mitp

Heinrich Kersten

Gerhard Klett

Mobile Device Management

Heinrich Kersten und Gerhard Klett

Mobile Device Management

Bibliografische Information der Deutschen Nationalbibliothek
Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über <http://dnb.d-nb.de> abrufbar.

ISBN 978-3-8266-9257-4
1. Auflage 2012

E-Mail: kundenbetreuung@hjr-verlag.de

Telefon: +49 89/2183-7928
Telefax: +49 89/2183-7620

www.mitp.de

Lektorat: Ernst H. Pröfener
Satz: III-satz, Husby, www.drei-satz.de

Inhaltsverzeichnis

Mobile Device Management

Vorwort und Einleitung

Die in den letzten Jahren zu beobachtende Evolution des Mobile Computing und der rasante Anstieg von mobilen Endgeräten wie Netbooks, Smartphones und Pad-Computer im Unternehmenseinsatz haben unsere Arbeitswelt und die IT-Infrastrukturen nachhaltig verändert. Mitarbeiter können orts- und zeitunabhängig auf Ressourcen im Unternehmensnetzwerk zugreifen, Geschäftsdaten abrufen oder E-Mails lesen. Leichter Zugriff von unterwegs mit den eigenen (Stichwort: »Bring Your Own Device«, BYOD) oder unternehmenseigenen mobilen Endgeräten auf Informationen und Ressourcen von Unternehmen steigert nachhaltig Produktivität und Motivation der Mitarbeiter. Der Einsatz mobiler Endgeräte erhöht jedoch die Risiken der Verletzung der Informationssicherheit signifikant und erfordert eine umfassende Integrationsstrategie.

In dem vorliegenden Werk möchten wir nach der Vorstellung der Charakteristika der Hardware der hauptsächlich in der Praxis verwendeten mobilen Endgeräte deren Betriebssysteme und ihre Abstammung diskutieren und einige Details zu ihren Administrationsmöglichkeiten sowie Sicherheitsfunktionen festhalten. Dazu zählt auch die Unterscheidung zwischen dem eigentlichen Betriebssystem und den spezifischen Softwareänderungen durch die Netzbetreiber, dem sogenannten »Branding«. Weiter ist es für die Geräteverwaltung wichtig, die Versorgungsprozesse (»Provisioning«) mit Applikationssoftware – den »Apps« – und Updates oder Patches für die Betriebssysteme zu untersuchen.

»Mobile Device Management« ist ebenfalls ein Thema in Sicherheitsstandards. Dazu betrachten wir die entsprechenden Controls in der ISO 27001 und den Maßnahmen in den Katalogen des BSI-Grundschutzes.

Wie wir bereits erwähnten, nehmen mit dem Einsatz von mobilen Endgeräten die Bedrohungslage und die damit verbundenen Risiken für die Ziele der

Informationssicherheit für die auf mobilen Geräten übertragenen, verarbeiteten und gespeicherten Daten stark zu. Diese Sicherheitsprobleme sind vielfältig; ein wesentliches Ziel des Mobile Device Management ist es, vorgegebene Sicherheitsstandards und Policies zu gewährleisten und die Verpflichtungen des Unternehmens zur Compliance gegenüber Gesetzen, Verträgen und Richtlinien einzuhalten.

Mit welchen Funktionen das Mobile Device Management dazu beiträgt, in welche Komponenten ein Managementsystem unterteilt werden kann und welche Betriebsprozesse damit verbunden sind, ist Inhalt eines weiteren Kapitels.

Bei der Betrachtung der Business Continuity wird gerne vergessen, dass kritische Geschäftsprozesse in immer größerem Maße auf mobilen Infrastrukturen abgebildet werden und dafür auch ein Notfallmanagement mit Business Impact Analysis und Desaster Recovery existieren muss.

Eine weitere Erschwernis der Verwaltung mobiler Endgeräte bringt die immer beliebtere Praxis, Endgeräte, die sich im persönlichen Besitz von Mitarbeitern befinden, für die betriebliche Verwendung in die Unternehmensinfrastruktur einzubinden. Wir betrachten hier das sogenannte »Bring Your Own Device« (BYOD), das zunehmend Anhänger findet, aber die Bedingungen für eine sichere Endgeräte-Administration sehr komplex gestalten kann.

Zum Abschluss des vorliegenden Buches gehen wir noch auf praktische Auswahlkriterien ein und stellen für die organisatorischen Belange des Mobile Device Managements entsprechende Vorschläge für Unternehmensrichtlinien vor.

1 Mobile Device Management – Eine Übersicht

1.1 Mobile Endgeräte

Kein Bereich der Wirtschaft weist so hohe Zuwachsraten und so kurze Innovationszyklen auf wie die Informationstechnik, insbesondere wenn es um Mobile Computing geht. Tragbare Computer sind endlich so klein und handlich, dass sie permanent mitgeführt werden können. Ihre Kommunikationsfähigkeiten verbinden sie an jedem Ort der Welt mit zahlreichen Informationsressourcen im globalen Internet und im Netzwerk des eigenen Unternehmens. »Always online« ist längst keine Fiktion mehr.

Informations- und Kommunikationstechnologien wachsen immer stärker zusammen. Wir erleben diese Konvergenz in Form immer handlicher werdender Netbooks, Smartphones, Tablets oder Pad-Computer. Wir bewegen uns mit diesen Mobile Devices in einer dritten – der digitalen – Lebenswelt. Als erste Lebenswelt wird die biologische, als zweite die Arbeitswelt angesehen.

In dieser dritten Lebenswelt begegnen wir Vernetzungsformen mit Bezeichnungen wie Wireless LAN (WLAN), Bluetooth oder Near Field Communication (NFC) – der modernen Form von Radio Frequency Identification. Objekte mit aufgeklebten oder implantierten Mikrochips werden in Netzwerke eingebunden, bilden ein kommunikationsfähiges Netzwerk in unserer Einkaufstüte und verbinden sich ohne Weiteres mit weiter reichenden, anderen Netzwerken. Neue Anwendungen für Logistik, Warenwirtschaft oder für das tägliche Leben entstehen.

Immer mehr kritische Geschäftsprozesse werden auf mobile Infrastrukturen abgebildet, und die dabei benötigten Rollen werden Personen übertragen, die mithilfe ihrer mobilen Endgeräte von irgendwo auf der Welt diese Rollen ausüben. Dazu benötigen sie die maximale Verfügbarkeit von Informationen zu jeder Zeit, an jedem Ort, in jedem üblichen digitalen Format und zwischen jedem Kommunikationspartner ohne langwierige Anmeldeprozeduren.

Die passenden mobilen Endgeräte sollen folgenden Kriterien genügen:

- Leicht, geringe Abmessung, kleiner »Formfaktor«
- Einfach ständig mit sich zu führen, häufiger »Milieuwechsel«
- Extensive Verwendung drahtloser Netzwerke, zahlreiche Kommunikationsmöglichkeiten
- Intuitive Benutzerschnittstelle mit »Touch«-Displays und Gestensteuerung
- Vielfältige Sensorik (GPS-Navigation, Lage-, Beschleunigungs- und Näherungssensoren etc.)
- Akkubetrieb mit langen Standby-Zeiten
- Schnittstelle für OTA-Verwaltung (»Over The Air«)
- Ausführung von Applikationen (»Apps«) für zahlreiche Bereiche

Durch die Kritikalität der Verwendung mobiler Endgeräte entsteht die Notwendigkeit, diese Gerätschaften entsprechend zu verwalten – egal zu welcher Zeit und an welchem Ort sie sich befinden.

Aber welche mobilen Endgeräte werden überwiegend eingesetzt?

1.2 Smartphones, Pads und Tablet-Computer

Praxisübliche mobile Endgeräte lassen sich prinzipiell in vier Klassen einteilen:

1. Notebooks oder Netbooks: Endgeräte mit leitungsfähigen Prozessoren, vollwertigen Tastaturen und Anzeigen, in ihrer Ausstattung vergleichbar mit stationären Rechnern. Zum Transport werden geeignete Taschen benötigt, das Betriebssystem ist das gleiche wie auf stationären Rechnern, meist von Microsoft oder eine Linux-Variante.
2. Tablet-Computer: Gerätekategorie zwischen Notebooks und Smartphones mit einem ähnlichen Aufbau wie Notebooks. Sie besitzen einen vergleichbaren Funktionsumfang wie Notebooks und haben ein Touch Display, welches mit Finger oder Stift bedient wird. Convertibles haben eine um 180 Grad kippbare konventionelle Tastatur. Als Betriebssystem kommt eine Version von MS Windows zum Einsatz, selten ein angepasstes Linux. Spezielle Applikationen unterstützen die Eingabe von Handschrift, z.B. für Notizen.

3. Smartphones: Mobilfunkgeräte mit Sensorik im Westentaschenformat, überwiegend ohne Tastaturen mit kleinen berührungsempfindlichen Anzeigen und einem Betriebssystem, welches die Ausführung von Applikationsprogrammen, kurz »Apps« genannt, erlaubt. Sie verfügen in der Regel über mehrere Kommunikationsschnittstellen und werden in der Kleidung transportiert.
4. Pad-Computer: »Große Smartphones« im A5-Format. Pad-Computer verwenden bis auf wenige Ausnahmen die angepassten Betriebssysteme von Smartphones und können ebenfalls »Apps« ausführen.

Diese Geräte werden heute hauptsächlich für den Zugriff auf Ressourcen im Unternehmen über Virtual Private Networks, die Nutzung öffentlicher Dienste und Netze, die Speicherung sensibler Daten, Synchronisation von PIM-Daten (Personal Information Manager) wie E-Mail, Kalender, Kontakte etc. und den mobilen Zugriff auf das Internet verwendet, beispielsweise für Cloud-Services.

Hardware und Betriebssystem mobiler Endgeräte bilden mobile Plattformen, welche zwei Kategorien zugeordnet werden können:

Kategorie 1: Die abgeschotteten Plattformen, der sogenannte »walled garden«, lassen keine Wahl zwischen der Hardware verschiedener Hersteller und unterstützen nur eine kontrollierte, eingeschränkte Applikationsentwicklung. Hardware und Betriebssystem kommen vom gleichen Hersteller. Typische Vertreter dieser Kategorie sind Apple mit iPhone und iPad und Research in Motion (RIM) mit BlackBerrys.

Kategorie 2: Bei den partneroffenen Plattformen hat man die Wahl der Hardware von unterschiedlichen Herstellern. Einige Plattformen sind offen für Eigenentwicklungen in Java, C etc. Typische Vertreter von offenen Plattformen sind Android und Symbian.

Für welche Kategorie man sich letztlich entscheidet, hängt vom Einsatzzweck, den Unternehmensrichtlinien und der Unternehmensstrategie ab. Abgeschottete Plattformen verfügen über Schnittstellen und Architekturen zum Mobile Device Management; bei partneroffenen Plattformen lässt sich das, wie wir später sehen werden, nicht voraussetzen.

Bei abgeschotteten Plattformen werden Apps vor der Aufnahme in einen Appstore dynamischen und statischen Tests unterzogen und zum Schutz vor Manipulationen mit einer elektronischen Signatur versehen. Das Endgerät

prüft vor der Installation die Signatur und verweigert die Installation bei einer fehlenden oder falschen elektronischen Signatur. Diese Sicherheitsmaßnahme reduziert entscheidend das Risiko, über abgeschottete Plattformen Computerviren und Trojaner zu verteilen.

1.3 Betriebssysteme mobiler Endgeräte

Über die Betriebssysteme von Notebooks und Tablet-Computer müssen wir nicht viele Worte verlieren: hier wird überwiegend Microsoft Windows eingesetzt – und seltener Linux-Varianten. Die Situation bei Smartphones und Pad-Computern ist komplexer; hier gibt es mehrere unterschiedliche Betriebssysteme, die jedoch Gemeinsamkeiten aufweisen.

1.3.1 »Branding«

Bei Smartphones und Pad-Computer kommen zu der eigentlichen Firmware des Herstellers der Betriebssysteme noch die speziellen Anpassungen des Netzbetreibers hinzu. Dieses Aufdrücken eines »Herdenstempels«, »Branding« oder »Customization« genannt, wird häufig von Tochterfirmen des Netzbetreibers vorgenommen.

Hinweis

Nicht nur Netzbetreiber führen »Branding« durch, sondern auch die Hardwarehersteller bei offenen Plattformen, was es ermöglicht, eine Firmware auf Geräten verschiedener Hersteller einzusetzen.

Die Änderungen der Betriebssysteme durch »Branding« umfassen erweiterte Funktionen wie die Einrichtung zusätzlicher Favoritenlisten im Browser und Rufnummerneinträge für (kostenpflichtige) Hotlines oder die Neubelegung von Tasten. Aber auch Sperrungen bestimmter Eigenschaften wie zum Beispiel die Wahlfreiheit bei der SIM-Karte durch die Einrichtung von SIM-Locks sind Bestandteile des »Branding«.

Für das Mobile Device Management von Smartphones und Pad-Computern erschwerend wirkt sich, wie wir später sehen werden, der Einfluss des »Brandings« auf Patches und Updates der Firmware aus, da das Betriebssystem der

Geräte aus den beiden Komponenten »Branding« und Firmware des Herstellers besteht. Bei der Verteilung von Patches und Updates über die Managementsysteme muss für die Endgeräte der »richtige« Patch, also das »richtige« Update der einzelnen Netzbetreiber verwendet werden.

Vorsicht

Die Betriebssysteme von Smartphones und Pad-Computer sind kein monolithisches Gebilde, sondern bestehen aus der Firmware des Herstellers der Betriebssysteme und den spezifischen Anpassungen der Netzbetreiber. Allerdings wird diese Unterscheidung in der Literatur häufig unterlassen und allgemein von Betriebssystemen gesprochen, auch wenn damit eigentlich die Firmware gemeint ist.

1.3.2 Firmware

Die heute auf dem Markt befindliche Firmware für Smartphones und Pad-Computer lässt sich in zwei Kategorien einteilen:

- Der Kernel der Firmware ist ein Unix (Beispiele: iOS, Android).
- Der Kernel ist eine Eigenentwicklung (Windows Phone 7, BlackBerry).

Die Firmware kann vom Benutzer nicht geändert werden und ist in der Regel durch Verschlüsselung, elektronische Signatur und herstellerspezifische Bootloader geschützt; allerdings gibt es dazu Hintertüren wie das »Jailbreaken« beim iPhone/iPad und das »Rooten« bei Androids.

Die zur Zeit (April 2012) am häufigsten auf dem Markt vertretenen Betriebssysteme (Firmware) sind:

- Android
- iOS
- Symbian
- Windows Phone 7
- BlackBerry

Wesentlich kleiner sind die Marktanteile von z.B. Meego, WebOS, Bada etc.

Dazu einige Statistiken und Zahlen:

World-Wide Smartphone Sales

Quarter	Android	iOS	Symbian	RIM	Microsoft	Bada	Other
2011 Q4 [5]	50.9%	23.9%	11.7%	8.8%	1.9%	2.1%	0.8%
2011 Q3 [4]	52.5%	15.0%	16.9%	11.0%	1.5%	2.2%	0.9%
2011 Q2 [6]	43.4%	18.2%	22.1%	11.7%	1.6%	1.9%	1.0%
2011 Q1 [7]	36.0%	16.8%	27.4%	12.9%	3.6%	1.7%	1.6%

Tabelle 1.1: Weltweiter Smartphone-Absatz[1]

Nach den Zahlen aus der Gartner-Studie Ende 2011 sind Android und Apples iOS die zur Zeit am häufigsten verwendeten Betriebssysteme. Interessanterweise haben wir hier an der Spitze mit Android einen Vertreter der offenen Plattformen mit zahlreichen Hardwareherstellern und mit Apple iOS eine sehr abgeschottete Plattform. Die Gründe liegen unter anderem einerseits an den niedrigen Einstiegspreisen für Android-Smartphones und -Pads und dem »Lifestyle«-Faktor von iPhones/iPads andererseits. Die nachfolgende Grafik vermittelt einen Eindruck über die Dynamik der Auf- und Abstiege einiger Betriebssysteme.

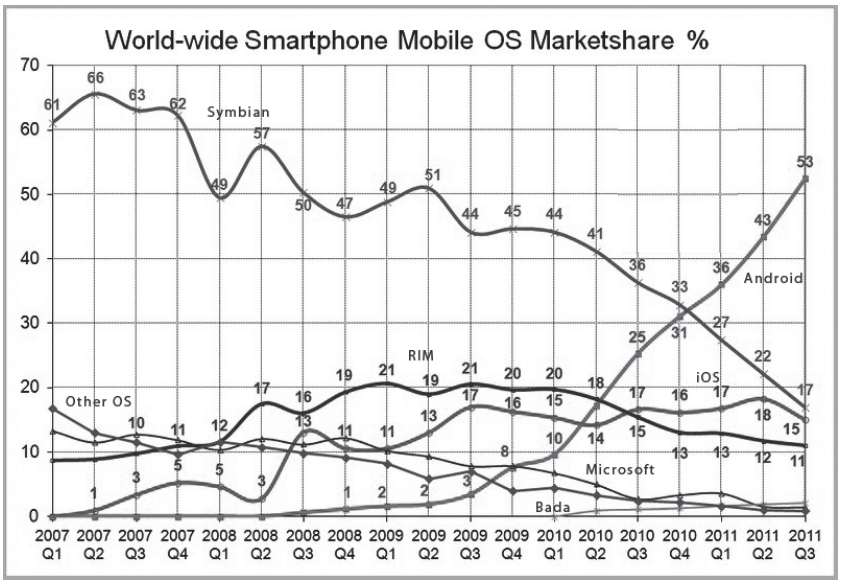

Abbildung 1.1: Weltweite Smartphone-Marktanteile[2]

1. *http://www.gartner.com/it/page.jsp?id=1924314*
2. *http://en.wikipedia.org/wiki/File:World-Wide-Smartphone-Market-Share.png*

Wir wollen im Weiteren die Spezifika der verbreiteten Betriebssysteme näher beleuchten.

1.3.3 Apple iOS

Apple iOS kam 2007 zusammen mit iPhone auf den Markt, das als »iPod, mobile phone and internet communicator«[3] angekündigt wurde. Zu bemerken ist hierbei, dass das iPhone ursprünglich als Medien-Player und Spielekonsole mit Telefonfunktionen für den Endverbraucher gedacht war und dann nach und nach aufgrund der sich einstellenden Nachfrage für den betrieblichen Einsatz weiterentwickelt wurde.

iOS ist im wahrsten Sinne des Wortes das bisher letzte Glied einer darwinistischen Entwicklung – stammt es doch von Darwin ab, einem POSIX-konformen Open-Source-Betriebssystem. Apple entwickelte Darwin aus mehreren frei zugänglichen Softwareprojekten wie zum Beispiel NeXTSTEP und BSD (Berkeley Software Distribution). Apples Mac OS X und das iOS basieren auf Darwin.

Halten wir fest: iOS ist also auch ein Unix-Derivat mit teils schon seit Jahrzehnten bekannten Komponenten. Das lässt schon erahnen, weshalb »Jailbreaks«, das Befreien von Restriktionen, fast zeitgleich mit neuen iOS-Versionen verfügbar sind.

Darwin unterstützt die 64-Bit-Varianten der Intel-x86-Prozessoren im Apple Mac und die 32-Bit-ARM-Prozessoren in iPhones, iPod Touch, iPads und Apple TV.

Darwin-Version	Datum	iOS-Release
9.0	26.10.2007	iOS 1
10.0	28.08.2009	iOS 4
11.0.0	20.07.2011	iOS 5

Tabelle 1.2: Darwin-Versionen und ihr Einsatz in iOS-Releases

3. Jobs, Steve (2007-01-19). Macworld San Francisco 2007 Keynote Address. San Francisco: Apple Inc.

iOS ist ein Betriebssystem für einen einzelnen Benutzer und war zunächst nicht multitaskingfähig. Ab iOS-Version 3.2.2 hat Apple ein begrenztes Multitasking für eine kleine Auswahl seiner Standard-Apps eingerichtet. Beispielsweise war die Ausführung der iPod-App, Mail, Safari und Telefon parallel im Hintergrund möglich. Erst ab der iOS-Version 4 und dem iPhone ab Version 3 ist Multitasking auch für Drittanbieter von Apps möglich. Apple stellt dazu sieben Background APIs (Application Programming Interface) zur Verfügung:

1. Hintergrund-Audio und Video
2. Voice over IP
3. Hintergrundlokalisierung
4. Push-Benachrichtigungen
5. Lokale Benachrichtigungen
6. Beendigung eines laufenden Prozesses im Hintergrund
7. Schnelles Wechseln von Apps

Zugleich wurden mit der Version iOS 4 über 1.500 neue APIs für Entwickler freigegeben, die umfangreiche Funktionen für das zentrale Mobile Device Management ermöglichen.

Für die Entwicklung von Apps für iOS benötigt man ein Apple Software Developers Kit (SDK) und das Entwicklungssystem Xcode. Das SDK besteht aus verschiedenen Komponenten für die Steuerung des Touch-Displays, für die Medienaufzeichnung und -wiedergabe, Netzwerkunterstützung etc., um nur einige zu nennen.

Das SDK wird von Apple frei zum Download angeboten. Zur Einstellung der damit entwickelten Apps in den App Store muss man sich in das kostenpflichtige »iPhone Developer Program« einschreiben und erhält nach einer Überprüfung Zertifikate für digitale Unterschriften, die für das Laden der Apps in den App Store benötigt werden. Das SDK lässt sich nur unter Mac OS X installieren und verwenden.

In Unix-Betriebssystemen werden Einstellungen in sogenannten *config files* innerhalb des Filesystems abgelegt. Das Filesystem von iOS ist für Benutzer nicht direkt zugänglich, eine der Restriktionen von Apple. Dafür existiert eine Schnittstelle, die sogenannte Konfigurationsprofile akzeptiert. Konfigurations-

profile sind XML-Dateien, die gerätespezifische Sicherheitsrichtlinien und Einschränkungen, VPN-Konfigurationsinformationen, WLAN-Einstellungen, Accounts für E-Mail- und Kalenderfunktionen und Authentifizierungszertifikate enthalten. Wir werden später bei der Administration von iPhones und iPads darauf genauer eingehen.

1.3.4 Android

Android Inc. war zunächst ein Softwarehersteller, der bis zum Jahr 2005 überwiegend Software für Mobiltelefone herstellte. In dieser Zeit entstand auch ein Unix-Derivat mit gleichem Namen. Google kaufte 2005 die Firma und gründete 2007 zusammen mit 85 anderen Anbietern von Hardware, Software und Telekommunikationsdiensten die »Open Handset Alliance«[4]. Innerhalb dieser Alliance bildete sich das »Android Open Source Project« (AOSP), welches bis heute die Wartung und Weiterentwicklung von Android zum Ziel hat. Android ist »Open Source«, und außer dem AOSP gibt es weitere, zahlreiche alternative Android-Entwickler[5].

Speziell bei Android sind die Anpassungen der Netzbetreiber und Hardwarehersteller, das bereits erwähnte »Branding«, zu beachten.

Wichtig

Android ≠ Android: Das Betriebssystem gleicher Bezeichnung ist zum Beispiel unterschiedlich bei verschiedenen Hardwareherstellern.

Basis von Android ist der Linux-Kern 2.6. Übernommen wurden die

- Speicher- und Prozessverwaltung,
- Netzwerkkommunikation,
- Abstraktionsschicht der Hardware für Software,
- Gerätetreiber für das System.

Wie iOS weist auch Android eine mehrjährige Entwicklungsgeschichte auf, bei der neben den obligaten Bugfixes weitere Funktionen für den wachsenden Markt und in Hinsicht auf die Entwicklung von Apples iOS eingebaut wurden. In der

4. *www.openhandsetalliance.com*
5. *http://forum.xda-developers.com*

nachfolgenden Tabelle sind zur Übersicht nur die letzten Stationen der Entwicklung aufgeführt und als Bemerkungen nur einige der wesentlichen Neuerungen und Ergänzungen gegenüber den Vorversionen genannt. Für weitere Details sei auf *http://de.wikipedia.org/wiki/Android_(Betriebssystem)* verwiesen.

Version	Release Datum	Bemerkungen
2.2 »Froyo«	20.05.2010	Arbeitsspeicher >256MB, Apps können auf SD-Karten gespeichert werden.
2.3 »Gingerbread«	06.12.2010	Unterstützung von HTML5, Near Field Communication, mehr Sensorik, EXT4 Dateisystem ...
3.x »Honeycomb«	23.02.2011	Unterstützung von Tablet-Computern, volle Verschlüsselung des Systems (dm-crypt)
4.x »Ice Cream Sandwich«	19.10.2011	Entsperren per Gesichtserkennung, Zusammenführen der Entwicklungslinien 2.x, 3.x und Google TV.

Tabelle 1.3: Wesentliche Entwicklungsschritte von Google Android

Auffällig ist, dass zur Zeit gerade die älteren Android-Versionen 2.2. und 2.3. noch am häufigsten eingesetzt werden.

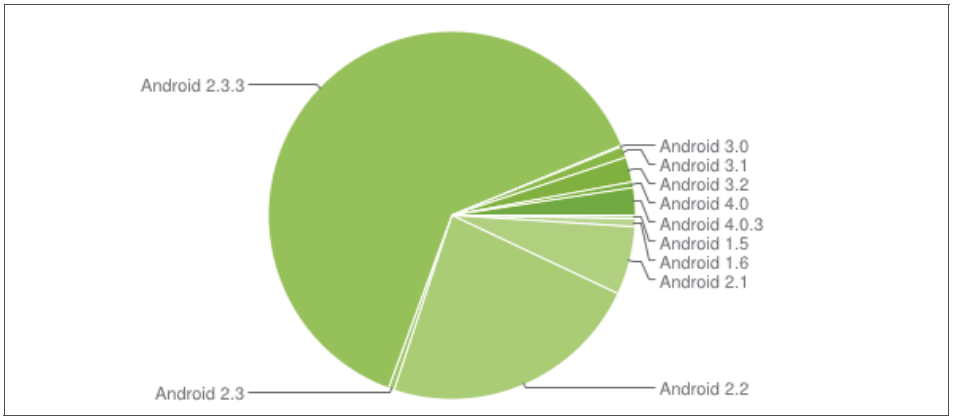

Abbildung 1.2: Verteilung der Android-Versionen nach Zugriff auf Google Play[6]

6. *http://developer.android.com/resources/dashboard/platform-versions.html*, 02.04.2012

Android dürfte heute das modernste Betriebssystem mit einem umfangreichen Rechtemodell für mobile Endgeräte sein. Problematisch für die Sicherheit sind die Apps aus diversen unsicheren Quellen; dazu später mehr in den folgenden Kapiteln.

Die Software Development Kits (SDK) sind Open Source und können für verschiedene Plattformen aus dem Internet geladen werden.

Platform	Package	Size	MD5 Checksum
Windows	android-sdk_r17-windows.zip	37417953 bytes	3af1baeb39707e54df068e939aea5a79
	installer_r17-windows.exe (Recommended)	37410775 bytes	5afaf6511ebaa52bd6d1dba4afc61e41
Mac OS X (intel)	android-sdk_r17-macosx.zip	33867836 bytes	52639aae036b7c2e47cf291696b23236
Linux (i386)	android-sdk_r17-linux.tgz	29706368 bytes	14e99dfa8eb1a8fadd2f3557322245c4

Tabelle 1.4: Android SDK[7]

Entwicklungen von Apps für Android finden überwiegend in Java statt, als Laufzeitumgebung dient »Dalviks Virtual Machine«. Bibliotheken in anderen Programmiersprachen können mit dem »Native Development Kit« (NDK) eingebunden werden. Zur Programmentwicklung werden im Internet zahlreiche Tools, Tutorials und Beispielprogramme angeboten, die eine Eigenentwicklung von Apps sehr vereinfachen. Verteilt und installiert werden Apps über das Android »Application Package File« (APK)[8] und können einfach, beispielsweise über Webportale, in den mobilen Endgeräten installiert werden.

7. *http://developer.android.com/sdk/index.html*
8. *http://www.androidguys.com/2008/10/21/market-index-getting-your-android-app-out-there/*