attac

Instant Messaging

Infoblatt für Attac-Gruppen und AktivistInnen

Instant Messaging (Sofortnachrichten-Dienst) ist eine Art der digitalen Kommunikation (Chat), bei der sich zwei oder mehrere Teilnehmer*innen per Textnachrichten unterhalten. Manchmal wird ein Sofortnachrichten-Dienst in Aktivist*innengruppen zur schnellen Kommunikation eingesetzt. Viele Dienste bieten heute sogenannte „Ende-zu-Ende-Verschlüsselung“, allerdings ist diese oft nicht überprüfbar, da der Quellcode der Anwendungen nicht verfügbar ist. Der Dienst *Telegram*, den viele von uns bisher genutzt haben, ist nicht Ende-zu-Ende-verschlüsselt. Alle Nachrichten werden zentral gespeichert, und somit ist die komplette Kommunikation abrufbar. *Telegram* hat seine Datenschutz-Bestimmungen verkompliziert und nennt nun auch explizit die Möglichkeit der Datenweitergabe (mehr dazu unter: https://steigerlegal.ch/2018/09/11/telegram-datenschutzerklaerung/)

Wir empfehlen daher ausschließlich Signal (https://signal.org/) einzusetzen, das ist sicherer.

Damit ihr unsere Empfehlung besser nachvollziehen könnt, hier eine **Gegenüberstellung:**

Signal

Signal ist ausnahmslos Ende-zu-Ende-verschlüsselt, wobei nicht einzelnen Identitäten, sondern einzelnen Geräten vertraut wird. Die Verschlüsselung ist deutlich ausgefeilter als bei anderen Diensten. Der Server (oder sonst jemand) kann keine Nachrichten lesen, sondern diese nur zwischenspeichern und zustellen. Dabei muss eine Nachricht für jedes empfangende Gerät extra verschlüsselt werden. Nach der Zustellung existieren diese Nachrichten nur noch auf den jeweiligen Geräten. Bei *Signal* ist immer ein Smartphone (Android, iOS) das Haupt-Gerät, über das desktop clients hinzugefügt und entfernt(!) werden können. Medien werden ausschließlich lokal gespeichert, das kann bei Geräten mit wenig Speicher für Probleme sorgen.
Signal unterstützt verschwindende Nachrichten. Die Nachricht bekommt also ein Ablaufdatum und das empfangende Gerät ist dafür verantwortlich, die Nachricht nach Ablauf des Datums zu löschen. So kann zumindest die Menge Nachrichten minimiert werden, sollte ein Gerät einmal in die falschen Hände gelangen. Der lokale Speicher kann mit einem App-Passwort verschlüsselt werden, was insbesondere auf Geräten mit unverschlüsseltem Speicher, Geräten mit alter Software, aber auch generell (stichwort Meltdown) empfehlenswert ist. Signal bzw. Open Whisper Systems (OWS), hat ein nachvollziehbares Geschäftsmodell, nämlich den Verkauf und die Anpassung dieses Protokolls, das trotzdem open source ist (!), z. B. an Facebook (Whatsapp) und Microsoft (Skype). Ob OWS gemeinnützig ist konnte ich auf die Schnelle nicht feststellen. In der Vergangenheit haben sie sich jedenfalls durch Spenden finanziert.

Telegram

Bei *Telegram* werden standardmäßig alle Nachrichten und Dateien auf dem Telegram-Server (ziemlich sicher unverschlüsselt) gespeichert. Daraus ergeben sich folgende Funktionen, die bei Signal so nicht gehen. Diese Funktionen weisen auch bei anderen Diensten auf eine unzulängliche Verschlüsselung hin:

- Nahtlose Synchronisation zwischen beliebig vielen Geräten pro Benutzer*in
- Ein nichts vergessendes gut durchsuchbares Archiv auch auf ganz neu angemeldeten Geräten
- Die Möglichkeit Nachrichten nach Versand am empfangenden Gerät zu löschen oder zu editieren
- Die Möglichkeit, Medien/Dateien vom lokalen Gerät zu löschen, aber trotzdem noch abrufen zu können.
- Die Möglichkeit für Geheimdienste zentral mitzulesen.

Sicherheit gibt es bei *Telegram* nur durch die "Transportverschlüsselung", also dass der Kommunikationskanal zum Server verschlüsselt ist. Die Nachrichten an sich sind nicht verschlüsselt. (Ein "geheimer Chat" kann geöffnet werden, dann fallen die oben genannten Vorzüge weg. Leider ist aber die Schwäche der Verschlüsselung schon wissenschaftlich belegt worden). Telegrams Geschäftsmodell dürften wohl Kundendaten und Payment-Dienstleistungen sein bzw. werden. Die Entwicklung wurde vom russischen Mark Zuckerberg, Pavel Durov, angestoßen. Nach eigenen Angaben sind sie gemeinnützig, es ist aber eine normale (https://de.wikipedia.org/wiki/Telegram#Geschichte_und_Hintergr%C3%BCnde).

zusammengestellt von Martin Mayr, Herbst 2018