Secure Smartphones

Secure Smartphones

Secure Smartphones

Mikro-Einführung, Lamberto Grippi

LineageOS

Ist ein ent-Googletes Android. Soweit wie möglich wurden die Verbindungen zu Google entfernt. Ohne Google-Layer gibt es keine Push-Notifications. Einige Apps sind jedoch von Google abhängig und funktionieren schlecht oder starten gar nicht. Deshalb empfiehlt es sich LineageOS mit MicroG zu installieren. MicroG simuliert quasi Goolge, damit Apps, die darauf angewiesen sind, funktionieren. In MicroG kann man sich beim Google-Store anmelden und das Smartphone registrieren (Device Registrierung) um die Push-Funktion zurückzubekommen. Es können granulare Einstellungen vorgenommen werden und somit nur einzelne Apps für die Registrierung auswählen. Viele Apps (z.B. Telegram, Fairemail) arbeiten auch ohne Device-Registrierung, weil sie im Hintergrund die Verbindung zum Provider offen halten und notifizieren sobald eine Nachricht eintrifft. Andere Apps (z.B. Threema) kann man so konfigurieren, dass sie regelmässig nach neuen Nachrichten pollen.

LineageOS gibt es für sehr viele Smartphones als Image-Datei mit entsprechender Installationsanleitung:

- Lineage ohne MicroG
- Geräte
- Lineage mit microG

/e/OS

Basiert auf LineageOS und kommt mit bereits vorinstalliertem MicroG daher. Die Entwickler haben sich auf die Fahne geschrieben ein ent-googletes Android bereitzustellen. Sie bieten ähnliche Cloud-Dienste wie Goolge an, sind aber für den einwandfreien Betrieb nicht notwendig.

/e/OS gibt es für sehr viele Smartphones als Image-Datei mit entsprechender Installationsanleitung. Ausserdem kann man Smartphones mit vorinstalliertem /e/OS kaufen:

- eFoundation
- eSolutions Shop

Weitere Infos

Viele Apps findet man im alternativen App-Store F-Droid. Es ist auch möglich Apps aus dem offiziellen Google-Store (z.B. Aurora) zu installieren. Selbst kostenpflichtige Apps (z.B. Fairemail, NetGuard, Threema) können bezogen werden. Dafür muss man sich mit dem jeweiligen Entwickler direkt in Verbindungen setzen.

Es existieren noch weitere Android-Alternativen:

Open Source Alternativen

AFWall+

Einige Apps bauen trotz Allem weiterhin unerwünschte Verbindungen auf. Dies kann mit einer lokalen Firewall überwacht und unterbunden werden. AFWall+ basiert auf IPtables und benötigt Root-Rechte.

NetGuard

Falls keine Root-Rechte vorhanden sind, empfiehlt sich NetGuard zu installieren. Diese App richtet ein lokales VPN ein und leitet sämtlichen Traffic durch den Tunnel. Somit können z.B. Tracker ausfindig gemacht und blockiert werden. Will man mit dem Smartphone einen weiteren VPN aufbauen, wird der bestehende NetGuard-Tunnel unterbrochen, weil i.d.R. nur ein einziger Tunnel aktiv sein kann.

Links

Mike Kuketz beschäftigt sich seit Jahren mit IT-Sicherheit und Datenschutz. Er veröffentlicht regelmässig interessante und kritische Blogs/How-Tos zu Android und vielen weiten Themen.

Kuketz Blog

Mobilsicher beschäftigt sich ebenfalls mit dem Schützen des Mobiltelefons und führt eine Datenbank in welchen ca. 30000 Apps nach Privacy-Grad kategorisiert sind.

Mobilsicher

Fazit

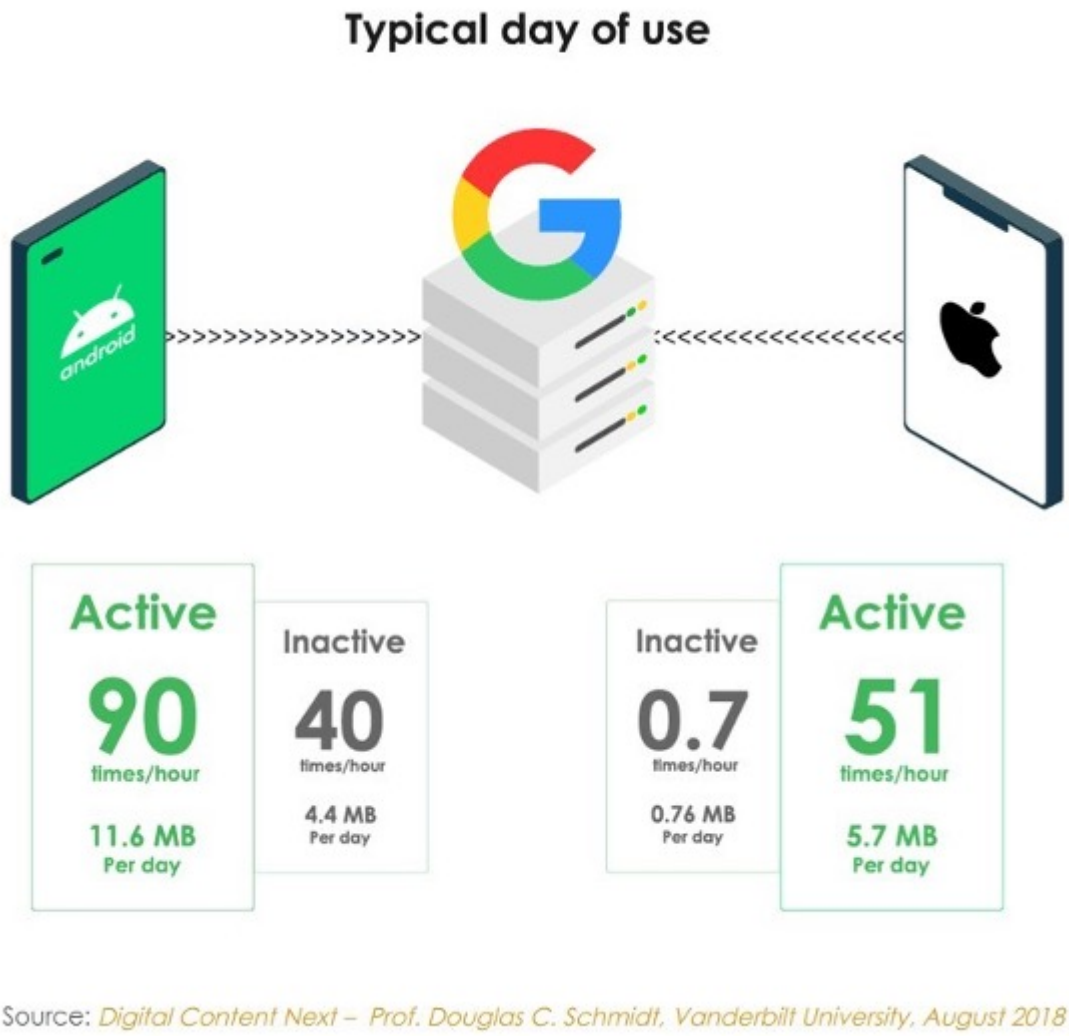
Wenn man bereit ist Zeit in die Installation zu investieren, ist LineageOS sicher die richtige Wahl. /e/OS basiert zwar auf LineageOS, man macht sicher aber von einem Hersteller abhängig. Ausserdem erscheinen Updates verzögert.

Wenn man auf die Google-Dienste angewiesen ist und nirgends Abstriche machen möchte, ist es besser bei Android zu bleiben.

Free Smartphone

Freiheitshandy - Warum ?

Smartphones sind mit Trackern und Software ausgestattet, die den Benutzer überwachen und unnötig viele Informationen an die Hersteller senden. Eine Grafik veranschaulicht das:



Source: *Digital Content Next – Prof. Douglas C. Schmidt, Vanderbilt University, August 2018*

Das Problem liegt nicht am Smartphone selbst, sondern an dem mitgelieferten Betriebssystem – Android oder iOS. Um die Überwachung zu beenden benötigt es ein Betriebssystem, das keine Daten aussendet. Bei einer Recherche stößt man tatsächlich auf eine Reihe von sog. OpenSource und de-googelten Alternativen. Bei tieferen Recherchen und eigenen Test stellt man schnell fest, dass die meisten Alternativen für Enthusiasten und Entwickler geeignet sind, aber völlig ungeeignet für normale Benutzer. Tatsächlich gibt es nur zwei bzw. drei Alternativen:

- GrapheneOS
- Lineage (/e/OS)

Versucht man ein Smartphone mit einem dieser drei Betriebssysteme bei einem Händler zu kaufen, stellt man fest, dass keine Smartphones mit Lineage verkauft werden. Man benötigt ein kompatibles Smartphone und danach muss man selber das Betriebssystem installieren. Das erfordert vergleichsweise tiefe technische Kenntnisse.

eFoundation

Die eFoundation bietet jedoch /e/OS vorinstalliert auf einem Smartphone an. Die Liste der kompatiblen Typen ist lang – mehr als 100 Geräte https://doc.e.foundation/devices. Allerdings bietet die eFoundation nur 5 Geräte out of the Box – also mit dem Betriebssystem zusammen – an:

https://esolutions.shop/

eFoundation bietet ein rundum Paket an:

- Support und updates garantiert für mehrere Jahre
- volle Kompatibilität mit Android Apps
- Ökosystem basierend auf nextCloud mit Email Account, Kalender, Dateispeicher, Adressverwaltung, Office Paket

Die Benutzung der eCloud ist optional. /e/OS basiert zu 100% auf Lineage. Es gibt zwei Unterschiede:

- microG vorinstalliert (Push notifications)
- Die Bedieneroberfläche (GUI) wurde so umgestaltet, dass sie wie iOS aussieht.

Nitrokey

Die deutsche Firma Nitrokey bietet zwei Smartphones mit vorinstalliertem GrapheneOS an:

https://shop.nitrokey.com/de_DE/shop

Die Benutzerobefläche ist nahezu identisch zu dem bekannten Android OS von Google. Neben den Smartphone bietet Nitrokey andere, sehr interessante Produkte aus dem Bereich Security an.

Nachteile:
Der Zugriffsschutz (als bei dem iPhone FaceID) ist deutlich unsicherer. Es wird Passwort und Fingerabdruck angeboten.
Einige Komfortfunktionen fehlen, z.B. Diebstahlschutz. Dies muss mit Hilfe von Apps manuell nachgerüstet werden.
Ich habe das Fairphone 4 mit /e/OS getestet. Der Fingerabdruckscanner ist per se nicht sicher und er ist an einer Stelle am Smartphone eingebaut, die eine sinnvolle Benutzung für mich nicht möglich machten. Daher habe ich fast immer mein Passwort verwendet, um mich anzumelden.

Migrationspfad

Android Smartphone → Nitrokey GrapheneOS (2 Modelle zur Auswahl) iPhone → eFoundation Smartphone mit /e/OS (5 Modelle zur Auswahl)

Erste Schritte

Nach dem Auspacken und Einschalten des Gerätes läuft eine Initialisierungsroutine ähnlich dem iPhone ab. Man muss Name, eMail Adresse und ein paar andere Eingaben tätigen. Optional kann man hierbei die eCloud konfigurieren (wenn man ein /e/OS Handy hat). Oder später eine andere Lösung konfigurieren.

Nach Beendigung der Initialisierung sollte man sofort den Appstore aufsuchen. Der heißt schlicht „Apps“ (wenn man ein /e/OS Handy hat). Die Bedienung ist sehr ähnlich zum Playstore oder dem AppleStore. Dort installiert man zwei Applikationen: F-Droid und Aurora. Alle weiteren Applikationen sollten aus diesen beiden zusätzlichen Appstores installiert werden. Primär aus F-Droid. Dort befinden nur geprüft de-googelte Applikationen. Wird man dort nicht fündig, kann man mit Aurora auf den kompletten Playstore von Google zugreifen. Aurora bietet einen anonymen Zugriff auf den Playstore, d.h. es müssen keine Benutzerinformationen bei Google hinterlegt werden.

Addtional links

Link Liste

https://itsfoss.com/linux-phones/

https://itsfoss.com/android-distributions-roms/

https://www.heise.de/ratgeber/Wie-Sie-Android-und-Apps-datensparsam-nutzen-6619662.html

https://www.heise.de/ratgeber/Security-Android-Smartphone-vor-unkontrollierten-Datenabfluessen-absichern-6613079.html

https://copperhead.co/android/

https://www.heise.de/select/ct/2023/2/2231213554550974365

Shops

Nitrokey Shop

https://liberateyourtech.com/

https://privatephoneshop.com/

Huawei

Der Huawei-Bann von 2019: Auswirkungen und Hintergründe

Im Mai 2019 setzte die US-Regierung Huawei auf die „Entity List“, was amerikanischen Unternehmen den Handel mit Huawei ohne Genehmigung untersagte. Die Begründung lag in nationalen Sicherheitsbedenken, insbesondere der Möglichkeit, dass Huawei-Technologie für chinesische Spionage genutzt werden könnte. Konkrete Beweise dafür wurden jedoch nie öffentlich vorgelegt. Während der Bann Huawei Milliarden kostete und die Entwicklung verlangsamte, profitierten US-Technologiefirmen erheblich.

Ein Vergleich

Der Fall Cisco in den 2000er Jahren zeigt einen klar bewiesenen Sicherheitsverstoß: Manipulierte Hardware wurde in Netzwerken der US-Regierung entdeckt, die absichtlich verändert wurde, um Zugang zu sensiblen Daten zu ermöglichen. Im Gegensatz dazu basiert der Vorwurf gegen Huawei weitgehend auf Vermutungen. Im Fall der Afrikanischen Union (2018) gab es Berichte über angebliche Datenübertragungen nach China, doch es wurden keine manipulativen Hardwareeingriffe nachgewiesen. Dieser Vergleich zeigt, dass die Huawei-Bedenken zwar ernst genommen werden, jedoch weitgehend auf hypothetischen Risiken und geopolitischen Spannungen basieren, anstatt auf klar belegten Vorfällen.

Dieser Vergleich verdeutlicht, wie unterschiedlich die Gewichtung von belegten Sicherheitsrisiken und unbelegten Befürchtungen sein kann, und unterstreicht den erheblichen Einfluss von wirtschaftlichen und geopolitischen Interessen auf solche Entscheidungen.

Vergleich von Datentransfers: Huawei P70, Android und iPhone

In einer Studie von Prof. Douglas C. Schmidt (Vanderbilt University, August 2018) wurde der Datenverkehr von Android-Smartphones und iPhones verglichen. Android-Geräte senden durchschnittlich 40 Mal pro Stunde Telemetriedaten, während iPhones dies nur 0,7 Mal pro Stunde

tun. Ein Test mit dem Huawei P70, betrieben mit HarmonyOS, zeigte ähnlich niedrige Übertragungsraten wie beim iPhone. Bemerkenswert ist, dass alle vom Huawei initiierten Verbindungen verschlüsselt waren und keine Daten nach China flossen; stattdessen wurden alle Verbindungen zu deutschen Telekom-Servern aufgebaut.

Technische Schlussfolgerung zur Privatsphäre

Die Testergebnisse legen nahe, dass HarmonyOS nicht nur datenschutzfreundlich agiert, sondern auch durchgängig verschlüsselte Datenübertragungen verwendet, was den Schutz vor unbefugtem Zugriff erheblich erhöht. Im Gegensatz zu vielen Android-Geräten, die häufig Telemetriedaten an Server weltweit senden, beschränkt sich HarmonyOS auf wenige, gut kontrollierte Datenübertragungen, die zudem ausschließlich an Server in Deutschland gesendet werden. Dies deutet darauf hin, dass Huawei mit HarmonyOS einen hohen Standard in Bezug auf Datenschutz und Datensicherheit setzt, was insbesondere für Nutzer, die ihre Privatsphäre schützen möchten, von Vorteil ist.