

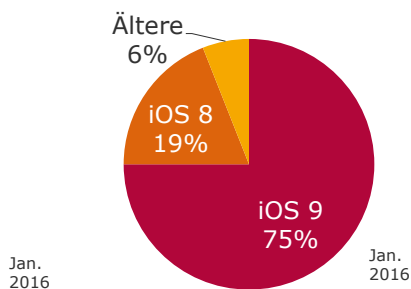


Mobile Plattformen

Mit der weiten Verbreitung der mobilen Betriebssysteme **Android** und **iOS** haben auch die entsprechenden App Stores - **Google Play Store** und **Apple's App Store** - an Bedeutung gewonnen

- Juli 2015
 - 1.600.000 Apps im Google Play Store
 - 1.500.000 Apps im Apple App Store

Android Version	Name	Anteil
2.2	Froyo	0,2%
2.3.X	Gingerbread	3,0%
4.0.X	Ice Cream Sandwich	2,7%
4.1 – 4.3	Jelly Bean	24,7%
4.4	KitKat	36,1%
5.0 – 5.1	Lollipop	32,6%
6.0	Marshmallow	0,7%



Veröffentlichung von Apps

- Entwickler muss sich beim jeweiligen Store anmelden
- Apps werden vom Entwickler elektronisch unterschrieben, um unbeabsichtigte Änderungen auszuschließen
- Store-Betreiber überprüft Apps auf bösartiges Verhalten bzw. Funktionalität

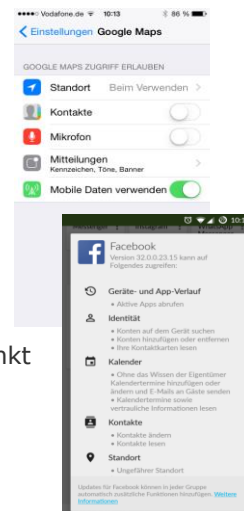
Apps werden in jeweils separaten Umgebungen ausgeführt

- Unberechtigte Zugriffe auf die Daten anderer Apps sollen dadurch unterbunden werden
- Informationsaustausch wird ermöglicht (z.B. Zugriff auf Kontakte im Adressbuch) durch definierte Schnittstellen und entsprechende Zugriffsrechte

Grundlegende Konzepte (2/2)

Berechtigungen

- Ermöglichen es dem Nutzer zu bestimmen, auf welche Informationen eine App zugreifen darf
- Häufig angefragte Berechtigungen:
 - Standort
 - Kamera
 - Adressbuch
 - ...
- Die von einer App angeforderten Berechtigungen sollten überprüft und gegebenenfalls eingeschränkt werden
 - Einige Funktionen können jedoch durch reduzierte Berechtigungen beeinträchtigt werden



- Vor allem für das Android Betriebssystem gibt es eine Vielzahl alternativer Quellen, über die Apps heruntergeladen werden können
- Um alternative App Stores nutzen zu können, muss man die Installation aus unbekannten Quellen erlauben
- Meist werden in diesen alternativen Stores keine umfangreichen Überprüfungen durchgeführt
 - Studie von F-Secure aus 2014 ergab:

Store	Malware-Anteil
Play Store	0,1%
AnZhi	3%
Baidu	3%
Mumayi	7%



Mobile Malware dient hauptsächlich zum Erbeuten von Geld

- Besonders häufig kommen folgende Methoden zum Einsatz:
 - Versand von Premium-SMS
 - Durchführen von Klickbetrug
 - Stehlen von Anmeldedaten für Online-Banking
 - ...
- Weitere Schadfunktionen:
 - Standort-Verfolgung
 - Diebstahl privater Daten und Informationen, z.B. Bilder oder Kontakte
 - Automatischer Download von weiteren Apps

Beispiele für mobile Malware: Dendroid

Dendroid ist eine Anwendung zur Fernwartung, die mit bösartige Absichten eingesetzt werden kann

- Dendroid wurde mit der Absicht entwickelt, die Sicherheitsüberprüfung des Google Play Stores zu umgehen
- Malware kann in gutartige Apps eingebettet und darüber verteilt werden
- Die App enthält folgende Funktionen:
 - Abfangen und blockieren von SMS
 - Aufnehmen von Fotos, Videos und Ton
 - Mitschneiden von Telefongesprächen
 - ...



Beispiele für mobile Malware: Brain Test

Brain Test Malware Familie wird hauptsächlich zum Erbeuten von Geld eingesetzt

- Am 29.12.2015 hat eine Antiviren Firma im Google Play Store 13 Apps identifiziert, die zur Brain Test Malware gehörten
- Die Malware kann sogar ein Zurücksetzen auf die Werkseinstellungen überstehen, was das Entfernen enorm erschwert
- Funktionalität der Malware kann von den cyberkriminellen Urhebern dynamisch erweitert werden
- Häufig kommen die folgenden Schadfunktionen zum Einsatz:
 - Einblenden von Werbung
 - Herunterladen und Bewerten von Apps aus dem Play Store
 - Stehlen von Zugangsinformationen
 - ...

Schwachstellen in Mobilien Betriebssystemen

Nicht nur Malware-Apps stellen ein Sicherheitsrisiko dar, sondern auch Schwachstellen in den mobilen Betriebssystemen

- Android wird häufig vom jeweiligen Smartphone-Hersteller angepasst, was das Aktualisieren des Betriebssystems erschwert
 - Daher erhalten die meisten Android Smartphones keine umfangreicheren Updates zur Beseitigung von Schwachstellen
- iOS läuft in der Regel nur auf Apple Geräten wie iPhone und iPad, wodurch die Entwicklung von Updates vereinfacht wird
 - Die meisten Geräte können so regelmäßige Updates erhalten, solange das Gerät noch unterstützt wird

Verbreitete Schwachstelle in Android

- Die **Stagefright** (2.0) Schwachstelle betrifft die Multimedia Player Komponente in Android
 - Missbrauch möglich über MMS Nachricht mit Video Inhalt
 - Ermöglicht die Ausführung von Schadfunktionen und die Erweiterung der Rechte
- Alle Android Versionen vor 5.1.1 sind verwundbar – ca. 1 Milliarde betroffene Geräte (Schätzung Oktober 2015)
- Schwachstelle behoben ab Android 5.1.1 und Android M (6.0) mit Sicherheits-Updates vom 01.10.2015 sowie spätere Versionen



- Schutz der Daten bei Diebstahl des Geräts
 - Verschlüsselung aktivieren
 - Verwendung einer PIN, Passwort, ... zum Entsperren
- Aktualisierung von Apps und Betriebssystem
 - Beim Kauf von Geräten auf Aktualität des Betriebssystems sowie Verfügbarkeit von Updates achten
- Installation von Apps nur aus vertrauenswürdigen Quellen
 - in der Regel sind das die offiziellen Stores
- Bei jeder App kritische Überprüfung der angeforderten Berechtigungen
 - Einschränkung von „überflüssigen“ Berechtigungen
 - Im Zweifel nach alternativen Apps suchen