Organisation nicht verletzt werden.

Ob Handy, Computer oder Fernseher - alle technischen Geräte werden irgendwann alt oder gehen schlicht kaputt und müssen ausgemustert werden, sie erreichen die Ende der Nutzungszeit.[9] An dieser Stelle können zwei Probleme für Organisationen auftreten: Nachhaltigkeit und Sicherheit. Da Organisationen mitunter versuchen langlebig mit Ressourcen umzugehen, worunter auch mobile Endgeräte zählen, sollen diese auch mit mobilen Endgeräten am Ende der Nutzungszeit nachhaltig umgehen. Gleichzeitig sollen aber auch die Sicherheitsrichtlinien der Organisationen eingehalten werden, auch nach Ende der Nutzungszeit.

Mit Anteilswachstum der mobilen Endgeräte in Organisationen wächst auch der organisatorische Aufwand in Organisationen, wie zum Beispiel:

- das Einrichten der Geräte für die Netzwerke der Organisation
- das Einrichten von Applikationen der Organisation
- die Verwaltung der vergebenen oder privaten Geräte
- das Verwalten von Rechten und Zugriffen auf die Daten der Organisation
- die Pflege und evtl. Reparaturen

[8] J. Dahms (2014)
[9] A. Sokolow (2011)

- die Aktualisierung für bessere Sicherheit
- die Rückgabe
- die sichere Entsorgung

Einige Punkte der Aufwendungen, wie zum Beispiel die Verwaltung der privaten Geräte, haben einen direkten Einfluss auf die Sicherheit und/oder auf die Nachhaltigkeit in Organisationen. Somit ergibt sich ein Spannungsfeld zwischen dem nachhaltigen Umgang mit mobilen Endgeräten und den Sicherheitsbedürfnissen von Organisationen.

1.3. Zielstellung

Die Etablierung und Aufrechterhaltung von IT-Sicherheits- und Nachhaltigkeits-management ist ein komplexer und komplizierter Prozess, der durch die Verwendung bewährter Verfahren beschleunigt und verbessert werden kann. Solche bewährten Verfahren werden in der vorliegenden Arbeit dargestellt und liefern beispielsweise Methoden und Anforderungen an ein leistungsfähiges Managementsystem für IT in Organisationen, aber auch Beschreibungen von Maßnahmen und Checklisten für deren Implementierung.[10]

Das Ziel dieser Masterarbeit ist es, einen Überblick zu erarbeiten, wie in Organisationen mit mobilen (Alt-)Geräten am Ende ihrer Nutzungszeit verfahren wird. Dabei soll die Frage beantwortet werden, ob und inwieweit die Sicherheitsrichtlinien einer Organisation die Nachhaltigkeitsstrategie beeinflussen. Zudem sollen mögliche Maßnahmen für eine Verbesserung der Nachhaltigkeitsstrategie, unter Berücksichtigung der existierenden Sicherheitsbedürfnisse, aufgezeigt werden.

Als Ergebnis und Antwort auf die Hauptfrage der Masterarbeit werden Empfehlungen erarbeitet mit dessen Hilfe die Organisationen die eigene nachhaltige Nutzung von mobilen Endgeräten verbessern und anpassen können.

[10] J. Hofmann, W. Schmidt (2010, S. 297 f.)

1.4. Aufbau der Arbeit

Im nächsten Kapitel (2. Grundlagen) werden mehr Informationen über die Thematik der mobilen Endgeräte dargestellt. Es wird versucht mehr in die Thematik und Problemstellung der Masterarbeit einzuführen. Außerdem werden hier die Begriffe „Endgerät“, „mobile Endgeräte“, „Betriebssysteme“, „Produktlebenszyklus“, „Obsoleszenz“, „Nachhaltigkeit“ und „Ökobilanz“ festgelegt und definiert.

Ein Überblick über den Einsatz, Nutzen und Gefahren der mobilen Endgeräte in Organisationen wird in Kapitel 3 (Mobile Endgeräte in Organisationen) aufgestellt. Ebenso wird hier beschrieben, wie die Verwaltung der mobilen Endgeräte in Organisationen realisiert werden kann. Außerdem wird hier die andere Möglichkeit mobile Endgeräte in Organisationen zu nutzen beschrieben – mitgebrachte private Geräte.

Der nachhaltige Umgang mit mobilen Endgeräten in Organisationen wird in Kapitel 4 (Nachhaltigkeit bei mobilen Endgeräten) beschrieben. In den Unterkapiteln wird versucht die Problematik der Faktoren, die auf die nachhaltige Nutzung der mobilen Endgeräte beeinflussen, genau zu untersuchen. Hier werden Problempunkte wie Produktlebenszyklus, Produktunterstützung durch den Hersteller, Aufbau der Geräten und Sollbruchstellen beschrieben und untersucht. Ebenso spiel hier die Ökobilanz und die Entsorgung von mobilen Endgeräten eine Rolle.

Um ein Überblick zu erarbeiten, wie in Organisationen mit mobilen (Alt-)Geräten am Ende ihrer Nutzungszeit verfahren wird, wird in Kapitel 5 (Ende der Nutzung) eine Literaturrecherche und ein persönliches Interview mit Geschäftsführer der Green Power GmbH Herrn Olrik Thonig durchgeführt. Nach der Grundlegender Analyse der Nutzungsmöglichkeiten der mobilen Endgeräte in Organisationen am Ende der Nutzungszeit werden hier mögliche Szenarien beschrieben und aufgestellt.

Nach den möglichen Szenarien der Nutzungsmöglichkeiten der mobilen Endgeräte in Organisationen am Ende der Nutzungszeit werden in Kapitel 6 (Sicherheit) jetzt auch die Sicherheitsaspekte aufgestellt. Hier werden die Gefahren der mobilen Endgeräte am Ende der Nutzungszeit mit Blick auf die Organisationseigene und mitgebrachte

mobile Endgeräte aufgestellt. Außerdem wird hier versucht auch die Sicherheitsrichtlinie für Organisationen aufzustellen.

Damit die Organisationen nachhaltiger und sicher mit mobilen Endgeräten am Ende ihrer Nutzungszeit umgehen können, wird in dem Kapitel 7 (Empfehlungen) versucht aus der Nachhaltigkeits- und Datensicherheitsperspektive Empfehlungen an Organisationen zu geben.

Abschließend, nach Recherchen, Interview, Untersuchungen, Auswertungen und Analysen, wird die gesamte Arbeit in dem Kapitel 8 (Zusammenfassung) noch mal zusammen gefasst und abgeschlossen.

2. Grundlagen

2.1. Die Endgeräte

Das Internet kann heutzutage mit verschiedenen Endgeräten genutzt werden. Unter einem Endgerät, oder auch Teilnehmerstation, versteht man in der IT und der Telekommunikationstechnologie (TK) ein Gerät (zum Beispiel ein PC, ein Telefon oder ein Anrufbeantworter), welches an einen Netzabschluss eines öffentlichen oder privaten Daten- oder Telekommunikationsnetzes angeschlossen ist.[11]

Die Vielfalt und die Art der Endgeräte sind sehr groß. Ein zentrales Endgerät wird der PC sein, weil er das am weitesten verbreitete Internet-Endgerät ist. Als Endgeräte kommen jedoch nicht nur PCs, sondern auch andere internetfähige Endgeräte wie Smartphones und TV-Geräte in Frage.[12] Die wichtigsten Endgeräte neben einem PC sind derzeit: Mobiltelefone, Smartphones, Tablets, Notebooks und Subnotebooks. Daneben gibt es Endgeräte mit sehr speziellem Einsatzgebiet, wie z.B. E-Book-Reader, TV-Geräten, Spielkonsolen, Smartwatch oder Spezialgeräte zur mobilen Datenerfassung. Als internetfähige Endgeräte (mobile Systeme) sind ebenfalls moderne Fahrzeuge mit ihrer Informationstechnik anzusehen.[13] Zum Beispiel durch den Einsatz von Board-Computern mit integrierten Navigationssystemen und SOS-Assistenten mit Internetverbindung.

Die Klassifikation der Endgeräte ist von unterschiedlichen Eigenschaften abhängig, wie z.B. der Größe von Gehäuse oder Display oder der Ausstattung mit bestimmter Hardware.[14] Da der Focus dieser Arbeit auf der Bearbeitung des Themas in Bezug auf mobile Endgeräte liegt, wird die Untersuchung der Definition auf die mobile Endgeräte fokussiert.

2.2. Mobile Endgeräte

2.2.1. Definition

[11] ReeseOnline (2014)
[12] H. Schwichtenberg (2000, S. 64)
[13] Bundesamt für Sicherheit in der Informationstechnik (2014)
[14] mobile zeitgeist (2010)

Die Geschichte mobiler Endgeräten reicht bis in die fünfziger Jahre zurück und begann mit den damals für den medizinischen Bereich entwickelten Pagern. Ende der siebziger Jahre kamen dann die ersten Mobiltelefone auf den Markt. Damals noch groß und unhandlich und damit für die mobile Nutzung außerhalb von Fahrzeugen eigentlich ungeeignet, haben sie sich zu einem Standard in der heutigen Zeit entwickelt, ebenso wie Anzahl an Gerätetypen.[15] Es gibt einige Ansätze mobile Endgeräte zu klassifizieren. Einige verstehen darunter Mobiltelefone, PDAs und Smartphones und andere wiederum weiten diesen Begriff auf Notebooks und Subnotebooks aus.[16] Unter mobilen Endgeräten versteht man grundsätzlich all diejenigen Geräte, die für den mobilen Einsatz konzipiert sind.[17]

Ein mobiles Endgerät ist ein singuläres mit Prozessoren ausgestattetes elektronisches Gerät das a) meistens drahtlos und mittels Batterie(n) an jeden beliebigen Ort transportiert werden kann, b) während des Transports (ohne zusätzliche Stützfläche) benutzt werden kann, c) über integrierte Ein- und Ausgabemodalitäten (z.B. Bildschirm, Tastatur, etc.) verfügt und d) alle Komponenten in einem Gehäuse vereint.[18] Die Klassifizierung erfolgt entsprechend der drei festgelegten Kriterien: Transportfähigkeit, Ablagefläche und Konnektivität. Dies inkludiert Form, Maße und Gewicht des Endgerätes. Es wird unterschieden, ob das Gerät eine feste Unterlage benötigt, in der Hand bedient werden kann, oder ob das Endgerät den menschlichen Körper selbst benötigt. Generell kann zwischen a) nicht-netzwerkfähigen mobilen Geräten, b) mobilen Geräten mit einer kabelgebundenen Verbindung und c) mobilen Geräten mit einer drahtlosen Konnektivität unterschieden werden.[19]

Es lassen sich die folgenden drei übergeordneten Geräteklassen ableiten: 1.) Transportable Geräte, 2.) Mobile Geräte und 3.) Wearables (tragbare Computersystemen). Die einzelnen Gerätetypen lassen sich den übergeordneten Geräteklassen zuordnen (cluster). Die überlappenden Kreise (siehe Abbildung 3) verdeutlichen die Ähnlichkeiten bzw. Verwandtschaften der einzelnen Gerätetypen.

[15] D. Kaczmarek (2005, S. 16)
[16] D. Krannich (2010, S. 42)
[17] T. Logara (2007, S. 73)
[18] D. Krannich (2010, S. 37)
[19] D. Krannich (2010, S. 42)

Es lassen sich, wie in Abbildung 3 dargestellt, die einzelnen Gerätetypen in die folgenden Gruppen zusammenfassen: Laptops, Ultraportable PCs, Ultramobile PCs und Mobile Kommunikationsgeräte[20]

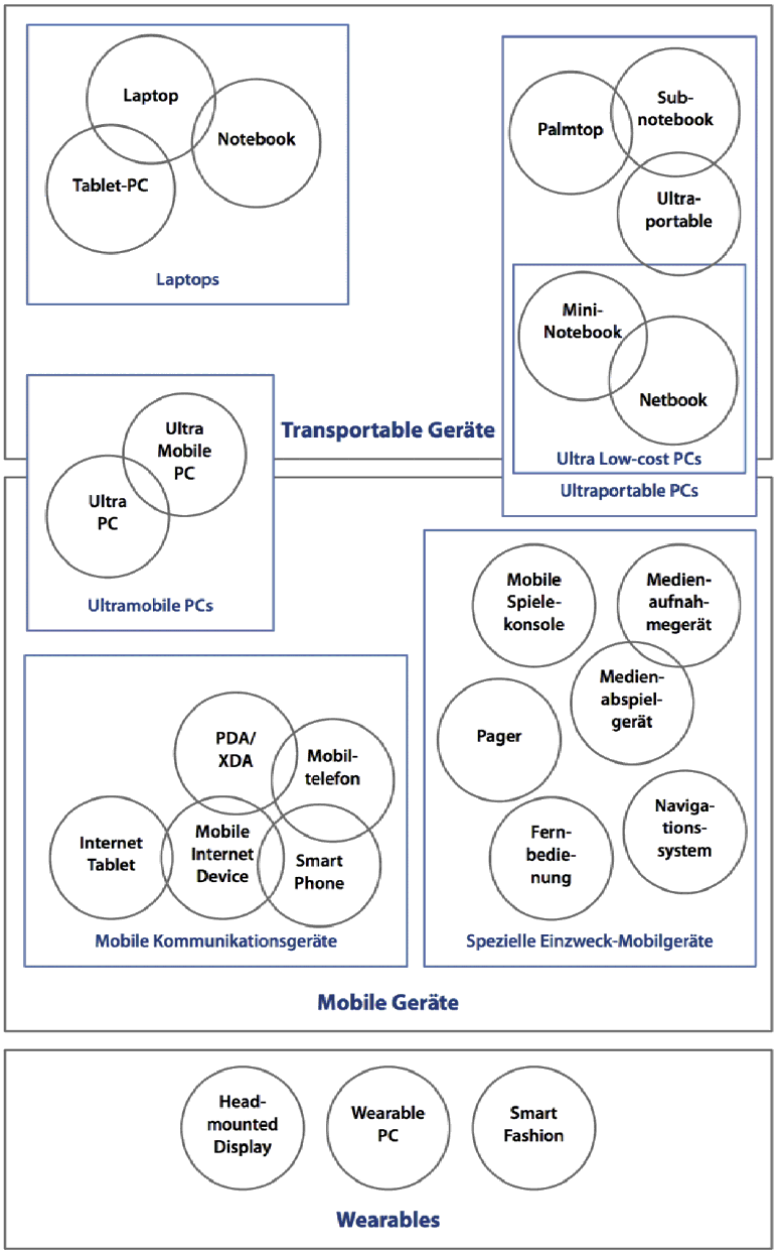


Abbildung 3: Mobile Geräteklassen: Gruppierung der Gerätetypen[21]

Im Gegensatz zu Desktop-Anwendungen unterscheiden sich mobile Endgeräte besonders in den Punkten: 1.) der Gestaltung und Informationsdarstellung, 2.) der

[20] D. Krannich (2010, S. 43)
[21] D. Krannich (2010, S. 44)

Art und Motivation der Benutzung, 3.) dem Kontext (vor allem räumlich und sozial), 4.) den Ein- und Ausgabemodalitäten und 5.) der Interaktion.[22]

Laut Analyse von Krannich lassen sich im weiteren Schritt daraus sechs untergeordnete Geräteklasen ableiten (siehe Abbildung 4), die vereinzelt die übergeordneten Geräteklassen überlappen, das heißt beispielsweise, dass ein Ultramobile PC aufgrund seine Größe auch ein Bestandteil der transportablen Geräte sein kann und umgekehrt.

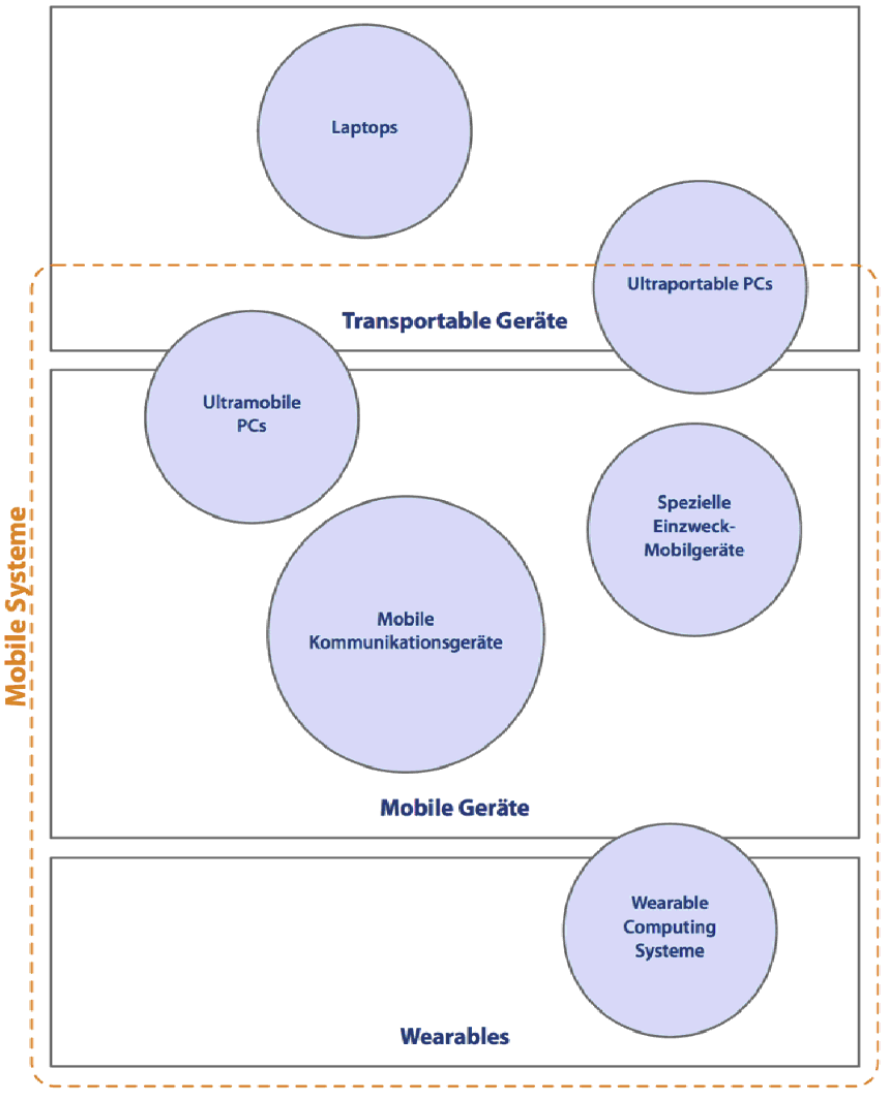


Abbildung 4: Mobile Geräteklassen: Über- und Untergeordnete Geräteklassen[23]

Bei der Analyse von Krannich ist es zu erkennen, dass die Notebooks abgegrenzt werden und nicht zu mobilen Endgeräten zählen.

[22] D. Krannich (2010, S. 37)
[23] D. Krannich (2010, S. 45)

Wie schon geschrieben, es gibt verschiedene Ansätze mobile Endgeräte zu klassifizieren. Laut Bundesamt für Sicherheit in der Informationstechnik werden z.B. Notebooks doch zu mobilen Endgeräten zugeordnet. Die wichtigsten mobile Endgeräte laut BSI sind derzeit: Mobiltelefone, Smartphones, PDAs, Tablets und Notebooks.[24]

2.2.2. Nutzung

Die mobilen Endgeräte ersetzen die großen Endgeräte dabei keineswegs. Vielmehr werden sie zusätzlich genutzt. Wer also mit dem Smartphone im Internet surft bzw. Apps nutzt oder mit dem Tablet online geht, verzichtet deshalb nur selten auf Desktop oder Laptop. Welches Gerät zum Einsatz kommt, ist jeweils abhängig von den genutzten Inhalten.[25] Interessant ist auch der Wandel der Endgeräte-Präferenz im Laufe des Tages (siehe Abbildung 5).[26] So erhöht sich die Aktivität der Seitenaufrufen oft per Smartphones morgens, Laptops oder PCs tagsüber und Tablets abends.

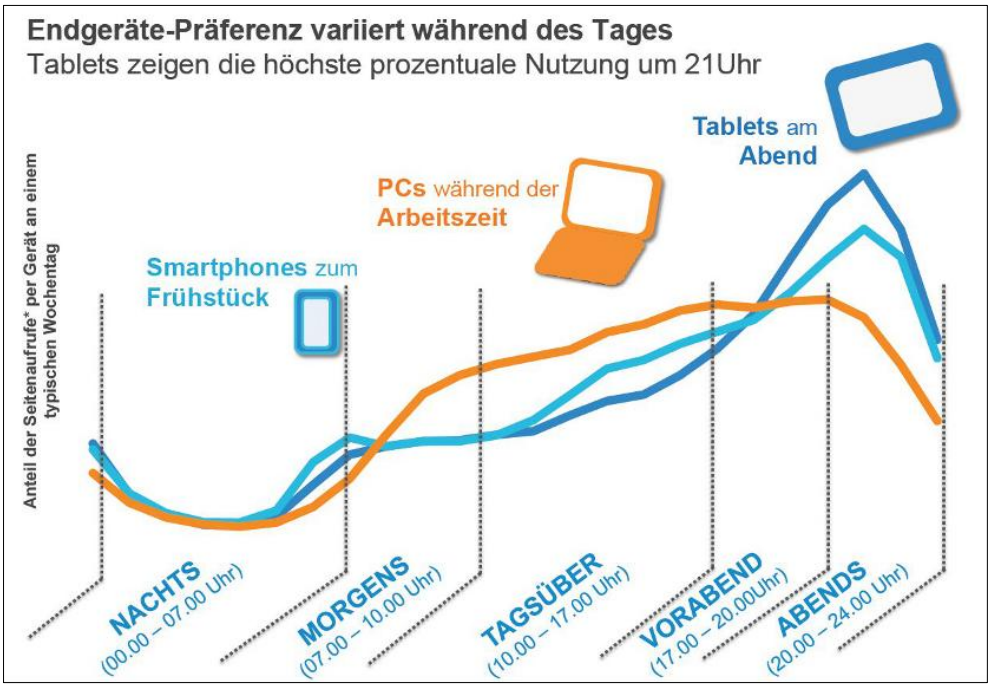


Abbildung 5: Endgeräte-Präferenz[27]

[24] Bundesamt für Sicherheit in der Informationstechnik (2014)
[25] Haufe Online Redaktion (2013)
[26] Jan Kirchner (2013)
[27] Jan Kirchner (2013)

2.2.3. Betriebssysteme

Ein Betriebssystem ist die Software, die die Verwendung (den Betrieb) eines Computers ermöglicht. Es verwaltet Betriebsmittel wie Speicher, Ein- und Ausgabegeräte und steuert die Ausführung von Programmen.[28] In mobilen Endgeräten kommen spezielle Betriebssysteme zum Einsatz. Die Konzepte der Betriebssysteme für mobile Endgeräte sind denen der PCs sehr ähnlich. Ihre Umsetzung unterscheidet sich allerdings von den Vertretern stationärer Geräte, da sie zum Beispiel spezielle Benutzungsschnittstellen und ein aufwändiges Energiemanagement unterstützen müssen. Üblicherweise werden Kommunikationsverfahren, wie etwa GSM, UMTS, LTE, Bluetooth und / oder WLAN, unterstützt. Daneben werden spezielle Dateisysteme eingesetzt, die den Anforderungen an den Betrieb von Flash-Speichern und dem Starten von Anwendungen ohne langen Ladevorgang gerecht werden. Das Konzept des virtuellen Speichers wird, wenn überhaupt vorhanden, meist anders umgesetzt, so dass weniger Speicher pro Anwendung verwendet wird.[29] Die Hersteller verwenden entweder eigene Entwicklungen oder lizenzieren ein existierendes Betriebssystem. Auf dem Markt mobiler Endgeräten haben sich die folgenden Betriebssysteme (alphabetische Reihenfolge) etabliert:[30]

Betriebssystemname	**Hersteller**	**Aktuelle Version**
Android	Google und Open Handset Alliance	4.4 (KitKat)
BlackBerry OS	RIM	7.1
iOS	Apple	7.1
OS X	Apple	10.9.3
Windows	Microsoft	8.1
Windows Phone	Microsoft	8.0

Tabelle 1: etablierte mobile Betriebssysteme[31]

[28] U. Baumgarten, H.-J. Siegert (2009, S. 3)
[29] Bundesamt für Sicherheit in der Informationstechnik (2006, S. 7)
[30] D. Krannich (2010, S. 51)
[31] D. Krannich (2010, S. 51 f.)

Die Architektur Mobiler Endgeräten besteht aus den folgenden vier Schichten (von oben nach unten):

Abbildung 6: Architektur Mobiler-Systeme[32]

Android

Der Softwarehersteller Android Inc. wurde 2005 von Google gekauft und zusammen mit 34 anderen Anbietern von Software und Hardware sowie Telekommunikationsdiensten wurde 2007 die "Open Handset Alliance" gegründet. Ein Jahr später, im Jahre 2008, veröffentlichen die "Open Handset Alliance" die erste offizielle Open-Source Version von Android. Aufgrund der Tatsache, dass Andorid als Open-Source verfügbar ist, gibt es zahlreiche Entwickler alternativer Betriebssysteme. So passen viele Hardwarehersteller die auf ihren mobilen Endgeräten installierte Android Version ihrer Hardware an. Derzeit verwendet jede dieser Android Versionen den Linux-Kernel 2.6. Die Hersteller der mobilen Endgeräte bauen häufig das Standard "Open Mobile Alliance Device Management" (OMA DM) in ihre Version des mobilen Betriebssystems ein, um "Mobile Device Management"-Herstellern (MDM) mehr Sicherheitsfunktionen zu bieten.

[32] D. Krannich (2010, S. 38)

Programme (Apps) laufen unter Android aus Sicherheitsgründen isoliert voneinander und können auch nur unter strikten Sicherheitsbeschränkungen auf System Ressourcen oder Hardware zugreifen. Die Entwicklung von Apps findet gegen eine Java-ähnliche API statt, die vom Umfang der Bibliotheken zwischen Java SE und Java ME angesiedelt ist. Entwickelt werden kann unter Windows, Mac OS X oder Linux.[33]

BlackBerry OS

Das vom kanadischen Unternehmen BlackBerry (ehem. Research in Motion) entwickelte Betriebssystem BlackBerry OS kommt ausschließlich auf den gleichnamigen Smartphones zum Einsatz. Der BlackBerry ist ein stark auf den Geschäftseinsatz ausgelegtes Smartphone mit Fokus auf Schreiben und Lesen von E-Mails und hohen Sicherheitsstandards (256-Bit Verschlüsselung des Datenverkehrs und am Gerät). Als Weiterentwicklung von PlayBook Os wurde 2013 das neue Betriebssystem BlackBerry 10 vorgestellt. BlackBerry 10 positioniert sich als Betriebssystem mit höchsten Sicherheitsansprüchen und einem Komfort, der mit Konsumentengeräten vergleichbar ist. Eine neuartige Funktion von BlackBerry 10 ist BlackBerry Balance. Damit ist es möglich, private Daten getrennt von geschäftlichen Daten am selben Gerät aufzubewahren. BlackBerry möchte damit eine saubere und sichere Trennung zwischen geschäftlicher und privater Nutzung erreichen. Mit BlackBerry 10 wurde der Markt für Entwickler weit geöffnet, und es werden eine Reihe von Technologien (C, C++, HTML5 WebWorks, Adobe Air Actionscript, Java für BlackBerry Apps und als Emulator für Android Apps) zur Entwicklung von Apps unterstützt.[34]

OS X

Apples OS X stammt von dem Ur-Unix „Vi“ ab, das 1971 von AT&T entwickelt wurde. Aus dem Ur-Unix wurde BSD-Unix entwickelt, welches den „Match Mikrokernel“ beinhaltete. Das ist ein Betriebssystemkern mit einem bewusst klein und übersichtlich gehaltenen Funktionsumfang. Um 1988 entwickelte das Unternehmen NeXT unter der Leitung von Steve Jobs mit dem Match Mikrokernel und der

[33] B. Wieczorek (2013, S. 11 f.)
[34] T. Sammer u.a. (2014, S. 152)

Programmiersprache Objective-C das Betriebssystem „Nextstep“. 1996 wurde das Unternehmen von Apple gekauft und entwickelte aus Nextstep die erste Version von Mac OS X.

iOS

Für das iPhone und iPad wurde Max OS X angepasst und von Apple iOS genannt. Im weiteren Verlauf der Entwicklung wurde ab der iOS 4 Version über 1500 neue APIs für Entwickler freigegeben, die umfangreiche Funktionen für das zentrale MDM ermöglichen.

Die Optimierung des Betriebssystems für den mobilen Einsatz führte dazu, dass Apple einige Restriktionen einbauen musste, damit die Sicherheit des mobilen Endgerätes nicht kompromittiert werden kann. So sind in einem nicht modifizierten iOS die Apps gegenüber anderen Apps sowie dem Kern des Betriebssystems isoliert und haben keinen Zugriff auf die Daten anderer Apps. Große Unternehmen haben die Möglichkeit, firmenspezifische Apps zu erstellen und über Ad-Hoc-Distributionen direkt auf die mobilen Endgeräte der Arbeitnehmer zu verteilen. Apps für das iOS werden in Objective-C entwickelt und können jederzeit nur auf einem Mac OS X entwickelt werden. Darüber hinaus ist ein kostenpflichtiger Zugang notwendig, um die entwickelten Apps, im Apple Store zur Verfügung zu stellen.[35]

Windows

Windows ist ein Desktop-Betriebssystem des US-amerikanischen Unternehmens Microsoft. Die Aktuelle Version ist Windows 8. Das System aus der Reihe Microsoft Windows wurde am 26. Oktober 2012 als Nachfolger von Windows 7 veröffentlicht. Das Betriebssystem enthält zwei Benutzeroberflächen: Einerseits Windows 8 Modern UI, eine speziell für Touchscreens optimierte Bedienoberfläche in „Kachelform“ und andererseits eine Desktop-Oberfläche mit einer Taskleiste. Die Bedienung erfolgt mittels Maus, Tastatur oder über Touchscreen-Gesten.

[35] B. Wieczorek (2013, S. 12 ff.)

In Windows 8 existieren statt der bisherigen zwei nun drei verschiedene Arten von Anwendungen: Erstens die traditionellen Windows-Anwendungen, die auf dem Desktop in einem Fenster laufen, zweitens die Konsolenanwendungen und drittens die neu eingeführten Windows-Apps, die innerhalb der neuen Modern User Interface (UI) ausgeführt werden. Die Windows-Apps unterscheiden sich sowohl in ihrer Laufzeitumgebung als auch – zumindest teilweise – in der verwendeten API.[36]

Windows Phone

Am. 29.10.2012 veröffentliche Microsoft das Windows Phone 8, den Nachfolger von Windows Phone 7, das nicht mehr auf CE, sondern auf Windows 8 RT basiert. Wie auch die Vorgänger unterstützt Windows Phone 8 OMA DM 1.2. Dieses Betriebssystem enthält Teile des Programmcodes von Windows 8 und wurde für ARM-Prozessoren und die Touch Bedienung optimiert.

Die Apps werden in der Programmiersprache C# entwickelt, wobei für die Entwicklung der Oberfläche XAML verwendet wird.[37] Für die Entwicklung werden Windows Phone Developer Tools benötigt, was von Microsoft kostenlos bereitgestellt wird. Jede App, die auf den Marketplace hochgeladen wird, unterliegt einem strengen Prozess der Zertifizierung.[38]

2.2.4. Eingrenzung

Da in der vorliegenden Arbeit die Grundschutzansätze des BSI betrachtet werden, werden in dieser Arbeit die Notebooks und Subnotebooks ebenso als mobile Endgeräte gesehen. In der vorliegenden Arbeit werden unter mobilen Endgeräten also folgende Endgeräte betrachtet: Notebooks, Subnotebooks, Netbooks, Tablets, Smartphones und Mobiltelefone. Unter den Begriffen „Geräte“, „Endgeräte“ und „mobile (Alt-)Geräte“ werden ebenso mobile Endgeräte gemeint. Außerdem werden Notebooks, Subnotebooks und Netbooks als ein Gerät betrachten. Hierfür wird Begriff Notebook verwendet.

[36] Wikipedia (2014b)
[37] B. Wieczorek (2013, S. 15)
[38] Walter Saumweber (2012)

Als mobile Betriebssysteme werden folgende in der Arbeit betrachtet: Android, iOS, OS X, Windows und Windows Phone. Das Betriebssystem BlackBerry OS wird in der Arbeit nicht betrachtet.

2.3. Produktlebenszyklus

2.3.1. Begriff

In der Literatur findet sich eine Vielzahl von Lebenszykluskonzeten, die sich grob einteilen lassen in Produkt-, Technologie-, und Branchenlebenszyklus sowie den Lebenszyklus von Organisationen. Gemeinsam ist den Konzepten die intuitive Gesetzmäßigkeit von Einführung, Wachstum, Reife, Sättigung und Niedergang des Bezugsobjekts. Die Anzahl der unterschiedenen Phasen schwankt je nach Autor zwischen drei und sechs, wobei sogenannte erweiterte Lebenszyklusmodelle auch die Phasen vor der Markteinführung berücksichtigen. Die Abbildung 7 zeigt schematisch das Konzept des Produktlebenszyklus.

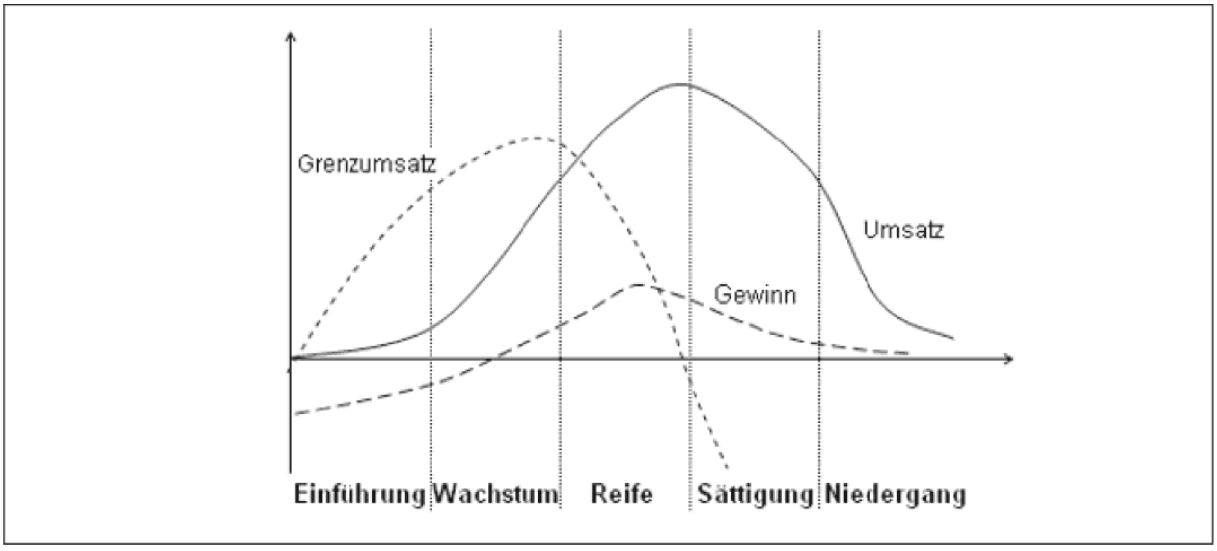


Abbildung 7: Produktlebenszyklus[39]

Der Umsatzverlauf folgt etwa einer Glockenkurve, wobei der größter Umsatzzuwachs, angezeigt durch das Maximum des Grenzumsatzes, in der Wachstumsphase erreicht wird. In dieser Phase fällt auch erstmals ein positiver Gewinn an, da die Einführungsphase von hohen Kosten begleitet wird. In der

[39] C. Raasch (2010, S. 13)

Sättigungs- und der Degenerationsphase sinken der Umsatz und damit auch der Gewinn.[40]

Wenn vom Produktlebenszyklus gesprochen wird, so meint man nicht die Lebensdauer eines einzelnen Produktes vom Kauf bis zur Entsorgung, sondern die Lebensdauer eines Produktes in einem Markt. Der Produktlebenszyklus wird von vielen Autoren stets ähnlich dargestellt, wobei eine Unterscheidung in bis zu 10 Phasen stattfindet. Der Produktlebenszyklus beginnt mit der Produktplanung und endet damit, dass das Produkt aus dem Markt genommen wird. Häufig muss bei Sachleistungsprodukten anschließend noch eine Versorgung mit Ersatzteilen über mehrere Jahre gewährleistet sein.[41]

2.3.2. Phasen

Die Produkteinführung ist noch durch geringe Erlöse gekennzeichnet. Da die Mengen noch sehr gering sind, können auch nur geringe Gewinne oder sogar Verluste erwartet werden. Es fallen noch erhebliche Kosten für Marketingmaßnahmen an, weil das Produkt erst bekannt gemacht werden muss.

In den Phasen Wachstum, Reife und Sättigung entstehen hohe Umsätze und auch Gewinne. Mit dem Erreichen des Break-Even-Points sind die Kosten der Vorleistung durch Gewinne ausgeglichen.

Der Anstieg in der Phase Wachstum hängt davon ab, wie schnell die Bekanntheit des Produktes zunimmt und ob bereits Wettbewerber mit vergleichbaren Erzeugnissen auf dem Markt gibt. Im weiteren Verlauf sinken die Kosten je Erzeugniseinheit.

In der Reife findet nur noch ein geringes Anwachsen des Umsatzes statt, da zunehmend Konkurrenz auftritt. In dieser Phase ergeben sich jedoch die höchsten Deckungsbeiträge.

[40] C. Raasch (2010, S. 13 f.)
[41] T. Grabner (2012, S. 50)

In der Phase der Sättigung muss häufig mit einem Preisverfall gerechnet werden. Immer mehr Wettbewerber treten in den Markt ein; der Neuheitsgrad des Produktes nimmt ab. Dem versucht man mit Rationalisierungsmaßnahmen entgegenzuwirken.

Mit Beginn der Sättigung und Einleitung des Niedergangs muss die Verfügbarkeit eines Nachfolgeproduktes sichergestellt werden. Parallel wird die Entwicklung der nächsten Generation vorbereitet. In der Phase des Abstiegs ergeben sich zunehmend geringere Umsätze, da preisgünstigere und weiter entwickelte Produkte in den Markt eintreten. Die immer geringer werdenden Stückzahlen führen dazu, dass keine Deckungsbeiträge mehr erzielt werden, so dass das Produkt aus dem Markt genommen wird.

Damit sind nicht zwangsläufig die Aktivitäten der Entwicklung und Konstruktion abgeschlossen. Insbesondere bei Industriegütern wird die Verpflichtung eingegangen, die Funktionssicherheit dieser Güter über 10 bis 20 Jahre sicherzustellen und dementsprechend Ersatzteile vorzuhalten. Dabei spielt die Abkündigung infolge von Veralterung (Obsoleszenz) eine große Rolle. Während das Enderzeugnis eine Produktlebensdauer von z.B. 20 Jahren hat, sind einzelne Komponenten wegen kürzerer Innovationszyklen bereits nach wenigen Jahren nicht mehr verfügbar. Es muss dann nach neuen technischen Lösungen gesucht werden und das Enderzeugnis muss gegebenenfalls daraufhin angepasst werden. Diese Problematik findet sich insbesondere in Verbindung mit Elektronikkomponenten.[42]

2.3.3. Geplante Obsoleszenz

Oft fallen Elektrogeräte vor der prognostizierten Lebensdauer aus und können nicht mehr repariert werden, höchstens mit hohen Kosten. Dieses Phänomen, bei dem ein Produkt auf natürliche oder künstlich beeinflusste Art verschleißt, heißt Obsoleszenz. Bei der Obsoleszenz gibt es viele Spielarten: geplant, psychologisch und technisch. Wenn ein Gerät vorzeitig ausfällt oder sich schlecht reparieren lässt, kann es viele Ursachen haben. So können die Elektrolytkondensatoren in Computern, Fernsehgeräten und anderen elektronischen Geräten unterdimensioniert oder die Materialien bei mechanischen Bauteilen, wie Zahnräder in Mixern oder Lager in

[42] T. Grabner (2012, S. 51 ff.)

Waschmaschinen, zu wenig belastbar sein. Ein anderes bekanntes Problem: Die Bauteile in mobilen Endgeräten wie Tablet-PCs oder Smartphones sind verklebt und deren Akkus lassen sich nicht austauschen. Festzustellen ist es, dass der vorzeitige Verschleiß von Produkten, egal wie er zustande kommt, wirkt sich negativ auf unseren Ressourcenverbrauch aus. In der Öffentlichkeit wird das Phänomen viel diskutiert, insbesondere im Zusammenhang mit Elektro- und Elektronikgeräten. Bei Elektro- und Elektronikgeräte besteht am häufigsten der Verdacht, vorzeitig zu altern oder kaputt zu gehen. Außerdem ändert sich deren Design und Produktpalette besonders dynamisch. Das Verbraucherverhalten kann auf die durchschnittliche Lebensdauer der Produkte ebenso auswirken. So kann die Wahl des Designs und der Software die technische Lebensdauer eines Produktes verlängern. Die Art und Weise, wie Menschen dieses im Alltag nutzen, kann die technisch mögliche Lebensdauer wiederum verkürzen.[43]

Um die wissenschaftliche Grundlage zu verbessern, hat das Umweltbundesamt nun das Öko-Institut e.V. zusammen mit der Universität Bonn mit einer Studie beauftragt. Diese hat im September 2013 begonnen, im Jahr 2014 wird sie erste Ergebnisse liefern und im Frühjahr 2015 abgeschlossen sein. Die Studie beschäftigt sich unter anderem mit der Frage wie lange ein Produkt in Stand bleiben und funktionsfähig sein muss. Außerdem soll geklärt werden, inwiefern der vorzeitige Defekt eines Produktes durch den Hersteller in Kauf genommen oder sogar bewusst durch eingebaute Sollbruchstellen – als geplante Obsoleszenz – erzeugt wird. Da die derzeitige Diskussion zu Obsoleszenz fast ausschließlich exemplarisch geführt wird, ist das Ziel der Studie vor allem die Ermittlung systematischer Informationen, um eine angemessene Beurteilung des Phänomens zu ermöglichen und daraus Handlungsempfehlungen abzuleiten.[44]

Die geplante Obsoleszenz ist dabei unabhängig vom Produktlebenszyklus, der sich nicht auf die Haltbarkeit des einzelnen Produkts, sondern den gesamten Zeitraum von der Entwicklung bis zum Verkaufsende bezieht.[45]

[43] Das Umweltbundesamt (2013a)
[44] Das Umweltbundesamt (2013a)
[45] Wikipedia (2014a)

2.4. Nachhaltigkeit

2.4.1. Begriff

Erstmals wurde der Begriff Nachhaltigkeit im Jahre 1713 von dem sächsischen Oberberghauptmann von Carlowitz geprägt. Dieser erkannte die Erfordernis, den Forstbestand kontinuierlich zu nutzen. Man sollte dem Wald die Zeit geben sich zu regenerieren, um eine langfristige Nutzung sicherzustellen. Im Zusammenhang mit der Forstwirtschaft tauschte der Begriff Nachhaltigkeit dann immer wieder auf und wurde schließlich unter der Bedeutung "fortlaufend" oder "andauernd" zum Bestandteil der deutschen Sprache. Der Begriff Nachhaltigkeit bedeutet in der Forstwirtschaft bis heute, dass aus einem Wald nicht mehr Holz geschlagen werden darf, als zwischen den Erntezyklen nachwachsen kann.

Der heutige interdisziplinäre und ganzheitliche Ansatz geht auf die "Internationale Weltkommission für Umwelt und Entwicklung" (WCED) zurück. Von diesem lässt sich ein Hauptziel der Nachhaltigkeit ableiten. Man geht davon aus, dass auch kommende Generationen in der Lage sein sollten, ihre Bedürfnisse mithilfe der vorhandenen natürlichen Güter zu befriedigen. Außerdem geht man hier von der Notwendigkeit einer gerechten Verteilung aus. Die Chancen zur menschlichen Bedürfnisbefriedigung sollten nicht nur innerhalb einer Generation, sondern auch generationsübergreifend gleich verteilt sein. Ein Ziel der Nachhaltigkeit ist demnach auch die Bekämpfung der Armut.[46]

Das moderne Verständnis des Begriffes Nachhaltigkeit umfasst, neben der ursprünglich hauptsächlich umweltbezogenen Perspektive, nun auch soziale und ökonomische Dimensionen. Mit einbezogen wurde hier, dass sich ein nachhaltiges Wirtschaften wechselseitig auch auf die sozialen und ökonomischen Interessen einer Gesellschaft auswirkt. In der Theorie geht man vielfach davon aus, dass diese drei Dimensionen gleichwertig sind und voneinander abhängen.[47]

[46] H. Buschenlange (2013, S. 7 f.)
[47] H. Buschenlange (2013, S. 9)

2.4.2. Dimensionen

Im Gegensatz zum historischen Verständnis von Nachhaltigkeit wie auch zur klassischen Umweltpolitik umfasst der gegenwärtige Nachhaltigkeitsgedanke nicht nur umweltbezogene Ziele wie den Schutz der natürlichen Lebensgrundlagen. Der Erhalt der natürlichen Ressourcen wirkt sich, wie bereits angesprochen, ebenso auf die wirtschaftliche und gesellschaftliche Entwicklung aus. Daher werden die drei Komponenten Ökologie, Ökonomie und Soziales als die Dimensionen der Nachhaltigkeit bezeichnet und zur Ausdifferenzierung dieses komplexen Entwicklungsziels in verschiedene Modelle integriert. Am häufigsten werden die Komponenten im sogenannten Drei-Säulen-Modell beziehungsweise im Nachhaltigkeitsdreieck dargestellt, wobei angenommen wird, dass um welt-, wirtschafts- und gesellschaftsbezogene Anteile in gleichwertiger und wechselseitiger Abhängigkeit zueinander stehen.[48]

Der ökologischen Dimension kommt die Auseinandersetzung mit dem Schutz der Ökosphäre zu. Durch Eingriffe des Menschen in Ökosysteme, beispielsweise durch Stoffeinträge (Schadstoffe, die der Umwelt zugeführt werden), landwirtschaftliche Nutzung oder Einnahme von Siedlungs- und Verkehrsfläche, sind diese inzwischen überwiegend anthropogen beeinflusst. Die Umformung dieser Systeme nach menschlichen Bedürfnissen führte zu verschieden starken Veränderungen, die sich unter anderem im Verschwinden von Tier und Pflanzenarten zeigen, sodass es teilweise unmöglich geworden ist, deren Nutzungsmöglichkeiten für zukünftige Generationen zu gewährleisten. Unter Berücksichtigung des natürlichen Wandels von Ökosystemen gilt es daher, ihre Belastbarkeit nicht zu überschreiten und den unerwünschten menschlichen Einflüssen Einhalt zu gebieten. Dies erfordert den achtsamen Umgang mit Ressourcen, Senken und Stoffen, die in die Natur übergehen sowie den Schutz der menschlichen Gesundheit.[49]

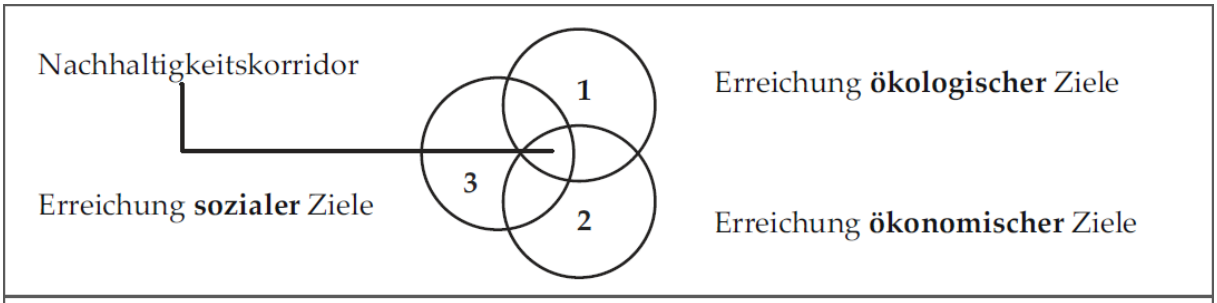
Die ökonomische Dimension zielt auf eine solide wirtschaftliche Entwicklung, ohne ökologische und soziale Belange zu vernachlässigen. Unter dem Einsatz der Ressourcen Arbeitskraft und Produktivität soll die Bevölkerung bestmöglich mit Gütern und Dienstleistungen versorgt werden. Dabei stehen unter dem System der

[48] C. Glathe (2010, S. 18 f.)
[49] C. Glathe (2010, S. 19)

sozialen Marktwirtschaft die Unterstützung des freien Wettbewerbs und die Verhinderung von Monopol- und Oligopolbildung im Zentrum der regulierenden Eingriffe des Staates. Infolge eines funktionierenden Wirtschaftsgefüges können Funktionen von Produkten verbessert, Produktionsabläufe optimiert und neue Produkte entwickelt werden und Organisationen in Abhängigkeit der Wertschätzung durch Konsumenten wachsen, schrumpfen oder aus dem Markt ausscheiden. Letztendlich soll über Arbeitsteilung, Spezialisierung und technischen Fortschritt die Menge an Gütern und Dienstleistungen gesteigert und drohende Knappheit durch effizientere Produktionsweisen vermindert werden.[50]

Im Fokus der sozialen Dimension liegt die Verteilungsgerechtigkeit – sowohl zwischen Individuen als auch zwischen Generationen. Gemeint ist dabei die gerechte Verteilung von Lebenschancen, Arbeit, Einkommen und gesellschaftlichem Wohlstand. Grundlegend hierfür sind die Solidaritäts- und Sozialstaatsprinzipien, die sich im demokratischen und rechtsstaatlichen System, in der sozialen Marktwirtschaft, im gesellschaftlichen Zusammenhalt und friedlichen Zusammenleben, in der Unterstützung von Schwächeren, der Risikoabsicherung durch Versicherungen, der Chancengleichheit der Geschlechter und Benachteiligter sowie in der Möglichkeit zu freien Entfaltung des Individuums widerspiegeln.[51] Die Abbildung 8 veranschaulicht Nachhaltigkeitskriterien sowie deren Verständnis des Drei-Säulen-Modells.

[50] C. Glathe (2010, S. 19 f.)
[51] C. Glathe (2010, S. 20)



-1- Ökologische Nachhaltigkeit

- Verbesserung der Umweltqualität
- Verringerung des Rohstoffverbrauchs
- Verringerung des Energieverbrauchs
- Schutz der biologischen Vielfalt
- Risikovermeidung für Mensch und Tier

-2- Ökonomische Nachhaltigkeit

- Funktionsfähigkeit des Wirtschaftssystems
- Vollbeschäftigung und soziale Sicherung
- Ökonomische Leistungsfähigkeit und Innovationskompetenz
- Intergenerationeller Ausgleich
- Internationale wirtschaftliche Stabilität

-3- Soziale Nachhaltigkeit

- Selbstbestimmte Lebensführung durch eigene Arbeit
- Umweltverträgliche Befriedigung der Grundbedürfnisse
- Chancengleichheit und gesellschaftliche Grundsicherung
- Aktive gesellschaftliche Teilhabe im Rahmen von Nachhaltigkeitsstrategien

Abbildung 8: Nachhaltigkeitskriterien im Drei-Säulen-Modell[52]

2.4.3. Strategien zur Umsetzung

Es existieren keine einfachen Lösungen oder fertigen integrierten Vorgehensweisen, um die unterschiedlich schweren und teilweisen irreversiblen Probleme, die sich auf Umwelt, Wirtschaft und Gesellschaft auswirken, gleichzeitig zu beheben. Den bisherigen Ansatzpunkt bilden die auf die ökologische Dimension ausgerichteten Strategien der Effizienz, Suffizienz und Konsistenz. Wie bei den meisten praktischen Umsetzungen ist die Orientierung an der ökologischen Komponente bisweilen dominierend, da viele Wissenschaftler diese Dimension als bedeutsame Vorbedingung für die Umsetzung der beiden übrigen Komponenten sehen.[53]

[52] C. Glathe (2010, S. 21)
[53] C. Glathe (2010, S. 29 f.)

Die Effizienzstrategie erstrebt einen verminderten Umweltverbrauch durch die Verringerung des Stoff und Energieeinsatzes pro Dienstleistung beziehungsweise Ware. Dazu ist eine Steigerung der Ressourcenproduktivität notwendig, die beispielsweise durch Produktinnovationen, verbesserte Organisations- und Produktionsweisen, Wiederverwendbarkeit, erhöhte Produktlebensdauer und Abfallvermeidung erreicht werden kann.[54]

Die Suffizienzstrategie beabsichtigt, eine geringere Umweltbelastung durch die Reduktion von Verbrauch zu erreichen. Mit dem Gedanken von Angemessenheit und Bescheidenheit soll nur so viel beansprucht werden, wie für sich selbst und andere zuträglich ist. Besonders gefragt sind hier die Konsumenten, die mit einer geringeren Nachfrage bis hin zum Konsumverzicht Einfluss ausüben können.[55]

Das Anliegen der Konsistenzstrategie ist die Vereinbarkeit von Umwelt und Technik. Damit sich industrielle und natürliche Stoffwechselprozesse gegenseitig nicht stören, sondern ergänzen, ist der Einsatz umweltverträglicher Stoffströme und risikoarmer Technologien notwendig. Gemäß dem Motto "in intelligenten Systemen gibt es keine Abfälle, nur Produkte" werden Überreste eines Produkts zum Ausgangsmaterial eines anderen (zum Beispiel das erhitzte Kühlwasser bei der Stromerzeugung zur Weiterleitung als Fernwärme).[56]

2.4.4. Ökobilanz

Um umweltrelevante Vorgänge zu erfassen und zu bewerten wird ein Verfahren "Ökobilanz" eingesetzt.[57] Die Ökobilanz (engl. LCA – Life Cycle Assessment) ist eine systematische Analyse der Umweltwirkungen von Produkten, Verfahren oder Dienstleistungen entlang des gesamten Lebenswegs ("von der Wiege bis zur Bahre"). Dazu gehören sämtliche Umweltwirkungen, die während der Produktion, der Nutzungsphase und der Entsorgung sowie den damit verbundenen vor- und nachgeschalteten Prozessen (z. B. Herstellung der Roh-, Hilfs- und Betriebsstoffe) entstehen (siehe Abbildung 9). Die Methode der Ökobilanz kann als Tool für

[54] C. Glathe (2010, S. 30)
[55] C. Glathe (2010, S. 30)
[56] C. Glathe (2010, S. 30)
[57] Das Umweltbundesamt (2013d)

umweltorientierte Entscheidungen herangezogen werden. Angewendet wird sie, um Produkte zu entwickeln und zu verbessern. Außerdem wird die Methode im Rahmen strategischer Planung, bei politischen Entscheidungsprozessen und im Marketing angewendet. Die Ökobilanz ist ein Teilelement der ganzheitlichen Bilanzierung und ist in ISO (Internationale Organisation für Normung) 14040 standardisiert.[58]

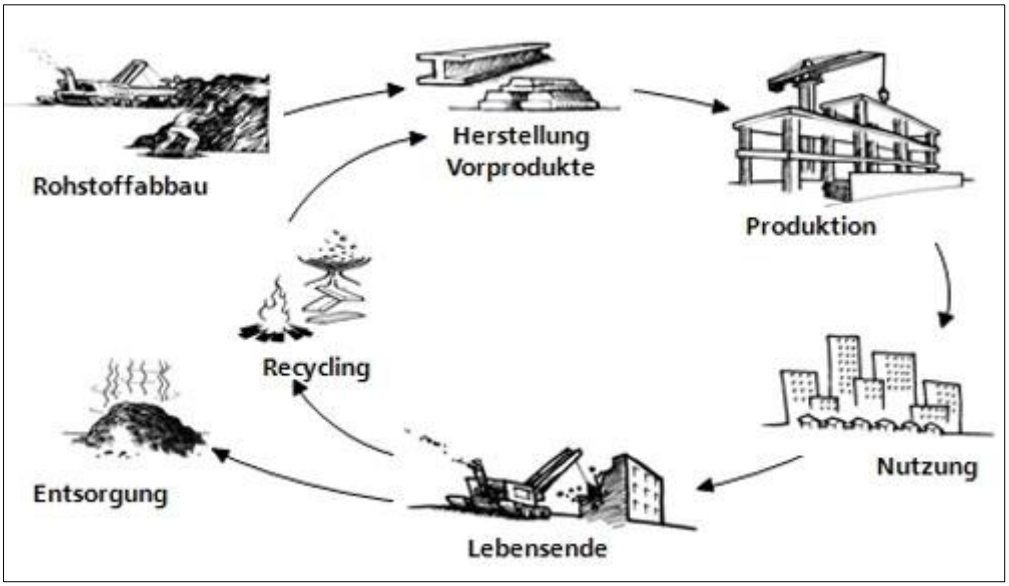


Abbildung 9: Lebenszyklus von Produkten[59]

Das prinzipielle Vorgehen bei der Durchführung einer Ökobilanz kann wie folgt beschrieben werden:

- Entlang des Lebenswegs eines Produktes werden die Stoff- und Energieströme des gesamten Produktsystems, also aller beteiligten Prozesse, analysiert.
- Emissionen in Luft, Wasser und Boden sowie der Natur entnommene Ressourcen werden systematisch erfasst und in der sogenannten "Sachbilanz" abgelegt.
- Die potenziellen Umwelteffekte wie Treibhauseffekt, Sommersmog, Versauerung, Überdüngung etc., werden anschließend im Rahmen der "Wirkungsabschätzung" ausgewertet.

Eine Ökobilanz ist in vier Schritte untergliedert (ISO 14040):

1. Festlegung des Ziels und Untersuchungsrahmens (engl. Goal and Scope)

[58] Fraunhofer IBP (2014)
[59] Fraunhofer IBP (2014)

Der erste Schritt der Ökobilanz legt das Ziel und den Untersuchungsrahmen fest. Dazu gehört beispielsweise die Definition der Systemgrenzen, der Funktion des Systems und der Anforderungen an die Datenqualität.

2. Sachbilanz (engl. LCI – Life Cycle Inventory)
   Die Sachbilanz beinhaltet die Datensammlung aller benötigten eingehenden (Ressourcen, Materialien) und ausgehenden (Emissionen, Abfälle) Stoff- und Energieströme, welche in einer Bilanz erfasst werden.

3. Wirkungsabschätzung (engl. LCIA – Life Cycle Impact Assessment)
   Bei der Wirkungsabschätzung werden die potenziellen Umweltwirkungen, Einflüsse auf die menschliche Gesundheit und Ressourcenverfügbarkeit mithilfe der Ergebnisse der Sachbilanz über entsprechende Charakterisierungsmodelle softwaregestützt errechnet.

4. Auswertung und Interpretation (engl. Results and Interpretation)
   Bei der Auswertung werden die Ergebnisse der Sachbilanz und Wirkungsabschätzung in Bezug auf das Ziel der Ökobilanzstudie interpretiert.[60]

3. Mobile Endgeräte in Organisationen

3.1. Einsatz und Nutzen

Der Einsatz der IT in Organisationen hat sich in den vergangenen Jahrzehnten grundlegend verändert. An der Stelle des vereinzelten IT-Einsatzes auf eine rein operative Ebene, etwa bei der Erstellung von Produktionsplänen oder der Steuerung von Werkzeugmaschinen, ist durch weitgehende Elektrifizierung und Vernetzung in vielen Unternehmen der strategische und flächendeckende IT-Einsatz durch die elektronische Abbildung der gesamten betrieblichen Leistungskette getreten. In großen Unternehmen wurde dies typischerweise durch die Einführung komplexer ERP-Systeme, in kleinen eher durch die Verwendung von Branchenlösungen erreicht. Resultierende Potentiale liegen beispielsweise in gemeinsamer

[60] Fraunhofer IBP (2014)

Datenhaltung, integrierter Workflow-Steuerung oder der zeitnahen Verfügbarkeit aggregierter, aufbereiteter Unternehmensdaten (Business Intelligence).[61]

An dieser Stelle können mobile Endgeräte mit neuen Funktionalitäten und immer steigender Leistungsfähigkeit ein breiteres Spektrum von Einsatzfeldern im betrieblichen Umfeld erschließen. PDAs und Smartphones als mobile Endgeräte ermöglichen Nutzern zeit- und ortsunabhängigen Zugriff auf sensible, personengebundene Daten, wodurch eine Produktivitätssteigerung ermöglicht wird.[62] Immer mehr Organisationen bieten ihren Mitarbeitern für die Kommunikation Smartphones oder Tablets an. Vor allem größere Organisationen mit mehr als 250 Beschäftigten stellen tragbare Geräte zur Verfügung (91%). In kleinen Unternehmen mit weniger als 50 Angestellten ist es immerhin noch knapp die Hälfte (48%). Bei weniger als zehn Angestellten sind es dagegen erst 31%. Dabei wird ihnen neben dem Zugriff auf das öffentliche Internet auch der Zugang zum unternehmenseigenen E-Mail-System (72%), auf interne Dokumente (44%) und Firmen interner Software gewährt.[63] Die Organisationen nutzen mobile Endgeräte außerdem, um zum Beispiel ihren Außendienstmitarbeitern Zugriff auf ihr Backend zu ermöglichen. Da hier die Daten einer Organisation sehr vertraulich sein können, muss der Zugang zu diesen Daten entsprechend sicher gestaltet sein.[64] Der Einsatz von mobilen Endgeräten kann folgende Vor- und Nachteile bringen:

Vorteile

- Bessere und längere Erreichbarkeit der Mitarbeiter
- Ortsflexible Verfügbarkeit von Informationen: mobile Endgeräte erlauben einen Zugriff von praktisch jedem Ort
- Zeiteinsparung: durch kürzere Antwortzeiten
- Medienbrüche entfallen: Daten können direkt in das Gerät eingegeben werden

Nachteile

- Aufwand für die Geräteverwaltung: Durchsetzen von Sicherheitsrichtlinien
- Eingeschränkter Support für die Geräte: vielfältige Plattform-/Geräte-Variationen

[61] K. Dr. Pousttchi, B. Thurnher (2006, S. 102)
[62] H. Rossnagel, T. Murmann (2005, S. 129)
[63] Haufe Online Redaktion (2012)
[64] H. Rossnagel, T. Murmann (2005, S. 129 f.)

- Sicherheits- und Datenschutzrisiken: bei Verlust oder ungenügender Absicherung der Geräte
- Mangelnde Robustheit der Geräte: z.B. im Vergleich zu Mobile Datenerfassung-Geräten[65]

Die Chancen dieser neuen Technologie sind viel versprechend. Um sie zu nutzen, hat das Bundesministerium für Wirtschaft und Energie (BMWi) im Rahmen seiner Technologieaktivitäten bereits 2006 das Förderprogramm "SimoBIT - sichere Anwendung der mobilen Informationstechnik (IT) zur Wertschöpfungssteigerung in Mittelstand und Verwaltung" gestartet und erfolgreich Ende 2010 beendet. In mehreren Modellprojekten wurden mit der Förderinitiative innovative Anwendungsmöglichkeiten mobiler Endgeräte aufgezeigt und Verfahren für mehr IT- und Informationssicherheit entwickelt und erprobt. Zudem wurden im Rahmen von SimoBIT zentrale Gemeinsamkeiten für die Erhöhung der IT-Sicherheit bei mobilen Geschäftsanwendungen herausgearbeitet und in einem Leitfaden zusammengestellt. Dazu gehören auch spezielle Checklisten für mobile IT-Anwendungen in Organisationen.[66]

3.2. Verwaltung

3.2.1. Definition

Das Mobile Device Management (MDM) bezeichnet eine Softwarelösung für das Systemmanagement von mobilen Endgeräten, mit dem diese verwaltet und kontrolliert werden können. Bei allen auf dem Markt befindlichen Lösungen haben sich über die Zeit bestimmte Basis Funktionen herausgebildet, die mittlerweile von jeder Lösung angeboten werden.[67] (im Kapitel 3.2.4 wird detailliert erzählt)

3.2.2. Standards

Im Rahmen des Mobile Device Managements haben sich über die Zeit einige Standards etabliert. Führend hierbei ist die Open Mobile Alliance (OMA), die sich aus

[65] Tim Gebler (2013)
[66] Bundesministerium für Wirtschaft und Energie (2011)
[67] B. Wieczorek (2013, S. 5)

mehr als 350 unterschiedlichen Mitgliedern (wie z.B. Nokia, IBM, Vodafone, Microsoft) aus dem Mobilfunksektor zusammensetzt. Von ihr wurde 2007 das OMA Device Management (OMA DM), ein Standard mit einer Reihe von Protokollen zum Remote Management (z.B. Softwareaktualisierungen, Konfiguration, usw.) von mobilen Endgeräten veröffentlicht. Zu den genaueren Spezifikationen von OMA DM gehören auch die Implementierung von Firmware over-the-air (FOTA) mittels dem Firmware Update Management Object (FUMO). Kommt FOTA zum Einsatz wird hier jeweils nur der Bestandteil der Firmware drahtlos übertragen der ausgetauscht werden muss. Nach dem Übertragen erfolgt dann die Installation im Hintergrund ohne den Anwender zu stören oder persönliche Daten zu verändern. die im Anschluss mit einem Neustart abgeschlossen werden muss. Eine Weiterentwicklung von FOTA stellt Software over-the-air (SCOTA) mittels dem Software Component Management Object (SCOMO) dar, mit der gezielt nur einzelne Bestandteile auf dem mobilen Endgerät drahtlos ausgetauscht werden können.[68]

3.2.3. Integration

Bei der Integration einer MDM wird unterschieden zwischen einer selbst verwalteten Lösung im Organisations eigenen Rechenzentrum (ein sogenanntes On-Premise Modell) oder einer Cloud Lösung (dem On-Demand Modell oder auch "Software as a Service" Modell; kurz SaaS genannt), die vom Hersteller bereitgestellt und größtenteils administriert wird. Entscheidet sich der Arbeitgeber für eine Lösung außerhalb des eigenen Rechenzentrums, können gleich mehrere Bestandteile des deutschen Datenschutzrechts, zum Schutz personenbezogener Daten, Anwendung finden. Denn abhängig davon, ob es sich bei den über die MDM erfassten Daten, um Gesetzlich schützenswerte personenbezogene Daten handelt oder nicht, wird der Anbieter laut Gesetz zum Auftragsdatenverarbeiter mit entsprechenden Pflichten. Hier ist insbesondere zu kontrollieren ob die Daten nur innerhalb oder auch außerhalb der Europäischen Union gespeichert werden. Im Einzelfalle sollte ein Fachanwalt hinzugezogen werden, der einen Auftragsdatenverarbeitungsvertrag ausarbeitet und den Arbeitgeber darüber hinaus zu dem Thema beraten kann. Hat sich der Arbeitgeber für ein On-Premise Modell entschieden, wird der jeweilige MDM-Server in der DMZ der Organisation installiert, sodass die mobilen Endgeräte aus

[68] B. Wieczorek (2013, S. 5 f.)

dem Internet heraus Zugriff auf den Server haben. Auf der Seite der mobilen Endgeräte muss bei jedem auf dem Markt befindlichen Hersteller eine MDM Software Komponente installiert werden. Dies ist nötig, da die Hersteller aufgrund des Aufbaus der derzeitigen Betriebssysteme nicht tief genug in das jeweilige Betriebssystem eingreifen können, wie es eigentlich für sie erforderlich wäre. Die installierte Komponente verbindet sich mit der eigentlichen MDM-Lösung und erlaubt damit eine zentrale Administration und Überwachung der mobilen Endgeräte. Zu beachten ist, dass die derzeitigen Betriebssysteme für mobile Endgeräte keine Rechtevergabe unterstützen, wie es z.B. vom Windows oder Linux Betriebssysteme her bekannt ist. Das bedeutet, dass der Anwender jederzeit die komplette Kontrolle über sein mobiles Endgerät behält und die MDM Software Komponente auch selbst deinstallieren kann.[69]

3.2.4. Basisfunktionen

Zu den Basisfunktionen gehören folgende Funktionen:

Provisionierung

Provisionierung (engl. Provisioning) beschreibt ein Prozess der Bereitstellung bzw. Verteilung von Hilfsmitteln, wie Einstellungen, Profile, Konfigurationen und Apps, zur Nutzung eines elektronischen Dienstleistungsangebotes. Sie werden in der Regel over-the-air (OTA), also drahtlos übertragen, wobei auch eine kabelgebundene Übertragung möglich wäre, aber bei eine großen Anzahlt von mobilen Endgeräten nicht praktikabel ist.

Richtlinienverwaltung

Eine Hauptaufgabe einer MDM-Lösung ist die Richtlinienverwaltung (engl. Policy Management). Die Richtlinienverwaltung hat die Aufgabe bestimmte Konfigurationsmöglichkeiten, die der Administrator zentral als Richtlinie(n) vorgibt, drahtlos im Hintergrund auf die mobilen Endgeräten zu übertragen. Dabei besteht eine Richtlinie systemintern aus ein oder mehreren XML-Dateien, die

[69] B. Wieczorek (2013, S. 6 f.)

gerätespezifische Sicherheitsrichtlinien und Einschränkungen, sowie Konfigurations- und Einstellungsinformationen (z.B. WLAN, E-Mail usw.) beinhalten. Das Ziel der Richtlinienverwaltung ist es, das jeweilige mobile Endgerät soweit einzuschränken, wie es für die Sicherheit der Organisation notwendig ist. Ein Bestandteil einer solcher Richtlinie könnte z.B. das Aktivieren und Erzwingen eines PIN-Codes für die Tastatur auf dem mobilen Endgerät sein.

Softwareverteilung

Eine weitere Aufgabe von MDM-Lösungen ist die Softwareverteilung. Mittels dieser ist es (abhängig von dem Betriebssystem des mobilen Endgerätes) möglich, Organisations-Apps zu definieren und auf die mobilen Endgeräte zu übertragen bzw. dem Arbeitnehmer die Möglichkeit zugeben freigegebene Organisations-Apps selbst zu installieren. Auch die Aktualisierungen von Apps, wie z.B. der MDM-Komponente und des Betriebssystems fallen in diesen Bereich.

Inventarmanagement

Das Inventarmanagement hat die Aufgabe alle der vom MDM verwalteten mobilen Endgeräte aufzulisten und diese ggf. zwecks einer besseren Übersicht zu gruppieren. Das Inventar Management dient ebenfalls als Startpunkt für die Fernwartung (engl. Remote Management), um so z.B. ein mobiles Endgerät zu löschen (engl. Remote Wipe).[70]

3.2.5. Bring Your Own Device

Eine andere Möglichkeit mobile Endgeräte in Organisationen zu nutzen bietet das Model „Bring Your Own Device“ (BYOD). Der Trend BYOD heißt übersetzt „Bring Dein eigenes Gerät mit“ und beschreibt die Möglichkeit für z. B. Mitarbeiter einer Organisation, ihre eigenen Computer, Smartphones oder ähnliche Geräte zum Arbeiten im Büro zu benutzen.[71]

[70] B. Wieczorek (2013, S. 8 f.)
[71] Anett Mehler-Bicher und Lothar Steiger (2012, S. 53)

Für die Organisationen und den Mitarbeiter ergeben sich hieraus zahlreiche Chancen, wie z. B. gesteigerte Produktivität der Mitarbeiter durch den Einsatz von z.B. Smartphones, erhöhte Erreichbarkeit des Mitarbeiters außerhalb der üblichen Bürozeiten und Kosteneinsparungen bei der Anschaffung. Außerdem kann ein Imagevorteil im Recruiting neuer Mitarbeiter aus der Altersgruppe der sog. Millennials (Junge Generation - Generation Y) durch BYOD gefördert. Abgesehen von diesen Vorteilen wirft BYOD aber auch Probleme im IT-Management der Geräte auf. Neben Sicherheitsrisiken ist hier vor allem auch der erschwerte Support zu nennen.[72] Die IT-Abteilung muss zusätzliche Ressourcen für die Administration und den Support von BYOD-Geräten vorhalten. Aufgrund der fehlenden zentralen Versorgung mit von der IT genehmigter Hardware, entsteht eine heterogene Gerätelandschaft. Diese Heterogenität hat zur Folge, dass grundlegende Techniken, wie das Erstellen einer VPN Verbindung zum Organisationsnetzwerk, individuell betreut und konfiguriert werden müssen. Ein ähnliches Problem ergibt sich, wenn organisationsinterne Anwendungen für mehrere Plattformen bereitgestellt werden müssen, die es den Mitarbeitern ermöglichen, mit ihren präferierten Systemen zu arbeiten. Ein weiterer Punkt, an dem der Administrationsaufwand deutlich wird, ist die Durchführung von Best-Practice Handlungen. Ein allumfassendes, zentrales Backup von allen Daten ist beispielsweise nur dann möglich, wenn Veränderungen an Datenbeständen von vornherein nicht lokal gespeichert werden können. Sollte dies nicht möglich sein, sind zusätzliche Schritte zur Absicherung der Geräte unabdingbar. Allerdings ist bei wichtigen Bereichen, wie Firewall und Virenscanner, eine Betriebssystemfragmentierung nicht von Vorteil. Das Problem hierbei sind oft voneinander abweichende Sicherheitseinstellungen für jede Version eines Betriebssystems.[73]

3.3. Gefahren der mobilen Endgeräte

In Organisationen finden die Subnotebooks, Notebooks, Tablets und Smartphones zunehmend Verbreitung. Durch den mobilen Einsatz entstehen jedoch gegenüber herkömmlichen Computern neue Gefahren für Datenschutz und Datensicherheit wie Diebstahl und unbeabsichtigter Verlust. Während in herkömmlicher Büroumgebung der Zugang zu den Geräten abgesichert werden kann, verlassen beim mobilen

[72] G. Müller, C. Prof. Dr. Seel (2013)
[73] G. Müller, C. Prof. Dr. Seel (2013)

Einsatz sowohl die Daten als auch das Gerät den Kontrollbereich der Organisationen. Mobile Geräte können im Auto vergessen oder in einem Sitzungssaal unbeaufsichtigt liegengelassen werden. Bereits ein kurzer Zugriff bietet vielfältige Gelegenheiten zur unbefugten Kenntnisnahme schutzwürdiger Daten. Missbrauchsgefahren entstehen aber nicht nur durch unbefugtes Lesen, sondern auch durch unbefugte Modifikation von Daten und durch Beeinträchtigung der Funktionalität.[74]

Die mobilen Endgeräte werden aber auch nach Ende ihre Nutzungszeit noch als Sicherheitsrisiko gesehen, weil die alten geheimen Daten auf den Geräten noch gelagert werden können. Die Geräte, die in Organisationen eingesetzt werden, müssen auch nach Ender ihrer Nutzungszeit besonders geschützt werden, um Datenverlust und somit einen evtl. wirtschaftlichen Schaden zu vermeiden. Dies kann zum Beispiel durch eine IT-Sicherheitsrichtlinie der Organisation, welche die zentralen Richtlinien der IT-Sicherheit festlegt, geregelt werden.[75]

3.4. Die Richtlinie

Eine Organisation wie Wirtschaftsbetriebe, staatliche Institutionen, Kirchen, Parteien oder auch Vereine ist grundsätzlich erst einmal ein sozialer Bereich, der durch bestimmte Verhaltensregeln strukturiert ist. In gewisser Weise ist eine Organisation eigentlich nichts anderes als ein Satz von Regeln, die festlegen, wie die Mitglieder der entsprechenden Organisation miteinander interagieren und kommunizieren, welche sozialen und beruflichen Rollen die Mitglieder einnehmen müssen, mit wem bestimmte Mitglieder interagieren müssen und mit wem nicht, welche Kriterien über den Erfolg bestimmter organisationsbedingter Tätigkeiten entscheiden und noch verschiedene Dimensionen organisatorisch fixierten Handelns mehr. Die speziellen Regeln einer Organisation legen also fest, wie sich die verschiedenen Mitglieder zu verhalten haben, um je nach Aufgabe den allgemeinen Zielen der Organisation gerecht zu werden.[76]

[74] Der Landesbeauftragte für den Datenschutz Niedersachsen (2014)
[75] M. Reiss, G. Reiss (2009, S. 81)
[76] C. Klüver, J. Klüver (2011, S. 11)

Ebenso das IT-Konzept ist ein strategisches Dokument mit Regeln, das der grundsätzlichen Einordnung der IT in die Organisation dient und die übergeordnete strategische Ausrichtung der Organisation im Hinblick auf die IT festlegt. So wird typischerweise im IT-Konzept festgelegt, ob die IT zentral oder dezentral strukturiert ist und mit welcher Ausprägung. Es sollte auch für die IT beschrieben, mit welcher Technik und welchem Verfahren die Organisation welche Zwecke verfolgt. Dabei soll es einen Orientierungsrahmen für die weitere Entwicklung und geplanten Maßnahmen aufzeigen.[77] So kann ein IT-Konzept auch Festlegungen (Methoden und Verfahren) zur Verwaltung der mobilen Endgeräten (Mobile Device Management) beinhalten. Ebenso schreibt die IT-Sicherheitsrichtlinie die zentralen Richtlinien für die IT-Sicherheit in einer Organisation fest. Sie definiert die Sicherheitsziele und Grundsätze für den Umgang mit Informationen sowie die Verantwortungsbereiche für die IT-Sicherheit. Vor allem für große Organisationen ist der Einsatz einer Sicherheitsrichtlinie wichtig, um übergreifende IT-Sicherheitsregeln in der ganzen Organisation durchzuführen. So kann beispielsweise in der Sicherheitsrichtlinie festgelegt werden, dass in der ganzen Organisation ausschließlich von der Organisation bereitgestellte mobile Endgeräte und Speichersysteme eingesetzt werden dürfen und diese technisch sicher stellen, dass keine Fremdgeräte Zugang zum lokalen Netzwerk erhalten.[78]

[77] M. Reiss, G. Reiss (2009, S. 81)
[78] M. Reiss, G. Reiss (2009, S. 81)

4. Nachhaltigkeit bei mobilen Endgeräten

4.1. Beeinflussende Faktoren

Außer Sicherheitsaspekten sollen die mobilen Endgeräte auch der Nachhaltigkeitsstrategie der Organisationen nachkommen, denn die Nutzung der mobilen Endgeräte in Organisationen ist mit aufwändiger Verwaltung der Geräte und intensiven Kosten verbunden. Die Innovationen und Verbesserungen bisheriger Technologien locken den Nutzer oft zu Neuanschaffung (besonders bei BYOD), um technisch auf dem neuesten Stand zu sein, da die Geräte immer leistungsstärker werden. Außerdem spielt der Produktlebenszyklus eine große Rolle, weil nicht alle neuen Applikationen auf den alten Endgeräten mit alten Versionen der Betriebssystemen laufen.

In den Nächten Unterkapiteln wird versucht die Problematik der Faktoren, die auf die nachhaltige Nutzung der mobilen Endgeräte beeinflussen, genau zu untersuchen.

4.1.1. Produktlebenszyklus

Die großen Hersteller, wie z.B. Apple, Samsung, Sony oder Nokia, bringen mittlerweile fast im Jahresrhythmus neue Modelle heraus und der Lebenszyklus der „älteren“ Versionen endet abrupt.[79] Die Produktlebenszyklen vieler Elektronikgeräte lehnen sich heutzutage an die Entwicklungsgeschwindigkeit der Chips an. Diese beträgt manchmal nur noch einige Monate, was die Entwicklung von neuen Geräten antreibt. Außerdem ist die Verkürzung von Produktlebenszyklen dem Wettbewerb geschuldet. Auf dem globalen Markt tummeln sich für ein und dieselbe Produktsparte viele Anbieter. Gerade in gesättigten Märkten müssen Hersteller ständig neue, innovative Produkte anbieten, um sich von der Konkurrenz abzuheben.[80]

Generell kann davon ausgegangen werden, dass die Erstnutzung von z.B. Smartphones im Durchschnitt zwei Jahre beträgt. Dies entspricht der in Deutschland

[79] D. Gerginov (2013)
[80] T. Scheimann (2011)

üblichen Laufzeit von Mobilfunkverträgen.[81] In diesem Fall kann davon auszugehen, dass die Nutzungsdauer deutlich mit der jeweiligen Vertragslaufzeit korreliert, da mit dem Abschluss eines Folgevertrages wird meistens automatisch ein neues Modell angeschafft und das alte außer Betrieb genommen.[82] Zudem kann davon ausgegangen werden, dass Smartphones oftmals in eine Zweitnutzung überführt werden, sodass insgesamt von einer Nutzungsdauer von durchschnittlich 2,5 Jahren ausgegangen werden kann.[83]

Auch die Konsumenten senden die falsche Botschaft an die Hersteller, denn die modernen Mobilgeräte sind zu Modeprodukten geworden, die die Mehrzahl der Verbraucher nach relativ kurzer Zeit nicht mehr verwenden wollen, weil sie nicht mehr im Trend sind. Auch daraus resultiert eine kürzere Nutzungsdauer.[84] Dadurch können die Endgeräte in einer Organisation oft erneuert werden, was mit aufwändiger Verwaltung der Endgeräte und Kosten der Neuanschaffung verbunden ist. Das führt wiederum zu einer schlechten Nachhaltigkeitsstrategie in Organisationen und deren Umweltunfreundlichkeit. Besonders bei BYOD, weil hier haben die Organisationen fast kein Einfluss. Damit mit den mobilen Endgeräten in den Organisationen nachhaltiger umgegangen werden kann, sollen in den Organisationen auch für mobile Endgeräte die Nachhaltigkeitsstrategien entwickelt werden.

4.1.2. Produktunterstützung durch den Hersteller

Durch den kurzen Produktlebenszyklus werden die alten Endgeräte oft nicht lange vom Hersteller unterstütz. Wer sich ein Android-Smartphone kauft, kann sich oft noch nicht einmal darauf verlassen, überhaupt jemals z.B. eines der größeren Software-Updates zu bekommen. Von 73, zwischen 2009 und 2011, in Deutschland erschienenen Android-Smartphones machten 23 Modelle keinen einzigen dieser großen Versionssprünge mit – also beispielsweise von Android-Version 2.2 auf 2.3 oder auf 4.0. Sie bekamen nur Updates mit Fehlerbeseitigungen und kleinen Optimierungen, zum Beispiel von 2.3.3 auf 2.3.7, aber keine Upgrades[85]. Auf einigen

[81] A. Manhart u.a. (2012, S. 17)
[82] A. Manhart u.a. (2012, S. 18)
[83] A. Manhart u.a. (2012, S. 17)
[84] B. Fuest (2013)
[85] A. Barczok u.a. (2013)

Geräten läuft sogar schon bei Auslieferung ein veraltetes Android: Das LG „Optimus Speed“ und das Motorola „Razr“ beispielsweise haben seit ihrem Erscheinungstermin bis zum heutigen Tag noch nie ein aktuelles Android gesehen.[86] In Abbildung 10 wird ersichtlich, wie schnell sich das Android-Betriebssystem in den letzten vier Jahren entwickelt hat und wie viele Versionen in dieser kurzen Zeit auf dem Markt erschienen sind.

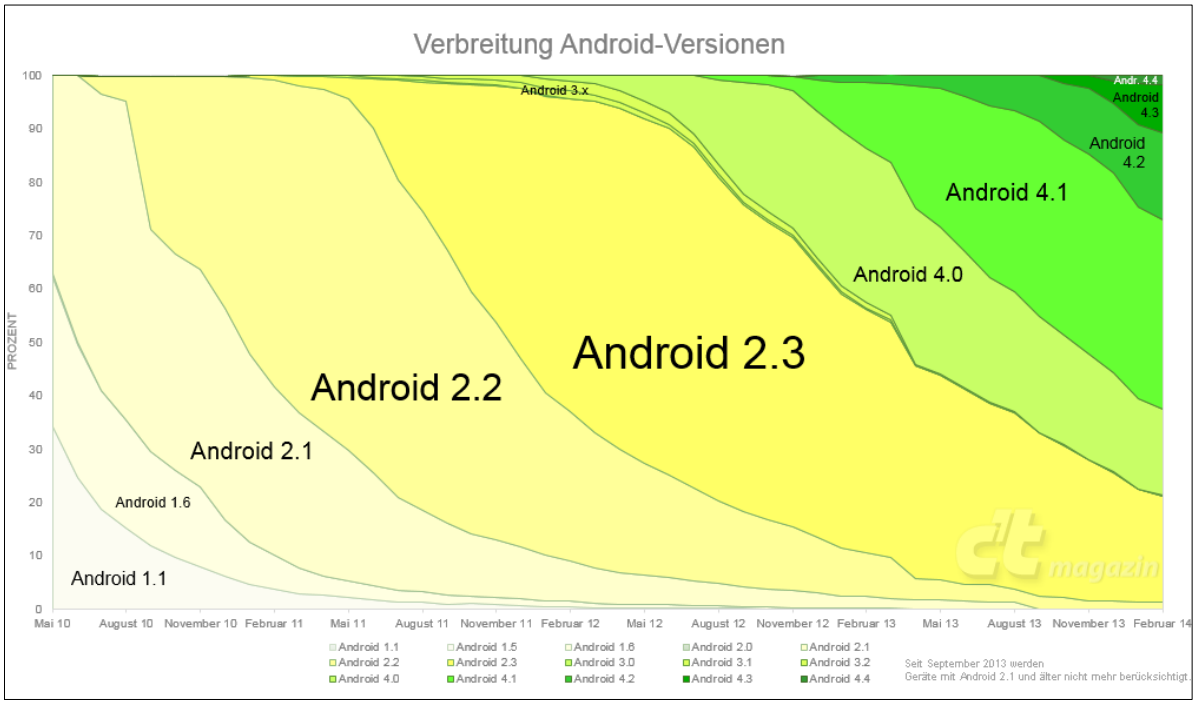


Abbildung 10: Android-Verteilung bis Februar 2014[87]

Bei einigen mobilen Endgeräten und bei Spezialgeräten gilt, dass der Hersteller der Hardware auch das Betriebssystem erstellt. Bei den meisten mobilen Endgeräten gilt jedoch, dass der Hardware-Hersteller ein Betriebssystem zukauft und an seine Hardware anpasst. Damit ist in der Regel mehr als ein Hersteller für das Schließen von Sicherheitslücken zuständig, was den Absicherungsprozess zusätzlich erschwert.[88] Nicht nur liefern Hersteller von Android-Smartphones selten Updates, auch währt die Update Versorgung unheimlich kurz. Während auf einem iPhone in der Regel für mindestens drei Jahre das aktuelle Betriebssystem läuft, ist bei Android spätestens nach zwei Jahren Schluss. Und selbst das ist die Ausnahme: Nur die Nexus-Serie von Google sowie Spitzenmodelle wie das Galaxy Note, das Galaxy S

[86] A. Barczok u.a. (2013)
[87] J. Wirtgen (2014)
[88] Bundesamt für Sicherheit in der Informationstechnik (2006, S. 7)

oder das Motorola Razr werden so lange mit Updates versorgt, bei den günstigeren Modellen muss man sich schon über 12 Monate freuen.[89]

4.1.3. Aufbau der Geräten

Die Bauteile von mobilen Endgeräten werden meist nicht verschraubt, sondern fast untrennbar miteinander verklebt. Das hat Vorteile bei der Herstellung - geht es um Reparatur und Recycling, entstehen aber große Probleme. Zum Beispiel der Touchscreen ist so ein Problem bei den Smartphones und Tablets. Bildet das Frontglas mit dem eigentlichen Display eine Einheit, werden mitunter bis zu 50% des Neupreises für ein Ersatzteil fällig. Bei reparaturfreundlichen Modellen ist das Frontglas separat austauschbar. Sind allerdings das Gehäuse oder einzelne Bauteile verklebt, wird es schwierig, das Gerät zu öffnen und vor allem auch wieder zu schließen. Nichts darf abbrechen, Klebstoffreste müssen sorgfältig entfernt und durch einen zulässigen Kleber ersetzt werden. Auch den Akku auszutauschen kann sehr schwierig sein. Denn zugunsten der superflachen Bauweise verzichten etliche Hersteller inzwischen auf ein Fach mit Klappe, in dem ein quaderförmiger Akku liegt. Flach und unregelmäßig geformt nutzt der Stromspeicher stattdessen jeden denkbaren Winkel zwischen den anderen Bauteilen. Um ihn freizulegen, muss man erst in vielen Einzelschritten das Gerät zerlegen – und anschließend wieder zusammenbauen.[90]

Auch bei den Laptops der jüngsten Generation von Apple, den sogenannten Retina-Modellen, ist die Problematik ähnlich. Sie verfügen ebenfalls über festverklebte Bildschirme, darüber hinaus werden die Batteriezellen mit dem Rechnerboden verklebt, vorgeblich um den Platz besser auszunutzen. Ist der Akku kaputt, wird die gesamte Baugruppe ausgetauscht – laut Apple Reparaturdokumentation inklusive des Alu-Bodens der Geräte.

Beim Recycling verursacht dies diverse Probleme. So kann sich ein Wiederverwerter bei der Trennung von Akku und Gehäuse verletzen und es sogar zu Bränden

[89] A. Barczok u.a. (2013)
[90] Bayerischer Rundfunk (2013)

kommen. Die Verklebung sorgt außerdem dafür, dass der Verwertungsprozess selbst länger dauert als bei anderen Rechnern.[91]

4.1.4. Sollbruchstellen

Außerdem achten die Hersteller von mobilen Endgeräten darauf, dass ihre Produkte nicht ewig halten, möglicherweise durch geplanten Verschleiß. Sowie trotz robusten Außeneindruck wie Gehäuse aus Aluminium, Innenrahmen aus Titan, Oberflächen aus Keramik oder speziell gehärtetem Glas sind die neuen mobilen Endgeräte nicht so langlebig, wie sie aussehen. Die Hersteller

- schließen Altgeräte von wichtigen Software-Upgrades aus (wie schon erwähnt),
- verkleben Verschleißteile wie den Akku nicht auswechselbar im Gehäuse oder
- erschweren Reparaturen oder machen sie wirtschaftlich unsinnig.[92]

Geräte mit z.B. herausnehmbarem Akku sind leichter zu reparieren, da der Akku eine begrenzte Lebensdauer hat. Einige Hersteller konstruieren ihre Geräte so, dass sich der alte Akku nicht durch einen neuen ersetzen lässt – und damit ist das gesamte Produkt nicht mehr zu gebrauchen.[93]

Ein klassisches Beispiel ist der Tintenstrahldrucker, bei dem ein verborgenes Programmmodul die Druckvorgänge zählt und nach Erreichen des vorgegebenen Limits einen Stopp-Befehl sendet.[94] Bei z.B. Notebooks sind häufige Schwachstellen der Bildschirmmechanismus und die Anschlussbuchse für das Netzwerkteil (das Netzteil schmilzt zum Beispiel manchmal im Laptopgehäuse fest).[95] Oftmals haben ganze Notebook-Serien mit Hitzeproblemen zu kämpfen, denn durch das geringe Platzangebot ist das Thema Kühlung bei mobilen Endgeräten ein Problem. Auch die tägliche Betriebsdauer zeigt großen Einfluss auf die Haltbarkeit der Hardware-Komponenten.[96]

[91] B. Schwan (2012)
[92] B. Fuest (2013)
[93] Berliner Morgenpost (2013)
[94] H.-A. Marsiske (2012)
[95] M. Strüber (2012)
[96] R. Haberer (2009)

4.2. Ökobilanz

Eine Studie im Auftrag des Umweltbundesamtes zeigt, dass es über 80 Jahre dauert, bis bei 10 prozentiger Energieeffizienzsteigerung zwischen zwei Notebook Generationen die Energie, die für die Herstellung des neuen Notebooks verwandt wird, kompensiert ist. Auch die Verwertung am Lebensende des Notebooks ändert daran nichts. Denn von den 380kg CO2, die insgesamt in 5 Jahren Nutzungsdauer durch Herstellung, Vertrieb, Nutzung und Entsorgung entstehen, entfallen 55% auf die Herstellung und 36% auf die Nutzung. Den Rest machen Vertrieb und Entsorgung aus. Nur mit langer Lebens- und Nutzungsdauer lässt sich ein Beitrag zum Klima- und Ressourcenschutz leisten. Deshalb: Je länger ein mobiler Endgerät genutzt wird, desto geringer ist der ökologische Fußabdruck. Voraussetzung dafür ist allerdings, dass Komponenten wie beispielsweise der Akku, ausgetauscht werden können, wenn sie defekt sind oder das Lebensende erreicht haben. Darüber hinaus können durch ein recyclinggerechtes Design die wertvollen Metalle wiedergewonnen werden. Unter den Metallen befinden sich auch solche, die in der Gewinnung und Aufbereitung sehr umweltbelastend oder die sehr selten sind.[97] Die Abbildung 11 zeigt, welche Rohstoffe durchschnittlich in einem Mobiltelefon entfalten sind.

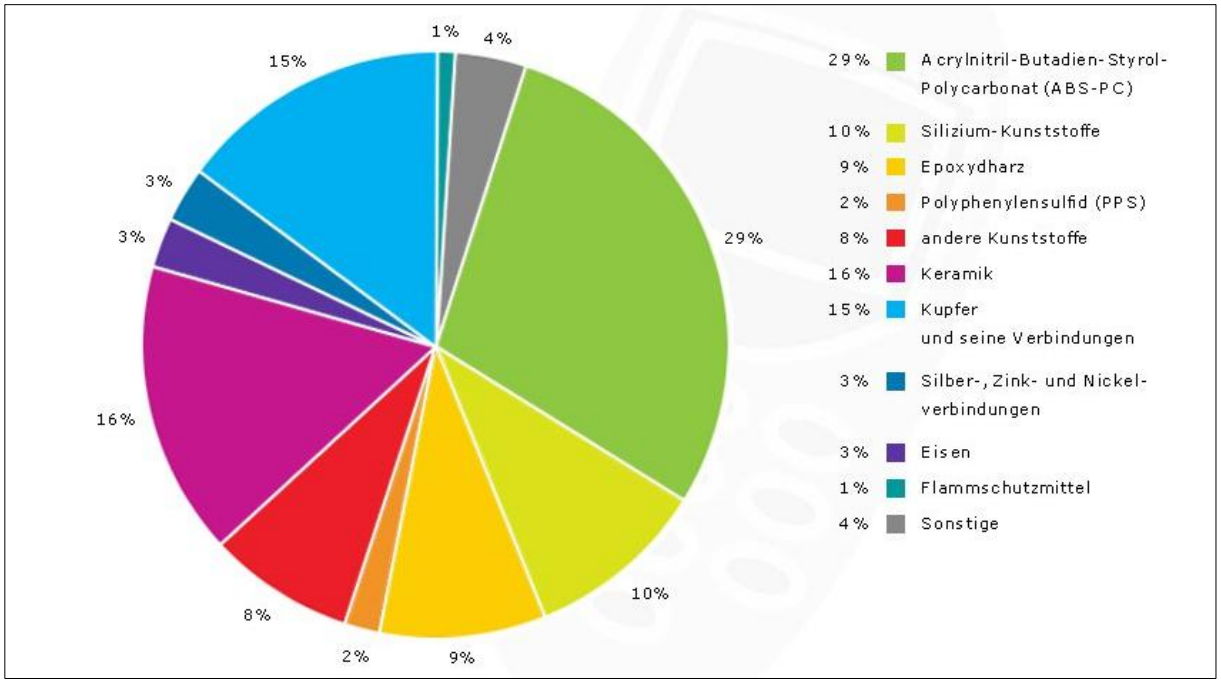


Abbildung 11: Rohstoffe in einem Mobiltelefon[98]

[97] Das Umweltbundesamt (2013c)
[98] A. Sokolow (2011)

Viele von ihnen haben eine strategische Bedeutung für wichtige Nachhaltigkeitstechniken (beispielsweise die Erzeugung erneuerbarer Energie durch Windkraftanlagen). Wenn die Geräte getrennt gesammelt werden, kann wenigstens ein Teil dieser Metalle zurückgewonnen werden.[99] Strategische Metalle können nicht in Deutschland gefördert werden, sondern müssen vollständig importiert werden. Die eigene Versorgungssicherheit hängt auch von unserer Fähigkeit ab einmal importierte Rohstoffe durch den Aufbau einer Kreislaufwirtschaft immer wieder zu nutzen.[100]

4.3. Entsorgung von mobilen Endgeräten

Das fachgerechte Recycling von Elektrogeräten ist wichtig, denn der Abbau der in den Elektrogeräten enthaltenen Rohstoffe ist deutlich belastender für die Umwelt, als die Rückgewinnung durch das Recycling der alten Hardware.[101] Das Recycling von mobilen Endgeräten kann schwierig sein – weil sie so stabil gebaut sind. Die komplette Demontage ist für Zerlege-Betriebe viel zu arbeitsaufwändig, sie nehmen nur den Akku heraus. Nickel-Metallhydrid-Akkus werden von Metallhütten eingeschmolzen, um das Nickel zurückzugewinnen, Lithium hingegen wird bislang nicht recycelt, weil sich das nicht rechnet. Trotzdem müssen auch Lithium-Ionen-Akkus aus den Geräten entfernt werden – aus Sicherheitsgründen. Denn die Geräte werden in Kupferhütten vor dem Einschmelzen zerkleinert, und dabei könnte ein Akku mit Restladung Feuer fangen.[102] Um eine umweltschonende Entsorgung zu gewährleisten, müssen die einzelnen Bauteile leicht zu trennen sein. Dies erhöht die Chance, viele verschiedene Teile wieder zu verwerten. Es ist daher wichtig, dass z. B. die Akkus leicht entnehmbar sind. Leider werden auch bei gutem Recycling nicht alle Metalle vollständig zurückgewonnen.[103]

Außerdem darf Elektroschrott nicht mehr im Hausmüll entsorgt werden. Nach dem Elektrogesetz (ElektroG) können Nutzer ausgediente mobile Endgeräte bei den kommunalen Sammelstellen kostenlos abgeben. In einigen Gemeinden stellen die

[99] Das Umweltbundesamt (2014)
[100] Bayerisches Staatsministerium für Umwelt und Verbraucherschutz (2012)
[101] Bjoern (2012b)
[102] Bayerischer Rundfunk (2013)
[103] Das Umweltbundesamt (2014)

Entsorger den Nutzern auch eigene Sammeltonnen für Elektro-Kleingeräte und andere Wertstoffe zur Verfügung, die abgeholt werden. Der kommunale Entsorger sammelt den elektronischen Schrott, welcher von den Elektronikherstellern zurückgenommen und entsorgt werden muss.[104] Deutschlandweit gibt es rund 1.500 kommunale Sammelstellen, die Elektroschrott entgegennehmen und verwerten. Die Kosten für das Recycling fallen dem jeweiligen Hersteller zu lasten.[105]

4.4. Der Blaue Engel

Damit Verbraucherinnen und Verbraucher sowie private und öffentliche Beschaffer beim Kauf von Produkten deren Umwelteigenschaften berücksichtigen können, sind sie auf zuverlässige Informationen und klare Kennzeichnungen angewiesen. Dabei hilft der "Blaue Engel", das Umweltzeichen des Bundesministeriums für Umwelt, Naturschutz, Bau und Reaktorsicherheit. Der "Blaue Engel" kennzeichnet Produkte und Dienstleistungen, die in einer ganzheitlichen Betrachtung besonders umweltfreundlich sind. Die Kriterien sind dabei so definiert, dass sie von schätzungsweise 20% der aus Umweltsicht besten Angebote einer Produktgruppe erfüllt werden können. Durch eine dynamische Anpassung der Vergabegrundlagen behält der "Blaue Engel" die zukünftige Entwicklung im Auge, um Schrittmacher für eine nachhaltige Produktentwicklung zu sein.[106] Mit ca. 12.000 Produkten - von über 1.200 Herstellern in ca. 120 Produktgruppen ist der "Blaue Engel" das erste und auch erfolgreichste Umweltzeichen der Welt. Es wurde 1977 vom damals zuständigen Bundesinnenministerium und den Bundesländern ins Leben gerufen. Seit nunmehr 35 Jahren ist das deutsche Umweltzeichen "Blauer Engel" ein unverzichtbares und wertvolles Instrument der Umweltpolitik, das den Nutzern den Weg zum ökologisch besseren Produkt weist.[107]

Der Blaue Engel gibt die Orientierung und setzt strenge Anforderungen. Zum Beispiel die Computer mit diesem Zeichen sind geräuscharm. Sie haben einen optimierten Energieverbrauch und sie sind arm an Schadstoffemissionen. Die Konstruktion und die Materialien sollen die Reparatur und Aufrüstbarkeit erleichtern und eine

[104] R. Trautmann, M. Eisinger (2014)
[105] T. Specht (2013)
[106] Bundesministerium für Umwelt, Naturschutz, Bau und Reaktorsicherheit (2013a)
[107] Bundesministerium für Umwelt, Naturschutz, Bau und Reaktorsicherheit (2013a)

Wiederverwendung oder stoffliche Verwertung ermöglichen, um Ressourcen zu schonen.[108]

Für mobile Endgeräte sind die Kriterien des Blauen Engels eine gute Orientierung. Eine wichtige Anforderung ist die vorsorgliche Begrenzung der elektromagnetischen Strahlung beim Blauen Engel. Um eine möglichst lange Nutzungsdauer der Geräte zu fördern, schreibt der Blaue Engel Möglichkeiten für Software-Updates des Betriebssystems, die nachträgliche Aufrüstung der Speicherkapazität sowie Kapazitätstests für die Akkumulatoren vor. Außerdem müssen die Akkus leicht austauschbar sein. Dies ist auch für die spätere recyclinggerechte Entsorgung der Geräte wichtig. Für eine problemlose Zweitnutzung soll das mobile Endgerät zudem über die Möglichkeit der Löschung oder Entnahme sämtlicher auf dem Gerät gespeicherten persönlichen Daten verfügen.[109]

[108] Der Blaue Engel (2014)
[109] Bundesministerium für Umwelt, Naturschutz, Bau und Reaktorsicherheit (2013b)

5. Ende der Nutzung

Bei den mobilen Endgeräten, besonders kleinen wie Mobiltelefonen oder Smartphones, passiert es deutlich häufiger, dass sie einfach in irgendeine Schublade aussortiert und dort vergessen werden. Nach Schätzungen von Industrie und Regierung liegen in deutschen Haushalten inzwischen mehr als 80 Millionen veraltete oder kaputte Mobiltelefone. Dabei können im mobilen Endgeräte verbaute Materialien - darunter wertvolle, aber auch potenziell schädliche Rohstoffe - inzwischen größtenteils wiederverwertet werden. Die Deutsche Telekom etwa schätzt den Anteil auf bis zu 80%.[110]

Um einen Überblick zu erarbeiten, wie in Organisationen mit mobilen (Alt-)Geräten am Ende ihrer Nutzungszeit verfahren wird, wurde außer Literaturrecherche ein persönliches Interview mit Geschäftsführer der Green Power GmbH Herrn Olrik Thonig durchgeführt. Nach einer Grundlegender Analyse der Nutzungsmöglichkeiten der mobilen Endgeräten in Organisationen am Ende der Nutzungszeit lassen sich zwei Möglichkeiten ableiten: die Weiterverwendung der alter Technik und endgültige Außerbetriebssetzung. Der detaillierte Überblick, wie es genau verfahren werden kann, wird in den nächsten Kapiteln erklärt.

5.1. Weiterverwendung

Die Nutzer und Organisationen können ältere, aber noch intakte mobile Endgeräte auch verschenken, verkaufen oder etwa als Not-Gerät behalten. Verschiedene Initiativen sammeln alte mobile Endgeräte, um Rohstoffe wiederzuverwerten oder die mobile Endgeräte in Entwicklungsländer zu verschicken.[111] Auch ältere Geräte könnten oft noch sinnvoll eingesetzt werden, zudem enthalten sie wertvolle Rohstoffe, die wiederverwertbar sind. Über 80% der verwendeten Materialien sind wiederverwertbar. Zwar sind die Rohstoffmengen in jedem einzelnen Gerät gering, Millionen Geräte können aber einen wichtigen Beitrag zum Ressourcen- und Umweltschutz leisten.[112] Doch abseits der fachgerechten Entsorgung gibt es noch

[110] A. Sokolow (2011)
[111] n-tv (2013)
[112] Bjoern (2012a)

weitere Möglichkeiten, sich umweltfreundlich von Alt-Geräten zu trennen, wenn diese noch funktionstüchtig sind.[113]

5.1.1. Verkauf

Funktionierende alte mobile Endgeräte können Verkauft werden. Ein guter Verkaufspreis setzt allerdings ein wenig Aufwand voraus: Fotos und eine ausführliche Artikelbeschreibung sind ein Muss.[114] Die Veräußerung ist über Kleinanzeigen in Zeitungen und Magazinen oder im Internet auf Anzeigen- und Auktionsportalen, z.B. eBay, möglich. Auch gibt es spezielle Firmen, die gebrauchte mobile Endgeräte zu Festpreisen kaufen, aufbereiten und dann weiterverkaufen. Solche Anbieter sind etwa "Wirkaufens", "Zonzoo" und "Rebuy".[115]

5.1.2. Spende

Als Alternative zum Verkauf bietet sich die Spende an.[116] Manche Umweltschutz-Organisationen (z.B. Computer Spende Hambug e.V.) nehmen ebenfalls alte mobile Endgeräte an (zum Teil in Kooperation mit Mobilfunkanbietern), um diese dann zu recyclen oder weiterzuverkaufen und den Erlös (zum Teil) in gemeinnützige Projekte fließen zu lassen. Die Rückgabe erfolgt hier zum Beispiel über Sammelstellen der Organisationen, die Shops des Mobilfunkunternehmens oder per Post. In den Geschäften von Mobilfunkanbietern können Geräte zudem, auch unabhängig von Projekten, entweder einfach abgegeben werden, oder der Kunde erhält einen Freiumschlag, um sie einzuschicken. [117]

Die Mobilfunkanbieter versuchen schon seit einiger Zeit, diesen Schatz an nutzlos herumliegender Technik zu heben. So bietet etwa die Telekom an, alte Mobiltelefone kostenlos per Post entgegenzunehmen - oder wahlweise gegen einen Gutschein von bis zu 200 Euro einzutauschen. Dabei arbeitet der Konzern mit dem Anbieter "Wirkaufens" zusammen, der auch Navigationsgeräte, Computer und Kameras aufkauft. Die Höchstmarke von 200 Euro wird allerdings nur mit relativ neuen und

[113] R. Trautmann, M. Eisinger (2014)
[114] Bjoern (2012b)
[115] n-tv (2013)
[116] Bjoern (2012b)
[117] R. Trautmann, M. Eisinger (2014)

funktionsfähigen Geräten erreicht. Ähnliche Aufkäufer im Internet sind etwa "handy-bestkauf.de", "handy-verkaufen.net", "quoka.de" oder "Mobile2cash".[118]

Eine andere Alternative ist das alte Gerät einfach zu verschenken. Ein noch funktionsfähiges Gerät kann gut gebraucht werden.[119] Die Organisationen können alte Geräte, die schon abgeschrieben sind, auch an Mitarbeiter schenken. Zum Beispiel sieben französische Großunternehmen, wie die Bahn SNCF und der Atomkonzern Areva, haben öffentlich beschlossen ausgemusterte Computer an ihre Mitarbeiter zu verschenken.[120]

5.1.3. Not-Gerät

Ein altes mobiles Endgerät kann auch als Not-Gerät für Mitarbeiter nutzen. Falls ein neues Gerät ausfällt, kann altes Gerät oft sofort eingesetzt werden.[121] Dies ist, nach Angaben der Green Power GmbH, oft der Fall bei den Organisationen. Da die Organisationen oft mehr als nur ein Gerät der gleiche Serienreihe kaufen, ist es auch für die Mitarbeiter sehr einfach, ein defektes Gerät durch den selben zu ersetzen und weiter zu nutzen.

5.2. Außerbetriebssetzung

Die zweite Möglichkeit ist die Außerbetriebssetzung. Das trifft meistens auch dann, wenn die mobilen Endgeräte tatsächlich defekt sind und nicht mehr funktionieren. In den Fällen folgen die Organisationen grundsätzlich zwei Möglichkeit: entweder werden defekte Geräte noch als Teilespender für gleiche Modelle gelagert oder die defekte Geräte werden endgültig Entsorgt.

5.2.1. Teilespender

Einzelteile aus den alten Geräten können auch in den neuen Geräten eingesetzt werden. Denn in veraltetem Gerät muss nicht alles reif für den Schrottplatz sein. Zum

[118] A. Sokolow (2011)
[119] R. Trautmann, M. Eisinger (2014)
[120] H. Lücke (2008)
[121] FOCUS Online (2013)

Beispiel die Festplatte aus einem alten Notebook kann auch für andere oder neuen Notebook verwendbar sein, auch der Arbeitsspeicher ist möglicherweise kompatibel.[122] Außerdem können teile wie Akkus, Gehäuse (z.B. Akku-Deckel), Zubehör und Speicherkarten noch nützlich sein, besonders für noch intakte und gleiche Modelle die in der Organisation noch im Einsatz sind.

5.2.2. Entsorgung

Umweltgerechtes Entsorgen alter Technik ist in den vergangenen Jahren deutlich einfacher geworden. Seit der Umsetzung einer entsprechenden EU-Richtlinie 2006 dürfen alte Elektrogeräte nicht mehr in den Hausmüll. Dafür werden sie kostenlos von mehr als 1500 kommunalen Sammelstellen entgegengenommen. Das Recycling müssen die Hersteller bezahlen.[123] Falls die mobilen Endgeräte endgültig entsorgt werden müssen, dann gehört es auf den Sondermüll.[124] Sie müssen professionell entsorgt werden. Nach Angaben des Branchenverbands BITKOM nehmen z.B. Mobilfunkanbieter ihre mobilen Endgeräte kostenlos zurück und spenden dafür oftmals etwas Geld an Hilfsorganisationen oder Umweltschutz-Initiativen. Einige Mobilfunkanbieter nehmen sogar Altgeräte auch beim Kauf neuer Modellen in Zahlung.[125]

[122] FOCUS Online (2013)
[123] A. Sokolow (2011)
[124] T. Specht (2013)
[125] n-tv (2013)

6. Sicherheit

6.1. Bedeutung von IT-Sicherheitsmanagement

Die wachsende Bedeutung einer möglichst umfassenden IT-Sicherheit in Unternehmen und damit der Notwendigkeit zur Etablierung von IT-Sicherheitsmanagement ergibt sich aus einer Reihe von Gründen:

- Die Durchdringung von Unternehmen aller Branchen und Größenordnungen mit IT und die daraus resultierende zunehmende Abhängigkeit von der IT erfordern ein hohes Maß an IT-Sicherheit. So beziffert beispielsweise der IT-Vorstand einer Versicherung den Verlust bei IT-Ausfall in einer einzigen Zweigniederlassung auf ca. 1 Million EUR pro Tag. Der IT-Leiter eines Automobilunternehmens hat die Überlebensfähigkeit des Unternehmens ohne IT auf maximal zwei Wochen eingeschätzt. Auch mittelständische Unternehmen sind zunehmend von IT-Systemen, z. B. für Angebots- und Auftragsbearbeitung oder Produktionsplanung und -steuerung, abhängig und würden bei längerem Ausfall der IT in ernsthafte Schwierigkeiten geraten.

- Das wachsende Bedrohungspotenzial, das sich durch den flächendeckenden Einsatz der Internettechnologien zum Teil exponentiell erhöht, stellt die IT-Sicherheit vor besondere Herausforderungen. Folgende Entwicklungen, die sich zum Teil verstärken, tragen hierzu bei:

  - Die Anzahl der Websites, der Internethosts und der Nutzer ist seit der "Erfindung" des WWW im Jahr 1990 explosionsartig gestiegen. Mobile Zugangstechnologien wie WLAN erhöhen die Nutzbarkeit des Internets und werden zusammen mit Internetdiensten wie VoIP oder Skype weiteres Wachstum generieren.

  - Im Internet laufen sehr viele geschäftskritische - auch unternehmensübergreifende - Anwendungen, auf die Mitarbeiter von Niederlassungen, vom HomeOffice oder bei Dienstreisen von unterwegs aus

über Fest- oder Mobilfunknetze ebenso zugreifen wie Logistikunternehmen, Lieferanten, Kunden und andere Geschäftspartner.

- Computerkriminelle schließen sich in organisierter Form zusammen und verfolgen vor allem finanzielle Vorteile. Das Bundeskriminalamt hat festgestellt, dass es die Täter im Internet vermehrt auf vollständige digitale Identitäten abgesehen haben. Dies wird erleichtert durch Einbruchswerkzeuge, die im Internet frei verfügbar sind und immer leichter anwendbar und effizienter werden. Als Folge davon werden die Schadprogramme immer ausgefeilter und effektiver. Die Struktur des Internet bietet zudem genug Freiraum, bei Angriffen unerkannt zu bleiben. Im Jahr 2007 wurden in Deutschland 180.000 Straftaten mit Hilfe des Internets begangen, bei der Wirtschaftskriminalität sind 10% der Straftaten auf Basis des Internets ausgeführt worden.

- Die Anzahl der jährlich gemeldeten Softwaresicherheitslücken, die verbreitete Betriebssysteme, Anwendungsprogramme und Netzkomponenten aufweisen und die potenziellen Einbrechern den Zugang erleichtern. Auch werden diese Sicherheitslücken immer schneller ausgenutzt, im Falle so genannter Zero-Day-Angriffe oft vor oder am gleichen Tag der öffentlichen Bekanntmachung.

- In zunehmendem Maße schreiben gesetzliche Vorschriften und Regelungen und andere Compliance-Vorgaben zumindest implizit ein funktionierendes IT-Sicherheitsmanagement vor.[126]

6.2. Gesetzliche Anforderungen

Rechtsvorschriften mit Konsequenzen für den Bereich der IT-Sicherheit sind nicht in einem Gesetz zusammengefasst, sondern verteilen sich auf eine Reihe von Gesetzen und Richtlinien. Neben diesen für nahezu alle Unternehmen gültigen Vorschriften gibt es branchenspezifische Vorschriften, z. B. für den Umgang mit Gesundheits- und Sozialdaten oder auch für Kreditinstitute durch das Kreditwesengesetz (KWG). Zu beachten sind für eine Reihe von Organisationen die

[126] J. Hofmann, W. Schmidt (2010, S. 287 ff.)

Regelungen für den Geheimschutz in der Wirtschaft. Demzufolge müssen Wirtschaftsunternehmen und Forschungseinrichtungen, die IT-Systeme für den Umgang mit staatlichen Geheimdaten (Verschlusssachen) nutzen, entsprechende Sicherheitsmaßnahmen ergreifen.[127] Die wesentlichen Gesetze und Rechtsverordnungen, die nahezu alle Organisationen betreffen, lassen sich in die Kategorien Datenschutz-, Buchführungs- und Archivierungs- sowie Risikomanagementregelungen einteilen (siehe Abbildung 12).[128]

Abbildung 12: Wesentliche gesetzliche Regelungen[129]

Als Unterpunkte sind die jeweilige Gesetzte bzw. Gesetzbücher angeben.

6.3. Gefahren am Ende der Nutzung

Immer mehr Beschäftigte nutzen mobile Endgeräte im geschäftlichen Alltag von unterwegs aus und greifen damit extern auf das Netzwerk der Organisation zu. Zudem versenden sie berufliche E-Mails mit Hilfe mobiler Endgeräte. Das bringt neben vielen Vorzügen auch neue Sicherheitsrisiken mit sich.[130] Für den Einsatz mobiler Endgeräte mit sensiblen Daten muss jedoch deren Sicherheit gewährleistet werden. Sensible Daten können beispielsweise Patientendaten, Kundenlisten oder Adressdaten sein.[131] Auch wenn die Kommunikation und der Zugang zum Backend gesichert sind, ist das mobiles Endgerät selbst nicht vor möglichen Angriffen geschützt. Falls Organisationsdaten auf dem Endgerät gespeichert werden, könnte ein Angreifer versuchen den Zugangskontrollmechanismus des Endgerätes zu

[127] J. Hofmann, W. Schmidt (2010, S. 291 f.)
[128] J. Hofmann, W. Schmidt (2010, S. 292)
[129] J. Hofmann, W. Schmidt (2010, S. 293)
[130] Bundesministerium für Wirtschaft und Energie (2011)
[131] H. Rossnagel, T. Murmann (2005, S. 129)

umgehen, um Zugriff auf die gespeicherten Daten zu erhalten.[132] Doch nur die wenigsten Firmen fühlen sich auch für die damit verbundenen Gefahren gerüstet - in Deutschland sind dies gerade 15%. Das zeigt eine weltweite Umfrage, die Kaspersky Lab zusammen mit B2B International im Jahr 2013 durchgeführt hat.[133]

Kaspersky Lab wollte auch wissen, welche Art von sicherheitsrelevanten Vorfällen in den letzten zwölf Monaten in Organisationen die schwerwiegendsten Folgen hatte. Hier nannten weltweit 6% der Befragten den Datenverlust auf Grund eines falschen Umgangs mit mobilen Geräten. In deutschen Organisationen schlägt besonders der Diebstahl oder Verlust der mobilen Endgeräte an sich mit 10% (weltweit 7%) zu Buche. Generell betrifft ein Diebstahl mobiler Endgeräte in 7% (weltweit 5%) aller Fälle Daten, die die Organisationen selbst als sensibel einstuft, und stellt damit ein besonders großes Gefahrenpotenzial dar. Auch deutsche Organisationen sind sich dabei der Gefahren durchaus bewusst.[134]

Das Modell „BOYD“ kann in vielen Fällen praktisch und kostensparend sein, birgt jedoch auch erhebliche Gefahren für die IT-Sicherheit in Organisationen, sofern BYOD nicht von entsprechenden Maßnahmen begleitet wird. Immerhin 66% der Organisationen in Deutschland (weltweit 65%) geben an, dass BYOD-Trend zunehmend problematisch für die Sicherheit der IT-Infrastruktur in Organisationen wird. Gleichzeitig sehen sich aber 35% (weltweit 34%) der Situation relativ machtlos gegenüber und glauben, dass sich der BYOD-Trend nicht mehr aufhalten lässt.[135]

Die IT-Abteilung muss deshalb ihre Fühler über das klassische Organisationsnetzwerk hinaus ausstrecken und Wege finden, um die mobilen Endgeräte lückenlos abzusichern und zu kontrollieren. Denn Nutzungsrichtlinien und Verbote taugen nur dann etwas, wenn man ihre Einhaltung auch genaustens nachvollziehen kann. Die IT sieht sich gleich mit mehreren Problemen konfrontiert: auf den Mobilfunkgeräten müssen wirksame Sicherheitseinstellungen implementiert

[132] H. Rossnagel, T. Murmann (2005, S. 130)
[133] Die Umfrage wurde von B2B International im Auftrag von Kaspersky Lab im Jahr 2013 durchgeführt. Dabei wurden mehr als 2.895 IT-Entscheider aus 24 Ländern befragt – u.a. 117 deutsche. Es wurden Unternehmen jeglicher Größe erfasst, in drei Klassen von 10 bis 99 Arbeitsplätzen, über 100 bis 1.500 Arbeitsplätzen und Unternehmen mit mehr als 1.500 Arbeitsplätzen. Die Studie ist eine Fortführung von zwei früheren B2B International-Umfragen, die Kaspersky Lab mit ähnlichen Themen bereits im Jahr 2011 und 2012 beauftragt hat.
[134] Institut für Internet-Sicherheit - if (2013)
[135] Institut für Internet-Sicherheit - if (2013)

werden. Bei der Verwaltung vieler Endgeräte kann eine zentrale Fernsteuerung in Frage kommen. Und sie sollen sich natürlich nahtlos und benutzerfreundlich in das Netzwerk und die Business-Prozesse integrieren. Eine Trennung zwischen Organisationseigenen und BYOD Geräten ist hier ohne technische Maßnahmen kaum möglich und die Absicherung der geschäftlichen Nutzung damit schwer zu bewerkstelligen. Der Wildwuchs an Geräten, Betriebssystemen und Apps erschwert eine vernünftige Kontrolle zusätzlich. Es entstehen Heterogene IT-Landschaften.[136]

6.4. Sicherheitsrichtlinien

Weltweit verfügen bislang nur 14% aller Organisationen (in Deutschland 15%) über voll implementierte Sicherheitsrichtlinien. Vielleicht noch bedenklicher ist aber ein anderes Ergebnis der Umfrage: 32% der deutschen Organisationen gaben an, noch keinerlei Richtlinien für den Umgang mit mobilen Geräten eingeführt zu haben. Weltweit ist das sogar bei fast jeder zweiten Organisation (45%) der Fall.

Dabei könnte gerade die Implementierung von organisationseigenen Richtlinien für einen bewussten Umgang der Mitarbeiter mit ihren mobilen Endgeräten die Risiken für Organisationen enorm reduzieren. In Deutschland geben aktuell 53% (weltweit 41%) der Organisationen an, zwar bereits Regeln entwickelt, diese jedoch noch nicht voll umgesetzt zu haben. 20% (weltweit 32%) wollen demnächst überhaupt erst einmal Richtlinien einführen. Und 12% (weltweit 13%) glauben, auch zukünftig ganz darauf verzichten zu können.

Oft scheitert die Umsetzung der Sicherheitsrichtlinien an finanziellen Fragen. 52% der deutschen Organisationen und 48% weltweit geben zu, dafür noch kein ausreichendes Budget bereitgestellt zu haben. Ganz ohne zusätzliches IT-Budget wollen demnach 16% auskommen.[137]

Ein Sicherheitskonzept sollte für die Nutzung von mobilen Endgeräten klare Regeln aufstellen. Sicherheitsregeln zum Umgang mit mobilen Endgeräten sollten auch die

[136] J. Pohl (2013)
[137] Institut für Internet-Sicherheit - if (2013)

private Nutzung der Geräte regeln, etwa ob den Mitarbeitern das Installieren von Apps erlaubt ist.[138]

Auch um zum Beispiel BYOD-Trend zuvorkommen können Organisationen die Richtlinien und Verfahren festlegen, in denen bestimmt wird, auf welche Inhalte von diesen Endgeräten aus zugegriffen werden kann, wie der Zugriff erfolgt und wie die Organisation bei einem Verlust oder Diebstahl eines Endgeräts verfährt, auf dem sich geschäftliche Informationen befinden. Auf diese Weise können die Mitarbeiter nach wie vor unterwegs, zuhause oder an einem Kundenstandort produktiv arbeiten und die Organisation reduziert das Risiko, dass Unbefugte Zugriff auf die Daten erhalten. Nachstehend ist ein Beispiel für Sicherheitsrichtlinien für mobile Endgeräte aufgeführt, was als Ausgangsbasis verwendet kann. Es eignet sich für private Endgeräte von Mitarbeitern und für solche, die von der Organisation bereitgestellt werden:

- Alphanumerisches Kennwort mit acht Zeichen für das mobile Endgerät
    - Ablauf alle 90 Tage
    - Sperre des Geräts nach 15 Minuten
    - Die Aufforderung zur Kennworteingabe auf dem Endgerät sollte nach jedem nicht erfolgreichen Anmeldeversuch in immer längeren Abständen erfolgen, um Schutz vor Brute-Force-Anmeldeversuchen zu bieten

- Bereinigung des Endgeräts
    - Über Fernzugriff (durch den Administrator), falls das Endgerät verloren geht oder gestohlen wird
    - Nach 10 Anmeldeversuchen mit ungültigem Kennwort, um Schutz vor Brute-Force-Anmeldeversuchen zu bieten

- Verschlüsselung von ruhenden Daten für Mitarbeiter mit Zugriff auf wertvolle oder sensible Daten
    - Mindestens 128-Bit-Verschlüsselung gemäß Advanced Encryption Standard (AES)

[138] BITKOM (2012b)

  - Schutz für die entsprechenden Verschlüsselungsschlüssel, die so ausgetauscht oder gespeichert werden, dass sie weder im Dateisystem noch bei der Übertragung problemlos in lesbarer Form abgerufen werden können
  - Verfahren zur Wiedergabe des Verschlüsselungsstatus eines bestimmten Endgeräts ausgehend von Nutzen, Anwendung von Richtlinien etc.

- Bluetooth-Konfiguration, die sicherstellt, dass das Gerät für andere unsichtbar ist und nur mit bereits bekannten, d. h. bereits gekoppelten, Endgeräten funktioniert, die diese Features unterstützen

- Regelung, dass Fernzugriff zur Datensynchronisation oder auf die Organisationsinfrastruktur über ein genehmigtes Gateway für den Fernzugriff erfolgt und die erforderliche Sicherheitsauthentifizierung unterstützt wird

- Lokale Synchronisation unter Verwendung von direkten USB, Infrarot, Bluetooth, WLAN, LAN oder mobilen Verbindungen

- Virenschutzprogramm auf allen Endgeräten mit Verbindung zum Organisationsnetzwerk

- Firewall-Programm auf dem mobilen Endgerät.[139]

Die Verwendung von IT-Standards und Richtlinien kann unter anderem zu folgenden Nutzeffekten führen:

– Kostensenkung

  Durch die Nutzung vorhandener und praxiserprobter Vorgehensmodelle wie beispielsweise dem BSI-Grundschutzmodell sind die Etablierung und Aufrechterhaltung von IT-Sicherheitsmanagement mit weniger Ressourcenaufwand realisierbar.

– Einführung eines angemessenen Sicherheitsniveaus

[139] IBM (2012, S. 4 f.)

Die Verwendung eines Standards gewährleistet die Orientierung am aktuellen Stand von Wissenschaft und Technik.

- Wettbewerbsvorteile

  Im Rahmen von öffentlichen oder privatwirtschaftlichen Vergabeverfahren werden zunehmend auf IT-Sicherheitsstandards basierende Zertifikate als Voraussetzung für die Teilnahme gefordert.[140]

[140] J. Hofmann, W. Schmidt (2010, S. 298)

7. Empfehlungen

Damit die Organisationen nachhaltiger und sicher mit mobilen Endgeräten am Ende ihrer Nutzungszeit umgehen können, wird in diesem Kapitel versucht aus der Nachhaltigkeits- und Datensicherheitsperspektive Empfehlungen zu geben. Hierfür werden Erkenntnisse aus der Literaturrecherche und persönlichem Gespräch mit Geschäftsführer der Green Power GmbH Herrn Olrik Thonig genutzt.

7.1. Nachhaltigkeit

7.1.1. Lange Lebensdauer

Die Umweltbelastungen von mobilen Endgeräten können Organisationen vor allem dadurch reduzieren, dass die Organisationen den mobilen Endgeräten möglichst lange nutzen. Auch wenn es hier keine einfachen Regeln für Nutzer gibt, können die Organisationen schon beim Kauf darauf achten. Zum Beispiel sollte die Speicherkapazität erweiterbar sein, damit Sie diese zu einem späteren Zeitpunkt selbstständig erweitern können. Auch eine integrierte Ladestandanzeige ist sinnvoll, die den aktuellen Stand der Batterieladung während der Nutzung und während des Ladevorgangs optisch sichtbar macht. Bei vielen Geräten ist der Akku fest mit dem Gerät verbunden. Falls der Akku kaputt geht, wird die Reparatur aufwendig und teuer. Empfohlen wird deshalb, Geräte zu kaufen, bei denen die Nutzer den Akku selber auswechseln können.[141]

Beim Kauf eines neuen mobilen Endgerätes sind die Kriterien des Blauen Engels eine gute Orientierung, wenn die Organisation Wert auf die Gesundheit und die Ressourcenschonung legt. Eine wichtige Anforderung ist die vorsorgliche Begrenzung der elektromagnetischen Strahlung beim Blauen Engel. Um eine möglichst lange Nutzungsdauer der Geräte zu fördern, schreibt der Blaue Engel Möglichkeiten für Software-Updates des Betriebssystems, die nachträgliche Aufrüstung der Speicherkapazität (z.B. durch SD-Karte) sowie Kapazitätstests für die Akkumulatoren vor.[142]

[141] Das Umweltbundesamt (2014)
[142] Bundesministerium für Umwelt, Naturschutz, Bau und Reaktorsicherheit (2013b)

Außerdem empfohlen werden Schritte aus einem Leitfaden-Katalog (im Anhang) für die umweltfreundliche Beschaffung von Notebooks des Umweltbundesamtes. Dieser Leitfaden wurde durch eine Arbeitsgruppe des Beschaffungsamtes des Bundesministeriums des Innern, des Bundesverbandes Informationswirtschaft, Telekommunikation und neue Medien e.V. (BITKOM) des Bundesministeriums für Umwelt, Naturschutz und Reaktorsicherheit (BMU) und des Umweltbundesamtes (UBA) erstellt.[143]

7.1.2. Geringe elektromagnetische Strahlung

Ein wichtiger Indikator für die gesundheitlichen Wirkungen der Funkwellen bei mobilen Endgeräten mit Mobilfunknutzung ist die spezifische Absorptionsrate, der SAR-Wert. Er wird ausgedrückt in Watt pro Kilogramm biologisches Gewebe und wird grundsätzlich bei maximaler Leistung des mobilen Endgeräts nach einem standardisierten Verfahren gemessen. Moderne mobile Endgeräte haben gegenüber älteren Modellen einen Vorteil. Sie senden oft im UMTS-Standard, der beim Verbindungsaufbau strahlungsärmer ist als der GSM-Standard. Neben Mobilfunkverbindungen können mobile Endgeräte in der Regel auch Wireless LAN nutzen. Wenn es die Wahl gibt, dann sollte mit dem mobilen Endgerät über Wireless LAN ins Internet statt über Mobilfunk eingewählt. Die Datenübertragung über Mobilfunk verbraucht wesentlich mehr Energie als über einen stationären Anschluss. Das Umweltzeichen „Blauer Engel“ fordert für mobile Endgeräte einen SAR-Wert kleiner 0,6 W/kg, um vorbeugend die Strahlenexpositionen gering zu halten.[144]

7.1.3. Richtige Entsorgung

Viele ungenutzte Geräte sind noch funktionsfähig und könnten eingesetzt werden. Eine Weitergabe oder ein Verkauf ist auch ein Beitrag zur Ressourcenschonung. Defekte Geräte sollten auf jeden Fall zurückgegeben werden, weil so seltene und wertvolle Rohstoffe wiederverwertet werden können.[145] Ausgemusterte Geräte werden aber oft noch aufbewahrt. Die Hauptgründe sind:

[143] Das Umweltbundesamt (2013b)
[144] Das Umweltbundesamt (2014)
[145] Carsten (2014)

- Jeder zweite (50%) Betroffene hebt das mobile (Alt-)Gerät als Ersatz für den neuen auf;
- gut jedem fünften (21%) ist die Entsorgung zu aufwändig;
- jeder neunte (11%) weiß nicht, wie er private Daten auf seinem mobilen (Alt-) Gerät löscht.

Weiteren 6% fehlen Informationen, wie sie die alten Geräte entsorgen können.[146]

Nutzer können nach dem Elektro- und Elektronikgerätegesetz ihre alten Geräte kostenlos bei kommunalen Sammelstellen abgeben. Viele Hilfs- und Umweltschutzorganisationen sammeln mobile Endgeräte für unterschiedliche karitative Zwecke.[147]

7.1.4. Aufrüsten

Nicht immer müssen Organisationen auf ein neues und schnelles Gerät wechseln. Selbst alte Geräte reichen meist für gängige Büroarbeiten aus. Aufrüsten statt komplett neu kaufen ist die bessere Alternative. In vielen Fällen genügt einfach ein schnellerer Prozessor, eine neue Grafikkarte oder eine schnellere Festplatte. Beispielsweise bringt der Wechsel von einer normalen Festplatte (HDD) zu einer Solid-State-Festplatte (SSD) sogar eine – zumindest gefühlt – größere Leistungssteigerung, als ein schnellerer Prozessor. SSDs sind wesentlich schneller, weniger störanfällig und verbrauchen weniger Strom als herkömmliche Magnetspeicher-Festplatten. So steigt die Akkulaufzeit und gleichzeitig werden die Daten schneller gespeichert. Auch der Betriebssystem-Start und das Laden von Programmen gehen wesentlich schneller vonstatten.[148] Allein damit erreichen viele ältere mobile Endgeräte Arbeitsgeschwindigkeiten, die denen aktueller Einsteiger- und Mittelklasse-Gerät kaum nachstehen. Darüber hinaus lassen sich bei vielen Geräten auch die oft veralteten WLAN-Module durch leistungsfähigere ersetzen und sogar Bluetooth-Chips nachrüsten.[149]

[146] Bjoern (2012a)
[147] Das Umweltbundesamt (2014)
[148] A. Maurer (2011)
[149] T. Rau (2012)

7.2. Sicherheit

Egal ob Entsorgung, Verkauf oder Lagerung als Not-Gerät sollten alle privaten oder Organisationsdaten auf den mobilen Endgeräten wie Adressbuch, Online-Banking-Zugänge sowie Fotos und Videos zuvor gelöscht werden. Mobile Endgeräte bieten eine Funktion, die sich sinngemäß "Daten löschen und Werkseinstellungen wiederherstellen" nennt. Wichtig ist zudem, Speicherkarten aus den Endgeräten zu entfernen oder mit einem Softwareprogramm zu löschen.[150] Detailliert wird in den nächsten Kapiteln erklärt.

7.2.1. Sicherheitsrichtlinie

Die Sicherheit von Organisationsdaten stellt insbesondere bei mobilen Endgeräten, die leicht verloren gehen oder gestohlen werden können, ein Problem dar. Das Sicherheitsrisiko wird durch die immer stärkere Nutzung mobiler Endgeräte von Mitarbeitern in vielen Organisationen noch weiter verschärft. Die Mitarbeiter gehen bei der Nutzung mobiler Endgeräte für geschäftliche Zwecke gerne den Weg des geringsten Widerstands, was zu Sicherheitsproblemen führen kann. Klar dokumentierte und durchsetzbare Richtlinien für die mobile Sicherheit sind unumgänglich, wenn das Risiko eines Datenverlusts reduziert werden soll.[151]

7.2.2. Datenträger formatieren

Festplattenlaufwerk

Um eine Festplatte weiter zu nutzen, muss es sicher sein, dass sich keine alten Daten auf der Platte finden. Die Festplatte muss sicher formatiert werden. Bei klassischen Festplatten funktioniert dies mittels Software, die die Platte mit neuen Daten überschreibt - zum Beispiel DBAN. Heutige Festplatten lassen sich dabei mit einmaligem Überschreiben sicher löschen - die entsprechenden Programme bieten aber auch das mehrmalige Überschreiben an. Hintergrund ist die Vermutung, dass der Festplattenkopf nicht immer genau dieselbe Spur trifft und daher quasi ein "Restrauschen" übrigbleibt. Das mehrmalige Überschreiben kann hier helfen. Eine

[150] n-tv (2013)
[151] IBM (2012, S. 2)

andere und sichere Möglichkeit ist die so genannte Gutmann-Methode, bei der die Festplatte ganze 35-mal mit unterschiedlichen Mustern überschrieben wird - das kann allerdings Tage dauern.[152]

Halbleiterlaufwerk

Bei Halbleiterlaufwerk (Solid-State-Drive) sieht das formatieren ein bisschen anders aus: Durch ihre Funktionsweise bringt das vorher genannte Verfahren bei diesen Datenträgern nichts, denn die Daten liegen nicht wirklich an der Stelle, an der das System sie verortet. Vielmehr lagert der zwischengeschaltete Controller die Daten an eine aus seiner Sicht sinnvollen Stelle und verknüpft so die virtuelle Adresse mit einer echten Adresse (das so genannte wear leveling). Hintergrund ist, dass die Zellen des Speichers gleichmäßig beschrieben werden sollen, um ein möglichst optimales Abnutzungsszenario zu erzeugen. Die SSDs halten Reserve-Kapazität bereit, um kaputte Zellen zu ersetzen. Somit ist mehr Speicher theoretisch verfügbar, als dem Nutzer real zur Verfügung steht - und so kann er auch nicht alle Bereiche erreichen.

Bei Solid-State-Drive hilft indes der so genannte Secure Erase. Das Feature kann die Platte „unwiederherstellbar“ löschen. Genutzt werden kann Secure Erase über Software des Herstellers oder zum Beispiel via Parted Magic. So können zum Beispiel wirklich alle Zellen zurück gesetzt werden - moderne SSD verschlüsseln allerdings die Daten, so dass hier auch ein Verwerfen des Schlüssels eine mögliche Variante ist. Die Daten befinden sich dann noch auf der Platte, sind aber nicht mehr entschlüsselbar und damit bei einem zuverlässigen Verschlüsselungsverfahren wertlos.[153]

7.2.3. Verschlüsselung der Datenlaufwerke

Dieses Verfahren ist auch bei klassischen Festplatten ein möglicher Weg. Anstatt sich später die Arbeit machen zu müssen, die Platte umständlich zu löschen, kann von Anfang an auf Verschlüsselung gesetzt werden. Ein sicheres Verfahren und ein sicheres Passwort vorausgesetzt, führt die Verschlüsselung dazu, dass sich der

[152] R. Trautmann (2014)
[153] R. Trautmann (2014)

Platteninhalt nicht wieder herstellen lässt. Bei Windows ist dies per Bitlocker (in Professional- und Enterprise-Versionen) möglich, eine kostenlose Alternative ist z.B. Truecrypt.[154]

7.2.4. Apps

Gefahren können auch von unseriösen Apps ausgehen. Die kleinen, scheinbar nützlichen Programme für mobile Endgeräte enthalten teilweise schadhafte Codes. Sie sollten deshalb grundsätzlich nur herunter geladen werden, wenn sie einen Nutzen im Geschäftsalltag bringen. Außerdem sollten die Nutzerinnen und Nutzer vor dem Download stets prüfen, ob sie von einem vertrauenswürdigen Anbieter stammen. Onlinerezensionen können dabei eine erste Orientierungshilfe bieten. Aber auch hier ist Vorsicht geboten und der vertrauenswürdige Hintergrund zu hinterfragen.[155]

7.2.5. Netzwerkverbindungen

Um die Risiken zu minimieren, sollten Bluetooth und WLAN nur aktiv sein, wenn der Benutzer die Verbindungen gerade benötigt. Benutzer und Benutzerinnen sollten außerdem nur durch WPA oder besser WPA-2 verschlüsselte WLAN-Verbindungen in Anspruch nehmen. Tauschen Beschäftigte sensible Daten auf mobilen Endgeräten über mobile Netzwerke aus, sollten sie das über ein durch VPN- oder SSL-Protokolle verschlüsseltes Netzwerk tun.

7.2.6. Gerätesperre

Nutzer sollten in jedem Fall die verfügbaren Sicherheitseinstellungen des Smartphones verwenden. Dazu gehört auch der Schutz des mobilen Gerätes durch die Einstellung einer automatischen Sperrung, verbunden mit einem starken Kennwort. Dieses sollte aus einer sicheren Kombination von mindestens acht Buchstaben, Ziffern und Sonderzeichen bestehen. Auch Notebooks und Tablets sollten immer durch ein sicheres Systempasswort geschützt sein. Wenn das Gerät

[154] R. Trautmann (2014)
[155] Bundesministerium für Wirtschaft und Energie (2011)

nicht genutzt wird, sollte man es grundsätzlich sperren, selbst wenn die Arbeitspausen nur kurz sind.[156]

7.2.7. Backup

Wenn auf einem mobilen Endgerät Organisationsdaten aufbewahren werden, dann sollte regelmäßig Sicherungskopien auf einem Organisationscomputer erstellt werden. Sensible Daten, wie Kundeninformationen oder Geschäftsgeheimnisse, sollten zudem verschlüsselt werden. So wird der mögliche Schaden bei Verlust oder Diebstahl minimiert. Wenn der Ernstfall dennoch eintritt und das mobile Endgerät in die falschen Hände kommt, gibt es unter Umständen Softwarelösungen zur Datenlöschung aus der Ferne, zum Beispiel MDM.[157]

7.2.8. MDM

IT-Administratoren in Organisationen können sich mit einer Software für das Mobile Device Management viel Aufwand ersparen. Solche MDM-Lösungen erfassen die vorhandenen Geräte in der Organisation und konfigurieren sie "over the air". Der Verwalter (z.B. IT-Abteilung) spielt Software und Updates auf, setzt den Datenschutz mit Verschlüsselung und Passwortrichtlinien um und regelt die Zugangskontrolle ins Netzwerk. Dem Administrator stehen auch Ferndiagnosen und Notfallpläne zur Verfügung. Bei Verlust kann er ein mobiles Endgerät in der Regel dauerhaft sperren, die Daten vom Speicher löschen oder das verlorene Gerät über GPS orten. MDM-Tools können auch mit einem eigenen App Store kommen, in dem sich Mitarbeiter zugelassene Organisationsanwendungen besorgen können, oder erweitern das reine Device-Management um ein App-Management.[158]

Außerdem führt das BSI in dem neunseitigen Whitepaper zum Thema MDM sehr gut aus, was bei der Entscheidung für ein MDM-System beachtet werden muss. Dieses Dokument soll Hinweise und Empfehlungen für die Auswahl und den Einsatz von MDM-Lösungen geben. Der Titel der Veröffentlichung, die in der Reihe BSI-

[156] Bundesministerium für Wirtschaft und Energie (2011)
[157] Bundesministerium für Wirtschaft und Energie (2011)
[158] J. Pohl (2013)

Veröffentlichungen zur Cyber-Sicherheit erschienen ist, lautet: EMPFEHLUNG: IT IM UNTERNEHMEN - Mobile Device Management. (siehe Anhang)[159]

7.2.9. BSI-Empfehlungen

Trotz der implementierten Sicherheitsmechanismen der Geräte und Dienste existieren viele Schwachstellen und potentielle Bedrohungen, die beim Einsatz mobiler Endgeräte gezielt beachtet und wirksam abgewehrt werden müssen. Hier können die Richtlinien und Empfehlungen des Bundesamtes für Sicherheit in der Informationstechnik hilfreich sein. Zum Beispiel die Broschüre "Mobile Endgeräte und mobile Applikationen: Sicherheitsgefährdungen und Schutzmaßnahmen" erläutert entsprechende Techniken und die möglichen Bedrohungen. Sie richtet sich sowohl an Benutzer mobiler Endgeräte und entsprechender Infrastrukturen, als auch an IT-Verantwortliche und steht in der Internetseite des BSI als Download bereit.[160]

[159] K. Düll (2013)
[160] Bundesamt für Sicherheit in der Informationstechnik (2010)

8. Zusammenfassung

Immer mehr Beschäftigte der Organisationen nutzen mobile Endgeräte im geschäftlichen Alltag. Das kann entweder mit Organisationseigenen oder mitgebrachten (BYOD), privaten mobilen Endgeräten geschehen. Das Model „Bring Your Own Device“ beschreibt die Möglichkeit, für z. B. Mitarbeiter einer Organisation, eigene bzw. private mobile Endgeräte zum Arbeiten im Büro zu benutzen.

Irgendwann erreichen die mobilen Endgeräte die Ende der Nutzungszeit und müssen ausgemustert werden. Nach einer Literaturrecherche und persönlichem Gespräch (Interview) mit dem Geschäftsführer der Green Power GmbH wurde ein Überblick, wie in Organisationen mit mobilen (Alt-)Geräten am Ende ihrer Nutzungszeit verfahren wird, ausgearbeitet. Der Überblick zeigt, dass die mobile Endgeräte werden entweder weitergenutzt (Zweitnutzung) oder endgültig stillgelegt. Dabei existieren mehrere Szenarien:

- Bei Weiternutzung können Organisationen die Geräte Verkaufen, Spenden oder als Not-Gerät behalten.
- Bei Außerbetriebssetzung können Geräte noch für Teile, wie z.B. Gehäuse, Hardwareteile, Zubehör etc., gelagert oder endgültig Entsorgt werden.

Um die nachhaltige Nutzung der mobilen Endgeräte auch am Ende der Nutzungszeit zu erreichen wurde eine Empfehlungsliste erarbeitet. Nach einer Untersuchung und Analyse werden folgende Nachhaltige schritte empfohlen:

- gekaufte mobile Endgeräte möglichst lange nutzen und somit die Geräte in Zweitnutzung geben,
- Geräte mit geringer elektromagnetischer Strahlung (SAR-Wert kleiner 0,6 W/kg) nutzen,
- mobile (Alt-)Geräte sachgerecht und richtig bei der kommunalen Sammelstelle entsorgen und
- wenn möglich die Geräte Aufrüsten statt neu kaufen.

Zu beachten sind hier auch die allgemeine Probleme bzw. beeinflussende Faktoren auf die Nachhaltigkeit bei mobilen Endgeräten. Es ist festzustellen, dass solche Faktoren wie Produktlebenszyklus, Produktunterstützung durch den Hersteller, Aufbau der Geräten und Sollbruchstellen ebenso auf die Nachhaltigkeitsstrategie der

mobilen Endgeräte in Organisationen beeinflussen. Alle diese Faktoren können dazu führen, dass die Geräte öfter und schneller erneuert werden.

Die mobilen Endgeräte werden aber auch nach Ende ihre Nutzungszeit noch als Sicherheitsrisiko gesehen, weil z.B. die alten geheimen Daten auf den Geräten noch gelagert werden können. Aufgrund der fehlenden zentralen Versorgung muss die IT-Abteilung zusätzliche Ressourcen auch für die Administration und den Support von BYOD-Geräten vorhalten. Zur Sicherheit wird folgendes empfohlen:

- Sicherheitsrichtlinien entwickeln und durchsetzen,
- Festplatten sicher formatieren und evtl. verschlüsseln,
- Netzwerkverbindungen verschlüsseln (z.B. durch WPA2) und nur dann aktivieren, wenn es tatsächlich verwendet wird,
- Backup regelmäßig durchführen,
- nur sichere Apps installieren,
- Geräte durch Passwort sperren,
- MDM-Lösungen nutzen, damit die sichere und einfache Stilllegung der Geräten am Ende der Nutzungszeit möglich wäre und
- Empfehlungen des BSI zu berücksichtigen.

9. Literaturverzeichnis

Sicherheit mobiler Endgeräte von Endbenutzern im Unternehmen 2012.
Anett Mehler-Bicher und Lothar Steiger (Hrsg.): Trends in der IT. Bring Your Own Device (BYOD), Mainz 2012.

Barczok, Achim u.a.: Der Update-Frust bleibt. Android-Smartphones im Update-Check: http://www.heise.de/ct/artikel/Der-Update-Frust-bleibt-1834133.html, eingesehen am 19.03.2014.

Baumgarten, Uwe; Siegert, Hans-Jürgen: Betriebssysteme. Eine Einführung, 6., überarb., aktualisierte und erw. Aufl, München, Wien 2009.

Bayerischer Rundfunk: Tablets und Smartphones: Warum Recycling und Reparatur so schwer sind: http://www.br.de/themen/ratgeber/inhalt/computer/recycling-tablet-e-book-reader-100.html, eingesehen am 15.06.2014.

Bayerisches Staatsministerium für Umwelt und Verbraucherschutz: Hintergrundinformationen - Rohstoffschatz Handy, Laptop & Co: http://www.handy-clever-entsorgen.de/hintergrundinformation/index.htm, eingesehen am 21.06.2014.

Berliner Morgenpost: Die "Sollbruchstelle" in Elektrogeräten gibt es wohl doch: http://www.morgenpost.de/web-wissen/web-technik/article114610124/Die-Sollbruchstelle-in-Elektrogeraeten-gibt-es-wohl-doch.html, eingesehen am 19.06.2014.

BITKOM: Smartphone-Funktionen: Internet wichtiger als Telefonieren: http://www.bitkom.org/de/presse/74532_72686.aspx, eingesehen am 23.03.2014.

BITKOM: Unternehmen häufig ohne Sicherheitskonzepte für mobile Geräte: http://www.bitkom.org/de/presse/74532_72996.aspx, eingesehen am 30.06.2014.

Bjoern: 20 Millionen alte Computer in deutschen Haushalten: http://www.greencomputingportal.de/green-it-news/20-millionen-alte-computer-in-deutschen-haushalten/, eingesehen am 29.05.2014.

Bjoern: Computer-Recycling: Wohin mit dem alten Rechner?: http://www.greencomputingportal.de/artikel/endlich-ein-neuer-computer-aber-wohin-mit-dem-alten-rechner/, eingesehen am 21.06.2014.

Bundesamt für Sicherheit in der Informationstechnik: Mobile Endgeräte und mobile Applikationen: Sicherheitsgefährdungen und Schutzmaßnahmen (2006).

Bundesamt für Sicherheit in der Informationstechnik: Mobile Endgeräte und mobile Applikationen: Sicherheitsgefährdungen und Schutzmaßnahmen: https://www.bsi.bund.de/DE/Publikationen/Broschueren/mobile/index_htm.html.

Bundesamt für Sicherheit in der Informationstechnik: Mobile Endgeräte: https://www.bsi.bund.de/DE/Themen/weitereThemen/MobileSecurity/MobileEndgeraete/mobileendgeraete_node.html, eingesehen am 31.03.2014.

Bundesministerium für Umwelt, Naturschutz, Bau und Reaktorsicherheit: Blauer Engel: http://www.bmub.bund.de/themen/wirtschaft-produkte-ressourcen/produkte-und-umwelt/blauer-engel/, eingesehen am 22.06.2014.

Bundesministerium für Umwelt, Naturschutz, Bau und Reaktorsicherheit: Tipp des Monats: Mobil kommunizieren mit dem Blauen Engel: http://www.bmub.bund.de/themen/wirtschaft-produkte-ressourcen/produkte-und-umwelt/blauer-engel/tipp-des-monats-blauer-engel/detailansicht/artikel/tipp-des-monats-mobil-kommunizieren-mit-dem-blauen-engel/, eingesehen am 22.06.2014.

Bundesministerium für Wirtschaft und Energie: IT-Sicherheit - Mobiles Arbeiten: http://www.it-sicherheit-in-der-wirtschaft.de/IT-Sicherheit/Navigation/Themen/mobiles-arbeiten.html, eingesehen am 10.06.2014.

Buschenlange, Hannes: Konsumgesellschaft und Wege zur Nachhaltigkeit: Perspektiven auf Konsum, geplante Obsoleszenz und Abfallproblematik, 1., Aufl, Hamburg 2013.

Carsten: Alte Computer: Deutsche horten rund 22 Millionen: undefined, eingesehen am 24.06.2014.

Dahms, Julia: Mobile Endgeräte sicher nutzen: http://www.kdrs.de/pb/kdrs,Lde/Home/Aktuelles/Mobile+Endgeraete+sicher+nutzen.html, eingesehen am 29.05.2014.

Das Umweltbundesamt: Defekte Elektrogeräte – zufällig oder geplant?: http://www.umweltbundesamt.de/presse/presseinformationen/defekte-elektrogeraete-zufaellig-geplant, eingesehen am 09.06.2014.

Das Umweltbundesamt: Empfehlungen für die umweltfreundliche Beschaffung von Notebooks: http://www.umweltbundesamt.de/publikationen/empfehlungen-fuer-die-umweltfreundliche-beschaffung, eingesehen am 29.06.2014.

Das Umweltbundesamt: Kein Ex und Hopp mehr – dem Klima zuliebe: http://www.umweltbundesamt.de/themen/kein-ex-hopp-mehr-dem-klima-zuliebe/index.htm, eingesehen am 09.06.2014.

Das Umweltbundesamt: Ökobilanz: http://www.umweltbundesamt.de/themen/wirtschaft-konsum/produkte/oekobilanz, eingesehen am 09.06.2014.

Das Umweltbundesamt: Smartphone: http://www.umweltbundesamt.de/themen/wirtschaft-konsum/umweltbewusstleben/smartphone, eingesehen am 19.06.2014.

Der Blaue Engel: Arbeitsplatzcomputer: http://www.blauer-engel.de/produktwelt/buro/arbeitsplatzcomputer, eingesehen am 22.06.2014.

Der Landesbeauftragte für den Datenschutz Niedersachsen: Notebooks und mobile Endgeräte: http://www.lfd.niedersachsen.de/portal/live.php?navigation_id=13070&article_id=56164&_psmand=48, eingesehen am 24.03.2014.

Düll, Klaus: Das BSI erklärt Mobile Device Manage-ment (MDM) — Das Thema per-fekt auf den Punkt gebracht!: http://pretioso-blog.com/das-bsi-erklaert-mobile-device-management-mdm-das-thema-perfekt-auf-den-punkt-gebracht/#.U7MbFpR_u_g.

Duschinski, Hannes: Web 2.0. Chancen und Risiken für die Unternehmenskommunikation, Hamburg 2007.

FOCUS Online: Medienserver oder Zweitgerät: So können Sie alte Computer weiterverwenden - Rechner im Unruhestand: http://www.focus.de/digital/computer/pc-tipps/tid-29678/medienserver-oder-zweitgeraet-so-koennen-sie-alte-computer-weiterverwenden_aid_908668.html, eingesehen am 22.06.2014.

Fraunhofer IBP: Ökobilanzierung: http://www.ibp.fraunhofer.de/de/Kompetenzen/ganzheitliche-bilanzierung/oekobilanzierung.html, eingesehen am 29.05.2014.

Fuest, Benedikt: Warum Elektronik häufig so schnell kaputtgeht: http://www.welt.de/wirtschaft/webwelt/article112418443/Warum-Elektronik-haeufig-so-schnell-kaputtgeht.html, eingesehen am 05.04.2014.

Gerginov, David: Produktlebenszyklus beim Handy: Schnell, schneller, neu: http://www.gevestor.de/details/produktlebenszyklus-beim-handy-schnell-schneller-neu-658706.html, eingesehen am 15.06.2014.

Glathe, Caroline: Kommunikation von Nachhaltigkeit in Fernsehen und Web 2.0, 1. Aufl, Wiesbaden 2010.

Grabner, Thomas: Operations Management. Auftragserfüllung bei Sach- und Dienstleistungen, Wiesbaden 2012.

Haberer, Roland: Langzeitstudie: Jedes dritte Notebook defekt: http://www.netzwelt.de/news/81224-langzeitstudie-dritte-notebook-defekt.html, eingesehen am 29.06.2014.

Haufe Online Redaktion: Mobile: Verbreitung mobiler Endgeräte in Unternehmen nimmt zu: http://www.haufe.de/marketing-vertrieb/crm/mobile-verbreitung-mobiler-endgeraete-in-unternehmen-nimmt-zu_124_156996.html, eingesehen am 22.03.2014.

Haufe Online Redaktion: Immer mehr internetfähige Geräte in deutschen Haushalten: http://www.haufe.de/marketing-vertrieb/online-marketing/technik-immer-mehr-internetfaehige-geraete-in-deutschen-haushalten_132_194448.html.

Hofmann, Jürgen; Schmidt, Werner: Masterkurs IT-Management. Grundlagen, Umsetzung und erfolgreiche Praxis für Studenten und Praktiker, 2., aktualisierte und erw. Aufl, Wiesbaden 2010.

Institut für Internet-Sicherheit - if: Sicherheitsrichtlinien für BYOD in Unternehmen: https://www.it-sicherheit.de/startseite/news/sicherheitsrichtlinien-fuer-byod-in-unternehmen/, eingesehen am 31.03.2014.

Jan Kirchner: Deutschland wird mobil – Die digitale Republik 2013: http://www.wollmilchsau.de/deutschland-wird-mobil-die-digitale-republik-2013/, eingesehen am 24.03.2014.

Kaczmarek, Daniel: Usability von Internetanwendungen für mobile Endgeräte. Unter Betrachtung von Designrichtlinien für Ergonomie und effizienter Benutzerführung sowie deren praktische Umsetzung an einem WAP-Prototypen, 1. Aufl, s.l 2005.

Klüver, Christina; Klüver, Jürgen: IT-Management durch KI-Methoden und andere naturanaloge Verfahren. Mit 30 Tab, 1. Aufl, Wiesbaden 2011.

Krannich, Dennis: Mobile System Design 2010.

Logara, Tomislav: Mobile Business im B2C. Komplexität als Ursache von Produktivitätsengpässen in den Distributionskanälen des deutschen B2C-Marktes, 1. Aufl, Norderstedt 2007.

Lücke, Hayo: Firmen verschenken alte Rechner an Mitarbeiter: http://www.onlinekosten.de/news/artikel/30365/0/Firmen-verschenken-alte-Rechner-an-Mitarbeiter, eingesehen am 22.06.2014.

Manhart, Andreas u.a.: Entwicklung der Vergabekriterien für ein klimaschutzbezogenes Umweltzeichen 2012.

Marsiske, Hans-Arthur: Geplante Obsoleszenz: Produkte mit Verfallsdatum: http://www.heise.de/ct/artikel/Verstecktes-Verfallsdatum-1626511.html, eingesehen am 16.06.2014.

Maurer, Andrea: Notebook-Tuning: Was lässt sich überhaupt aufrüsten?: http://www.gamestar.de/hardware/praxis/notebooks/2323984/notebook_tuning_teil_1.html, eingesehen am 30.06.2014.

mobile zeitgeist: Was ist ein mobiles Endgerät?: http://www.mobile-zeitgeist.com/2010/03/09/was-ist-ein-mobiles-endgeraet/, eingesehen am 18.03.2014.

Müller, Gordon; Seel, Christian Prof. Dr.: Zur Organisationsrichtlinie „Bring your own Device“ – eine empirische Untersuchung, Landshut 2013.

n-tv: Vom Müll zum kleinen Dazuverdienst: Was tun mit alten Handys und Tablets?: http://www.n-tv.de/ratgeber/Was-tun-mit-alten-Handys-und-Tablets-article11984661.html, eingesehen am 18.05.2014.

Pohl, Jacqueline: Sicherheit nur durch Kontrolle. Smartphones und Tablets im Unternehmen verwalten: http://business.chip.de/artikel/Smartphones-und-Tablets-im-Unternehmen-verwalten_54342518.html.

Pousttchi, Key Dr.; Thurnher, Bettina (Hrsg.): Einsatz mobiler Technologie zur Unterstützung von Geschäftsprozessen, Aachen 2006.

Raasch, Christina: Der Patentauslauf von Pharmazeutika als Herausforderung beim Management des Produktlebenszyklus, 2., durchgesehene und korrigierte Aufl, Wiesbaden 2010.

Rau, Thomas: Aufrüsten statt neu kaufen: http://www.presseportal.de/pm/8232/2283664/aufruesten-statt-neu-kaufen-pc-welt-gibt-tipps-zum-notebook-tuning, eingesehen am 30.06.2014.

ReeseOnline: Endgerät | Was ist Endgerät - Definition, Bedeutung, Herkunft: http://www.fremdwort.de/suchen/bedeutung/Endger%C3%A4t, eingesehen am 13.04.2014.

Reiss, M.; Reiss, G.: Praxisbuch IT-Dokumentation 2009.

Rossnagel, Heiko; Murmann, Tobias (Hrsg.): Sicherheitsanalyse von Betriebssystemen für Mobile Endgeräte 2005.

Sammer, Thomas u.a.: Mobile Business. Management von mobiler IT in Unternehmen, Zürich 2014.

Scheimann, Thorsten: Immer schneller neuer: http://www.tagesspiegel.de/wirtschaft/produktlebenszyklen-immer-schneller-neuer/4041756.html, eingesehen am 15.06.2014.

Schwan, Ben: Reparatur von Apple-Geräten: Verklebt und vernagelt: http://www.taz.de/!107434/, eingesehen am 16.06.2014.

Schwichtenberg, Holger: Internet Bill Presentment and Payment als neue Form des Electronic Billing, 1. Aufl, s.l 2000.

Sokolow, Andrej: Alte Handys und Computer: Entsorgen, verkaufen oder spenden?: http://www.spiegel.de/netzwelt/gadgets/bild-754190-75322.html, eingesehen am 18.05.2014.

Specht, Thorsten: Handy entsorgen – die besten Tipps: http://praxistipps.chip.de/handy-entsorgen-die-besten-tipps_3154, eingesehen am 21.06.2014.

statista: Infografik: Traffic Explosion - Kennzahlen zur Entwicklung des mobilen Datenvolumens: http://de.statista.com/infografik/131/prognose-mobiles-datenvolumem/, eingesehen am 16.03.2014.

Strüber, Meike: Geplante Obsoleszenz – Kaufen für den Schrotthaufen: https://de.finance.yahoo.com/nachrichten/geplante-obsoleszenz-%E2%80%93-kaufen-f%C3%BCr-den-schrotthaufen.html, eingesehen am 16.06.2014.

Tim Gebler: Nutzenpotenziale von mobilen Endgeräten in Unternehmen: https://www.it-standpunkte.de/mobility/nutzenpotenziale, eingesehen am 27.04.2014.

Trautmann, Ralf: Festplatten und SSDs sicher löschen: http://www.teltarif.de/computer/festplatten-ssd-sicher-loeschen.html, eingesehen am 24.06.2014.

Trautmann, Ralf; Eisinger, Martina: Handys, Computer und anderen Elektroschrott richtig entsorgen: http://www.teltarif.de/handy/entsorgung.html, eingesehen am 21.06.2014.

Walter Saumweber: Eigene Windows Phone Apps erstellen, in: PC Magazin (Jul. 2012): http://www.pc-magazin.de/ratgeber/eigene-windows-phone-apps-erstellen-1316756.html, eingesehen am 04.05.2014.

Wieczorek, B.: Implementierung von BYOD im MS Exchange Umfeld. Eine Evaluierung von Mobile-Device-Management-Lösungen auf Basis einer Nutzwertanalyse, Hamburg 2013.

Wikipedia: Geplante Obsoleszenz: http://de.wikipedia.org/w/index.php?oldid=131137287, eingesehen am 10.06.2014.

Wikipedia: Microsoft Windows 8: http://de.wikipedia.org/w/index.php?oldid=131127523, eingesehen am 09.06.2014.

Wirtgen, Jörg: Android-Verteilung: Updates ziehen langsam an: http://www.heise.de/newsticker/meldung/Android-Verteilung-Updates-ziehen-langsam-an-2133882.html, eingesehen am 05.04.2014.

10. Anhang

A. Ausgewählte Seiten aus der Publikation des Umweltbundesamtes „Empfehlungen für die umweltfreundliche Beschaffung von Notebooks“

1 Verlängerung der Lebensdauer, Rücknahme und Verwertung

Umweltgerechte Produktgestaltung trägt entscheidend zur langen Einsatzfähigkeit von Produkten bei. Die Modulbauweise ermöglicht die leicht durchführbare Funktions- bzw. Leistungserweiterung, sowie eine Reparatur im Bedarfsfall. Ferner wird dadurch beim Produktrecycling eine hohe Verwertungsquote sichergestellt.

1.1 Modularer Aufbau

Kriterium	Nachweis
Bewertung	Hersteller-Erklärung mit Verweis auf technische Spezifikation (gemäß Leitfaden »Produktneutrale Ausschreibung«, Kapitel 4)

Die Systemeinheit ist modular aufgebaut, damit Komponenten ohne Einsatz von Spezialwerkzeugen ausgetauscht bzw. aufgerüstet werden können, insbesondere:

- Arbeitsspeicher
- Festplatte
- Laufwerke

1.2 Bereithaltung von Ersatzteilen

Kriterium	Nachweis
Bewertung	Hersteller-Erklärung

Mechanische Ersatzteile, die bei üblicher Nutzung erforderlich werden können (z. B. HDD, DVD), stehen mindestens 5 Jahre nach Liefertermin zur Verfügung. Komponenten/Teile, die regelmäßig die durchschnittliche Lebensdauer des Produktes überdauern, müssen nicht als Ersatzteile vorgehalten werden.

1.3 Kennzeichnung von Kunststoffteilen > 25g

Kriterium	Nachweis
Bewertung	Hersteller-Erklärung

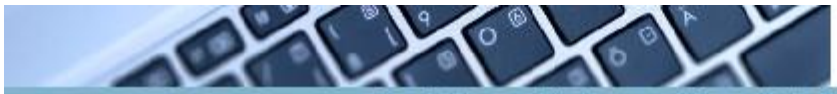
Kunststoffteile mit einer Masse oberhalb 25 Gramm sind gemäß ISO 11469:2000 dauerhaft gekennzeichnet.

1.4 Unentgeltliche Rücknahme von ITK-Altgeräten

Kriterium	Nachweis
Ausschluss	Hersteller-Erklärung

Die Rücknahme der Geräte erfolgt bei Bedarf des Kunden unentgeltlich bei einer vom Bieter benannten Annahmestelle gemäß Elektro- und Elektronikgerätegesetz (ElektroG §10 Abs. 2.) .

4



2 Energie

Bei der Lebenszyklus-Betrachtung eines Notebooks ist der Betrieb eine wichtige Phase mit Einsparungspotenzial. Energieeffiziente Geräte helfen Geld zu sparen und die CO_2-Emissionen zu senken.

Die Verordnung über die Vergabe öffentlicher Aufträge (Vergabeverordnung, VgV) vom 14.03.2012 fordert in §4(5)1. das höchste Leistungsniveau an Energieeffizienz.

2.1 ENERGY STAR

Kriterium	Nachweis
Ausschluss	1. Hersteller-Erklärung und 2. Prüfbericht gemäß Testvorschrift des jeweils gültigen ENERGY STAR (Aktuell V5.0) oder ein Dokument, das folgende Angaben enthält: ■ Name des Prüflabors (externes oder firmeninternes Prüfinstitut) ■ Unterschrift der autorisierten Person vom Labor (z. B. Laborleiter) ■ Bestätigung über Einhaltung der Energiewerte gemäß Anforderungen nach 2.1 Prüfbericht oder Dokument nur auf Nachfrage vor Zuschlags-Erteilung

Das Gerät genügt vollständig den Anforderungen des jeweils gültigen ENERGY STAR Programms für Notebooks (www.eu-energystar.org).

Die aktuellen Anforderungen des ENERGY STAR V5.0 für Notebooks (gültig ab Juli 2009):

Typical Energy Consumption (TEC):

- Kategorie A: ≤ 40,0 kWh
- Kategorie B: ≤ 53,0 kWh
- Kategorie C: ≤ 88,5 kWh

Der TEC-Wert repräsentiert den typischen jährlichen Elektrizitätsverbrauch des jeweiligen Gerätes. Dieser wird unter Verwendung eines angenommenen typischen Arbeitszyklus in Kilowattstunden (kWh) gemessen.

Optional sind zum TEC noch zu addieren:

- 0,4 kWh für jedes über 4 GB hinausgehende GB Speicherkapazität
- 3 kWh für zusätzlichen internen Speicher
- 3 kWh für »Premium Graphics« (nur Kategorie B)

2.2 Energieanforderungen nach Blauem Engel

Kriterium	Nachweis
Bewertung	Hersteller-Erklärung

Das Gerät erfüllt die Anforderungen der jeweils gültigen Vergabegrundlage des Blauen Engel für Tragbare Computer (Notebooks).

Aktuelle Anforderungen des Blauen Engel für Tragbare Computer RAL-UZ 78d (Ausgabe März 2013):

Typischer Energie Verbrauch (BE-TEC):

- Kategorie A: ≤ 30,0 kWh
- Kategorie B: ≤ 39,79 kWh
- Kategorie C: ≤ 66,38 kWh

Die aktuellen Anforderungen des Blauen Engel sind unter www.blauer-engel.de zu finden.

BITKOM Umwelt Bundes Amt Beschaffungsamt

2.3 Energieverwaltung

Kriterium	Nachweis
Ausschluss	Hersteller-Erklärung

Das Gerät wird mit einer aktivierten Energieverwaltung gemäß dem jeweils gültigen ENERGY STAR Programm ausgeliefert.

Aktuelle Anforderungen des ENERGY STAR V.5: Bei Inaktivität:

- ≤ 30 min Sleep mode, z. B. ACPI S3 und ≤ 15 min Monitor ausschalten

2.4 Angaben zum Energieverbrauch

Kriterium	Nachweis
Ausschluss	Hersteller-Erklärung

Der TEC-Wert ist in Kilowattstunden (kWh) anzugeben. Dies ist gemäß VgV §4(6)1. vorgeschrieben.

2.5 Ein- und Ausschalter

Kriterium	Nachweis
Ausschluss	Hersteller-Erklärung

Das Gerät muss über einen Ein- und Ausschalter verfügen. Durch seine Betätigung muss das Gerät mindestens in den Schein-Aus-Zustand (ACPI S5 oder vergleichbar) versetzt werden können.

2.6 Anforderungen zum Akkumulator

Kriterium	Nachweis
Bewertung	Hersteller-Erklärung

Die Möglichkeit zum Austausch des Akkumulators dient einer möglichst langen Nutzungsdauer und somit der Ressourcenschonung und der Abfallvermeidung. Weiterhin, wenn Geräte durch einen Akkuwechsel länger nutzbar sind, ergeben sich dadurch auch wirtschaftliche Vorteile für den Bedarfsträger.

Der im Notebook enthaltene Akkumulator muss ohne Spezialwerkzeug austauschbar sein.

3 Geräuschemissionen

Bei Geräten, die in unmittelbarer Nähe zum Arbeitsplatz stehen, ist ein möglichst geräuscharmer Betrieb von großer Bedeutung. Geräuscharme Geräte sind ein Beitrag zum Gesundheitsschutz.

Der garantierte Schallleistungspegel, der auf Grundlage der EN ISO 7779 in Verbindung mit ISO 9296 ermittelt wurde, ist in Bel (B) anzugeben.

3.1 Begrenzung des Schallleistungspegels nach ITI TC6

Kriterium	Nachweis
Ausschluss	1. Hersteller-Erklärung und 2. Prüfbericht nach ISO 7779 einer nach ISO 17025 akkreditierten Stelle, oder ein Dokument, das folgende Angaben enthält: ■ Name des Prüflabors (externes oder firmeninternes Prüfinstitut) ■ Akkreditierungsnachweis des Prüflabors nach ISO 17025 für Messungen nach ISO 7779 ■ Unterschrift der autorisierten Person vom Labor (z. B. Laborleiter) ■ Schallleistungswerte mit zwei Nachkommastellen in Bel (B)

Die Schallleistung (LWAd) soll im Leerlaufbetrieb 4,50 B und im Betrieb (Aktivierung des Festplattenlaufwerkes) 4,80 B nicht überschreiten.[2]

3.2 Begrenzung des Schallleistungspegels nach Blauem Engel

Kriterium	Nachweis
Bewertung	Hersteller-Erklärung

Im Leerlaufbetrieb werden 3,50 B und im Betrieb (Aktivierung des Festplattenlaufwerkes) 4,00 B Schallleistung nicht überschritten.

2 Schallleistungswerte sind nach ISO 7779 direkt um das Gerät gemessen und somit unabhängig von der Distanz zwischen Gerät und Benutzer. Angaben zu »Operator Position« oder »Bystander Position« gehören zur Definition des Messpunkts bei Schalldruckangaben (LpA), welche hier nicht betrachtet werden

4 Materialeigenschaften/ Stoffbezogene Anforderungen

Tragbare Computer bestehen aus einer Vielzahl von Einzelkomponenten und verschiedenen Stoffen. Durch den Ausschluss bestimmter Stoffe wird der Eintrag umweltschädigender Stoffe in die Umwelt reduziert. Dadurch wird ein wesentlicher Beitrag zum Umwelt- und Gesundheitsschutz geleistet.

4.1 Ausschluss bestimmter Halogenverbindungen

Kriterium	Nachweis
Ausschluss	Hersteller-Erklärung

Gehäusekunststoffe sind nicht aus halogenhaltigen Polymeren (z. B. PVC). Ferner sind keine chlor- oder bromhaltigen Flammschutzmittel in Gehäusekunststoffteilen > 25g zugesetzt.

4.2 Ausschluss bestimmter Stoffe

Kriterium	Nachweis
Ausschluss	Hersteller-Erklärung

Stoffe, die nach der Verordnung EG Nr.1272/2008 Anhang VI mit den folgenden Gefährlichkeitsmerkmalen eingestuft sind, dürfen den Kunststoffen für Computergehäuse (Teile >25g) nicht zugesetzt sein.

- Karzinogene Stoffe der Kategorien 1A, 1B
- Keimzellmutagene Stoffe der Kategorien 1A, 1B
- Reproduktionstoxische Stoffe der Kategorien 1A, 1B

4.3 Verpackung

Kriterium	Nachweis
Ausschluss	Hersteller-Erklärung

Die für die Verpackung der Geräte verwendeten Kunststoffe dürfen keine halogenhaltigen Polymere (z. B. PVC) enthalten.

4.4 Ausschluss bestimmter Stoffe in Flüssigkristallmischungen

Kriterium	Nachweis
Ausschluss	Hersteller-Erklärung

Die Flüssigkristallmischungen dürfen keine Substanzen enthalten, die als krebserzeugend, erbgutverändernd oder fortpflanzungsgefährdend in Kategorie 1, oder 2 oder als giftig bzw. sehr giftig nach Tabelle 3.1 des Anhangs VI der EG-Verordnung 1272/2008 eingestuft sind.

4.5 Quecksilberfreie Hintergrundbeleuchtung

Kriterium	Nachweis
Ausschluss	Hersteller-Erklärung

Die Hintergrundbeleuchtung des Bildschirms darf kein Quecksilber enthalten.

5 Hersteller-Erklärungen, Prüfberichte und Nutzerinformationen

Kriterium	Nachweis
Ausschluss	Hersteller-Erklärung, Prüfberichte, Handbücher

Der Nachweis für die Einhaltung der aufgestellten Kriterien kann abhängig vom jeweiligen Kriterium durch Hersteller-Erklärungen oder Prüfberichte erbracht werden. Technische, umwelt- und gesundheitsrelevante Nutzerinformationen unterstützen den Nutzer/die Nutzerin u. a. beim umwelt- und gesundheitsgerechten Umgang mit dem Notebook.

Bei Produkten, die das Umweltzeichen Blauer Engel tragen, darf gem. § 8 Abs. 5 VOL/A-EG (analog für den Unterschwellenbereich) davon ausgegangen werden, dass sie nachweislich alle hier aufgeführten Kriterien erfüllen. Ein gesonderter Nachweis ist für diese Produkte nicht nötig. Zu beachten ist, dass der Blaue Engel zwar als Nachweis (neben anderen geeigneten Beweismitteln) zugelassen werden darf, nicht hingegen die Aufnahme o.g. technischer Spezifikationen in die Leistungsbeschreibung ersetzen kann.

Eine mögliche Formulierung könnte sein:

- Hersteller-Erklärungen (z. B. Eco Declaration ECMA-370) und Prüfberichte gemäß ENERGY STAR, Blauer Engel oder gleichwertig können in deutscher oder englischer Sprache vorgelegt werden.

- Handbücher mit technischen, umwelt- und gesundheitsrelevanten Nutzerinformationen stehen in elektronischer Form in deutscher Sprache z. B. als CD oder zum Download zur Verfügung.

6 Anhang

Die Empfehlungen orientieren sich an fünf Grundprinzipien:

- Lenkungswirkung: Anbieter (Industrie) und Nachfrager (Beschaffungsverantwortliche der öffentlichen Hand, von Unternehmen und Organisationen) sollen durch die Nutzung des Beschaffungsportals einen Anreiz erhalten, die Umweltfreundlichkeit von ITK-Geräten zu erhöhen. Wenn Nachfrager zunehmend die umweltfreundlichsten Geräte beschaffen, wird hiervon ein Impuls auf die Industrie ausgehen, noch mehr Aktivitäten hinsichtlich umweltfreundlicher Geräte zu entfalten.

- Umweltfreundlichkeit: Innerhalb der Produktgruppe Notebooks zählen jene zu den umweltfreundlichsten, die die hier aufgestellten Kriterien erfüllen. Prinzipiell ist bei einer Beschaffungsentscheidung - die auf den Verbrauch bezogene - umweltfreundlichste Systemlösung zu wählen.

- Ambitioniertheit bei gleichzeitiger Erfüllbarkeit durch Ausschluss- und Bewertungskriterien: Die Zielwerte müssen ehrgeizig sein, damit sie die auf dem Markt befindlichen, umweltfreundlichsten Geräte abbilden (Status Quo) und zugleich Trends (Entwicklungspotenziale) aufgreifen. Die gewählten Zielwerte dürfen aber nicht zu ehrgeizig sein, weil dann nur noch ein verschwindend geringer Anteil der Marktteilnehmer sie einhalten kann. Der vorliegende Leitfaden löst diese Herausforderung durch den Einsatz von Ausschluss- und Bewertungskriterien.

- Verständlichkeit: Beschaffer sollen die Aussagekraft der Kriterien nachvollziehen können. Die Auswahl und Formulierung der Kriterien erfolgte daher nach folgenden Prinzipien:
  - entscheidende Umweltkriterien (»Qualität«)
  - überschaubare Zahl (»Quantität«)
  - verständliche Darstellung (»Lesbarkeit«)

- Nachprüfbarkeit: Beschaffer sollen kontrollieren können, ob die Geräte, die in den »Selbsterklärungen« angegebenen Werte einhalten. Der Leitfaden nennt daher standardisierte Messmethoden, die eine Reproduzierbarkeit der Messwerte (Überprüfbarkeit) und Nachvollziehbarkeit (beispielsweise durch »akkreditierte Prüflabore« oder »Testat Dritter«) ermöglichen.

Die im vorliegenden Leitfaden aufgestellten Kriterien sind direkt für die Leistungsbeschreibung nutzbar. Die Aufnahme von Umweltaspekten in die Leistungsbeschreibung ist unter vergaberechtlichen Gesichtspunkten unkritisch: In den Vergabe- und Vertragsordnungen (VOL/A, VOB/A und VOF) ist explizit geregelt, dass Umweltaspekte Teil der technischen Anforderungen sein können und Umwelteigenschaften zulässige Zuschlagskriterien sind.

Eine allgemeine Einführung zum Thema »Umweltfreundliche Beschaffung« und Hinweise zu den speziellen Anforderungen der unterschiedlichen Stufen des Vergabeverfahrens gibt beispielsweise das Handbuch der Europäischen Kommission: Buying Green! sowie eine Zusammenfassung in deutscher Sprache (http://ec.europa.eu/environment/gpp/buying_handbook_en.htm).

B. Richtlinie zum Umgang mit mobilen Geräten des KIT

Karlsruher Institut für Technologie
Chief Information Officer

Internetadresse: www.cio.kit.edu

Richtlinie zum Umgang mit mobilen Geräten des KIT

Motivation

Der Umgang mit mobilen Geräten wie PDAs, Smartphones oder Notebooks ist heutzutage für jedermann Alltag. Um das Risiko eines (ungewollten) Datenverlustes zu verringern, sind nachfolgende Regeln zu beachten. Häufig tritt Datenverlust durch Diebstahl eines Geräts auf. Neben dem unmittelbaren Verlust des Geräts kommt erschwerend hinzu, dass die Daten, die sich auf dem Gerät befunden haben, durch den Täter eingesehen und missbräuchlich genutzt werden können.

Diese Richtlinie orientiert sich an den Empfehlungen des BSI „Mobile Endgeräte und mobile Applikationen: Sicherheitsgefährdungen und Schutzmaßnahmen". Nachfolgendende Maßnahmen entsprechen der Gliederung des Dokuments des BSI, reflektieren jedoch auch die zum Zeitpunkt der Ausgabe bestehenden technischen Möglichkeiten der Absicherung innerhalb des KIT. Diese Richtlinie wird in regelmäßigen Abständen auf Aktualität geprüft und bei Änderung in einer neuen Version veröffentlicht.

Ergänzend zu dieser Richtlinie sind auch die Empfehlungen zu Dienstreisen ins außereuropäische Ausland zu beachten.

Gültigkeitsbereich

Der Gültigkeitsbereich der Richtlinie wird durch die zum Zeitpunkt der Veröffentlichung gültigen Nutzungsordnungen und Betriebsvereinbarungen des KIT geregelt.

Maßnahmen zum Schutz vor Datendiebstahl

- **Identifizierung des Nutzers**: Aktivieren von Identifizierungsmaßnahmen für den Nutzer (zum Beispiel Einschaltkennwort oder PIN). Eine automatische passwortgeschützte Sperrung bei Inaktivität (z. B. Bildschirmschoner, Tastensperre) ist ebenfalls zu aktivieren, falls technisch möglich. Der Zeitraum der Inaktivität bis zur Sperrung sollte nicht mehr als 30 Minuten betragen.
- **Datenverschlüsselung**: Wenn Daten auf Geräten transportiert werden, sollten diese verschlüsselt werden. Dies gilt sowohl nur für aktiv genutzte Geräte, als auch für mobile Datenträger (USB-Sticks, mobile Festplatten etc.). Manche Geräte erlauben die Verwendung eines Festplattenkennworts – es wird empfohlen, von dieser Möglichkeit Gebrauch zu machen. Wenn der Speicher des Gerätes über Speicherkarten (zum Beispiel SD-Karte) erweitert wird, ist auch der Inhalt dieser Karten nach Möglichkeit zu verschlüsseln.
- **Physische Sicherung**: Mobile Geräte sind nach Möglichkeit physisch zu sichern (zum Beispiel mit einem Kensingtonschloss), um einen Gelegenheitsdiebstahl zu vermeiden.

Maßnahmen zum Schutz vor Gerätemanipulation

- **Weitergabe**: Die Weitergabe des Geräts an Dritte oder Fremde ist - (auch vorübergehend) nicht zulässig.
- **Verlustmeldung**: Melden Sie sowohl Ihrem zuständigen IT-Verantwortlichen als auch der geräteausgebenden Stelle, falls ein Gerät verloren gegangen ist. Dies gilt auch, falls sich Geräte nach kurzer Zeit wieder auffinden. Nur mit dieser Meldung kann in der Situation entsprechend reagiert werden (zum Beispiel durch Sperrung der SIM-Karte oder Neu-Initialisierung des Geräts).
- Lassen Sie das Gerät nie unbeaufsichtigt.

Maßnahmen zum Schutz vor Angriffen auf die Kommunikation

- **Schnittstellen deaktivieren**: Sämtliche Funk- (WLAN, Bluetooth etc.), Infrarot- und andere Kommunikationsschnittstellen sind zu deaktivieren, sofern diese nicht benutzt werden.

Karlsruher Institut für Technologie

- **Kommunikationssicherheit**: Wo möglich, muss eine Datenübertragung über verschlüsselte Kanäle erfolgen, um ein Ausspähen von Daten zu erschweren.

Maßnahmen bei Außerbetriebnahme des Gerätes

- **Datenlöschung**: Vor Außerbetriebnahme eines Gerätes sind die auf dem Gerät gespeicherten Daten bei Bedarf entsprechend zu sichern und in jedem Fall unwiederbringlich zu löschen. Die Konfiguration des Gerätes ist zurückzusetzen, so dass mit dem Gerät nicht mehr auf geschützte Unternehmensressourcen (zum Beispiel VPN-Zugang) zugegriffen werden kann.

Allgemeine Empfehlungen

- **Datensparsamkeit**: Wenn Daten unbedingt auf mobilen Geräten benötigt werden, sollte die Auswahl der Daten auf das Nötigste beschränkt werden. Gegebenenfalls können Daten über die bekannten Remotezugänge des KIT nachgeladen werden. Es wird insbesondere darauf hingewiesen, dass die Speicherung von Passworten im Klartext nicht zulässig ist. Zudem sollten die für die Benutzerauthentifikation und die Verschlüsselung verwendeten Passwörter in jedem Fall die derzeit gültigen Anforderungen hinsichtlich Passwortlänge und Komplexität erfüllen.
- Allgemeine Vorkehrungsmaßnahmen gegen Diebstahl sollten getroffen werden (Auch in verschlossenen Fahrzeugen dürfen Geräte nicht sichtbar gelagert werden).

Version

Diese IT-Sicherheitsrichtlinie wurde in der Version 1.0 von ASDUR am 24.03.2010 empfohlen.

Veröffentlichung

Sie tritt zum 24.03.2010 in Kraft und wird auf den Internetseiten des CIO als Sicherheitsrichtlinie für das KIT veröffentlicht. Der IT-Sicherheitsbeauftragte kommuniziert deren Veröffentlichung im Auftrag des CIO in den entsprechenden Gremien.

Weiterführende Informationen

- Weiterführende Informationen zum Umgang mit mobilen Geräten erhalten Sie auf den Internetseiten des BSI unter folgendem URL: https://www.bsi.bund.de/cln_156/ContentBSI/Publikationen/Broschueren/mobile/index_htm.html
- Hinweise zur sicheren Datenlöschung erhalten Sie auf den Webseiten der ZENDAS unter folgenden URL: http://www.zendas.de/themen/vernichtung/speichermedien.html

C. EMPFEHLUNG: IT IM UNTERNEHMEN - Mobile Device Management

Bundesamt
für Sicherheit in der
Informationstechnik

EMPFEHLUNG: IT IM UNTERNEHMEN

Mobile Device Management

Der Wandel des Arbeitsumfelds vom stationären zum mobilen Arbeitsplatz hat zur Folge, dass auch die Arbeitsgeräte mobil sein müssen. Der Zugriff auf Unternehmensdaten ist praktisch von jedem Ort aus notwendig und mittlerweile auch möglich. „Mobile Daten" sind kein neues Phänomen, sondern schon seit Langem im täglichen Einsatz. Mit dem Laptop wurden Unternehmensdaten erstmals flächendeckend mobil. Die Geräte wurden zunächst offline betrieben, das heißt, die Daten wurden im Unternehmen aufgespielt und konnten unterwegs verwendet werden. Erst mit Anschluss an das Intranet des Unternehmens wurden aus diesen mobilen Daten synchronisierte mobile Daten. Hier hat sich ein enormer Wandel vollzogen: Jederzeit und an jedem Ort liegen jetzt aktuelle Dokumente und Zahlen vor, E-Mails erreichen den Benutzer zeitnah und Termine werden online mit Kollegen und Geschäftspartnern organisiert. Mobile Endgeräte sind aus der heutigen Arbeitswelt nicht mehr wegzudenken.

Smartphones und Tablet-Computer mit den Betriebssystemen *iOS* von Apple, *Android* von Google oder *Windows Phone* von Microsoft sind mit modernen, einfachen Bedienkonzepten eher für den Consumer-Markt gedacht und weniger für den geschäftlichen Einsatz. Damit unterscheiden sie sich grundlegend von anderen Konzepten mobiler Endgeräte, wie beispielsweise *Blackberry*, das speziell für den Unternehmenseinsatz konzipiert wurde. Trotzdem sind Geräte mit iOS und Android in der Geschäftswelt angekommen und verdrängen zunehmend etablierte Lösungen. Sie müssen in die Geschäftsprozesse integriert, beziehungsweise die Geschäftsprozesse müssen an sie angepasst werden. IT-Abteilungen stehen vor der Herausforderung, den Zugang der Geräte zur IT-Infrastruktur zu ermöglichen, diese Geräte zentral zu verwalten und gleichzeitig das Sicherheitsniveau des Unternehmens aufrechtzuerhalten. Als Möglichkeit zur Lösung dieser Aufgabe werden Mobile Device Management-Lösungen (im Folgenden *MDM-Lösungen*) angeboten.

Dieses Dokument soll Hinweise und Empfehlungen für die Auswahl und den Einsatz von MDM-Lösungen geben. Es ist in vielen Bereichen plattformübergreifend geschrieben, die genannten Beispiele zielen allerdings speziell auf die verbreiteten mobilen Betriebssysteme Android und iOS ab.

Die Empfehlungen sollen aber nicht die hinlänglich bekannten Konfigurationsempfehlungen für MDM-Lösungen wiederholen, zumal die Menüs der Verwaltungskonsolen in der Regel die Möglichkeiten der Plattform-Konfigurationen ausschöpfen und soweit selbsterklärend sind. Vielmehr sollen die zentralen Gesichtspunkte betrachtet werden, auf die bei der Auswahl und dem Betrieb einer MDM-Lösung geachtet werden sollte. Gleichwohl werden zur Veranschaulichung am Ende dieses Dokuments einige exemplarische Empfehlungen für die Konfiguration von iOS- und Android-basierten Smartphones und Tablets gegeben.

Die Empfehlungen sind bewusst kurz gehalten und erheben keinen Anspruch auf Vollständigkeit. Sie sollen in regelmäßigen Abständen aktualisiert und erweitert werden. Anregungen sind daher sehr willkommen.

Wandel hin zur Unsicherheit

Die Hardware und Systemsoftware der klassischen Mobilgeräte Laptop und Notebook sind sehr ähnlich bis identisch zu stationären Computern. Auch sie arbeiten hauptsächlich mit Windows, Mac OS X oder Linux als Betriebssystem. Damit gibt es praktisch keinen großen Unterschied bei der Verwendung dieser mobilen Geräte. Sind sie einmal über einen sicheren Kanal mit dem Intranet des Unternehmens verbunden, kann man wie gewohnt damit arbeiten. E-Mail, Kontakte, Kalender und Zugang zu Netzdiensten sind vorhanden, zentrale Administration, Patch- und Backup-Management werden transparent durchgeführt. Wichtig ist auch die Tatsache, dass die Absicherung der Geräte durch Sicherheitssoftware wie beim Desktop-Computer funktioniert und dass Sicherheitsrichtlinien wie gewohnt durchgesetzt werden können.

Anders sieht es bei der Klasse der Handheld-Computer – Smartphone und Tablet – aus. Diese sind bezüglich Ausstattung und Leistungsvermögen durchaus in der Lage, Geschäftsprozesse zu verarbeiten; Hardware, Systemsoftware und Bedienungskonzept unterscheiden sich aber meist grundlegend von den „klassischen" mobilen Endgeräten Laptop und Notebook.

Problematisch ist dabei die Vielfalt der Plattformen von Smartphones und Tablet-Computer mit ihren systembedingten Eigenschaften, die jeweils einzeln berücksichtigt werden müssen. Hinzu kommen noch Unterschiede innerhalb der Betriebssysteme. Das Betriebssystem Android – als mittlerweile führendes mobiles Betriebssystem (Stand 2012) – wird von den Smartphone-Herstellern speziell an die von ihnen entwickelten Geräte angepasst. Dabei werden auch grundlegende Funktionalitäten verändert wie beispielsweise die Bedienoberfläche. Das Patch-Management liegt vollständig in den Händen dieser OEM-Hersteller. Verzögerungen bei der Auslieferung von neuen Betriebssystem-Versionen sind unabdingbar, wenn man bedenkt, dass eine neue Version von Android zunächst von Google herausgegeben wird, dann vom Hardware-Hersteller an die einzelnen Geräte angepasst werden muss und schließlich vom Provider nochmals verändert wird (etwa zur Anpassung an den Zugangspunkt, über den Datenvolumen abgerechnet werden). Hinzu kommen noch Zeiten für Zertifizierung und Abnahme. Verzögerungen von bis zu einem halben Jahr sind keine Seltenheit. Oft kommen neue Geräte schneller auf den Markt, als vorhandene aktualisiert werden.

„Bring Your Own Device" (BYOD), also die (zusätzlich) dienstliche Verwendung privater Smartphones, stellt IT-Abteilungen vor immer neue Herausforderungen. Nicht die IT-Abteilung wählt die Geräte aus, sondern der Benutzer. Dies geht sogar soweit, dass Nutzer plattformbedingte Einschränkungen in Kauf nehmen, nur um mit bestimmten Geräten arbeiten zu können.

Auch der Einsatzort birgt ein erhöhtes Risiko. Zwar werden auch Laptops in unsicheren Umgebungen eingesetzt, bei Smartphones ist dies aber wesentlich leichter. Sie müssen nicht gebootet werden, sondern sind nach dem Einschalten sofort betriebsbereit. Die geometrischen Abmessungen erlauben den Gebrauch an fast jedem Ort. Vielfach stehen dem Benutzer freie, kostenlose Zugänge in nicht kontrollierbare WLANs zur Verfügung. Kommen die Geräte einmal abhanden, das heißt gehen sie verloren oder werden gestohlen, besteht für den Administrator nur die Möglichkeit, das Gerät aus der Ferne zu sperren und/oder zu löschen (wenn das Gerät noch erreichbar ist). Diebe, die an den gespeicherten Daten interessiert sind, werden daher diesen letzten Fernzugriff verhindern.

Für die Fernverwaltung muss die weitgehend gekapselte Infrastruktur des Unternehmens weiter aufgeweicht werden. Das heißt, teilweise ist es notwendig, Verwaltungs- und Kommunikationsserver in die DMZ zu stellen, damit eine Verbindung zwischen dem Intranet und den mobilen Endgeräten möglich wird.

Mobile Device Management in Unternehmen

Die Absicherung der Kommunikation, die Verarbeitung der Daten auf dem Gerät, die sichere Speicherung der Daten auf dem Gerät, die Trennung von dienstlicher und privater Nutzung sowie der Schutz der Geräte vor Schadsoftware sind Anforderungen, die von IT-Abteilungen im Desktop-/Laptop-Bereich sicher beherrscht werden. In Bezug auf mobile Endgeräte fehlt aber vielfach die Umsetzung von Lösungsmöglichkeiten, bzw. müssen Lösungsmöglichkeiten von Betriebssystem-Hersteller und Drittanbietern erst noch geschaffen werden. Diesen Anforderungen kann durch den Einsatz von Mobile Device Management – primär

im Hinblick auf zentrale Fernverwaltung – begegnet werden. Einige Lösungen bieten über die Verwaltung hinaus zusätzliche Funktionalitäten für die Absicherung geschäftlicher Daten auf dem mobilen Endgerät an.

MDM-Lösungen bauen im Wesentlichen auf den vier Säulen *Hardwareunterstützung*, *Softwareunterstützung*, *Kommunikation und deren Absicherung* sowie *Datensicherheit auf den mobilen Endgeräten* auf.

Die Hardwareunterstützung beinhaltet neben der generellen Unterstützung verschiedener Plattformen auch die Integration einer MDM-Lösung in die jeweilige Plattform, sodass der Betrieb des mobilen Endgerätes durch die Lösung nicht nachteilig beeinflusst wird, beispielsweise bezüglich der Batterielaufzeit. Zur Softwareunterstützung gehören unter anderem die Einbindung von neuen mobilen Endgeräten in die Verwaltung, die Verteilung von Konfigurationsprofilen, wie auch die Unterstützung der IT-Infrastruktur eines Unternehmens. Der Schutz der Daten auf den Kommunikationswegen durch die Verwendung von Verschlüsselung auf definierten Zugangspunkten spielt eine zentrale Rolle. Gleiches gilt auf den mobilen Endgeräten in Bezug auf sichere Konfiguration, Verschlüsselung, Benutzereinschränkungen usw. aber auch für die sichere Entfernung aus der Verwaltung.

Vorbereitungen zur Auswahl einer MDM-Lösung

Bevor die Entscheidung für eine bestimmte MDM-Lösung getroffen wird, muss grundsätzlich festgelegt werden, was diese Lösung leisten soll. Welche Plattformen sollen unterstützt werden? Welche Unternehmensdaten sollen auf dem mobilen Endgerät verarbeitet werden? Müssen neben den üblichen PIM-Daten (Kalender, Kontakten, Aufgaben und Notizen) und E-Mails auch Unternehmensdokumente verarbeitet werden? Wie werden diese Daten abgesichert bzw. von anderen auf dem mobilen Endgerät bearbeiteten (privaten) Daten separiert? Hat das Unternehmen eigene Apps, die verwaltet werden müssen und wird dazu ein eigener App-Store benötigt? Wird die Verwendung privater Smartphones für dienstliche Belange erlaubt?

Wenn man diese Fragen beantwortet hat und dazu einen entsprechenden Testplan vorbereitet hat, sollte man sich eine Vorauswahl von MDM-Lösungen ansehen. Vertrauen Sie nicht den Marketing-Abteilungen der Anbieter. Auch das Studium der Produktdokumentation allein reicht nicht aus. Teststellungen und eine intensive Beschäftigung mit dem Thema sind notwendig, um die Tauglichkeit der beworbenen Funktionalitäten auch wirklich in der Praxis bewerten zu können. Lassen Sie sich Referenzprojekte zeigen und profitieren Sie von den Erfahrungen dieser Unternehmen.

Bauarten

MDM-Server werden als reine Software-Lizenz oder als Appliance für den Einsatz im Unternehmen angeboten. Sie bestehen entweder aus einem einzelnen Server oder aus mehreren Komponenten und stehen – in Firewalls eingebettet – in der DMZ. Dort bilden sie das Bindeglied zwischen der IT-Infrastruktur des Unternehmens und den mobilen Endgeräten. Zudem enthalten sie die Verwaltungs-Konsole für die Konfiguration, Monitoring, Logging, Backup der mobilen Endgeräte usw. und können auch einen eigenen App-Store enthalten.

Daneben bieten einige Anbieter vollwertige MDM-Lösungen auf eigenen Servern als Clouddienst an. Vorteilhaft ist diese Lösung vor allem bei kleinen Installationen mit wenigen mobilen Endgeräten. Über einen solchen Clouddienst kann man eine MDM-Lösung auch ohne viel Aufwand ausgiebig testen, vorausgesetzt, sie erfüllt alle Anforderungen, die in einer eigenen Installation benötigt werden.

Wer die Installation einer eigenen MDM-Lösung scheut und sich bewusst für einen Clouddienst entscheidet, muss sich darüber im Klaren sein, dass sämtliche mobilen Daten – Geschäftsdaten, wie auch personenbezogene Daten – auf einem Fremdserver gehostet werden. Weitere Informationen dazu siehe Kapitel „Datenschutz".

"Sicherheit"

Eine der wichtigsten Fragen im Bereich Mobile Device Management ist die nach der Absicherung der Geschäftsdaten auf dem mobilen Endgerät. Sowohl iOS- als auch Android-basierte Geräte wurden ursprünglich für den Consumer-Markt konzipiert, müssen jetzt aber in die geschäftlichen/dienstlichen Prozesse eingebunden werden. iOS wie Android bieten durchaus die Möglichkeiten zur Bearbeitung dienstlicher Belange (PIM-Daten, E-Mail usw.), haben darüber hinaus aber auch Funktionalitäten, die eher für den Privatgebrauch gedacht sind, beispielsweise die Integration von Twitter oder Facebook beziehungsweise YouTube oder Google+ in das Betriebssystem. Es gibt Hunderttausende Apps in den App-Stores, mit denen die Funktionalitäten eines Gerätes in jede denkbare Richtung erweitert werden können.

Sicherheitsbegriffe werden in den Produktbeschreibungen von MDM-Lösungen leider häufig verallgemeinert, was bedeutet, dass beworbene Sicherheitseigenschaften oft nur auf eine Teilmenge der unterstützten Geräte einer Plattform anwendbar sind. So gibt es beispielsweise Lösungen, die spezielle Programmierschnittstellen (APIs) bestimmter Hersteller/OEMs nutzen, um Android-basierte Smartphones zu verwalten und abzusichern. Dass dieser Mechanismus nicht für Geräte anderer Hersteller gilt und zudem nur für bestimmte Geräte eines Herstellers nutzbar ist, wird in der Produktpräsentation nicht genannt. Ebenso muss man sich darüber im Klaren sein, dass die Unterstützung unterschiedlicher Plattformen sowie deren Verwaltung in einer gemeinsamen Konsole nicht bedeutet, dass Konfigurationen und Richtlinien auf allen Plattformen in gleicher Weise umgesetzt werden. So gibt es beispielsweise systembedingte Unterschiede zwischen iOS und Android bei der Bereitstellung von Apps in einem eigenen App-Store (siehe dazu Kapitel „App-Management").

Grundsätzlich muss man zwischen der Absicherung der Datenflüsse einerseits und der Absicherung der Daten auf dem Smartphone selbst unterscheiden („data in motion" vs. „data at rest").

Die Absicherung der Kommunikationswege haben MDM-Lösungen in der Regel sicher im Griff, auch wenn sie dazu auf Fremddienste angewiesen sind (siehe Kapitel „Fremddienste"). Beispiele sind die Verwendung von sicheren Protokollen und Zertifikaten, VPN-Konfigurationen, WLAN-Einstellungen sowie die Anbindung der MDM-Server an die IT-Infrastruktur des Unternehmens.

Für die Absicherung der Daten auf dem Smartphone können in der Regel nur die von der Smartphone-Plattform zur Verfügung gestellten Konfigurationsmöglichkeiten verwendet werden, wie Verschlüsselung, Kennworteinstellungen, Benutzereinschränkungen usw. Die Gefährdung der Unternehmensdaten durch fremde Apps, die beispielsweise auf Kontaktdaten zugreifen, wird von MDM-Lösungen nur dann berücksichtigt, wenn die Plattform entsprechende Schutzmechanismen zur Verfügung stellt. Eine saubere Abtrennung der dienstlichen Verwendung des Smartphones vom Privatgebrauch ist so ohne Weiteres nicht leistbar.

Durch das Sandbox-Prinzip, sowohl von Android als auch iOS, werden Apps und ihre Daten vor dem Zugriff durch andere Apps geschützt. Aufbauend auf dieser Grundsicherung haben einige Anbieter ihre MDM-Lösung um einen „App-Container" erweitert, innerhalb dessen die geschäftlichen Belange bearbeitet werden (siehe Kapitel „Contentmanagement auf dem Smartphone").

Datenschutz

Flankierend zu der Absicherung der Datenkommunikation zwischen mobilem Endgerät und MDM-Server sollte sich ein Unternehmen auch über die Auswirkungen des Einsatzes einer solchen Lösung auf den Datenschutz im Klaren sein. Die meisten Anbieter von MDM-Lösungen stammen nicht aus Deutschland oder der Europäischen Union und betreiben ihre Server außerhalb dieser Zone (etwa in den USA). Das heißt, dass diese Firmen nicht deutschem oder europäischem Datenschutzrecht unterliegen, sondern entweder gar keinem oder einem von Europa nicht anerkannten Datenschutzrecht. Aus diesem Grund hat die Europäische Union mit den USA das sogenannte „Safe Harbor"-Abkommen geschlossen, das die Übermittlung personenbezogener Daten an Server in die USA zumindest rechtlich regelt (Safe Harbor).

Außerdem wird an dieser Stelle speziell auf §11 des Bundesdatenschutzgesetzes (BDSG) „Erhebung, Verarbeitung oder Nutzung personenbezogener Daten im Auftrag" hingewiesen. Dieser besagt, dass bei der Bearbeitung personenbezogener Daten durch andere Stellen (beispielsweise bei Nutzung einer Cloud-Lösung für MDM), der Auftraggeber nach wie vor für die Einhaltung des BDSG verantwortlich ist (Bundesdatenschutzgesetz).

Contentmanagement auf dem Smartphone

Eine weitere Herausforderung für eine MDM-Lösung besteht darin, die geschäftlichen Prozesse auf dem Gerät so zu separieren, dass sie nicht durch die sonstige (vor allem private) Verwendung beeinflusst oder gefährdet werden.

Die meisten MDM-Lösungen bieten dazu keine eigenen Mechanismen an. Zur Bearbeitung der dienstlichen Belange werden die nativen Apps verwendet. Das heißt, das Smartphone wird so genutzt, wie von der Betriebssystem-Plattform vorgesehen. Es findet also keine komplette Trennung zwischen dienstlicher und sonstiger Nutzung statt.

Daneben gibt es die sogenannte ***Containerlösung***. Es handelt sich dabei um eine normale Smartphone-App, in der die dienstlichen Belange bearbeitet werden. Sie enthält sämtliche PIM-Daten, E-Mails und Dokumente sowie auch die für die Bearbeitung dieser Daten notwendigen Programmfunktionen, das heißt E-Mail-Client, Kalender, Kontaktverwaltung usw. Weiterhin muss auch ein Browser vorhanden sein, da nur über ihn auf Unternehmens-Server zugegriffen werden darf. Außerhalb dieser App kann das Gerät normal verwendet werden. Diese Art der dienstlichen Verwendung führt beim Benutzer häufig zu Akzeptanz-Problemen, kann man das Smartphone im dienstlichen Bereich doch nicht nach den Möglichkeiten nutzen, die im Privatbereich zur Verfügung stehen. Dennoch bietet diese Lösung eine grundsätzliche Trennung der dienstlichen und privaten Nutzung.

Ein weiterer Lösungsansatz zur Bearbeitung dienstlicher Belange auf dem mobilen Endgerät ist eine Terminalserver-Sitzung, bei der die Verarbeitung und Speicherung der Daten auf dem Terminalserver verbleibt. Das Mobilgerät wird nur für die Darstellung und Eingabe verwendet, das heißt, von/zum Mobilgerät werden nur Texteingaben, Bildschirminhalte und Eingabe-Gesten übertragen. Entsprechende Lösungen gibt es sowohl für das iPad als auch für Android-Smartphones/Tablets. Nachteilig können sich Engpässe bei der Datenübertragung auswirken, insbesondere dann, wenn die Datenverbindung des Smartphones über ein Mobilfunknetz hergestellt wird. Außerdem wird auf dem Smartphone/Tablet-Display oft ein Windows-Desktop dargestellt, der nicht für die Darstellung und Bedienung auf einem Touchscreen-Smartphone/Tablet optimiert ist. Hier gilt: Lassen Sie sich vor der Einführung einer solchen Lösung Referenzprojekte zeigen und testen Sie ausgiebig.

Bei Android gibt es außerdem verschiedene neue Ansätze, durch Virtualisierung zwei Betriebssysteme gleichzeitig auf einem Smartphone zu betreiben. Ein Lösungsansatz enthält zwei vollständige Android-Versionen, die gleichzeitig gestartet werden und zwischen denen man während des Betriebs wechseln kann. Ein anderer Lösungsansatz betreibt ein zweites Betriebssystem als App innerhalb des nativen Betriebssystems. Erfahrungswerte aus einem breiten praktischen Einsatz liegen jedoch noch nicht vor.

Doch die Entwicklung der mobilen Plattformen schreitet voran. So steht in Version 4.2 von Android eine Mehr-Benutzer-Verwaltung für Tablets zur Verfügung, die eine bessere Trennung verschiedener Benutzer oder Einsatzszenarien ermöglicht. Eine Neuerung in Version 6 von iOS ist beispielsweise die Möglichkeit zur Einrichtung eines globalen HTTP-Proxies, sodass die IT-Abteilung den Internetverkehr über einen kontrollierten Kanal leiten könnte.

Fremddienste

Die Datenverbindung zwischen dem mobilen Endgerät und dem MDM-Server wird entweder über einen Mobilfunk-Provider (via GPRS, EDGE, UMTS, HSDPA, LTE) oder über eine WLAN-Verbindung hergestellt. Die zugewiesene IP-Adresse ist nicht vorhersehbar beziehungsweise nicht erreichbar, sodass das Gerät nicht

von einem MDM-Server kontaktiert werden kann. Der Verbindungsaufbau zum Server muss demnach vom Smartphone aus erfolgen.

Mit dem sogenannten *Apple Push Notification Service* (APNS) beziehungsweise dem *Google Cloud Messaging* (GCM) bieten die Hersteller Dienste an, über die iOS- beziehungsweise Android-Geräte trotzdem kontaktiert werden können. Diese Dienste sind in das Betriebssystem integriert und können nicht abgeschaltet werden. Will ein MDM-Server eine Kommunikation mit einem Client aufbauen, sendet er eine Nachricht mit dem Kommunikationswunsch über APNS beziehungsweise GCM an das Smartphone, damit dieses eine Verbindung zu seinem MDM-Server aufbaut. Ohne diese Dienste müsste das Smartphone periodische Anfragen beim Server stellen, um seinen Status abzufragen.

Es gibt eine ganze Reihe von Apps, die Push Notifications empfangen können, bei iOS beispielsweise Erinnerungen, Kalender, Passbook, „Freunde finden" usw. Es sollte geprüft werden, für welche Apps Push Notifications wirklich notwendig sind und bei welchen Anwendungen dieser Dienst deaktiviert werden kann.

Diebstahlschutz

Unter „Diebstahlschutz" versteht man im Kontext von Mobile Device Management nicht den Schutz vor dem Abhandenkommen des Gerätes. Gemeint sind die Maßnahmen, die die IT-Abteilung oder der Besitzer nach Verlust oder Diebstahl einleiten können, um die auf dem Gerät befindlichen Daten vor Missbrauch zu schützen. Wird der Administrator über den Verlust informiert, kann er von der MDM-Konsole aus entsprechende Kommandos, wie etwa „Remote Lock", absenden. Manche MDM-Lösungen besitzen auch ein Web-Portal, über das der Benutzer selbst solche Kommandos abgeben kann.

„Remote Lock" sperrt das Gerät, eine weitere Verwendung ist nur mit dem Passcode möglich. „Remote Wipe" löscht die Datenbestände auf dem Smartphone entweder vollständig oder selektiv. Neben den Unternehmensdaten müssen auch die Konfigurationsprofile, beispielsweise Zugangsdaten und Zertifikate, gelöscht werden. Bei der Verwendung einer SD-Karte zur Speicherung von Unternehmensdaten muss weiterhin darauf geachtet werden, dass diese in den Löschvorgang mit einbezogen wird. Dies sollte in jedem Fall getestet werden.

Weitere Möglichkeiten im Bereich „Diebstahlschutz" sind:

- Löschen nach einer bestimmten Anzahl von fehlerhaften Passcodeeingaben
- Lokalisieren des Geräts mit übermittelten GPS-Koordinaten
- Tonausgabe zum Wiederauffinden

Weitere Informationen finden Sie im Kapitel „Notfallmaßnahmen / Notfallübungen".

Eine besondere Situation besteht dann, wenn das Smartphone neben der dienstlichen Verwendung auch privat genutzt wird. Wenn eine MDM-Lösung bei dem Löschvorgang nicht zwischen dienstlichen und privaten Daten unterscheiden kann. Wird ein Gerät beispielsweise in den Auslieferungszustand zurückgesetzt, gehen auch alle privaten Daten verloren. Dies sollte in einer Dienstvereinbarung geregelt sein, da der Mitarbeiter ansonsten vor der jeweiligen Löschung seiner privaten Daten im Ernstfall erst um seine Zustimmung gebeten werden muss.

Bring Your Own Device (BYOD)

Bei der dienstlichen Nutzung von Privatgeräten bestehen rechtliche Konflikte bezüglich des Software-Lizenzrechts (dienstliche Nutzung privater Lizenzen und umgekehrt) sowie bezüglich Notfallmaßnahmen (Löschung des gesamten Datenbestands), Datenschutz und -sicherheit usw.

Außerdem ist der Eigentümer nicht mehr Herr über sein Gerät, da es von der IT-Abteilung fernverwaltet wird. Dies kann zu Akzeptanz-Problemen führen, insbesondere, weil die IT-Abteilung die gewählten Konfigurationen auf den Smartphones durchsetzen muss, was zwangsläufig zu Benutzereinschränkungen führt.

Im Android-Umfeld kommt die mittlerweile unüberschaubare Vielfalt von Geräten von verschiedensten Herstellern hinzu. Die Leistungsfähigkeit dieser Smartphones variiert sehr stark vom einfachen Einsteigergerät bis zum „Alleskönner" aus dem High-End-Segment. Fast täglich erscheinen neue Modelle auf dem Markt. Eine IT-Abteilung ist nicht in der Lage, jedes einzelne Gerät hinsichtlich seiner Qualifikation für den Einsatz im Unternehmensumfeld zu prüfen. Dazu kommt bei Smartphones auf Android-Basis noch die bekannte Update-Problematik. Geräte, die nicht zeitnah oder gar nicht mehr mit Systemaktualisierungen versorgt werden (egal ob Privatgerät oder Dienstgerät), sollten nicht für dienstliche Belange eingesetzt werden.

Aus diesen Gründen ist das Konzept „Bring Your Own Device" für den Unternehmenseinsatz grundsätzlich abzulehnen. Wird eine gleichzeitige Nutzung von dienstlichen und privaten Belangen auf diesen Geräten dennoch erlaubt, ist eine Dienstvereinbarung unter frühzeitiger Beteiligung der Personalvertretung notwendig.

Anmerkung: Dem Konzept „Bring Your Own Device" steht ein anderes Konzept „Private Use Of Corporate Equipment" (PUOCE) gegenüber. Das Unternehmen könnte Smartphones beschaffen, die alle plattformbedingten Forderungen erfüllen, die von der MDM-Lösung vollständig unterstützt werden und in gewissem Maße privat genutzt werden dürfen. Die oben genannten rechtlichen Bedenken bleiben aber auch hier bestehen.

Jailbreak / Root-Erkennung

Das Sandbox-Prinzip von iOS wie auch von Android basiert auf einer Rechtestruktur des Betriebssystems, die den Zugriff von Apps auf andere Apps und auf Systemressourcen limitiert und dafür sorgt, dass sie nur in ihrem lokalen Bereich Daten manipulieren können. Durch den sogenannten „Jailbreak" bei iOS-basierten Geräten beziehungsweise dem „Rooten" bei Android-basierten Geräten wird dieses Rechtekonzept außer Kraft gesetzt, sodass Apps Root-Rechte erhalten. Ein Trojaner auf einem manipulierten Gerät kann volle Kontrolle über das Smartphone erlangen und so sämtliche Daten – dienstliche, wie private – abgreifen. Apple hatte ab Version 4.0 von iOS eine Jailbreak-Erkennung in das Betriebssystem eingebaut. Die entsprechende Programmschnittstelle (API) konnte von MDM-Lösungen verwendet werden, um manipulierte Geräte zu erkennen. In Version 4.2 entschied sich Apple jedoch gegen dieses Konzept und baute die Schnittstelle wieder aus. Seitdem müssen MDM-Anbieter wieder eigene Jailbreak-Mechanismen verwenden, entsprechendes gilt für Android.

Eine MDM-Lösung braucht in jedem Fall eine effektive Jailbreak/Root-Erkennung, die von der IT-Abteilung getestet werden muss. Nur so lassen sich manipulierte Geräte, von denen ein hohes Risiko für das Unternehmen ausgeht, erkennen. Die IT-Abteilung muss daher auch entsprechende Geräte zum Test vorhalten.

Leider sind jedoch die Möglichkeiten von Techniken zur Jailbreak/Root-Erkennung begrenzt, da sie auf Software-Abfragen basieren und solche Funktionen durch geschickte Gegenmaßnahmen getäuscht werden können.

App-Management

Jeder kennt die App-Stores für Smartphones, aus denen Hunderttausende von Apps – kostenlose wie kostenpflichtige – heruntergeladen und installiert werden können. Für iOS-basierte Geräte ist dies der Apple „App Store", Apps für Android-basierte Geräte werden im offiziellen Google Store „Google Play", aber auch in vielen anderen Stores (z. B. Amazon App-Store) angeboten. Installationspakete für Android (apk-Dateien) sind aber nicht an einen Store gebunden. Im Prinzip kann man sie von jedem beliebigen Ort laden und installieren.

Viele MDM-Lösungen bieten einen „eigenen" App-Store für Unternehmens-Apps und/oder ausgewählte öffentliche Apps als Web-Portal an. Neben der „Grundbetankung" mit Apps im Auslieferungszustand hat ein Unternehmen damit die Möglichkeit, den Mitarbeitern eine Auswahl von erlaubten (und möglichst geprüften) Apps zur Verfügung zu stellen.

Die Ausprägungen der App-Stores sind unterschiedlich, vom einfachen Bereitstellen von öffentlichen Apps, über spezielle Unternehmens-Apps, bis hin zu einem umfassenden App-Management (Verteilung, Kontrolle, Überwachung). Bei Letzteren können angebotene Apps für Android (und teilweise iOS) über sogenannte „Wrapping"-Mechanismen mit zusätzlichen Kontrollfunktionen „umhüllt" werden. Dies ermöglicht der MDM-Lösung anschließend die Kontrolle von Funktionalitäten oder Berechtigungen.

Die regelmäßige Kontrolle der installierten Apps auf dem Smartphone des Mitarbeiters ist notwendig, um einer missbräuchlichen Verwendung des mobilen Endgerätes entgegenzuwirken. Einige MDM-Lösungen bieten dazu Inventarisierungs-Funktionalitäten an.

Gruppen-/Benutzerverwaltung, Mandantenfähigkeit

Als Mandantenfähigkeit einer Verwaltungssoftware wird häufig die Möglichkeit bezeichnet, verschiedene Unternehmen zu verwalten, also beispielsweise verschiedene Kunden eines IT-Dienstleister. Dies ist nicht falsch, aber nur ein Teilaspekt dieses Themas. Bei der Verwaltung mobiler Endgeräte steht die IT-Abteilung vor dem gleichen Problem wie auch bei der Verwaltung von Desktop-Computern. Bei größeren Unternehmen müssen verschiedene Niederlassungen, Abteilungen und Gruppen (beispielsweise Entwicklung, Vertrieb, Verwaltung) über eine Konsole unterschiedlich konfiguriert werden können. Möglicherweise existieren verschiedene Teilnetze in der IT-Infrastruktur, die gesondert berücksichtigt werden müssen. Die IT-Infrastruktur muss also auch in der Verwaltungskonsole der MDM-Lösung abbildbar sein.

MDM-Lösungen müssen in jedem Fall eine Gruppen- und Benutzerverwaltung für verschiedene Endgerätrollen beinhalten. Darüber hinaus können sie auch mandantenfähig (im oben genannten Sinne) sein. Werden über eine MDM-Lösung in einer größeren Umgebung verschiedene „Mandanten" verwaltet, so ist zu klären, wer die Verwaltung übernimmt. Sinnvoll ist ein Haupt-Administrator, der die grundlegenden Einstellungen trifft, sowie mehrere Verwaltungs-Administratoren, die für Teilbereiche zuständig sind. Es sind rollenbasierte und/oder lokationsbasierte Administratoren denkbar.

Notfallmaßnahmen / Notfallübungen

Der Verlust oder Diebstahl eines Smartphones oder Tablets ist gleichbedeutend mit dem Verlust oder dem Diebstahl von Geschäftsdaten. Das Gerät muss schnellstmöglich gesperrt und/oder ferngelöscht werden. Es ist also äußerst wichtig, dass der Benutzer den Verlust so früh wie möglich meldet. Mitarbeiter sollten diesbezüglich in regelmäßigen Abständen sensibilisiert werden. Enthält die MDM-Lösung ein Self-Service-Portal für diese Zwecke, müssen die Mitarbeiter mit dem Umgang vertraut gemacht werden. Außerdem ist ein Notfallplan zu erstellen, der klare Anweisungen enthält, die auch von einem Vertreter des zuständigen Administrators durchgeführt werden können.

Zusätzlich zu der Fernsperrung/Fernlöschung des verlorenen Gerätes muss der Zugang des Smartphones zum Unternehmen in der Verwaltungskonsole komplett gesperrt werden, damit kein unberechtigter Zugriff mehr erfolgt.

Schutzprogramme

Apps zum Schutz vor Malware auf Android-basierten Smartphones arbeiten mit den gleichen Einschränkungen wie alle anderen Apps auch. Sie sind in eine Sandbox eingesperrt und müssen bei der Installation ihre Berechtigungen anmelden. Es besteht keine Möglichkeit mit Systemberechtigungen (Root/Administrator-Rechten) in den Tiefen des Betriebssystems zu agieren.

Schadprogramme werden anhand der Installationsdatei (apk-Datei) erkannt. Durch die Android-Berechtigung „Aktive Apps abrufen" ist die Schutz-App in der Lage, installierte Programmpakete gegen eine Blacklist zu prüfen. Diese Blacklist mit bekannten Malware-Programmpaketen ist entweder im Schutzprogramm enthalten oder wird online abgerufen. So können infizierte Apps „on demand" oder bei der Installation erkannt werden.

Daneben gibt es je nach Ausbaustufe noch weitere Schutzfunktionen, beispielsweise Schutz vor unberechtigtem Zugriff auf Kontaktdaten oder SMS- und Anruffilter. Weitere Schutzfunktionen sind „SIM-Kartenwechsel erkennen und Gerät sperren" sowie „Remote Wipe"-Funktionalitäten.

Unter iOS ist es grundsätzlich technisch nicht möglich, solche zusätzlichen Schutzmaßnahmen zu installieren. Apple stellt hierfür keine geeigneten Schnittstellen zur Verfügung, sondern wehrt Angriffe über betriebssystemeigene Mechanismen ab.

Zusätzliche Informationen zum Android-Berechtigungssystem finden Sie auf der Internetseite „BSI für Bürger" unter Exkurs: App-Berechtigungen bei Android.

Konfigurationsempfehlungen (exemplarisch)

Im Folgenden werden einige wenige ausgewählte Konfigurationsempfehlungen für iOS und Android vorgestellt. Sie sollen in späteren Versionen dieses Dokuments erweitert werden. Vorschläge für Konfigurationsempfehlungen, die nicht trivial sind oder eine besondere Bedeutung für die Datensicherheit darstellen, werden gerne entgegengenommen (gerne auch für andere mobile Betriebssysteme).

Die beschriebenen Konfigurationen sind jeweils von einem für das Unternehmen verantwortlichen System-Administrator durchzuführen und per Passwort vor Änderungen durch den Benutzer zu schützen. Sofern möglich sollten die Anpassungen zentral über die MDM-Lösung vorgenommen werden.

Android: Externer Speicher

Die Speicherung dienstlicher Daten auf Standard-SD-Karten sollte nach Möglichkeit verhindert werden, Datendiebe können die Speicherkarte schnell und leicht vor dem Zugriff durch die MDM-Lösung schützen. Prüfen Sie zumindest, ob die gespeicherten Daten auf dem externen Speicher verschlüsselt werden. Prüfen Sie auch, ob ein „Remote Wipe"-Befehl die Daten der SD-Karte überhaupt löscht.

iOS: Konfigurations-Profile

Einstellungen von iOS-basierten Geräten werden über Konfigurations-Profile vorgenommen. Technisch sind das Dateien im XML-Format, die an das Gerät gesendet und dort verarbeitet werden. Wird eine Einstellung durch den Administrator geändert, muss die entsprechende Konfigurations-Datei (.mobileconfig-Datei) erneut an das Gerät (die Geräte) gesendet werden. Verschiedene MDM-Lösungen konfigurieren iOS-Geräte über ein einziges Konfigurations-Profil. Dies hat zur Folge, dass bei der Änderung einer einzigen Einstellung die gesamte Konfiguration erneut verarbeitet wird und eine vollständige Synchronisation der Daten stattfindet. Die Folge ist die erneute (unnötige) Übertragung der Daten. Deshalb ist eine Aufteilung der Konfigurationen auf mehrere Konfigurations-Dateien sinnvoll, was von einigen MDM-Lösungen gemacht wird.

iOS: „Öffnen in ..."

Verschiedene Apps bieten die Option „Öffnen in ..." (engl. „Open in ...") für die Bearbeitung von Dateien an. In der Option werden Apps angezeigt, die in der Lage sind, die Dateiinhalte zu verarbeiten. Beispiel: Bei pdf-Dateien hat man u. a. die Möglichkeit, den Inhalt in der „iBooks-", „Chrome-" oder „Kindle-" App zu lesen. Mit „Öffnen in ..." kann man aber auch Dateien zu einem Speicherdienst in der Cloud (wie beispielsweise „Dropbox") verschieben.
Wenn möglich, muss diese Option durch die MDM-Lösung deaktiviert werden.

Mit den BSI-Veröffentlichungen publiziert das Bundesamt für Sicherheit in der Informationstechnik (BSI) Dokumente zu aktuellen Themen der Cyber-Sicherheit. Kommentare und Hinweise können von Lesern an info@cyber-allianz.de gesendet werden.