

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 Google, 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 Google 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.

Revision #2

Created 10 December 2023 21:11:18 by Admin

Updated 18 February 2024 14:44:05 by Admin