

Schluss mit Facebook: Fünf WhatsApp-Alternativen im Überblick

Es gibt viele Gründe, WhatsApp abzulehnen. Die richtige Messaging-Alternative zu finden, ist aber alles andere als leicht.

Es gibt kaum eine App, die im Leben so vieler Menschen eine Rolle spielt wie WhatsApp. 2009 von Jan Koum und Brian Acton gegründet, entwickelte sich der Dienst rasant zu einer Konkurrenz für SMS und andere Messenger, die auf veraltete Protokolle setzten. Zu Beginn war die Anwendung nicht mehr als eine Art schwarzes Brett für Statusmeldungen. Nutzer konnten ihre Gedanken posten, Freunde hatten die Möglichkeit, diese Meldungen zu lesen. Mit der Zeit verwandelten die Entwickler ihre Erfindung in einen Kurznachrichtendienst.

Die Vorteile von WhatsApp damals lagen auf der Hand: plattformübergreifende Kommunikation mit dem Smartphone und das auch noch kostenlos. Eine einfache Registrierung und der ebenfalls mögliche Austausch von Fotos und Videos taten das Übrige dazu. Seitdem ist viel Zeit vergangen und in der Welt von WhatsApp hat sich einiges getan. Nach der Übernahme durch Facebook für 19 Milliarden US-Dollar entstanden bei so manchem Nutzer Sorgenfalten. Der Umgang mit Nutzerdaten durch das soziale Netzwerk wurde schon damals kritisch beäugt. Befürchtungen, dass [WhatsApp](#) ein ähnliches Schicksal droht, waren alles andere als unbegründet.

Zusicherungen, dass sich nichts verändert und die beiden Erfinder das Ruder in der Hand behalten würden, sollten besorgte Nutzer beruhigen. Auch die Implementierung von End-to-End-Verschlüsselung brachte etwas Ruhe. Mittlerweile sind die Gründer aus Unzufriedenheit nicht mehr bei [Facebook](#) am Werk, der Zuckerberg-Konzern hat mit der Verschmelzung seiner Plattformen begonnen und bald soll auch Werbung in der App erscheinen. Dass Facebook auch noch Zugriff auf jede Menge Metadaten von WhatsApp hat und den Vorwurf nicht los wird, die Ende-zu-Ende-Verschlüsselung nur schlampig implementiert zu haben, sollte Grund genug sein, sich nach Alternativen umzusehen.

Signal

2010 als TextSecure und RedPhone gestartet, zählt Signal heutzutage zu den Vorreitern in Sachen Sicherheit. Der für iOS, [Android](#) und einige andere Plattformen verfügbare Kurznachrichtendienst ist nicht erst seit der Empfehlung von Edward Snowden die erste Anlaufstelle für Verfechter des Datenschutzes.

Unter dem Projektnamen „Open Whisper Systems“ stetig weiterentwickelt, gibt es gleich mehrere Gründe, die für Signal sprechen. Die App ermöglicht plattformübergreifende Kommunikation, selbst auf Betriebssystemen, die nicht so stark verbreitet sind. Der Quellcode ist öffentlich einsehbar und kann von jedermann kontrolliert werden. Die implementierte End-to-End-Verschlüsselung gilt als das Nonplusultra auf seinem Gebiet. Ebendiese kommt etwas überraschend sogar bei WhatsApp zum Einsatz. Wenn es um Features geht, ist der Messenger dafür eher zurückhaltend. Grundfunktionen wie Gruppenkonversationen, Dateiversand und Sprachanrufe sind vorhanden. Auch ein Zerstörungsmodus für Nachrichten gibt es. Ausschweifende Experimente mit besonderen Features sind bei Signal aber nicht zu erwarten.

Gerne kritisiert wird auch, dass Signal eine Registrierung nur via Telefonnummer zulässt. Signal überträgt bei Nutzung der App aber immerhin nur einen Hash. Die Server der Anwendung bekommen also nie die Nummern im Klartext zu sehen und versuchen über verschiedene Methoden auch möglichst keine Spuren der Daten zu hinterlassen. Kritisch beäugt werden auch die vielen Berechtigungen, die vor allem auf Android-Geräten eingefordert werden. Wer auf Nummer sicher gehen will, muss aber kaum eine dieser Berechtigungen erteilen, um die App verwenden zu können. Eine umfangreiche Auflistung erklärt außerdem, wofür welche Berechtigungen genutzt werden.

Signal ist kostenlos für [iOS](#) und [Android](#) erhältlich.

Threema

Der in der Schweiz ansässige Messaging-Dienst Threema wird immer wieder in einem Atemzug mit Signal genannt, unterscheidet sich in manchen Punkten jedoch massiv. Erstmals 2012 auf dem Markt erschienen, möchten die eidgenössischen Entwickler eine sichere Alternative zu WhatsApp und Co. anbieten. Deshalb geht man beim Konzept der App an manchen Stellen einen eher ungewöhnlichen Weg. Zuallererst sind da die Kosten. Im Vergleich zu den vielen anderen Anbietern ist Threema eine der wenigen Messaging-Apps, die ihre Services nur gegen Geld anbietet. Diese macht gleich aus mehreren Gründen Sinn, hat aber auch entscheidende Nachteile.

So werden die Infrastruktur und Entwicklung ausreichend finanziert. Gleichzeitig scheinen sich die Kosten aber auch auf die Verbreitung auszuwirken. Mit Nutzerzahlen im niedrigen einstelligen Millionenbereich ist es eher unwahrscheinlich, viele Freunde in der App zu finden. Was die Features angeht, bringt die Schweizer App alles mit, was ein guter Messenger braucht. Gruppenfunktionen, Versand von Fotos und Videos, Sprachanrufe und eine Art Safe für die Sicherung von Daten sind vorhanden. Eine Besonderheit ist die Anmeldung bei Threema. Hier ist man einer der einzigen Anbieter, der keine E-Mail-Adresse oder Handynummer verlangt.

Stattdessen kann auch über die Threema-ID kommuniziert werden. Diese fördert die Anonymität und kann jederzeit widerrufen werden. Die Server von Threema befinden sich in der Schweiz, unterliegen also der Schweizer Rechtsprechung und der DSGVO. Einen entscheidenden Nachteil hat der Dienst aber beim Code. Dieser ist nicht öffentlich einsehbar, kann also nicht ohne weiteres von unabhängigen Stellen kontrolliert werden. Stattdessen ist man auf den guten Willen des Anbieters angewiesen, der externe Firmen zu Audits zulässt. Diese haben zwar bereits mehrmals stattgefunden und resümierten positiv, vollständig sicher sein kann man sich bei Closed-Source-Anwendungen trotzdem nie.

Threema ist um 3,49 Euro bzw. 2,99 Euro für [iOS](#) und [Android](#) erhältlich.

Telegram

Von vielen als der große Konkurrent für WhatsApp angesehen, ist Telegram ein besonderer Messenger. Und das sowohl im positiven als auch negativen Sinn. Die App erfuhr mehrere Schübe bei den Nutzerzahlen, die Übernahme von WhatsApp durch Facebook katapultierte Telegram damals ganz nach oben in den App Stores. Ins Leben gerufen wurde der Dienst vom Russen Pavel Durov, der unter anderem für Russlands größtes soziales Netzwerk vKontakte verantwortlich zeichnete.

Nach Querelen mit der Regierung und dem erzwungenen Verkauf von vKontakte wanderte der Russe ins Exil aus und entwickelte Telegram. Beliebt ist Telegram bei Nutzern vor allem wegen des Reichtums an Features. Von Supergruppen über Sticker bis hin zu Bots und umfangreiche APIs ist alles bei Telegram vorhanden. Für viele gilt die Anwendung außerdem als Anlaufstelle für sichere Kommunikation, was aber nur bedingt richtig ist. Zwar bietet Telegram Ende-zu-Ende verschlüsselte Nachrichten an, die Integration wird aber von Sicherheitsexperten regelmäßig aus gleich mehreren Gründen kritisiert. So sind etwa Unterhaltungen nicht standardmäßig vollverschlüsselt, sondern müssen gezielt im verschlüsselten Modus gestartet werden.

Normal versendete Nachrichten verbleiben sogar unbegrenzt auf den Servern. Auch Gruppenkommunikation kann gar nicht verschlüsselt werden. Viel schwerwiegender ist, dass Telegram ein eigenes entwickeltes Verschlüsselungsprotokoll verwendet, das kryptografische Verfahren nur unzureichend bzw. falsch einsetzt. Auch der Ruf von Telegram, als Plattform für Terrorpropaganda zu dienen, wirkt sich immer wieder negativ auf das Image des Dienstes aus.

Telegram ist kostenlos für [iOS](#) und [Android](#) erhältlich.

Viber

Die von vier israelischen Entwicklern erfundene App fristet in Europa eher ein Schattendasein. Weltweit genießt die App ein hohes Ansehen und kann nach eigenen Angaben mit rund einer Milliarde Nutzern aufwarten. Die Messaging-App im violetten Design ist seit 2014 in japanischen Händen, der Rakuten-Konzern ließ sich die Übernahme fast 900 Millionen US-Dollar kosten. In Sachen Technik orientierte sich Viber anfangs eher an Skype.

Die Anwendung wollte kostengünstige Anrufe vor allem ins Ausland anbieten und eine Konkurrenz für die damals recht günstigen Tarife von Skype sein. Erst nach und nach kamen Features wie Instant-Messaging, Video-Calling und Sticker hinzu. Bis 2016 war die App nur sehr spartanisch verschlüsselt. Erst im April des selben Jahres führte man dann - auch nach öffentlichem Druck - End-to-End-Verschlüsselung ein. Auch bei Viber ist der Code aber nicht öffentlich einsehbar, Nutzer und Sicherheitsexperten haben also keinerlei Möglichkeiten, hinter die Kulissen der Anwendung zu schauen. Stattdessen ist man auch hier auf externe Audits angewiesen.

Zwar verweist man auf eine „Signal-ähnliche“ Verschlüsselung und interne Audits, überzeugend sind die Ausführungen des Unternehmens aber keineswegs. Immerhin sind von Anrufen bis zu Chats sämtliche Inhalte durchverschlüsselt. Theoretische Bedienungsfehler, wie etwa bei Telegram sind hier also ausgeschlossen. Der Mutterkonzern Rakuten ist in Europa aber noch ein recht unbeschriebenes Blatt. Die Intentionen in Sachen Datenschutz lassen sich nicht vollständig durchschauen. Für alle jene, die einfach nur der Datenkracke Facebook entkommen wollen, ist Viber aber eine angemessene Alternative.

Viber ist kostenlos für [iOS](#) und [Android](#) erhältlich.

Wire

Unter den fünf genannten Apps ist Wire für viele wohl die am wenigsten bekannte Anwendung. Erst 2014 gestartet, ist der im Schweizer Zug beheimatete und in Berlin entwickelte Dienst auch einer der jüngsten Anbieter. Gegründet wurde die Wire Swiss GmbH von ehemaligen Mitarbeitern von Microsoft und Skype. Anfänglich als einfacher Messaging-Service gestartet, hat sich die App mit der Zeit zu einer Art Geheimtipp entwickelt.

Mit an Bord sind sämtliche Funktionen, die man sich von einem Kurznachrichtendienst im Jahr 2019 erwartet. Nachrichten, Fotos, Videos und Dateien lassen sich unkompliziert verschicken. Auch Sprachnachrichten und -anrufe sowie Videokonferenzen sind möglich und allesamt verschlüsselt. Finanziert wird Wire unter anderem durch Kommunikationsdienste für Firmen, die über eine Abo-Modell genutzt werden können. Während anfangs nur eine einfache Server-Client-Verschlüsselung genutzt wurde, wird seit etwa drei Jahren durchgehend Ende-zu-Ende verschlüsselt. Wire verfolgt dabei ein an Signal angelehntes Konzept namens Proteus.

Zu Beginn wurden sowohl die Verschlüsselungsmethode als auch die fehlende Transparenz beim Quellcode kritisiert. Wire hat aber mittlerweile in beiden Punkten nachgebessert. Audits des Verschlüsselungsprotokoll fanden nur noch kleine, unkritische Fehler, die die Sicherheit beeinträchtigen könnten. Neben dem Client-Sourcecode ist mittlerweile auch der Servercode frei auf Github einsehbar und kann somit von unabhängigen Stellen überprüft werden. In einem eigenen Whitepaper erklärt der Dienst außerdem, wie mit anfallenden Daten umgegangen wird.

Wire ist kostenlos für [iOS](#) und [Android](#) erhältlich.

Fazit

Wenn es um das reine Angebot geht, sind mehr als genug Alternativen zu WhatsApp vorhanden. Sämtliche Apps ähneln sich in Handhabung und Funktionsumfang stark. Die richtige App zu finden, ist dabei auch eine Frage des Geschmacks. Wer auf volle Sicherheit setzt, wird nicht um Signal herum kommen. Nutzer, die einfach nur aus den Fängen Facebooks flüchten möchten, sind auch bei den anderen Alternativen gut aufgehoben.