To-Do Liste

Hinweiss:
Gerade Geräte aus China (Xiaomi, Poco, RedMi, Huawei, Realme, Oppo, Lenovo,.....) lassen sich sehr schlecht entkernen und funken trotz aller Mühe, fleißig nach Hause. (Spreche hier auch aus eigener Erfahrung) *1

Der erste Ansatz wäre es, bei der Ersteinrichtung des Gerätes es ohne Google-Konto zu versuchen (oder wenn vorhanden löschen) und bei dem Punkt 2.2 Einzusteigen

1. Bei der Kontoerstellung: (Schwierigkeitsgrad leicht)

1.1 Phantasie - Daten nutzen:

Dabei bitte bedenken, eine kurze Recherche, ob es die Straße, Hausnummer gibt in der Stadt / Ort, das wäre nicht schlecht.

Bei Angabe von Telefonnummer bietet sich der Dienst "Frank geht ran" an (https://digitalcourage.de/frank-geht-ran) Handy: 01631737743 Festnetz: 052116391643 die Betreiber Digitalcourage beschreiben den Dienst so: 24 Stunden im Dienst: Der Anrufbeantworter von Frank hilft, nervige Anrufer.innen loszuwerden. Weitere Fake- Nummern („Filmrufnummern“ oder, „Drama Numbers“) von der Bundesnetzagentur finden sich unter *2 bei dem Punkt "Rufnummern für Medienproduktionen"

1.2 Es empfiehlt sich, alle Einstellungen durchzugehen und alles, was mit Tracking zu tun hat, abzuschalten, auch wenn du dein Konto schon länger nutzt, schau bitte erst recht dein Konto durch. Es lohnt sich, um wieder ein Stück Privatsphäre zurückzugewinnen.

2. Ersteinrichtung des Gerätes:

2.1 Mobilsicher empfiehlt hier, für jedes Gerät ein neues Konto anzulegen (wenn es ohne Anmeldung nicht geht), wenn du nicht als Nutzer wiedererkannt werden möchtest oder ein Kind das Gerät nutzen soll. (mit den zuvor empfohlenen Parametern für ein Google Konto).

2.2 Beim Einrichtungsvorgang gilt es, in Ruhe die Einstellungen durchgehen und was geht abzuwählen. Das reduziert den Output und es fallen weniger Daten an.

! *Bitte auch beachten, viele Hersteller (Samsung, Xiaomi, Nothing,....) fordern euch auf, bei ihnen auch noch ein Konto zu erstellen, um auch in den Genuss ihres Ökosystems zu kommen (Teils eigener App Store, Datenbackup, usw.). Lasst es, so gehen nicht noch zusätzliche Daten an die Hersteller*!

-2.3 Wenn ihr den Sprachassistenten (Google Assistent, Bixbi usw.) nicht benötigt, überspringt es einfach. (Ich empfehle einfach darauf zu verzichten)

- 2.4 Einige Hersteller bieten die Möglichkeit, vorinstallierte Apps abzuwählen, macht davon Gebrauch.

3. Nach der Ersteinrichtung:

- Als Erstes gilt es, ein Blick in die **Schnelleinstellungen** zu werfen, hier Ortungsdienste, Bluetooth und NFC ausstellen.

3.1 Nun geht es weiter in die Einstellungen für das Smartphone:

• Einstellungen» Standort: Alle Schalter aus (ob man Erdbebenanzeige und Notfall-Standortdienst ausschalten will, sollte jeder selbst entscheiden)

• Einstellungen » Google » Anzeigen: Alle Wahlmöglichkeiten bei „Datenschutz bei Anzeigen“ alles ausschalten, vermindert die Treffergenauigkeit bei Anzeigen und Werbung. Nun geht es bei den Punkten „Werbe ID zurücksetzten“ und „Werbe ID Löschen“, vorher bitte einen Schritt zurückgehen. Nun löscht hier beides, damit nehmt Ihr die nächste Gleichung aus dem Spiel.

• Einstellungen » Google » Autofill: auch hier alle Punkte abwählen. Hierfür werden wir später eine bessere Alternative als Passwortmanager installieren.

• Einstellungen » Google» Einstellungen für Google Apps: Google Kontakte synchronisieren alle Punkte abwählen, wir werden uns an einen späteren Punkt und um eine Alternative kümmern. Den Rest sollte man dennoch nochmal durchgehen.

• Einstellungen » Google » Geräte und Teilen: Alle Einstellungen mal durchgehen und was man nicht braucht einfach abwählen

• Einstellungen » Google » Nutzung von geteilten Daten personalisieren: Externe Medien und Kontakte auf dem Gerät abwählen.

• Einstellungen » Apps: Hier bitte mal durchgehen und Apps, die Ihr nicht braucht, löschen / deaktivieren, in einem späteren Teil werden wir Für E-Mails, Dateiverwaltung usw. Datenschutz freundliche Apps mit vergleichbaren Funktionen. An dieser Stelle (danke an Mobilsicher.de) sollte man auch die Zugriffsrechte der Apps prüfen und nicht benötigte Rechte wieder abwählen. Die Apps Google Play-Store, Google Play Dienste / Services, Android System WebView, SIM-Toolkit, und Einstellungen müssen auf dem Gerät bleiben.

Mein Bonustipp: *Geräteeinstellungen nach jedem Update zur Vorsicht mal durchsehen, manche Einstellungen werden hier gern wieder auf Standard gesetzt.*

4. Andere Infrastruktur:

Standardmäßig sind Google Suche, Google Drive und G-Mail als Standard voreingestellt, unser Ziel ist es jetzt, Alternativen zu nutzen, die Datenschutz freundlicher sind und keine Daten an Google (oder auch andere) weitergeben.

Hier gilt der Grundsatz:

„Wenn du nichts für das Produkt zahlen musst, bist du das Produkt“. Heißt E-Mail und Cloud werden uns was kosten, auf der anderen Seite zahlen wir auch bei Google (und auch andere wie Web.de, Gmx, usw.), nur eben mit unseren persönlichen Daten.

4.1 E-Mail: Hier empfehlen sich Deutsche Anbieter mit Focus auf Datenschutz. Zu nennen wären hier Posteo.de, ProtonMail, Mailbox.org, Tutanota. Für die ambitionierten oder technisch interessierten Menschen wäre selbst hosten auch eine Möglichkeit.

4.2 Cloud: Hier gelten die selben Anforderungen wie bei den E-Mails. Nennbare Alternativen wären unter anderen Hetzner, Admin Forge usw., alternative kann man auch selbst hosten, wie unter den Punkt 4.1

4.3 Suchmaschine: Auch hier empfehle ich alternative und Datenschutz freundliche Suchmaschinen. Warum? Vieles, was wir wissen wollen, suchen oder recherchieren wollen, endet meist in einer Suchmaschine, wo wir Daten hinterlassen. Die Frage ist, was will ich preisgeben? Bei Google klar, für personalisierte Werbung und Analyse. Auch empfehle ich nicht: Google, Bing, Yandex und Konsorten.

Meine Alternativen wären: Startpage, SwissCows, MetaGer, Mojeek, Ecosia. Mehr Infos zu dem Thema findet man hier unter *3.

Nicht empfehlenswert sind aus meiner sicht:
DuckDuck Go, zum einen hosten sie Ihren Dienst bei eNom.com, bei Amazon, und zweitens stehen die Server in den USA und unterliegen somit dem Patriot Act.(Quelle Wikipedia *4)

Und Qwant, bedenklich ist, dass der Axel-Springer-Verlag Teilhaber ist, zusätzlich der Mitbegründer Eric Léandri, der nach seinem Ausscheiden ein Unternehmen gründete, das auf digitale Überwachung spezialisierte ist mit dem Namen „Alternative“. (Quelle Wikipedia *5)

5. Alternativer App-Store:

Wie schon angedeutet, kommen wir nun an den Punkt, dass wir App Alternativen brauchen. Der Playstore ist nun unser nächster Punkt, den wir austauschen und auch, wenn man auf einige Apps aus dem Playstore angewiesen sind, werden wir uns später eine Alternative ansehen.

5.1 Was ist ein alternativer App-Store?

Kurz gesagt ein App-Store ist vergleichbar ist mit dem Playstore, nur mit dem gewaltigen Unterschied, dass wir hier trackingfreie und Open Source Apps vorfinden.

Man findet hier neben Alltags- Apps auch viele Dinge, die Google aus gutem Grund nicht listet, wie beispielsweise Werbe- und Trackingblocker, für diesen Appstore gibt es 3 Clients.

Was ist ein Client?

Ein Client ist eure Oberfläche und Zugangstor zu dem F-Droid Angebot. Das könnt ihr, mit sogenannten Paketquellen oder auch Repositorys genannt, erweitern. Für Linux User nichts Neues, für andere eher Neuland. Diese Paketquellen beinhalten ein bis mehrere zusätzliche Angebote an Apps von einem Server eines oder mehreren Appprogrammierern. Ihr erweitert damit euer App Angebot. Aber mit dem gewaltigen Unterschied, dass wir hier trackingfrei unterwegs sind.

5.2 Hier stell ich die Clients Kurz vor:

- F-Droid ist der erste Kandidat und offizielle Client, mit seinem klassischen und etwas in die Jahre gekommenen Aussehen, ist er zwar nicht für jeden Geschmack etwas, erfüllt er aber dennoch seinen Job.

Link: https://f-droid.org/

- Neo Store ist der zweite Kandidat. Er besitzt eine frischer wirkende Oberfläche nach dem Mazerial You Design, eine von Google entwickelten Designsprache. Er besitzt die selben Funktionen wie F-Droid, mit nur mehr Einstellungsmöglichkeiten und mehr Repos mit. Seit seinen letzten Update kann man hier auch Einstellungen und Repo exportieren und importieren.

Link: https://f-droid.org/packages/com.machiav3lli.fdroid/

Droidi-fy ist der letzte Kandidat hier, er ist vom Design her ähnlich wie der NeoStore, mit dem Unterschied, dass er etwas schlichter daherkommt. In meinen Augen bietet dieser Client zwei Vorteile, erstens er ist aktueller als der vorherige Client und wird aktiver weiter entwickelt (Letzte Aktualisierung Januar 2024). Zum zweiten kann man hier seine Einstellungen und Repo exportieren und importieren. Das ist gerade für Menschen ideal, die noch andere Repos hinzufügen und auf neue Geräte mitnehmen wollen. Oder wenn ihr Später anderen Menschen aus euren näherem Umfeld diesen Client auf ein Gerät installiert.

Link: https://f-droid.org/packages/com.machiav3lli.fdroid/

5.3 Wie installiere und nutze ich den Client?

Das ist ganz einfach:

- Einen der oberen drei Clients von der Originalseite herunterladen als APK
- Im Download Ordner Datei suchen, installieren und den Appstore, den du gewählt hast öffnen
- Auf die drei Punkte oben rechts gehen und auf Paketquellen.
- Paketquellen auswählen.

Ich würde diese Quellen empfelen:

F-Droid, Guardien Projekt, Izzy on F-Droid, NewPipe, Collabora Office, Firefox, Molly F-Droid (für Signal Nutzer eine Foss Client Alternative), Fedilab Apps, Cronite

Damit habt ihr schon mal einen guten Start.

- Quellen aktualisieren

Und Ihr seid bereit für den nächsten Schritt.

6. App Alternativen.

In diesen Schritt stelle ich euch einige alternativ Apps für den täglichen Gebrauch vor:

- Alternativer Playstore Client: Aurora Store ist ein inoffizieller FOSS-Client für Google Play, der ohne Konto funktioniert
- Browser: Mull Browser, ein Zweig von Firefox, Fenec Browser, auch ein Firefox Fork. Cromite, ein auf Cromium basierender Browser ohne Googel Code. Er beinhaltet einen integrierten AD Blocker und einige Privacy Features. Alternative geht auch noch Brave, mit einigen Anpassungen (dem Thema „Browser“ widmen wir uns im nächsten Unterpunkt)
- E-Mail: K-9 Mail oder Fair Mail. K-9 ist ein simpler E-Mail Client mit den nötigsten Einstellungen. Fair Mail hingegen bietet eine Vielzahl an Einstellungsmöglichkeiten, wovon es einige nur in der Provariante gibt.
- Kontakte App: ConectYou, Simpel Contacts Pro SE, Open Contacts, Fossify Contacts
- Telefon App: Welefon, Koler, Fossify Telephone

- SMS: S2MSP, DekuSMS, Fossify Message

- YouTube: NewPipe, LibreTube, FreeTube Android, Sky Tube

  wenn diese alternativ Clients einmal nicht gehen, ist Clipious eine gute Fallback Lösung

- Music Player: Metro, Phonograph Plus, Apollo, Odysee Musik Player, Vinyl Music Player, Gramophone, Auxio, Fossify Musik Player, Symphony

- Video Player: VLC, Nova Video Player, Just (Video) Player, Next Player,

- Podcasts: AntennaPod, Escapepod, Podcini

- Rss-Feed: Feeder, Handy Reading, Read You, Capy Reader

- Web-Radio: RadioDroid, URL-Radio, Radioupnp, Transistor

- ÖPVN: Öffi, Transport

- Dateiverwaltung: Material Files, Litle File Explorer, Amaze, Fossify Dateiverwaltung

- Bilder: Aves, Fossify Galarie

- Kalender: Etar, Fokus, Fossify Kalender

- Datenaustausch: LocalSend

- Übersetzer: translateyou, monocles translator, libretranslator

- Tastaturen: HelioBoard, Unexpectet Keyboard, Fossify Keyboard *6

- Kamera: OpenCamera

- Notizen: Noto, Notepad

- Navigations App: Organic Maps, Pocket Maps, GraphHoper Maps, OSMand+

- ToDo Listen.: 1List, OpenToDoList,

- Taschenrechner: Calculator++, OpenCalc, Calculator-Inator

- Audio Recorder: Record You, Audio Recorder, Audio, Fossify Voice Recorder

- Nina Alternative: Foss Warn

- Wetter: omWeather, Kleine Wettervorschau, Clima, QuickWeather, Breezy Weather

- Mediathek: Zapp

! Tipp: *Um einen besseren Gewinn zu haben, empfiehlt es sich unter Einstellungen » Apps » Standard-Apps dort die Voreingestellten Apps, durch eure F-Droid Apps zu ersetzen*!

6.1 Dienste in den Browser verlegen

Versuche Apps von Dienst Anbietern, so weit wie möglich in den Browser zu verlegen (Reduziert die gesammelten Daten). Beispiele wären hier: News, Verkaufsplattformen (E-Bay, Kleinanzeigen, Amazon und Co)

6.2 Browser Sicherer Konfigurieren

Auch der Browser ist ein wichtiger Teil der Privatsphären Strategie.

Vieles recherchieren, lesen oder erledigen wir Tagtäglich im surfen auf dem Smartphone über einen Browser. Um so wichtiger ist es hier, einen Browser zu nutzen, der uns dabei unterstützt. Noch wichtiger ist, unseren Browser auch in den Einstellungen anzupassen und (sofern möglich) einige Erweiterungen (aber auch nicht zu viel) in das Boot zu holen. Ich werde hier für Einstellungen der Browser hier auf den Kuketz Blog verlinken. Bevor wir loslegen, noch ein Hinweis zu dem Thema Einstellungen „Dies sind meine persönlichen Einstellungen, die ich aufgrund meiner Vorlieben, Netzwerkeinstellungen und Infrastruktur vorgenommen habe. Die Einstellungen sollten nicht 1:1 übernommen werden – passt sie an eure Anforderungen an. „(Mike Kuketz) habt das im Hinterkopf:

- Fenec:

Ein Firefox Fork, der etwas mehr auf Privatsphäre getrimmt wurde.

Einstellungen: https://www.kuketz-blog.de/fennec-und-mull-sichere-und-datenschutzfreundliche-android-browser-teil-5/

Hier bis Unterpunkt „3. Fennec“ Scrollen (sofern man etwas mehr über den Browser lesen möchte) ansonsten Direkt zu „3.3 Empfohlene Einstellungen/Add-ons“ Scrollen und die Einstellungen durchgehen.

Empfohlene Add-ons:

- ublock Origin (Werbe- und Tracking-Blocker)
- CanvasBlocker (Verändert einige JS-APIs, um Fingerprinting zu verhindern),
- ClearURLs (entfernt Tracking aus URLs)

- Brave:

  Ein Browser, mit dem Mittelweg zwischen Sicherheit und Datenschutz. Zwar ist sein Sende-verhalten durchwachsen, aber nach den Anpassungen in den Einstellungen bekommt man diese und einige andere Mankos in den Griff. Dafür ist Brave nach den angepassten Einstellungen ,der mit Sicherheit und ausgereifter Fingerprinting überzeugen kann. Wer mehr dazu wissen möchte, siehe unter *7

  Bezugsquelle: Entweder via Aurora Store oder Ihr Installiert euch aus F-Droid FFUpdater, ein Aktualisierungsprogramm für datenschutzfreundliche Browser, und bezieht ihn daraus.

  Einstellungen: https://www.kuketz-blog.de/einstellungen/#brave-android

  Empfohlene Add-ons: -

Wer noch etwas mehr zum Thema „Browser“ erfahren möchte, kann gerne mal einen Blick in die Podcast folge von „Captain it's Wednesday - Folge 107 – Surfhaltung“ werfen. Dort reden Ralf Hersel und ich ausführlich über dieses Thema. *8

6.3 App Berechtigungen Prüfen

Überprüft regelmäßig die Berechtigungen eurer installierten Apps auf dem Smartphone.

Machen kannst du das unter Einstellungen » Apps » Alle Apps und dann kannst du deine Apps durchgehen und anpassen.

Beispiel: Eine Taschenlampen App braucht kein zugriff auf deine Kontakte.

7. Launcher

Launcher ist die Bedienoberfläche eures Smartphones. Hier gibt es eine Vielzahl an Ansätzen. Von minimalistischen, zum üblichen Android Standard gibt es für jeden Geschmack etwas:

7.1 minimalistisch: Aster Launcher, Zext Launcher, Unlauncher, OLauncher, Luna Launcher, mLauncher

7.2 Standard Android Ansatz: Open Launcher, Neo Launcher

7.3 Kiss Prinzip: Kiss Launcher, Monocles Launcher, TiniBit Launcher

7.4 Mal ein etwas anderer Ansatz: PieLauncher, Kvaesito, SmartDock, OXLauncher

8. Apps und Eigeninitiative zur Erhöhung der Privatsphäre (Mittlerer Schwierigkeitsgrad)

Nachdem wir uns nun um einen alternativen Appstore gekümmert haben, den Zugriff auf Datenschutz freundliche Apps haben, wo durch wir unserer Standardapps nun ersetzen können, haben wir schon einiges erreicht.

In den nächsten Schritten geht es darum, wo eine Abhängigkeit auf Apps aus dem Playstore besteht, diese zu isolieren und bei nicht Gebrauch einzufrieren. Im Anschluss werden wir unser Gerät von unnötigen Apps, die vorinstalliert sind, befreien. Zu guter Letzt werden wir dem Tracking sowie der Werbung selbst einen Riegel vorschieben. Zusätzlich werden wir noch durch einige kleine Tricks das Gerät so anpassen, das wir unser Ziel im Anschluss erreicht haben.

8.1 Universal Android Debloater Next Generation

Als nächstes starten wir mit dem Programm „Universal Android Deeploader Next Generation“. Mit diesem Tool entfernt ihr unnütze Apps, die man nicht braucht oder ersetzt hat und sich nicht so einfach vom Gerät entfernen lassen. Geräte, bei denen sich vorinstallierten Apps wie Spiele usw. nicht entfernen lassen, sind nervig, greifen unsere Daten ab und verbrauchen auch im Hintergrund Akku. Der Vorteil ist, dass man gerade als Einsteiger auch hier schon einiges erreichen kann. Die Apps, die man auswählt, werden in einen Tiefschlaf versetzt und eingefroren. Ich werde mich an dieser Stelle etwas kurz halten und an weiterführende Quellen verweisen, mit dem Ihr Euch selbst einarbeiten und dann loslegen könnt.

- Universal Android Debloater Next Generation Download:https://github.com/Universal-Debloater-Alliance/universal-android-debloater-next-generation/releases
- Tutorial (Video) 1: https://youtu.be/GKzxWjURuMo
- Tutorial (Video) 2: https://youtu.be/7lK-cwM_Wmc
- Tutorial (Webseite) 2: https://www.heise.de/news/c-t-3003-Vorinstallierte-Schrott-Apps-loeschen-mit-Universal-Android-Debloater-7131487.html
- Tutorial (Webseite) 3: https://tarnkappe.info/tutorials/universal-android-debloater-der-bloatware-hoelle-den-kampf-ansagen-265572.html

- Tutorial (Webseite)4: https://gnulinux.ch/google-apps-und-weitere-bloatware-loswerden-mit-dem-universal-android-debloater-next-generation

8.2 Passwortmanager

Als Passwortmanager empfiehlt sich Keepass DX, da dies Lokal und verschlüsselt auf dem Endgerät abgelegt werden kann. Nehmt euch Zeit, um diese App kennenzulernen.

Für die technisch etwas versierteren Teilnehmer/ Leser bietet es sich vielleicht an, auch selbst einen Passwortmanager zu Hosten wie z.B. Vaultwarden. Mehr zu diesem Thema findet ihr weiter unten (Vortrag aus dem Gulga Nürnberg)*9

8.3 UntrackMe

Um unseren täglichen Verhalten datenschutzfreundlicher zu gestalten, empfiehlt es sich noch UntrackMe zu installieren und einzurichten.

Was macht UntrackMe?

Diese App leitet, wenn sie eingerichtetet ist, auf Open-Source-Alternative Server für Twitter, YouTube, Instagram, Reddit, Wikipedia und Google Maps um. Auf diese Weise wird sichergestellt, dass der Datenabfluss geringer wird.

8.4 Shelter oder Insular

Für den nächsten Schritt instalieren wir die App Shelter (alternativ gibt es noch Insular). Anschließend Starten wir die App, womit uns ein Arbeitsprofil eingerichtet wird. Der Vorteil besteht darin, dass wir nun ein zweites Profil nutzen, mit dem wir das oben erwähnte umsetzen.

Hinweis: Shelter bietet keinen Schutz vor Tracking oder Datenabgriff durch nicht vertrauenswürdige Apps, sondern sorgt dafür, dass diese Apps keinen Zugriff auf die normalen Daten wie Kontakte, Kalender & Co haben. Der Entwickler weist zudem auf den Umstand hin, dass Shelter keine Sandbox ist. Die App schützt also nicht vor Sicherheitslücken in Android oder dem Kernel und Hintertüren (Backdoors) in der Android ROM betreffen auch Shelter.*10

Anleitung:

Nach dem Start der App, wird auf dem Gerät, wie schon gesagt, ein Arbeitsprofil angelegt, was je nach Smartphone eine Weile dauern kann. Im Anschluss installieren wir uns den Aurora App Store. Mit diesem können wir ohne Anmeldung und anonym die Apps, die wir benötigen aus dem Playstore beziehen. Aber das machen wir erst hinterher. Nach der Installation öffnen wir Shelter und klicken auf den Aurora App Store und gehen auf Klonen zu Shelter. Anschließend möchte die App das Recht zur Installation von Apps eingeräumt bekommen, diese wird zur Installation in das Arbeitsprofil benötigt. Bevor wir weitermachen, werfen wir kurz einen Blick in die Einstellungen. Dort setzen wir einen Haken bei „Blockiere Suche nach Kontakte“ und „Auto-Frost Dienst“. Nun gehen wir in das Arbeitsprofil (unten Links, wo Shelter steht), drücken auf den Aurora-Store und gehen auf Starten. Nun gehen wir durch den Startvorgang. Bei dem Punkt „Anmelden mit“ bitte anonym wählen. Und alle, die noch dem Vortäuschen eines drauf setzen wollen, können unter den Einstellungspunkt Vortäuschen, ihr Smartphone als ein anderes Ausgeben.

Nun könnt Ihr alle Apps, auf die ihr angewiesen seid, installieren. Nun ist noch ein Punkt wichtig, alle installierten Apps müsst ihr nun durchgehen, anklicken und den Haken bei „Autofrost“ setzen. Dadurch könnt ihr all Apps mit einem Klick, oder wenn ihr den Bildschirm sperrt, dann einfrosten. bedeutet, diese Apps laufen dann nicht. Wenn ihr sie braucht, könnt ihr sie mit dem Punkt „Auftauen und Starten“ wieder starten. Wichtig ist nur, wenn ihr diese Apps auf Updates prüfen wollt, müsst ihr sie in Shelter alle auftauen und dann via den Aurora App Store updaten. Anschließend könnt ihr mit dem Autofrost Symbol alle wieder schlafen legen. Wichtige Regel ab jetzt, Apps aus dem F-Droid Store können regulär installiert werden, nur Apps aus dem Playstore werden via Shelter in Isolationshaft geschickt und bei nicht Gebrauch gefrostet. An dieser Stelle haben wir eine weitere Etappe erreicht.

8.5 AdAway

Unser nächster Schritt an dieser Stelle ist die App AdAway (oder auch personalDNSfilter).

Hiermit schicken wir unseren Datenverkehr durch einen Filter, den wir durch verschiedene Listen aufbauen.

Anleitung :*Quelle 11

Als erstes Installieren wir AdAway aus dem F-Droid Store. Anschließend starten wir die App und wählen „VPN-basierender Ad-Blocker“ aus. Im nächsten Schritt bestätigen wir die Verbindungsanfrage via VPN. Nun könnt Ihr selbst entscheiden, ob ihr Telemetrydaten an den Entwickler senden wollt, oder nicht. Standardmäßig ist es nicht ausgewählt. Im Anschluss aktualisieren sich die Filterlisten erst einmal automatisch.

Nun geht es weiter in den Einstellungen, dahin gelangen wir über die drei Striche (Hamburger Menü) und gehen dann auf Einstellungen. Hier aktivieren wir erst mal „IPv6 aktivieren“. Anschließend konfiguriert ihr den Punkt „Automatische Updates“ nach euren Wünschen. Unter den Punkt „VPN basierender Ad-Blocker“ unter Allgemein würde ich beide Punkte aktivieren.

Der nächste und abschließende Punkt betrifft die Filterlisten. Mit Klick auf den mittleren Kasten „Quellen“ hier kann man noch zusätzliche Quellen hinzufügen über das +. Mike Kuketz empfielt diese noch zwei zusätzlichen Listen:

https://github.com/StevenBlack/hosts#list-of-all-hosts-file-variants

https://github.com/badmojr/1Hosts#1hosts-pro

Wer möchte, kann natürlich selbst noch einige recherchieren. Wichtig ist jedenfalls eine Blockliste für euren Smartphonehersteller einzurichten. Schließlich wollen sie ja auch Nutzerdaten sammeln. Im Gebrauch der App im Hintergrund kann es passieren, dass einige Dienste nicht mehr sauber laufen, das nennt man Overblocking und ist im ersten Betrieb normal. Da muss man dann eben selbst Hand anlegen. Ich lasse hier den schon erwähnten Mike Kuketz zu Wort kommen:

Wie bereits angedeutet kann das Phänomen des Overblockings eintreten, was unter Umständen dazu führen kann, dass eine App/Website bzw. bestimmte Funktion nicht mehr korrekt funktioniert. Persönlich konnte ich das bisher nicht beobachten – allerdings bin ich diesbezüglich auch nicht der geeignete Maßstab, da ich gezielt auf Dienste von Google, Facebook und Co. verzichte.

Sollte eine App/Website also nicht wie gewohnt funktionieren, solltet ihr zunächst über den Menüpunkt DNS-Abfrage-Protokoll anzeigen die Berichtsfunktion aufrufen. Aktiviert dann die Aufzeichnung und startet anschließend jene App, die nicht korrekt funktioniert. Anschließend öffnet ihr erneut die Berichtsfunktion. Alle protokollierten DNS-Anfragen werden euch dann aufgelistet. Im nachfolgenden Beispiel habe ich den DB-Navigator der Deutschen Bahn gestartet, der bekanntlich einige (illegale) Tracker integriert hat. Diese werden alle zuverlässig von AdAway bzw. den hinterlegten Filterlisten blockiert. Nachfolgend erlaube ich beispielhaft die Tracking-Domain »firebase-settings.crashlytics.com«, indem ich auf das Häkchen in der Mitte tippe. Diese Auswahl wird sich AdAway anschließend merken und die Domain auf die Positivliste setzen bzw. nicht mehr filtern.

Über den Hauptscreen könnt ihr mit einem Fingertipp auf den mittleren Bereich (Gestattet) eigene Domains hinterlegen, die anschließend von der Filterung ausgeschlossen werden. Am unteren Displayrand könnt ihr zwischen verschiedenen Ansichten wechseln:

- Blockiert: Zu den bereits bestehenden Domains könnt ihr weitere hinzufügen, die AdAway blockieren soll. Das ist gewissermaßen eine Ergänzung zu den bereits bestehenden Filterlisten, die ihr selbst beeinflussen könnt.
- Gestattet: Wie bereits aufgezeigt, kann es unter Umständen zum Overblocking-Effekt kommen. Falls dies eintritt, könnt ihr eine Domain über die Positivliste wieder erreichbar machen.
Die Positivliste gilt immer vor den Filterlisten – die Domain ist also wieder erreichbar, wenngleich sie in einer der Filterlisten enthalten ist.
- Umgeleitet: Bei Bedarf könnt ihr für bestimmte Domains IP-Umleitungen aktivieren. Die Domain »facebook.com« könntet ihr bspw. auf die IP-Adresse 130.211.198.204 (disney.com) zeigen lassen. Ruft ihr die Domain »facebook.com« anschließend im Browser auf, werdet ihr auf disney.com umgeleitet.

( )

Wichtig ist darauf zu achten, dass AdAway eben auch aktiv ist, auf euren Smartphone.

Für technisch versiertere Menschen gibt es auch die Möglichkeit Zuhause ein Pi-Hole / AdGuard Home / E-Blocker in das Netzwerk mit einzubinden und Via VPN das Smartphone im heimischen Netz zu Belassen. Auch hier findet ihr zu dem Thema mehr weiter unten (Vortrag aus dem Gulga Nürnberg)*12

Damit haben wir nun das getan, was man bei einem Standard Android Handy machen kann. Der letzte Sprung wäre nun noch auf einen Custom Rom ohne Google, ein alternatives Betriebssystem für eure Geräte, aber das würde den Rahmen sprengen und bräuchte einen Workshop für sich selbst.

9. Abschließende Tipps:

- Für den letzten Feinschilf solltest du auch das Captive-Portal ändern. Mit dem Captive-Portal-Check will Android sicherstellen, dass ein Gerät nicht nur eine IP-Adresse vom Access Point bzw. Internet Service Provider erhalten hat, sondern auch tatsächlich Ziele im Internet erreichen kann. Wie das geht, findest du hier: https://www.kuketz-blog.de/empfehlungsecke/#captive-portal
- Setze zuerst auf Apps aus der F-Droid, bevor du aus dem Aurora (Playstore) die eine App nutzt
- Überlege dir in welchen sozialen Netzwerken du dich bewegst. Auch Meta (Instagramm, Facebook und Whatsapp) und Co Sammeln Daten über dich.
- Brauchst du wirklich WhatsApp? Oder ist nicht ein Messenger wie Signal, Matrix und Co nicht die bessere Alternative?
- Nutze nur Apps, die du wirklich brauchst.
- Mach dir bewusst, was du an digitaler Freiheit gewonnen hast und feiere es.
- Informiere dich weiter zu diesem Thema und bleib informiert.

Einzelnachweise

*1 Quellen:

https://gnulinux.ch/datensparsames-android-mit-der-android-debug-bridge-teil-3-weitere-geraete-und-plattformen

https://dspace.networks.imdea.org/bitstream/handle/20.500.12761/618/imc18-final148.pdf

*2 https://www.bnetza.de/DE/Sachgebiete/Telekommunikation/Unternehmen_Institutionen/Nummerierung/Rufnummern/Rufnummern_node.html#doc268386bodyText4

*3 Suchmaschienen: https://gnulinux.ch/artikelindex?search=Suchmaschinen

*4 DuckDuckGo: https://de.wikipedia.org/wiki/DuckDuckGo

*5 Qwant: https://de.wikipedia.org/wiki/Qwant

*6 Tastaturen:
https://gnulinux.ch/tastatur-serie-alternative-smartphone-tastaturen-das-versp%C3%A4tete-intro

https://gnulinux.ch/artikelindex?search=Tastatur+Serie

HeliBoard: Android Tastatur Empfehlung:
https://www.kuketz-blog.de/heliboard-android-tastatur-empfehlung/

*7 Quellen:
Fingerprinting: https://de.wikipedia.org/wiki/Fingerprinting_(Trackingtechnik)

https://www.kuketz-blog.de/brave-browser-warum-ich-ihn-gecko-basierten-browsern-firefox-vorziehe/

*8 Captain it's Wednesday - Folge 107 – Surfhaltung:

https://gnulinux.ch/ciw107-podcast

*9 Vaultwarden:

Script:

https://wiki.gluga.de/talks/Vaultwarden-Vortrag.pdf

Befehle: https://notebin.de/?52ae98d8e5105403#3Uoz2tymSSQ12pC4pWuMzxJpsycqJhkifUK3hr27v5DH

Aufzeichnung:

https://live-23.lusc.de/playback/presentation/2.3/c4e835f8f86ad67945f1b61ab0fe880143b1fdde-1675269427763

*10 Quelle:
https://www.kuketz-blog.de/shelter-big-brother-apps-isolieren-take-back-control-teil7/

*11 Quelle:
https://www.kuketz-blog.de/adaway-werbe-und-trackingfrei-im-android-universum/

*12 Mobil sicher unterwegs mit Werbeblocker

Script:
https://wiki.gluga.de/talks/Vortrag_mobil_sicher_unterwegs_mit_Werbeblocker.pdf

(PeerTube) Video :
https://tube.tchncs.de/w/6ytKyckAaz3WyBvPFtvv3p

Weiterführende Links zum Thema:

Fakenummern:

- Frank Geht Ran:

  https://digitalcourage.de/frank-geht-ran

- Bundesnetzagenturen Drama Nummer:

  https://www.bnetza.de/DE/Sachgebiete/Telekommunikation/Unternehmen_Institutionen/Nummerierung/Rufnummern/Rufnummern_node.html#doc268386bodyText4

- Ich habe doch nichts zu verbergen, Gegenargumente:

  https://www.kuketz-blog.de/empfehlungsecke/#verbergen

- Privacy Handbuch:

  https://privacy-handbuch.de/

- Smartphone, don't spy!

  https://smartphone-dont-spy.de/

- Mobilsicher:
  https://mobilsicher.de/

- AppCheck von Mobilsicher:
  https://appcheck.mobilsicher.de/

- 30 saubere App-Empfehlungen aus dem F-Droid Store (Mobilsicher):
  https://mobilsicher.de/ratgeber/fdroid-app-empfehlungen

- Empfehlungsecke Kuketz Block:
  https://www.kuketz-blog.de/empfehlungsecke/

- Befreie dein Android
  https://fsfe.org/activities/android/android.de.html

Podcasts / Videos zum Thema

- Dem Sozialen Dilemma entkommen (Podcast)
  https://lcdn.letscast.fm/media/podcast/8674e934/episode/bc70bfe0.mp3?t=1705675147

YouTube-Videos:

- Callcenter Abzocke - Die negativen Seiten von Google, welche sicheren Alternativen gibt es – Infovideo:
  https://video.fosswelt.org/watch?v=B2qSHEpUO0A

- PrivacyTutor - Die dunkle Seite des Internets: Wie deine Daten verkauft werden
  https://video.fosswelt.org/watch?v=EztDDd8xYlo

- Weltmacht Google - Wie ein Konzern unser Leben beeinflusst

  https://video.fosswelt.org/watch?v=zb7jw-VVdl8

- MrWissen2go - Die Wahrheit über Google [feat. @SoManyTabs]

  https://video.fosswelt.org/watch?v=3ZXGvYQI5Y8

YouTube Playlists:

- FrickelFieber Datenschutz - Datensicherheit - Privatsphäre Der Weg zum Googlefreien Handy:

  https://www.youtube.com/playlist?app=desktop&list=PLK9le4FHfUsykHPzR-vYLLbV-NRxNRHEY&cbrd=1&ucbcb=1

- Mobilsicher mit Inga:

  https://youtube.com/playlist?list=PLJvgFtvC0MwxDas-hzfr51PLZyMJT5OKS

- fosstopia (MichelFranken) Android:

  https://youtube.com/playlist?list=PLy1PHp-EWtxNYl1aPMSC4rZWDwTmm_QSE