Das Handy – dein unbekannter Begleiter

Inhaltsverzeichnis

Einleitung....2
Los geht's....3
Vorbemerkung zur Hardware....3
Erstes Anschalten....3
Erste „Probleme“....4
Ein Google Konto abmelden....4
Der Wechsel des Google Kontos....4
Ein Reset des Geräts....5
Weitere Probleme....5
Das Berechtigungskonzept von Android....6
Personalisierung....10
Benutzung....10
Zugriff auf Dateien....11
Verhalten einzelner Apps....12
Verhalten im W-LAN....13
Verhalten mit SIM-Karten....13
Verhalten bei der Standorterkennung (GPS)....14
Das Matrix Erlebnis....14
Datenhunger von Apps....16
Untersuchung zum Datenhunger bei verschiedenen Betriebssytemen....17
Android säubern....19
Navigation mit freier Software....20
Open Source als Strohhalm gegen das Ausgespäht-werden....21
Kommunikation nach „außen“....22
Was möchte man erreichen?....22
Verschlüsselt Mailen....22
Telefonieren über das W-LAN....24
Gibt es sichere Messenger?....25
Sicheres Surfen....26
Möglicherweise sinnvolle Apps....27
Ein Smartphone rooten....30
Überblick für Android....30
Rooten oder lieber nicht?....30
CyanogenMod-Nachfolger Lineage als Alternative....31
Wie sollte man beim Rooten vorgehen?....31
Ein iPhone rooten....33
Links....34

Copyright: © 2018, Aktion Freiheit statt Angst e.V., Berlin, www.a-fsa.de

Dr. Rainer Hammerschmidt, Vorstandsmitglied
MA Beate Baum, Wissenschaftliche Fachberatung

Einleitung

Es geht bei dieser Veröffentlichung darum über Probleme und Gefahren zu informieren, die sich nach dem Kauf eines Smartphones „von selbst einstellen“. Wir wollen Tipps geben, wie man den größten Teil des Frusts vermeiden kann. Es wird leider nicht ohne Frust ablaufen ...

Das ist die Zusammenfassung einer zweiteiligen Vortragsveranstaltung im Antikriegscafé COOP von **Aktion Freiheit statt Angst** aus dem Frühjahr und Herbst 2017.

Wir dokumentieren hier die Inhalte eines Vortrags "**Ich und mein Handy**" und der Diskussion der **Anonym-Mäuse** im 2. Teil der Sendereihe.

Beide Teile wurden von **Uniwut Freies Fernsehen** mitgeschnitten und stehen nach der Ausstrahlung durch Alex-TV, den Offenen Kanal Berlin, auch zum Download in unserer Mediathek und auf unserem Youtube-Kanal zur Verfügung.

Die Links sind

- "**Ich und mein Handy**" https://youtu.be/q3xZiZgwb_0
- "**Die Anonym-Mäuse sichern ihre Smartphones**" https://youtu.be/r8V4XX415iA

Zum Nachlesen sind die beiden Teile dieser Vortragsreihe "**Ich und mein Handy**" und der zweite Teil "**Die Anonym-Mäuse sichern ihre Smartphones**" unter www.a-fsa.de/d/2T1 in unserem Web aufzurufen.

Die Inhalte gliedern sich wie folgt:

- 1. Teil:
  - Was ist nach der Inbetriebnahme auf einem Handy drauf?
  - Was geht alles nicht
  - Was ist gut, was schlecht,
  - Gefahren eines Backup in der Cloud
  - Anmeldezwang bei Google,
  - Nervendes Verlangen nach Datenfreigaben;
  - Telefonieren über VoIP
  - Navigation mit OSMand
- 2. Teil:
  - Welche Apps sind sinnvoll, was kann weg?
  - Mail auf dem Handy
  - Verschlüsselt Mailen
  - Sicherer surfen ohne Google
  - Sicher surfen mit Tor, Orbot, OrFox und OrWeb
  - Der Kunde zahlt für seine eigene Überwachung

Los geht's

Vorbemerkung zur Hardware

Während es bei Geräten mit dem Apple Betriebssystem IOS nur einen Hersteller, nämlich die Firma Apple, gibt, ist bei Android und Windows-Phone Betriebssystem verschieden, was auf welchem Gerät wie funktioniert. Diese Vielfalt konnten wir nicht untersuchen. Wir haben mit folgenden Geräten gearbeitet:

- Handy/Tablet Archos mit Android 5.1 Lollipop, 4G LTE, Quad Core 1GHz, IPS 7“, Bluetooth, GPS, WiFi, Kamera 3MPx, DualSIM, MicroSD, GooglePlay , Display 1600x600
- Handy/Tablet Odys, mit Android 6, Marshmallow, 4000mAh Akku, Laufzeit 4h, 2 SIM, 1 MicroSD, GPS, 2Mpx Kamera, 300MB von 4GB internem Speicher belegt
- Huawei Smartphone Y100, mit Android 4.x
- Samsung Tablet mit Android 6, Marshmallow

Erstes Anschalten

Erste Warnung: Es wird keine SIM Karte gefunden. Ein WLAN wird nicht gesehen.

Zumindest ist es schon mal klar, dass das Gerät auch ohne SIM Karte starten und funktionieren kann! Als Netzverbindung wird ein WLAN angemeldet.

Wunsch des startenden Android:

Als erstes bietet der PlayStore nach Google Anmeldedaten und bietet einem Gutscheincode für bis zu 90% Rabatt. „Akzeptieren“ ist erlaubt, das Feld „Weiter“ bleibt dagegen grau, nur die „Zurück“-Taste hilft daran vorbei.

Danach wird man 3x gefragt nach Kontodaten PayPal, Visa und von allein öffnet sich ein H5-GameCenter, obwohl diese App in der Liste der Apps auch unter „alle“ nicht sichtbar war.

Direkt nach dem Einschalten unseres Androiden werden wir aufgefordert einen Google-Account anzulegen oder den bereits bestehenden mit dem Gerät zu verknüpfen. Wir werden in die Cloud gedrängt und sollen uns keine Sorgen um unsere Daten machen, sondern vielmehr den Anbietern voll vertrauen.

Beim ersten Start möchte das System zusätzlich ca. 6 Apps installieren, „für die Google aber keine Verantwortung hat“. Es handelt sich wohl um Spiele.

Beim Start fast jeder der vorinstallierten Apps wird nach einem Google Konto gefragt (z.B. Telefonkontakte, Google Maps, Mail, Play Store …). Apps wollen den Standort, über Funkmasten oder GPS ermittelt, ohne Begründung oder erkennbaren Nutzen an ihre Hersteller weitergeben.

Es folgt das Angebot künftig alle Daten in der Cloud zu sichern und ein Angebot für ein ständiges Backup (irgendwo im Netz).

Die installierte Wetter App, aktualisiert von allein, macht also push statt pull, dabei kann/wird sie Zugriff auf die bei der Installation verlangten Daten haben.

Nach Installation der App zip2go geht der Dateimanager nicht mehr und liefert die Meldung „Die Netzwerkfreigabe ist nicht geladen“. Abhilfe schafft nur ein neuer Dateimanager.

Eines der oben angegebenen Geräte war bereits in Gebrauch. Dort bemerkten wir: Nach Erwerb eines gebrauchten Geräts muss über Einstellungen/Sichern/Zurücksetzen ein Reset ausgeführt werden. Das soll angeblich alle alten persönlichen Daten löschen. Das Widget Fotos sieht trotzdem noch alte Fotos (thumbnails), der Dateimanager jedoch nicht. Diese Thumbnails liegen scheinbar im Ordner Android/data/com.android.gallery3d/cache/ der beim Reset „übersehen“ wurde.

Erste „Probleme“

- Die als Probeversion installierte Apps, die die Nutzung von MS Office Dateien erlauben soll funktionieren nicht ohne Netz.
- Die für Word Dateien zuständige App kann keine Open Office .odt Datei öffnen.
- Eine .odp Präsentation wird von der App Google Präsentation nicht geöffnet.
- Eine .ods Tabelle wird von der App Sheets nicht geöffnet.
- Es fehlen wichtige Apps wie ein Terminal, ein Texteditor, … Selbst die App „Notizen“ will eine Google Anmeldung – wozu?.
- Die App Google Foto möchte ein Google Konto, geht aber dann auch ohne Anmeldung.
- Apps installieren geht nur über den Google PlayStore mit einem Google Konto.

Um diesem Desaster zu entkommen holen wir uns die **App F-Droid,** einen **freien Android App Store** als .apk Datei und installieren sie.

Das Deinstallieren des Google Play Store geht, wie viele andere Google Apps nicht. Es bleibt die Möglichkeit diese zu deaktivieren aber nicht sie zu löschen.

Ein Google Konto abmelden

Hat man doch mal den Fehler gemacht und hat sich ein Google Konto angelegt, z.B. um über den Play Store Apps zu installieren oder weil man Google Maps oder Mail genutzt hat, so muss man (verrückterweise) so vorgehen:

Man meldet sich bei GMail an und wählt unter Kontoeinstellungen „Konto löschen“. Man erhält die Meldung „Adresse kann künftig nicht mehr von Ihnen oder von einer anderen Person verwendet werden“. Dann wählt man bei Einstellungen, „Konto löschen“, „gesamtes Konto löschen“ und muss sich dann nochmal anmelden und wählt nun endgültig „Konto löschen“. Erklärt wird dies unter https://support.google.com/accounts/answer/61177?hl=de

Der Wechsel des Google Kontos

Wenn man nach dem Abmelden des Google Konto und dem Abschalten beziehungsweise Deaktivieren aller von Google vermuteten Anwendungen zu der Notwendigkeit gelangt, dass man aus irgendeinem Grund einen erneuten Zugriff auf den Google Play Store benötigt, so wird man mit folgenden Problemen konfrontiert:

Wie von Google beim „Konto löschen“ vorgewarnt, benötigt man einen neuen Google Account. Zur Anmeldung bei Google muss man also einen neuen Benutzer generieren. Die Anmeldung auf dem Smartphone war mit den bereits eingangs beschriebenen und abzulehnenden Aufforderungen zu PayPal Registrierungen für den PlayStore möglich. Als Folge ergab sich jedoch nach der

Anmeldung, dass man auf dem Gerät ein neuer Nutzer ist und das Schreiben oder sogar Lesen von eigenen Dateien in bestimmten Ordnern (des ehemaligen Nutzers) nicht mehr möglich war.

So konnten Dateien die früher von Twitter oder dem Privacy Browser heruntergeladen worden waren, plötzlich nicht mehr gelesen oder gelöscht werden.

Die eigene Kontaktliste war leer und grau, das heißt, es ließen sich keine Kontakte mehr eintragen. Erst das Löschen beziehungsweise deaktivieren der Google Kontakte App und das Ersetzen durch eine andere Kontakte App ermöglicht es wieder Kontakte anzulegen.

Und zu allem Ärger noch das: Wenige Monate nach dem Anlegen des neuen Google Kontos kommt von Google die Anfrage, dass man eine zweite E-Mail-Adresse eingeben möchte, um seine Identität zu bestätigen. Im anderen Fall wäre es nicht möglich weitere Updates zu erhalten.

Ein Reset des Geräts

Für ein Reset, also eine komplette Neuinstallation, des Geräts kann schnell mal notwendig werden. Wir hatten den Fall bereits beim Erwerb eines gebrauchten Gerätes. Ein anderer „Fall“ ließ nicht lange auf sich warten: Um den Zwang zu Google-Anmeldungen los zu werden haben wir nacheinander die Apps von Google „deaktiviert“ (löschen geht nicht s.o.). Allerdings ist die „Google App“ ein zentraler Baustein von Android. Nach ihrer Deaktivierung geht nichts mehr.

Die Taste zum Anschalten tut nichts, keine Reaktion alles bleibt schwarz, evtl. hat man noch ein kurzes Aufblitzen und dann den wiederholten ergebnislosen Versuch eines Neustarts.

Bei Geräten, wo sich der Akku nicht entnehmen lässt hilft nur ein Reset mit einer Büroklammer. Allerdings geht ein Reset nicht im ausgeschalteten Zustand und das Anschalten auch nicht.

Für ein Reset muss man so vorgehen - und alles ist wieder wie beim Auspacken:

Für ein Reset mit Büroklammer oder Stecknadel und gleichzeitig die „leiser“- und die „an/aus“-Taste drücken braucht man Geschick oder 3 Hände. Es erscheint:

- Android Recovery und die Auswahl:
    - Reboot system now
    - Reboot to bootloader reboot
    - Apply update vom ADB
    - Apply update from SD card
    - Wipe data/factory reset Formatting /data
    - Wipe cache partition
    - Mount /system Suported API: 3
    - View recovery log alte Logs
    - Power off

Mit „Wipe data/factory reset“ erhält man nach einigen Minuten ein neu installiertes Gerät.

Weitere Probleme

Wenn man eine SD Karte im Gerät einlegt, wird diese entweder als „zusätzliches Speichermedium“ erkannt oder dem „internen Speicher hinzugefügt“. In der Auswahl zwei ist das Medium nicht mehr als externer Speicher an anderen Geräten nutzbar. Bleibt die SD ein „zusätzliches Speichermedium“ so kann sie an anderen Geräten genutzt und mit Daten versehen

werden. Diese Dateien sind jedoch nicht von allen Apps nutzbar (s. Berechtigungskonzept).

Lässt man die SD Karte als externen Speicher, so wird man beim Start des Gerätes (Odys Tablet) wiederholt bis zu fünfmal gefragt, ob man die SD Karte als externen oder internen Speicher verwenden möchte. Diese Frage erscheint unsinnigerweise auch mehrmals wieder nach dem man sich für die externe Anwendung entschieden hat.

Diese Frage erscheint auch noch nach Tagen unter den offenen Tasks, wenn man auf dieses Feld geht. Beim Antippen wird man wieder gefragt ob man die Karte als intern formatieren möchte.

Ein völlig anderes Verhalten beobachten wir bei einem Samsung Tablet mit gleichem Betriebssystem (Marshmallow 6). Dort lässt sich eine SD Karte überhaupt nicht als „intern“ formatieren. Damit sind „allgemeine Ratschläge“ für ein Betriebssystem eigentlich nicht möglich, die Gerätehersteller entscheiden scheinbar im Endeffekt welches Verhalten von ihnen bevorzugt wird. Ein App Programmierer bestätigt uns, dass im Endergebnis das Verhalten von Gerät zu Gerät verschieden sein kann.

Wird das Gerät per USB an einen PC angeschlossen, so wird es dort gemounted über das mtp-Protokoll, z.B.: mtp://[usb:001,045]/Interner%20Speicher. Mit einem Dateimanager der dieses Protokoll beherrscht lassen sich einige Dateien kopieren, einige Verzeichnisse insbesondere vom internen Speicher werden jedoch nicht angezeigt. Ein Nutzung über ein Terminal mit den Befehlen ls, ssh, rsync, … sind leider nicht nutzbar.

Zu sehen ist auch nur der Userspace auf dem Gerät. Man hat für die anderen Ordner keine (root) Rechte. Die erlaubten Verzeichnisse werden nach dem USB (Kabel-) Anschluss erst angezeigt, wenn man sich auf dem Android-Gerät auch angemeldet hat (kein Zugriff ohne Anmeldung).

Ein großes (unerklärliches) Manko ist die mangelhafte Übertragungsgeschwindigkeit zum Android Gerät. Die Datenrate bei vielen Dateien ging „manchmal“ auf 80kB/s. Die SD-Karte kann mit 3,6MB/s schreiben (wer drosselt und warum?).

Die Rechteverwaltung von Android verhindert manchmal auch das Umbenennen von Ordnern, die über USB angelegt wurden (Warum?)

Hinzu kommt, dass manche Android Installationen von Hause aus keinen Dateimanager mitbringen. Der Nutzer soll **nur** über die installierten Apps Zugriff auf seine**(!)** Daten haben.

Das Berechtigungskonzept von Android

Obwohl Dateien über eine Kabelverbindung von einem PC auf das Smartphone übertragen (und nicht mittels der SD „untergeschoben“) wurden, gibt es für einige/alle(?) Apps keine Schreib- und für einige auch keine Lese-Berechtigung dieser Daten. Da die SD Karte ein FAT32 Dateisystem enthält, welches keine Rechteverwaltung kennt, muss Android das simulieren – aber nach welchen Regeln?

Standardmäßig werden alle Android-Apps in einer „Sandbox“ ausgeführt - einem isolierten Bereich. Wenn sie auf Daten außerhalb dieses „Sandkasten“ zugreifen, diese bearbeiten oder löschen wollen, muss das Systems dies gestatten.

Bereits mit Android 4.4 wurde der Verwendung von SD Karten als (externe) Speicher wegen der Möglichkeit des Einschleppen von Malware ein Riegel vorgeschoben. In den folgenden Versionen gab es wieder einige kleine Verbesserungen. Es bleibt jedoch bei der Einteilung der

Berechtigungen für Apps in die „normalen“ und die „gefährlichen“.

„Normale“ Berechtigungen werden standardmäßig vergeben und benötigen keine Zustimmung des Users, das sind der Zugriff aufs Internet, die Icon-Erstellung, Bluetooth-Verbindung und ?(welche noch)?.

Um einer App eine der „gefährlichen“ Berechtigungen zu geben braucht es eine Bestätigung durch den Nutzer. Es gibt in der „gefährlichen“ Kategorie neun Berechtigungsgruppen. Erhält eine App den Zugriff auf eine Gruppe, so sind automatisch alle Berechtigungen der gleichen Gruppe gestattet, ohne dass eine zusätzliche Bestätigung notwendig wäre.

Eine App, die z. B. die Berechtigung zum Lesen von SMS erhält, darf auch SMS verschicken, MMS-Nachrichten lesen und andere Aktionen dieser Gruppe durchführen.

Die Berechtigungsgruppen in Android

Gruppe	Erlaubt	Kommando	Gefahr
Kalender	Im Kalender gespeicherte Ereignisse lesen, ändern, löschen, neue hinzufügen	READ_CALENDAR WRITE_CALENDAR	Tagesplanung weitersagen; Termine löschen oder ändern
Kamera	Kann Fotos und Videos aufnehmen	CAMERA	Heimlich Videos oder Fotos aufnehmen
Kontakte	Kontakte lesen, bearbeiten oder neue hinzufügen; Nutzer Accounts auslesen	READ_CONTACTS WRITE_CONTACTS GET_ACCOUNTS	Adressbuch für Spam verwenden und verändern Accounts in sozialen Netzwerken nutzen
Standort	Den ungefähren (Mobilfunkmasten) und den genauen (GPS-Position) Standort abfragen	ACCESS_COARSE_LOCATION ACCESS_FINE_LOCATION	Verfolgen aller Bewegungen des Nutzers Einbrechern die Abwesenheit zu Hause mitteilen
Mikrofon	Audiodateien mit dem Mikrofon aufnehmen	RECORD_AUDIO	Mitschneiden aller Unterhaltungen und Geräusche
Telefon	Die Telefonnummer, IMEI u.a. Daten auslesen Anrufe machen Anruflisten lesen und ändern Mailbox hinzufügen VoIP nutzen Anrufberechtigung	READ_PHONE_STATE CALL_PHONE READ_CALL_LOG WRITE_CALL_LOG ADD_VOICEMAIL USE_SIP PROCESS_OUTGO	Das Telefon gehört damit dieser App. Es können beliebig Kosten erzeugt werden.

	en sehen und ändern	ING_CALLS	
Bodysensoren	Zugriff auf Gesundheitsdaten	BODY_SENSORS	Die App erhält Zugriff auf alle Sensoren, die mit dem Gerät verbunden sind oder waren.
SMS	Lesen, senden und verwalten SMS, MMS und Push-Nachrichten	SEND_SMS READ_SMS RECEIVE_SMS RECEIVE_WAP_PUSH RECEIVE_MMS	Die eigenen Nachrichten und die von Partnern sind einsehbar und veränderbar. Es können beliebig Kosten erzeugt werden.
Speicher	SD Karten und andere Speicher lesen, verändern und löschen	READ_EXTERNAL_STORAGE WRITE_EXTERNAL_STORAGE	Die App kann alle auf dem Gerät gespeicherten Dateien lesen, ändern oder löschen.

Damit wird klar, welche Gefahren solche Berechtigungen beinhalten können. Gut, dass man sie (theoretisch) jeder App einzeln geben und entziehen kann. Wie das praktisch gehen soll steht hier https://www.androidauthority.com/android-app-permissions-explained-642452/
für Entwickler der Apps und hier
https://www.androidauthority.com/app-permissions-886758/
für die Nutzer. Und da folgt auch sofort die Einschränkung: *Older apps that haven't been updated might crash or fail to work correctly if you deny some permissions.*

Wenn man also bei der Installation nach den gefragt wird, kann ein Abschalten der „Wünsche“ die App auch lahmlegen. Theoretisch kann man jeder App auch später Berechtigungen entziehen über „Einstellungen/Apps/Optionen/Berechtigungen“, allerdings nicht in der oben angegebenen Freiheit.

Nachtrag: *Na ja, was sie scheinbar auch dann nicht (sofort) tut, wenn man den Speicher der SD Karte zum Internen macht.*

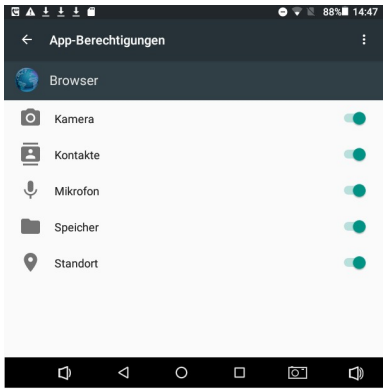
Auch wenn es eigentlich nicht gewollt war, wurde die SD Karte schließlich zum internen Speicher transformiert, um den Browser dazu zu bekommen, die dort liegenden HTML Dateien anzuzeigen. Damit wurde in Kauf genommen, dass die mehreren Gigabyte an Daten über das Netzwerk oder die ebenfalls (seltsamerweise) langsame USB-Kabelverbindung übertragen werden mussten.

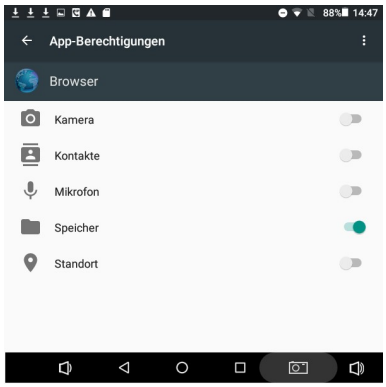
Nun hätte der Browser seine Berechtigung „Speicher“ voll ausleben können. Es zeigte sich jedoch das folgende völlig unlogische Verhalten:

- beim Antippen eines Links zu einer intern gespeicherten HTML Datei wurde ein Tab geöffnet und der Fortschrittsbalken erreichte 60-80% und verblieb dort ohne Anzeigen irgendwelcher Daten,
- beim Festhalten (drauftippen und warten) eines Links wurde die Auswahl „Öffnen“ und „Öffnen in einem neuen Tab“ angeboten, beide Möglichkeiten führten zur Anzeige der Datei ohne Fehler.

Welche Absichten mag der Programmierer damit verfolgt haben?

Nun zurück zu den Berechtigungseinstellungen, im folgenden Beispiel wollten wir der Google-App „Browser“ ganz normale Berechtigungen zum Lesen der SD Karte geben, damit sie lokale Bilder und Webseiten aus dem lokalen Speicher anzeigen kann (was sie von zu Hause aus nicht tut) – *eigentlich das normalste und ungefährlichste der Welt.*





Vorher: Der Browser hat **alle** Berechtigungen „von Hause aus“ mitgebracht, die wir ihr schnellstens abschalten.

Nachher: Nur der Zugriff auf den Speicher ist eigentlich gewollt, lässt sich aber nicht explizit auf die SD Karte erweitern.

Für die praktische Verwendung heißt das, dass dem Nutzer keine Möglichkeit gegeben wird, sich die Berechtigungen auszuwählen, die seiner bevorzugten Verwendung entsprechen. Das ist kein Fehler des Berechtigungskonzepts sondern seiner Umsetzung durch die Programmierer der Apps. Die wirklich vorhandenen Berechtigungen sind durch fehlende Schalter unter Einstellungen/Apps erstens nicht sichtbar und die gewünschten Berechtigungen sind damit auch nicht auswählbar.

Bei der Verwendung von **SD Karten**, insbesondere als interner Speicher, sollte man außerdem beachten, dass diese die Leistung des Geräts bremsen können, wenn sie von Apps häufig genutzt werden.

Zu viele Schreibvorgänge können auch ihre Lebensdauer verkürzen. Zugriffe mit 10MB/s sollten die Karten schon verkraften können.

Typ	**Leistung**
Class 2	2 Mbyte/s
Class 4	4 Mbyte/s
Class 6	6 Mbyte/s
Class 10	10 Mbyte/s
UHS Class 1	10 Mbyte/s
UHS Class 3	30 Mbyte/s

Personalisierung

Vom ersten Start an wird man gedrängt alle seine Daten zur Verfügung zu stellen:

- Ein bereits bestehendes Google Konto soll mit der Handynummer und/oder einer „Ersatzmailadresse“ verifiziert werden.
- Die Einstellung „Standortdaten verwenden“ ist scheinbar nicht ausschaltbar.
- Verwendete Apps, Passwörter, Werbung, der Webseiten-Verlauf und die benutzten Geräte sollen zur „Optimierung“ gespeichert werden.
- In den „Google Einstellungen“ lässt sich wenigstens der Kontakt zu „Nearby Geräten“ ausschalteten.
- In den „Google Einstellungen“ steht auch eine persönliche Google Werbe ID, die das Gerät einfach ohne Nachfrage erzeugt hat.
- Einstellungen sollen „diensteübergreifend“ gespeichert werden.
- „Smart Lock“ speichert alle Passwörter in der Cloud bei Google. Dies lässt sich ausschalten.
- Die Speicherung des Web-Verlaufs im Google Browser ist scheinbar nicht ausschaltbar.
- Die persönliche Kontaktliste enthält (ohne einen eigenen Eintrag) ca. 30 unerwünschte Einträge mit 90% Werbung (von ADAC über Lidl, Taxiruf, …).
- Die App Google Maps möchte Standortdaten speichern „zur Optimierung“. Dies scheint nicht ausschaltbar zu sein.
- Die Lizenz von Google Maps verbietet die Nutzung der Daten, Karten, Skripte für eigene Zwecke.
- Sich nur aus dem Google Account auszuloggen geht nicht, nur ein Löschen ist auf dem oben beschriebenen komplizierten Weg möglich.

Installiert man erstmals eine App aus einer anderen Quelle als dem Google PlayStore, so erhält man zuerst eine Warnung, das ist noch ok, dann möchte Google diese App regelmäßig überprüfen. Das erlaubt sich Google selbst, ein „Nein“ wird nicht akzeptiert.

Benutzung

An eine Handy-Benutzung muss man sich erst gewöhnen. Kenntnisse im Umgang mit Laptops nützen wenig, da keine Maus vorhanden ist. Die Wisch- und Tast-Funktionen sind im Manual erklärt und müssen geübt werden.

Beim „Fotos machen“ kommt es oft zur Auslösung von vielen mehrfachen Fotos oder es passiert nichts.

Auch das Kopieren von Text will gelernt sein - die Beschreibung erklärt: Zunächst tippen Sie ähnlich eines Doppelklicks zwei Mal auf eines der zu markierenden Worte, bis dieses farbig hinterlegt ist. Am Anfang und am Ende des Wortes erscheinen nun zwei Cursor. Indem Sie den ersteren nach links an den Beginn der zu kopierenden Textstelle ziehen und den zweiten Cursor ans Ende des zu kopierenden Textes legen, werden die darin eingeschlossenen Worte markiert und so zum Kopieren bereit gemacht.

Der Kopiervorgang wird fortgeführt, indem Sie auf die Schaltfläche "Kopieren" in dem sich neu öffnenden Kästchen drücken.

Um den kopierten Text an anderer Stelle wieder einzufügen müssen Sie zu der Stelle wechseln, in die der kopierte Text eingefügt werden soll. Sie können auch eine andere App öffnen. Wenn Sie die gewünschte Stelle bzw. das entsprechende Textfenster gefunden haben, tippen Sie einmal lange auf den Screen. Nun öffnet sich erneut ein kleines Kästchen, in dem Sie den Button "Einfügen" auswählen, um den Kopier- und Einfüge-Vorgang abzuschließen.

Leicht gesagt, vor allem das „Cursor zur kopierenden Textstelle ziehen“ ist eine taktile Meisterleistung für das ein Finger geboren sein muss.

Einen Screenshot erzeugt man durch „gleichzeitiges Drücken des Leiser Button und Power Button für einige Sekunden“. Die Bilder liegen nach vielen vergeblichen Versuchen im Ordner Screenshots.

Zugriff auf Dateien

Im Gegensatz zu Android 4 sind die Zugriffsberechtigungen in Android 5 oder 6 wesentlich restriktiver. So ist das Kopieren von Dateien aus dem internen Speicher auf eine SD Karte, die nicht als interner Speicher formatiert ist, vielfach nicht möglich. Das Problem sind fehlende Schreibrechte für die Apps auf SD Karten seit Android 4.4

Google möchte, dass wir statt der externen Speicherkarten den hauseigenen Cloud-Speicher und das Cloud-Backup nutzen. Auch Musik solle heute vor allem gestreamt werden. Hier wird wieder deutlich, dass man hinter unserem Geld her ist, denn solche Dienste können schnell kostenpflichtig werden oder sind es bereits.

Die Aussage von Google zu dem Problem: "Apps dürfen niemals auf sekundäre Datenträger schreiben. Diese Beschränkung sorgt dafür, dass Android das System korrekt bereinigen kann, wenn Anwendungen deinstalliert werden." - Nein danke, meine SD Karte kann ich selber löschen.

Die seit Android 4.4. eingeführten Änderungen sind für die Besitzer von Smartphones äußerst ärgerlich, denn viele Nutzungsszenarien sind jetzt nicht mehr möglich:

- Dokumente mit einem Cloud-Dienst synchronisieren und dann mit anderen Apps weiter bearbeiten? Geht nicht.
- Dokumente auf der Speicherkarte sowohl am Tablet als auch am Notebook bearbeiten? Kaum mehr möglich.
- Auch Backups von Apps lassen sich jetzt nicht mehr ohne weiteres auf der Speicherkarte ablegen.

Als einzige Lösungen bieten sich an das Gerät zu „rooten“ oder die App SDfix im Google Store, solange es sie noch gibt.

Der Wahnsinn ist, dass die Maßnahme, die angeblich die Sicherheit erhöhen soll, die Sicherheit und den Komfort des Anwenders massiv reduziert.

Die App-Berechtigungen unter Android 6.0 (Marshmallow) sind in engen Grenzen konfigurierbar. Dazu muss man in der App „Einstellungen“ das Menü „Apps“ und darin das Menü „App-Berechtigungen“ auswählen.

Unter den folgenden Links ist beschrieben

- wie man externe Speicher im „mixed_mode“ betreiben kann: https://www.android-user.de/mixed-mode-microsd-karte-unter-android-marshmallow-als-internen-und-externen-speicher-nutzen/
- oder verschlüsselte SD-Karten (als interner Speicher) entschlüsselt: http://nelenkov.blogspot.de/2015/06/decrypting-android-m-adopted-storage.html

Spätestens wenn man versucht die App-Systemeinstellungen zu ändern unter „Einstellungen“ Menü „Apps“ und im Menü „Systemeinstellungen ändern“ feststellt, dass sich nichts ändern lässt, kommt man wieder auf das „rooten“ zurück.

Verhalten einzelner Apps

- Bilder können von der App Foto oder der App Galerie geöffnet werden. ok
- Lokale html Dateien werden vom HTML-Viewer nicht geöffnet: ERR_AcessDenied
  der Google Browser kann auf diese Dateien zugreifen. Nicht ok
- OSM Dateien mit Landkarten für OSMand können wegen des gesperrten Zugriffs auf die SD Karte nur im internen Speicher abgelegt werden

Diese ärgerlichen „Sicherheits-Features“ werden durch die „willkürliche“ Speicherverwaltung in Android erzeugt. Als User wird bei selbst auf die SD Karte kopierten Dateien root:everybody eingetragen. Dateien haben im internen Speicher die Rechte rwxr--r-- , auf der SD Karte rwxrwx--- , so dass die Apps auf diese nicht zugreifen können.

Eine SD Karte als zusätzlicher Speicher wird unter external_sd eingehängt und vom Betriebssystem nicht verändert sondern nur (anders als erwartet) mit besonderen (Nicht-) Rechten eingehängt.

```
/
    - emulated/         interner Speicher
        - 0/            hier hat niemand (außer root) Zugriff
                …       interner Dateibaum mit Rechten 744 (rwxr--r--)
    - external_sd/      SD Karte
        …               Dateibaum der SD Karte mit Rechten 770 (rwxrwx---)
```

Da die SD Karte immer noch mit FAT32 formatiert ist und dieses Format keine Unix-Besitzerrechteverwaltung kennt, haben wir es mit einem willkürlichen „Sicherheitsfeature“ von Android zu tun.

Zu dem Punkt Zugriffsrechte sei noch erwähnt, dass eine SD Karte, die als Erweiterung zum internen Speicher hinzugefügt wurde, verschlüsselt wird und nicht an anderen Geräten lesbar ist (/dev/mmcblk0). Am Ende des vorigen Kapitels wurde ein Link zu einem Hack dieser Verschlüsselung angegeben.

Verhalten im W-LAN

Das W-LAN wird unter „Einstellungen“ , „W-LAN“ konfiguriert. Sichtbare W-LANs werden angezeigt und können verbunden werden. Bekannte W-LANs werden ohne Ankündigung verbunden, sobald sie verfügbar sind. Das gilt z.B. auch für unverschlüsselte Netze wie freifunk.net auf der Straße.

Die Netzverbindungen können am komfortabelsten mit der Funktion „Flugmodus“ abgeschaltet werden.

Bei allen verwendeten Apps ist zu prüfen ob sie eine Verfügbarkeit von „Netzen“ sofort zur Kommunikation ausnutzen. Die App K9-Mail bietet unter „Einstellungen“ / „Aktionen“ / „automatisch synchronisieren“ die Möglichkeiten an: „immer“, „im W-LAN“, „nie“. „Immer“ kann teuer werden!

Die Twitter-App bietet unter Einstellungen zum Bandbreite sparen nur an: „keine Bilder in Timeline“ und „keine Videos automatisch abspielen“, die Kommunikation selbst läuft jedoch immer.

Verhalten mit SIM-Karten

In den verwendeten Geräten konnten 2 SIM Karten genutzt werden. Beim Anschalten wird jeweils die PIN für die SIM Karte(n) abgefragt, erst danach das Geräte-Passwort. Es kann in den „Einstellugngen“ unter „SIM Karte“ ausgewählt werden welche, bzw. ob man die Karte für Gespräche und SMS nutzen möchte. Leider kann man einer Datennutzung nur generell zustimmen ohne dies auf einzelne Apps zu beschränken.

Gefahren:

- Es gibt Telefon-Anbieter, die ohne zu fragen Datenverbindungen zulassen und berechnen, obwohl die Karten (zu Urzeiten) nur zum Telefonieren gekauft wurden. Dort können erhebliche Kosten entstehen, z.B. bei Fonic 24ct/MB.
- Bei einer Prepaid Karte kann man beim Provider online ein Lastschrift Konto anlegen. Dabei muss man nur eine (irgendwoher bekannte) gültige IBAN und BIC hinterlegen und kann dann sofort (max) 25€ aufladen lassen und diese verbrauchen. Dazu wird keine PIN und TAN benötigt. Eine Sperre erfolgt erst nach der zu erwartenden Rücklastschrift.
- Immer wieder verlangen Apps bei der Registrierung die eigene Telefonnummer als Identifier. Dies gilt es zu verhindern, da jegliche Anonymität dahin ist und der Wechsel der Telefonnummer erschwert wird. Am besten (mindestens bei diesen Aktionen) keine SIM Karte einlegen.
- Grundsätzlich beruht die Verschlüsselung bei Handygesprächen noch immer auf den von US Geheimdiensten bei der NIST 2005 standardisierten „fehlerhaften“ Elliptic Curve Zufalllszahlengenerator, der in Sekunden zu knacken ist – also praktisch telefoniert man mit dem Handy unverschlüsselt. https://www.aktion-freiheitstattangst.org/de/articles/403-20170411-ueberwachung-durch-unternehmen.htm

Die meisten Provider bieten nach Verbrauch des Datenkontingents für die Laufzeit (z.B. 30 Tage) Verbindungen mit 64kb/s. Diese Beschränkung stellt sich erst mit der Zeit ein, d.h. es ist möglich zu Beginn der Nutzung noch Downloads mit 1 MB/s zu bekommen.

Verhalten bei der Standorterkennung (GPS)

Einen „GPS an/aus Schalter“ gibt es nicht. Auch im Flugmodus ist der Empfang von GPS Signalen möglich. Unter „Einstellungen“/“Standort“ sind Apps gelistet, die auf GPS zugreifen. Ob dies wirklich alle sind, ist nicht bekannt.

Google verlangt penetrant, dass man zustimmt, dass zur „Genauigkeitserhöhung“ GPS Daten „anonym“ an Google übertragen werden. Ob diese „Genauigkeitserhöhung“ wirklich ohne einen Bezug zu unserem Gerät mit den Mobilfunk-Antennenkoordinaten abgeglichen werden, die ja wieder unsere IMEI (die Geräte-ID) enthalten ist ebenfalls fraglich.

Google Maps ist Google, also muss im ersten Schritt die Google Maps App deaktiviert werden und durch eine Open Source Anwendung wie Navit oder OSMand ersetzt werden. OSMand kann auf lokal gespeicherten Karten des Open Street Map Projekts arbeiten, so dass überhaupt keine Netzverbindung zur Navigation notwendig ist.

Das Matrix Erlebnis

Betrachten wir die folgende wirklich erlebte Geschichte als (Anti-) Werbe-Einblendung.

1. Das Geschehen

Auf einem Smartphone mit Google Anmeldung und PlayStore ohne SIM-Karte wird die App OSMand zur Navigation verwendet. Zur Absicherung gegen Stromausfall wird ein PowerPack verwendet. Bei der Wanderung in der Nähe eines großen Campingplatzes, der eventuell ein freies WLAN anbietet, wurde bemerkt, dass sich das Gerät abgeschaltet hat.

Nach einem Neustart „mitten in der Natur“ befindet sich das Gerät im Auslieferungszustand. Sämtliche selbst installierten Programme sind verschwunden, dafür sind viele Anwendungen installiert die zum einen von Google sind, zum anderen Anwendungen von Microsoft wie zum Beispiel das Officepaket als Testversion.

Alle eigenen Daten auf dem Gerät sind verschwunden.

OSMand oder ein anderes offline arbeitendes Navigations-Programm sind nicht mehr vorhanden. Das Gerät wird ausgeschaltet. Die weitere Wanderung findet ohne elektronische Hilfsmittel statt - aber die Wanderer überleben. ;-)

Nach dem Start des Gerätes am nächsten Tag ist plötzlich alles wieder in Ordnung. Das Gerät befindet sich in dem Zustand wie zum Beginn der Wanderung am Vortag. Der einzige Unterschied zu dem alten Zustand war, dass der Name der SD Karte durch Zeichensalat ersetzt worden war. Zugriffe waren jedoch weiterhin normal möglich. Das Ändern/Umbenennen, der SD Karte war jedoch nicht möglich. Dieser Zeichensalat lässt sich nur durch eine Neu-Formatierung der SD Karte beheben.

2. Die Möglichkeiten

A.) ein fremder Zugriff über ein freies WLAN
B.) ein elektrischer Schlag durch das Verbinden mit dem PowerPack

Der erste Gedanke war, dass das Gerät einen Reset durchgeführt hat und sich dadurch wieder im Werkszustand befand. Da es am nächsten Tag jedoch wieder den alten Zustand zeigte, kann es

sich nur um einen Recovery-Start gehandelt haben, der das Gerät im Auslieferungszustand aus dem ROM Bereich des Speichers gestartet hatte.

Es bleibt die technische Frage unbeantwortet, ob so ein Recovery-Start überhaupt möglich ist ohne den normalen Speicher zu überschreiben. Wir würden uns über Tipps freuen, denn alles „Googeln“ (natürlich mit Open Source Suchmaschinen) blieb ohne Erkenntnisse über ähnliche Erlebnisse oder Erklärungen dazu.

3. Das Fazit

Es bleibt das Gefühl dem Gerät ohnmächtig ausgeliefert zu sein. In einer echten Wildnis wäre man im obigen Fall verloren gewesen. So ein Verhalten nagt schwer am Vertrauen zu dem Gerät.

Datenhunger von Apps

Auch Apps, die von ihrer Funktion überhaupt keinen ersichtlichen Grund dafür haben, fragen nach Zugriffsmöglichkeiten auf unsere Daten.

Apps WOLLEN Zugriff auf: WLAN, Medien, Kontakte, ansonsten verweigern die die Installation, so will z.B. Twitter Zugriff auf ca 10 Datengruppen (wohl auf alles). Nach dem Standort wird nochmal extra gefragt, obwohl es keinen Grund dafür gibt, warum der Ort für meinen Tweet wichtig sein sollte.

Und im übrigen: http://www.golem.de/news/ueberwachung-google-sammelt-gespraechsprotokolle-von-android-geraeten-1606-121856.html

"Wir speichern Informationen zu Telefonanrufen nur dann, wenn Google-Apps und -Dienste verwendet werden" sagt Google zu den Vorwürfen einer „privaten Vorratsdatenspeicherung“.

OK, dann ist ja alles klar: Runter mit den Google Diensten! Leider versagt hier die "Technik", denn Google-Apps lassen sich nicht deinstallieren, man kann sie lediglich "ruhen" lassen, also deaktivieren. (http://a-fsa.de/d/2Et)

Auch bei der Installation von Skype (von Microsoft): Die Liste der verlangten Berechtigungen umfasst praktisch Alles. Und telefonieren auf unsere Kosten möchte die App auch: „Das Skype Guthaben darf auch zum Einwählen in öffentliche Hotspots verwendet werden“. Damit verliert man jegliche Kontrolle ob die Kommunikation über das WLAN oder über ein Mobilfunknetz genutzt wird.

Unschön ist es auch, dass Apps bei/nach der Installation ihre Datei, die .apk löschen. Sie sind dann einfach nicht mehr auffindbar, um sie z.B. auf anderen Geräten oder irgendwann später erneut zu nutzen.

Unsicher und gefährlich

Wie zu lesen ist, ist „Verschlüsselung von vielen Android-Geräten peinlich unsicher“. http://t3n.de/news/full-disk-encryption-721928/

Das geht soweit, dass die App uns einfach belauscht: Shazam song-identification program keeps your mic on, even when you turn it off. https://t.co/p8NXr52nuV

Dies ist ein grundsätzliches Problem nicht-offener SW - deshalb streiten wir für offene Protokolle in der Kommunikation und offene Software (Open Source).

Untersuchung zum Datenhunger bei verschiedenen Betriebssytemen

Welche Verbindungen bauen die Geräte auf, obwohl man versucht die Einstellungen auf minimalen Datenaustausch zu stellen? Das deutsche Institut für Vertrauen und Sicherheit im Internet (DIVSI, https://www.divsi.de) hat dazu Messungen gemacht.

	Android	BlackBerry OS	iOS	Windows Phone 8
Endpunkte	22	20	55	25
Verbindungen	97	296	202	69
Datenvolumen	10,89 MB	1,28 MB	68,19 MB	1,76 MB

DIVSI

Danach kommunizieren alle Geräte auf Kosten des Kunden über dessen Verbindungen (WLAN oder Mobilfunk-Datentarif).

Welche Verbindungen bauen die Geräte trotz der zuvor beschriebenen Minimaleinstellungen auf?

Diese Frage wurde in praktischen Tests der vier Betriebssysteme vom DIVSI geklärt. https://www.divsi.de/publikationen/studien/wissenswertes-ueber-den-umgang-mit-smartphones/5-basisdienste-und-datenuebermittlung/5-1-smartphone-einrichten/5-1-2-minimale-einstellungen-der-praxis/

Kurz nach Verbinden des Gerätes mit dem Internet wurden bei Android und iOS Verbindungen aufgebaut (Apple Push Service, Android Chat, Google+ Hangouts), die beinahe über den gesamten Testzeitraum aufrechterhalten wurden.

Bei **Android** ließ sich eine Verbindung zu Werbezwecken beobachten. Der Endpunkt dieser Konversation lässt sich der Firma DoubleClick zuordnen, einem Unternehmen der Google-Gruppe.

Bei **IOS** lässt sich die Verbindung zum Push Service (APNS) vom iPhone aus nicht deaktivieren, außer durch das Abstellen der Netzwerkverbindung. Eine Verbindung mit www.wu.apple.com ist unverschlüsselt und lässt sich auf eine vorinstallierte Aktien-App zurückverfolgen. Für die Aktien-App ist standardmäßig die Hintergrundaktualisierung aktiviert. Aus der Konversation kann man herauslesen, welche Daten abgefragt werden, d.h. welche Aktien den Nutzer „interessieren“.

Das **Windows Phone** überträgt bei Netzzugang unmittelbar eine (vermutlich) eindeutige ID für das Gerät, Zeitstempel des Berichtes, Gerätetyp, Betriebssystemversion sowie kompatible Prozessorarchitektur.

Ebenfalls unmittelbar nachdem das Gerät mit dem Internet verbunden ist, wird eine verschlüsselte Verbindung zu einem Server aufgebaut, dessen Hostname *api.live.net* lautet und über den ggf. der Nutzer später sein Microsoft Konto anlegt. Dort können Webservices mit entsprechender Autorisierung alle Daten abrufen, die mit einem Microsoft-Konto verbunden sind.

Das **Windows Phone** baute Verbindungen mit einem Endpunkt auf, der Dienste zur Standortbestimmung anbietet. Laut Microsoft werden von diesem Dienst Zellinformationen sowie

Informationen über Drahtlosnetze in Reichweite erfasst. Falls diese Daten tatsächlich erfasst und gesendet werden, steht dies im Widerspruch zu der im Test gewählten minimalen Einrichtung, bei der „WLAN-Verbindungsdaten zur Erkennung von WLAN in der Umgebung sichern“ explizit deaktiviert wurden.

Blackberry OS: Kurz nach dem Aufbau der Verbindung zum WLAN wird automatisch eine Verbindung zu BlackBerry (blackberry.com) aufgebaut, die über den gesamten Testzeitraum aktiv ist. Zwei Verbindungen werden zu Servern mit „Eyeball AnyFirewall Engines“ aufgebaut. Eventuell werden hier Technologien zur Umgehung von NAT-Firewalls für VoIP-Verbindungen eingesetzt, wie sie in vielen Heimnetzwerken zu finden sind.

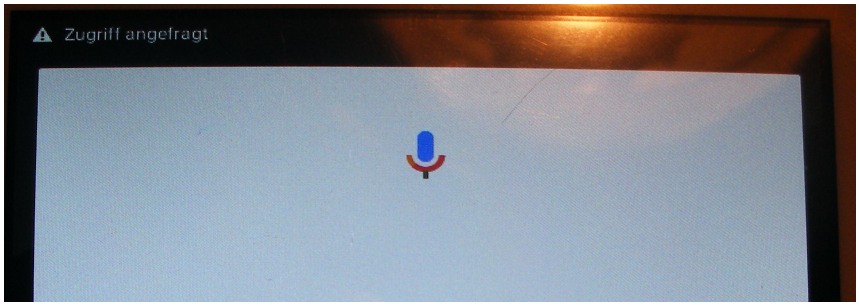
Das traurige Fazit: Alle diese Betriebssysteme sind aus Datenschutzsicht nicht zu empfehlen.

Folgende Links können beim Verständnis der Studie helfen:

- Minimale Einstellungen
- Studien des DIVSI
- Wissenswertes zum Umgang mit Smartphones

Android säubern

Auch ohne gleich den Root-Zugriff auf das Gerät herzustellen, kann man schon mal aufräumen und alle „datenhungrigen“ und unnötigen Apps entfernen oder zumindest deaktivieren. So wollen wir sicher nicht, dass uns Google zuhört ...



Viele Google Apps lassen sich in Android ohne Root-Zugriff nicht entfernen sondern nur deaktivieren.

App	Funktion oder Gefahr
Google Account Manager	Google Accounts
Google Backup Transport	Backup bei Google
Google Kalender	Kalender
Google Partner Setup	?
Google Play Manager	? Konfiguration des Play Stores
Google Play Movies	Video player (auch online)
Google Play Music	Music player (auch online)
Google Kontakte Sync	Adressbuchverwaltung in der Cloud
Google Suche	suchen
Google Tastatur	? welche zusätzliche Funktion?
Google Plus	?
Google Framework	?
Play Store	Apps installieren
Play Games	Spiele installieren
Maps	Navigation
Street View	Navigation und Ansichten
GMail	Google Mail
E-Mail	Vorinstallierter E-Mail Client lässt keine Verschlüsselung zu
Sheets	Tabellenkalkulation bearbeiten Öffnet keine .ods Dateien
Präsentationen	Präsentationen bearbeiten Öffnet keine .odp Dateien

Die App „**Google App**“ ist in obiger Liste nicht enthalten, denn sie darf nicht deaktiviert werden, sonst startet Android nicht mehr. In diesem Fall hilft nur noch ein Reset.

Navigation mit freier Software

Sehr empfehlenswert für die Navigation ist die App OSMand, da sie ihre Kartendaten auf dem Gerät ablegen kann und damit keine Kommunikationsressourcen benötigt. Man bleibt damit anonym.

OSMand (https://osmand.net/)

- nutzt die weltweite Kartendatenbank des freien Open Street Map (https://www.openstreetmap.de/)
- bietet Navigation für Kfz, Radfahrer und Fußgänger
- speichert zurückgelegte Wege als GPX Tracks und Orte (POIs)
- holt seine OSM Karten vorher; Kartensätze nach Bundesländern und Staaten verfügbar
- aufgezeichnete Tracks können zur Navigation genutzt werden
- im Dialog "Karte konfigurieren" kann man auswählen, was alles angezeigt werden soll, z.B. alte Wege, dazu "GPX-Track" einschalten. Aus der Liste vorhandener Strecken sind diese anzukreuzen.

Wenn der Datenordner von OSMAnd im externen Speicher liegt, kann man ihn auch direkt oder über USB von außen nutzen. Standardmäßig liegen die Daten im internen Speicher. Wenn man auf dem Gerät nicht alle Zugriffsrechte hat, muss man unter Umständen OSMand noch einmal löschen, dann den Datenordner auf den externen Speicher ändern und die Karten neu per WLAN herunterladen.

Dialog "Karte konfigurieren". Hier können Sie auswählen, was alles angezeigt werden soll. Schalten Sie den "GPX-Track" ein. Die App zeigt eine Liste vorhandener Strecken. Kreuzen Sie eine oder mehrere davon an.

OSMtracker (https://wiki.openstreetmap.org/wiki/DE:OSMTracker_(Android)

speichert zurückgelegte GPX Tracks, muss aber seine genutzten OSM Karten ständig aktualiseren, braucht also eine Netzverbindung.

Navit (http://www.navit-project.org/)

Zur Navigation ist die App Navit ebenfalls geeignet. Die Kartendaten werden von Open Street Map geholt. Dazu ist unterwegs eine Datenverbindung notwendig.

Die weltweiten Karten von Open Street Map sind in Europa und Nordamerika von gleicher Qualität wie käufliche Produkte oder Google Maps. Von Vorteil ist außerdem ihre Aktualität, für die man bei gekauften Navis oft zusätzlich Geld ausgeben muss. Ein Dank gebührt allen freiwilligen Sammlern der Daten zu denen auch Aktive von Aktion Freiheit statt Angst gehören (http://a-fsa.de/d/1WJ).

Durch die vielen Datensammler sind aktuelle auch kurzfristige Änderungen oder Einschränkungen von zurückgelegten Wegen schnell in der Datenbank, die Gesellschaft/Gemeinschaft organisiert sich das Funktionieren der Software selbst.

Open Source als Strohhalm gegen das Ausgespäht-werden

Weiter sind als Ersatz für neugierige Apps z.B. folgende Open Source Programme sinnvoll:

- F-Droid ersetzt den Google Play Store und bietet für viele Apps aus dem Open Source Bereich.
- Open Office Viewer ermöglichen das Lesen von Libre Office Dateien.
- K6-Mail stellt ein vollständiges Mailprogramm für mehrere Mailkonten zur Verfügung und bietet die Möglichkeit der Verschlüsselung.
- Open Key Chain und ehemals APG ermöglichen die Verschlüsselung von Mails mit K6.
- Für die Navigation wurden bereits die Apps OSMand und Navit als Beispiele genannt.
- Zum Surfen steht der Firefox Browser oder der Privacy Browser zur Verfügung.
- Anonymes Surfen über das Tor Netzwerk ermöglichen Orfox oder Orweb mit der App Orbot.
- Die Apps CsipSimple oder Linphone ermöglichen das Telefonieren über VoIP. (https://en.wikipedia.org/wiki/CSipSimple und http://www.linphone.org/)
- Amaze ist eine App zur Dateiansicht, die auch Dateien und Ordner im .zip Format komprimieren und wieder auspacken kann.

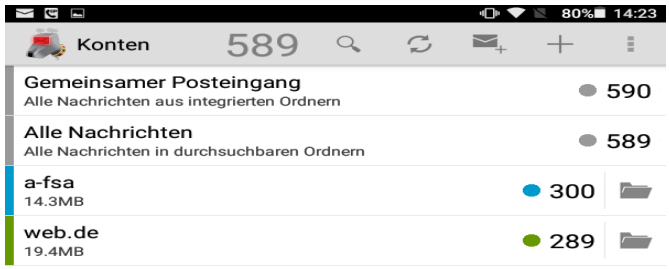
Kommunikation nach „außen“

Was möchte man erreichen?

- **Vertraulichkeit**: Daten dürfen lediglich von Berechtigten gelesen bzw. modifiziert werden. Dies gilt sowohl beim Zugriff auf gespeicherte Daten, wie auch während der Datenübertragung.
- **Integrität**: Daten dürfen nicht unautorisiert und unbemerkt verändert werden. Alle Änderungen müssen nachvollziehbar sein.
- **Authentizität**: Nachweis der Echtheit und Glaubwürdigkeit von Daten oder Subjekten, anhand eindeutiger Identität oder Eigenschaften
- **Verbindlichkeit**: Schutz vor unzulässigem Abstreiten durchgeführter Handlungen, d.h. niemand kann nicht abstreiten, dass eine Aktion durchgeführt wurde.
- **End-to-End Encryption**: Ende-zu-Ende Verschlüsselung sorgt dafür, dass niemand außer den beiden Teilnehmern die Inhalte lesen kann.
- **Freie, quelloffene Software**: Vom Client bis hin zum Server sollte jeglicher Quellcode frei für jeden einsehbar sein. Das macht die Anwendung nicht per se sicher, sorgt allerdings für die notwendige Transparenz und ermöglicht eine Überprüfung des Quellcodes auf Fehler und Hintertüren. Tausend Augen sehen mehr als die Entwickler in einer Software Firma.
- **Vermeidung von Metadaten**: Insbesondere die Metadaten sagen oftmals viel mehr über eine Person aus, als sich die meisten überhaupt vorstellen können. Gerade in Bezug auf die Privatsphäre sollte es Unternehmen, den Geheimdiensten und Co. so schwierig wie möglich gemacht werden, diese Metadaten einfach abzugreifen.
- **Dezentralisierung**: Möglichst keine zentralisierte Infrastruktur nutzen, sondern eine Dezentralisierung anstreben.

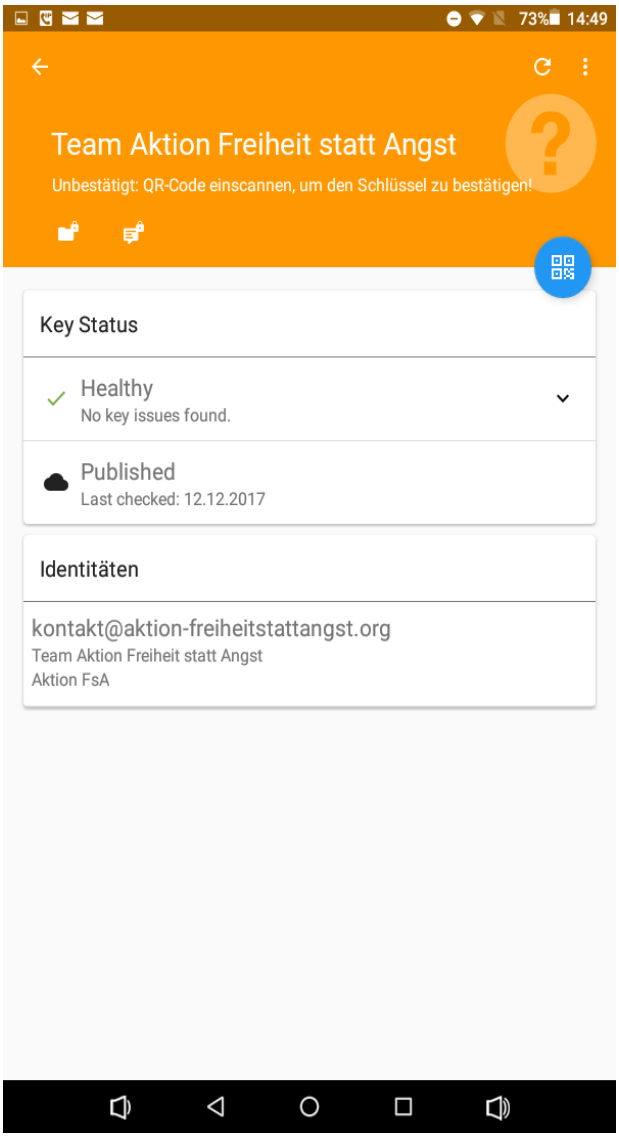
Verschlüsselt Mailen

Als Programm mit beliebig vielen Postfächern (E-Mail Adressen) bietet sich die im F-Droid Store erhältliche Open Source App K9-Mail an. (https://k9mail.github.io/)



Zur Zusammenarbeit K9-Mail und OpenKeyChain

Manchmal lassen sich Keys aus Mails nicht in Open Key Chain importieren. (https://www.openkeychain.org/) Wichtig ist in K9 in dem entsprechenden Mailkonto auf Kontoeinstellungen/Kryptographie zu gehen und OpenKeyChain als PGP-Client anzugeben. Dann sollte es gehen. Es ist noch einzustellen wie man seine Mails verschicken möchte als **PGP/Mime** mit Anhängen oder **PGP/Inline** nur Text.



Zusammenarbeit K9-Mail und APG

Eine ältere Variante ist die Verschlüsselung mit der App APG. Wichtig ist hierbei, dass APG zuerst installiert sein sollte und dann erst K6 eingerichtet wird. Eventuell ist K6 noch einmal neu zu installieren. Auch hierbei muss in den K9-Mail Einstellungen / Konto-Einstellungen / Kryptographie das Programm APG zur Verschlüsselung eingetragen werden.

APG kann wie auch **Open Key Chain** Schlüssel erzeugen, verwalten und im- und exportieren. Die Apps können auch genutzt werden um Dateien auf dem Smartphone symmetrisch mit GPG zu verschlüsseln.

Bitseal leider nicht empfehlenswert

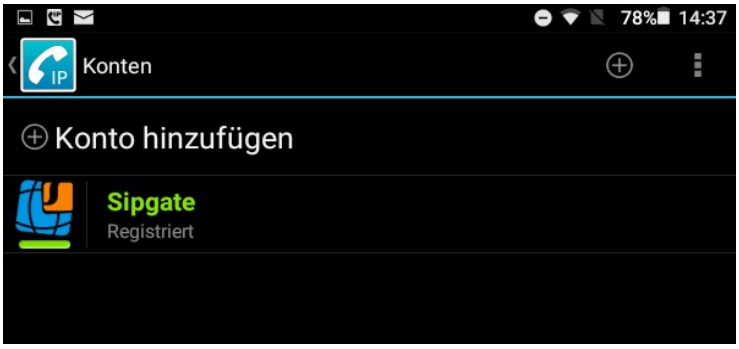
Das Bitmessage Programm für Android Smartphones tut leider nicht so richtig. Entweder beendet es sich sofort nach der Start oder es tut über Stunden nichts, außer dass es bei jeder Gelegenheit Aktualisierungen runterlädt – hier hilft nur abwarten auf bessere Implementierungen, während die Versionen für Linux, Windows und Mac ohne Probleme funktionieren.

Secrecy

Die App erlaubt das Verschlüsseln von Ordnern und Dateien. Allerdings sind bei einem Zugriff über eine USB Verbindung auf das Smartphone die Dateinamen in den verschlüsselten Ordnern trotzdem lesbar, nur die Inhalte sind verschlüsselt

Telefonieren über das W-LAN

CSipSimple oder Linphone sind zwei Apps, die das Telefonieren über VoIP ermöglichen. Wir haben CSipSimple erfolgreich getestet. (https://en.wikipedia.org/wiki/CSipSimple)



Über W-LAN ist man damit kostenlos weltweit erreichbar und kann über diverse VoIP-Telefonanbieter zu günstigen Tarifen ebenso in das Festnetz oder in Mobilfunknetze telefonieren, bei Sipgate z.B. für 2,5ct/Min ins deutsche Festnetz.

sipgate

https://www.sipgate.de/

Gibt es sichere Messenger?

Wer wegen des Abziehen von privaten Daten, wie z.B. um meine privaten Kontakte, um WhatsApp einen Bogen machen möchte, muss 1. eine Alternative suchen und 2. seine Kommunikationspartner davon überzeugen sich diese App ebenfalls herunterzuladen. Wir haben eine Liste von Privatsphäre-schützenden Apps gesammelt.

Vor der Benutzung von Facebooks Produkt WhatsApp können wir nur warnen. Trotz seiner angeblichen Ende-zu-Ende Verschlüsselung aller Nachrichten ist die App ständig auf der Suche nach den persönlichen Daten auf dem Handy (Kontakte, E-Mail Adressen, Standort, …).

Neben der proprietären, also geheimen und nicht nachprüfbaren, Verschlüsselung nutzt WhatsApp Server in den USA. Was es alles an Facebook zu kritisieren gibt steht hier https://www.aktion-freiheitstattangst.org/de/articles/2532-20111130-facebook-privatsphaere-leitfaden.htm

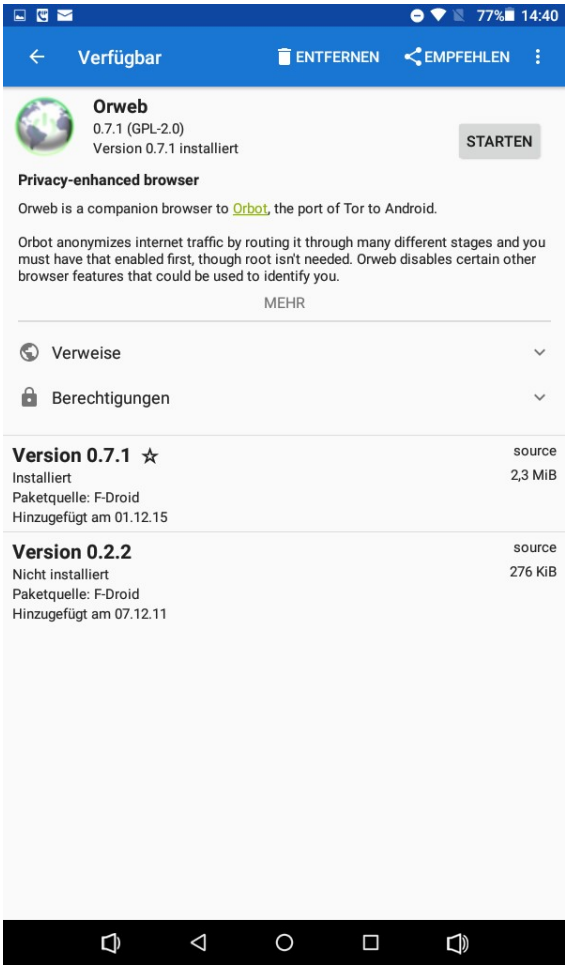
Tabelle: **Privatsphäre-schützende Messenger**

App	+	-
Briar Beta	Ende-zu-Ende verschlüsselt, Kontakte müssen sich einen persönlichen Qrcode zeigen	Kontakte erzeugen geht nur, wenn man sich trifft und ist manchmal auch noch schwierig. Die Version ist noch im Beta-Stadium.
ChatSecure	Open Source XMPP kann mit OTR Ende-zu-Ende verschlüsselt werden	Im Original nur SSL/TLS-verschlüsselt zwischen den Servern, dort aber unverschlüsselt
Conversations	Ende-zu-Ende verschlüsselt	Installation schwierig, fehlerhaft auf Linux Desktop (heißt dort gajim)
Signal	Open Source Client Ende-zu-Ende verschlüsselt, von Edward Snowden empfohlen,	geht nicht auf Samsung Tab A, SM T580
Telegram	Open Source Client Anleitung https://telegram.org/faq/de	Geheime Server-Software, Desktop Version kann nicht verschlüsseln, Verschlüsselung geheim, zentralisierte US-Server, Kontakt- und Metadaten werden gespeichert
Threema	Open Source Client	Geheime Server-Software, Verschlüsselung geheim,
Tigase	XMPP Messenger	Messenger mit offenem Protokoll
Wire	Messenger mit Telefon und Video	Sicher verschlüsselt aber propiertär; wire.com
Xabber, ….	Open Source XMPP kann mit OTR Ende-zu-Ende verschlüsselt werden	Im Original nur SSL/TLS-Verschlüsselt zwischen den Servern, dort aber unverschlüsselt
Yaxim	XMPP Messenger	Messenger mit offenem Protokoll

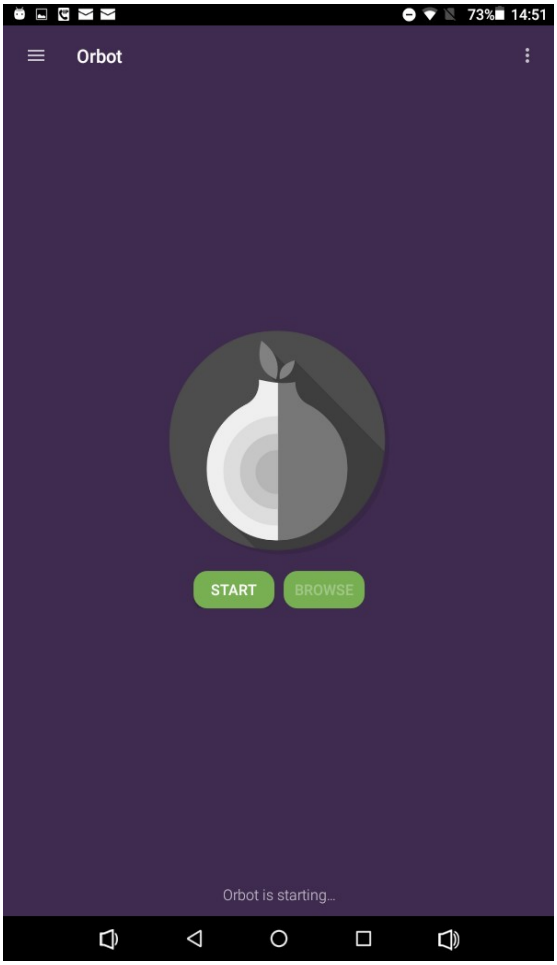
Sicheres Surfen

Der Google Browser will sich bei Google anmelden, ist dann aber auch ohne Anmeldung nutzbar. Alternativ wäre neben dem Browser von Mozilla Firefox der Privacy Browser, der prinzipiell keine Daten speichert, allerdings leider auch keine Tabs unterstützt.

Um über das Tor Netzwerk anonym zu surfen benötigt man aus dem F-Droid Store die Apps Orbot und Orfox, bzw. Orweb. Die App Orbot stellt die Netzverbindung zum Tor-Netzwerk her sobald man Orfox startet. Eventuell sind diese Apps nicht im F-Droid Store sichtbar. Dann muss man unter „Einstellungen“ „zusätzliche Quellen“ hinzufügen, z.B. das Guardian Project https://guardianproject.info/apps/orbot/



Die Installation von OrWeb im F-Droid Store



Vor dem Surfen ist Orbot zu starten, dies erfolgt automatisch beim Aufruf von Orweb.

Über Orbot können unter „Einstellungen“ auch weitere Apps ausgewählt werden, um über das Tor Netzwerk anonym ins Internet zu gehen. Dann ist zusätzlich diesen Apps der lokale Port 9050 als Proxy mitzuteilen.

Möglicherweise sinnvolle Apps

Die folgende Liste ist beliebig erweiterbar, sie enthält z. Zt lediglich die Apps (ohne die oben bereits aufgelisteten Messenger), die wir im Laufe unserer Arbeiten ausprobiert und zumindest nicht für sinnlos gehalten haben.

Tabelle: **Möglicherweise sinnvolle Apps**

App	Nutzen	Links/Hinweise
APG	Encrypt email and files, z.B. für K6 Mail	https://f-droid.org/repo/org.thialfihar.android.apg_11199.apk
APK4Fun	App Store	Ein Google-freier App Store neben F-Droid, allerdings mit Werbeeinblendungen
Amaze Filemanager	Filemanager	Kann Dateien und Ordner mit zip ein- u. auspacken
BitSeal	Bimessage für Android	Funktioniert leider nicht. Arbeitet stundenlang ohne Erfolg oder Fehlermeldung
BlueJabber	XMPP Messenger	Messenger, der auch über Bluetooth läuft
Bluetooth Easy Voice Recorder	Audio hören und sprechen über Bluetooth	Geht nicht mit jedem Gerät o. jeder Android Version
Bluetooth Parrot	Audio hören und sprechen über Bluetooth	
Bluetooth SGH-I537 running 4.4	Audio hören und sprechen über Bluetooth	
Bluetooth Audio Recorder	Audio hören und sprechen über Bluetooth	
Bluetooth Voice Recorder	Audio hören und sprechen über Bluetooth	
Connect Bot	ssh Verbindungen	Kann nur ssh1, das ist nicht mehr sicher.
CSipSimple:	Telefonieren über WLAN	Encrypted Voice Over IP (VOIP)
FLV	FLV Media Player	Kann Playlisten, stürzt aber auch ab
F-Droid	App Store für Zugang zu Freien Apps	https://f-droid.org/FDroid.apk
fennec	Firefox Browser	
GoSecured Mail	Verschlüsselter Mailer	proprietär, Subscription notwendig
HoloBackup	Einfaches Backup und Restore	Ehemals: Simple ADB Backup
Jabiru	XMPP Messenger	
K-9	E-Mail Client für mehrere Postfächer	Kann mit OpenKeyChain oder APG Mails Ende-zu-Ende verschlüsseln https://mailbox.org/einrichtung_mit_android_smartphone_und_k9_mail/

Linphone:	Telefonieren über WLAN	Encrypted Video und Voice Over IP (VOIP)
Linux Deploy	Linux neben dem Android installieren	Benötigt Root-Rechte https://technik.blogbasis.net/linux-auf-dem-android-smartphone-parallel-installieren-14-06-2013
Mercury SSH	Ssh Client	Benötigt ein .json config File,Bsp im Help
Navit	Navigation	Karten werden stets online übers Netz abgerufen
OpenKeychain	Encrypt files and communications with OpenPGP	Unterstützt Ende-zu-Ende Verschlüsselung z.B. in K6 Mail
Orbot	Zugang zum Tor-Netzwerk	
OrFox	Tor Browser auf Basis von Firefox	
Orweb	Tor Browser auf Basis von Firefox	
Osmand	Navigation mit Offline Maps	http://osmand.net http://www.appsapk.com/osmand/ http://www.gerold-dreyer.de/Homepage/Anleitungen/Gebrauchsanleitungen%20zu%20Programmen/android_osmand/android_osmand.htm
OSMtracker	OSM GPS Software	Kann Tracks als gpx speichern; lädt Karten übers Netz
PGP Mail	Verschlüsselte Mail	
PlugIns	Für Firefox Browser: NoScript ublock oder AddblockPlus	Blockiert Java Script blockiert Werbung
Quick SSHd	Ssh Server	
RootChecker	Prüft root Zugriff	
Secrecy	Encrypt files in Container	AES-verschluesselt; Dateinamen bleiben unverschlüsselt
Simple Text	Texteditor	
SSH Autotunnel	stellt Kommandos für Tunnel bereit	Android muss vorher gerootet sein
SSH Client	Ssh Client	
SSH Remote Executer	stellt Liste von Remote Kommandos auf Tastendruck bereit	
SSH Server	Ssh Server	Android muss vorher gerootet sein. Dafür benötigt wird: system/bin/sh
Titanium Backup	Backup Programm	Android muss vorher gerootet sein. Backup für alle Apps (inkl.systemapps)

Ted	Texteditor	Ist langsam
Termux	Terminal	Android muss vorher gerootet sein. Shell Zugriff als User
VNC Viewer	VNC Viewer	Gut um, z.B. auf einen Host/RasPi zu schauen, selbst die Maus wird gut emuliert.
WinAmp	MusicPlayer	Kann Playlisten abspielen, aber wo werden diese abgelegt? (nicht erweiterbar)
xPrivacy	Berechtigungseinstellung	Android muss vorher gerootet sein. Berechtigungen für installierte Apps einstellen

Anmerkung: Das XMPP-Protokoll basiert auf dem offenen XML-Standard und es gibt viele quelloffene Implementierungen. Viele davon sind mit OTR auch Ende-zu-Ende zu verschlüsseln.

Viele weitere sichere Apps gibt es hier https://guardianproject.info/apps

Ein Smartphone rooten

Überblick für Android

Nach all dem Ärger, den man durch die ständigen Nachfragen oder Beschränkungen vom Android Betriebssystem erfahren musste, ist der Wunsch nach Alternativen geweckt. Davon gibt es eine ganze Reihe - aber leider auch mit Einschränkungen, je nach dem Gerät was man besitzt.

Der grundlegende Unterschied zwischen einem iPhone und einem Android Smartphone liegt in der Vielfalt der Hersteller, die ihre Geräte mit Android ausliefern. Während Apple durch die eigene Herstellung der Hardware die Hand darauf hat, welche Komponenten verbaut werden, ist das bei Android nicht der Fall.

Dadurch gibt es schon im „Verkaufszustand“ Unterschiede bei der Auswahl der installierten Apps. Sobald man nun das Betriebssystem ändert, muss man hinnehmen, dass gerade für das vorhandene Gerät diese oder jene Funktion nicht mehr läuft.

So gibt es z.B. eine Übersichtsliste welche Funktionen bei welchem Gerät noch laufen, wenn man Linux darauf installiert. Link xx

Die vielen Lücken in dieser Übersicht haben kürzlich auch Canonical nach jahrelanger Entwicklung die Arbeit an seinen Smartphone-Ambitionen einstellen lassen. https://www.golem.de/news/ubuntu-canonical-gibt-unity-8-und-smartphone-konvergenz-auf-1704-127171.html Systeme wie das geplante Ubuntu Phone sind auf die Treiber der Geräte-Hersteller angewiesen und diese wechseln einfach zu schnell.

Um dies zu verhindern hat das Projekt Sailfish OS von Jolla mit einer festen Hardware (der ehemaligen Nokia Mitarbeiter) gearbeitet. Es bietet also für einen Betriebssystemwechsel auf anderer Hardware keine Alternative. https://jolla.com/

Das Projekt mit dem Codenamen Halium beginnt zur Zeit den notwendigen Android-Unterbau aus Kernel und Init-System für diverse Geräte zu sammeln und in einer gemeinsamen Bibliothek zur Verfügung zu stellen. https://www.golem.de/news/plasma-mobile-ein-smartphone-os-von-und-fuer-die-community-1507-115472.html

Benutzbar ist solange nur das Android-Community-Projekt LineageOS, das aus Cyanogenmod hervorgegangen ist. Informationen findet man dazu unter

- CyanogenMod, Offenes Android System, https://wiki.cyanogenmod.org
- Lineage, https://www.lineageos.org/

Rooten oder lieber nicht?

Bevor wir uns entschließen können ein freies Betriebssystem zu installieren, müssen wir erst einmal Root-Rechte auf unserem Gerät besitzen. Bei den ersten Android Versionen war das mit der Nachfrage beim Hersteller nach einer ID erledigt. Das ist nicht mehr „üblich“. Obwohl wir das Gerät und die Software gekauft haben, wird uns die vollständige Nutzung verwehrt.

Wir müssen den Root-Zugriff erst mit verschiedenen Tricks erlangen, wobei die Hersteller uns mit dem Erlöschen der Garantieansprüche drohen.

Was sollte man wissen bevor man beginnt? Hier eine Liste mit Tipps und Tricks:

- Howto https://www.oneclickroot.com/how-to-jailbreak-android/
- https://www.androidpit.de/android-rooten
- Chip: http://www.chip.de/news/Root-Tools-Anleitungen-Android-entsperren_62725588.html
- Chip: http://www.chip.de/news/Android-rooten-Vorteile-und-Nachteile_62681106.html
- FSFE: https://fsfe.org/campaigns/android/liberate.de.html
- Tools: http://www.chip.de/news/Root-Tools-Anleitungen-Android-entsperren_62725588.html
- Hardware Liste: http://www.xda-developers.com/root/#others
- Rooten: https://www.android-user.de/so-funktioniert-der-root-zugriff-unter-android/
- Android Theorie: https://www.droidwiki.org/wiki/Root
- Root Odin3: http://www.chip.de/downloads/Odin3_12992520.html
- Root Huawei Y300: http://huawei-y300.tumblr.com/post/47366836617/how-to-unlock-and-root-huawei-ascend-y300-all

CyanogenMod-Nachfolger Lineage als Alternative

Die zentrale Softwarekomponente basiert auf dem Nachfolger des freien CyanogenMod oder einem vergleichbaren Custom-ROM und trägt nun den Namen Lineage. https://www.lineageos.org/

Diese Android-Betriebssystemvariante steht für viele Smartphones zur Verfügung, wird von einer aktiven Community stetig weiterentwickelt und enthält von Haus aus keine Google-Apps.

Auch Google-Reste sollen daraus künftig entfernt werden. Im Kuketz-Blog ist eine Anleitung beschrieben, mit der wir den Network Log kontrollieren, um zu prüfen ob unsere Apps noch „nach Hause telefonieren“. https://www.kuketz-blog.de/your-phone-your-data-teil1/

Wie sollte man beim Rooten vorgehen?

Grundsätzlich läuft das saubere „Rooten“ so ab:

- Bootloader entsperren
- Modifiziertes Boot-System oder Custom-ROM installieren
- Superuser-App installieren

Wenn uns dafür keine Programme zur Verfügung stehen, bleibt nur der "unsaubere" Root-Vorgang:

- System auf (bekannte) Sicherheitslücken prüfen
- Sicherheitslücke ausnutzen
- Superuser-App installieren

Einen ausführlichen Bericht über das Rooten der uns zur Verfügung stehenden Geräte ist in unserem Web verfügbar. https://www.aktion-freiheitstattangst.org/de/articles/6361-20180203-ein-smartphone-rooten.htm

In der Kurzfassung läuft es (mit KingoRoot) so ab:

- USB-Debugging aktivieren (unter Einstellungen > Entwickleroptionen).
  Falls keine Entwickleroptionen angezeigt werden: sieben Mal unter „Über das Telefon“ auf den Eintrag „Build-Nummer“ tippen.

- Auf einem Laptop/PC mit Windows die Software ADB Server und KingoRoot installieren
- Gerätetreiber in Windows aktualisieren lassen
- Laptop und Smartphone mit USB Kabel verbinden
- KingoRoot sucht nach dem Gerät und fragt ob es gerootet werden soll
- nach dem Rooten zeigt die App KingoRoot auf dem Smartphone den Erfolg an

Man kann nun (leider nur vom angeschlossenen Laptop) die Berechtigungen auf dem Smartphone einstellen und muss es dazu jedes mal mit dem USB Kabel verbinden.

Hier noch einige hilfreiche Links:

- Rooten Odys Xelio 7 Pro https://www.youtube.com/watch?v=KfU4MnXVFus
- Hilfe für Odys Xelio https://www.android-hilfe.de/forum/root-hacking-modding-fuer-das-odys-xelio.608/cm9-cyanogenmod-auf-dem-xelio.274790.html
- Vroot über Windows https://www.youtube.com/watch?v=KfU4MnXVFus
- Root-Pakete https://tabletcommunity.de/android-tablet-rooten/
- SuperOneClick http://superoneclick.us/
- Kingo http://de.kingoapp.com/android-root/devices.htm

Ein iPhone rooten

Das Rooten eines iPhone heißt Jailbreak und wird ebenfalls mit jeder neuen Version schwieriger. Auch hier kann man das iPhone von den Nutzungsbeschränkungen des Apple Betriebssystems befreien – mit den gleichen Risiken wie bei Android. Deshalb hat man das Thema „Jailbreak“ beim iPhone im letzten Jahr schon fast endgültig beerdigt https://www.mobiflip.de/iphone-jailbreak/

Beim iPhone ist zwischen einem kurzfristigen (tethered) und dem dauerhaften „Jailbreak“ zu unterscheiden. Bei einem tethered iPhone Jailbreak muss man das iPhone nach jedem Neustart erst an einen Computer anschließen, um das Gerät mit der Jailbreak Software erneut zu starten. Die notwendige Software gibt es z.B. hier: „Yalu102“-Jailbreak http://iphone-tricks.de/anleitung/47474-jailbreak-ios-10-1-ios-10-2-anleitung und eine Beschreibung hier: https://de.wikipedia.org/wiki/Jailbreak_(iOS) .

Was man für einen iPhone Jailbreak braucht:

- 5 Minuten Zeit
- Laptop/PC mit Windows, Mac OS X oder Linux
- iTunes
- iPhone ab iOS 6.0 (s. „Einstellungen“ / „Allgemein“ / „Info“)
- USB Kabel um das iPhone mit dem Computer zu verbinden

  Bitte beachten:
- Vor dem Jailbreak ein Backup erstellen
- Die Code Sperre des iPhone deaktivieren
- Während des Jailbreak Vorgangs iTunes und iOS nicht benutzen

Sollte wider Erwarten die Software während des Jailbreak Vorgangs abstürzen, so ist das kein Problem. Man kann jederzeit das iPhone und die Software auf dem PC neu starten und den Vorgang wiederholen.

Links

Die Links in der Reihenfolge ihres Auftretens

"Ich und mein Handy" https://youtu.be/q3xZiZgwb_0

"Die Anonym-Mäuse sichern ihre Smartphones" https://youtu.be/r8V4XX415iA

Zum Nachlesen in unserem Web www.a-fsa.de/d/2T1

Berechtigungen in Android https://www.kaspersky.de/blog/android-permissions-guide/9743/

Hinweise Google Konto löschen https://support.google.com/accounts/answer/61177?hl=de

Hinweis: externe Speicher im „mixed_mode“ betreiben https://www.android-user.de/mixed-mode-microsd-karte-unter-android-marshmallow-als-internen-und-externen-speicher-nutzen/

verschlüsselte SD-Karten entschlüsseln http://nelenkov.blogspot.de/2015/06/decrypting-android-m-adopted-storage.html

Der „fehlerhafte“ Elliptic Curve Zufalllszahlengenerator https://www.aktion-freiheitstattangst.org/de/articles/403-20170411-ueberwachung-durch-unternehmen.htm

Überwachung durch Google http://www.golem.de/news/ueberwachung-google-sammelt-gespraechsprotokolle-von-android-geraeten-1606-121856.html

Google Apps deaktivieren http://a-fsa.de/d/2Et

Verschlüsselung von Android-Geräten peinlich unsicher http://t3n.de/news/full-disk-encryption-721928/

Berechtigungen für Android-Apps
https://www.kaspersky.de/blog/android-permissions-guide/9743/
https://www.androidauthority.com/android-app-permissions-explained-642452/
https://www.androidauthority.com/app-permissions-886758/

Erklärung Open Source https://de.wikipedia.org/wiki/Free/Libre_Open_Source_Software

Deutsches Institut für Vertrauen und Sicherheit im Internet https://www.divsi.de

DIVSI Studien https://www.divsi.de/publikationen/studien/wissenswertes-ueber-den-umgang-mit-smartphones/5-basisdienste-und-datenuebermittlung/5-1-smartphone-einrichten/5-1-2-minimale-einstellungen-der-praxis/#schriften

OSMand https://osmand.net/

Open Street Map https://www.openstreetmap.de/

OSMtracker https://wiki.openstreetmap.org/wiki/DE:OSMTracker_(Android)

Navit http://www.navit-project.org/

Mit OSM die Welt verbessern http://a-fsa.de/d/1WJ

Freier App Store, F-Droid https://f-droid.org/

Libre Office https://de.libreoffice.org/

CsipSimple, Telefonieren über VoIP https://en.wikipedia.org/wiki/CSipSimple

Linphone, Telefonieren über VoIP http://www.linphone.org/

Open Source App K9-Mail https://k9mail.github.io/

Open Key Chain https://www.openkeychain.org/

VoIP Anbieter, Sipgate https://www.sipgate.de/

Kritik an Facebook Was es an Facebook zu kritisieren gibt, steht hier https://www.aktion-freiheitstattangst.org/de/articles/2532-20111130-facebook-privatsphaere-leitfaden.htm

Messenger Telegram https://telegram.org/faq/de

Das Guardian Project, Orbot https://guardianproject.info/apps/orbot/

Das Guardian Project https://guardianproject.info/apps

GPG App, APG https://f-droid.org/repo/org.thialfihar.android.apg_11199.apk

App Store, APK4fun https://www.apk4fun.com/

App K-9 Mail https://mailbox.org/einrichtung_mit_android_smartphone_und_k9_mail/

Linux Deploy https://technik.blogbasis.net/linux-auf-dem-android-smartphone-parallel-installieren-14-06-2013

Linux Handy Betriebssystem https://www.golem.de/news/ubuntu-canonical-gibt-unity-8-und-smartphone-konvergenz-auf-1704-127171.html

Handy Betriebssystem, Plasma Halium https://www.golem.de/news/plasma-mobile-ein-smartphone-os-von-und-fuer-die-community-1507-115472.html

CyanogenMod, Offenes Android System https://wiki.cyanogenmod.org

Lineage https://www.lineageos.org/

Smartphone rooten https://www.aktion-freiheitstattangst.org/de/articles/6361-20180203-ein-smartphone-rooten.htm

Ein iPhone rooten https://www.mobiflip.de/iphone-jailbreak/