Privatsache

Messenger-Apps. Selbst am Marktführer WhatsApp führt ein Weg vorbei. Hier lernen Sie die Alternativen kennen.

Der Markt ist riesig und doch überschaubar – in Österreich, europaweit, ja mit wenigen länderspezifischen Ausreißern sogar weltweit. WhatsApp liegt derzeit unangefochten voran, in einigem Abstand folgt der Facebook-Messenger und danach kommt lange nichts. Allen Datenschutzskandalen zum Trotz ist also der hinter beiden Diensten stehende Facebook-Konzern der dominierende Anbieter.

Allerdings wird der Wunsch nach sicheren – oder genauer gesagt: sichereren – Alternativen stärker. Denn eines müssen wir klarstellen: Es geht nicht primär um die Sicherheit der Kommunikation (hier haben viele Messenger zueinander aufgeschlossen), sondern darum, was mit unseren persönlichen Daten geschieht, auf die diese Dienste Zugriff haben. Facebook und WhatsApp gleichen ja ungeniert die Nutzerdaten ab. Das betrifft nicht nur die Privatsphäre. Diverse Metadaten werden erhoben und gespeichert, nach dem Muster: Wer kommuniziert mit wem wie oft und wie lange? Für solche Daten interessieren sich beispielsweise auch die Strafverfolgungsbehörden. Angenommen, ein Facebook-Kontakt begeht ein Wirtschaftsdelikt und sein Chatverlauf wird ausgewertet. So geraten Personen, die mit ihm kommuniziert haben, in den Verdacht der Mitwisserschaft. Auch der zukünftige Verkauf der gesammelten Daten an interessierte Unternehmen kann nicht ausgeschlossen werden; Stichwort: Bonitätsbewertung anhand des Social-Media-Umfelds (siehe KONSUMENT 12/2018).

Was man ebenfalls nie vergessen sollte, ist die Tatsache, dass es sich um Smartphone-Apps handelt und die Nutzung der mobilen Geräte an sich schon mit Datenschutzrisiken behaftet ist. Der erzielbare Grad an Sicherheit kann sich folglich immer nur darauf beziehen, was auf einem handelsüblichen Smartphone unter den gängigen Betriebssystemen Android und iOS überhaupt möglich ist.

Doch nicht so sicher

Während man selbst bei WhatsApp auf hohem Standard Ende-zu-Ende-verschlüsselt kommuniziert und somit nicht einmal der Anbieter die Nachrichten mitlesen oder Gespräche abhören kann, ist die Verschlüsselung beim **Facebook-Messenger** nicht standardmäßig aktiviert und für Gruppenchats gar nicht verfügbar. Gleiches gilt für den russischen Messenger-Dienst **Telegram**, der zu Unrecht eine gewisse Verbreitung als WhatsApp-Alternative erfahren hat. Möchte man bei Telegram oder beim Facebook-Messenger verschlüsselt kommunizieren, muss man einen sogenannten geheimen Chat eröffnen.

Diese beiden Dienste sind zwar vielseitig, von beiden ist jedoch abzuraten, wobei Facebook-Nutzer dem eng und hartnäckig mit dem Benutzerkonto verknüpften Messenger gar nicht so einfach entkommen können. Zumindest kann man ihn aber durch Nichtnutzung abstrafen, denn er ist in erster Linie eine Datensammelmaschine. Telegram wiederum speichert sämtliche Chatinhalte in einer Cloud (daher die Möglichkeit des geräteübergreifenden, an ein Benutzerkonto gebundenen Zugriffs). Die verwendete Verschlüsselung ist zum Teil eine Eigenentwicklung, ihre Sicherheit schwer zu beurteilen. Die Tatsache, dass die App selbst Open Source ist (für Experten ist also nachvollziehbar, wie sie programmiert wurde), kann die Minuspunkte nicht wettmachen.

Ebenfalls abraten müssen wir von **WeChat**. Die hohen Nutzerzahlen rühren daher, dass der Messenger quasi das WhatsApp von China darstellt. Dort lauscht ganz offiziell der Staat mit. Die dafür notwendigen Hintertüren sind standardmäßig in die App eingebaut.

Umfangreiche Datenweitergabe

Kaum Vorteile gegenüber Facebook und WhatsApp bieten der altbekannte Microsoft-Dienst **Skype** und der zum japanischen Rakuten-Konzern gehörende Dienst **Viber**. Anders als die übrigen Messenger, die für den Versand von Textnachrichten konzipiert wurden und später eine zusätzliche Telefonfunktion verpasst bekamen, machten sie genau die umgekehrte Entwicklung durch, was aber – zumindest am Smartphone – mittlerweile keinen Unterschied mehr macht. Beide sind als Datensammler verschrien, aber immerhin stellen sie recht transparent dar, was mit den Daten geschieht (Viber sogar DSGVO-konform). Microsoft verfügt zwar über Serverstandorte im EU-Raum, Teile der Daten von europäischen Kunden können aber auch in die USA ausgelagert werden, wo sie einer anderen Gesetzgebung unterliegen (konkret der Privacy-Shield-Vereinbarung zwischen den USA und der EU). Es gibt zwar in beiden Messengern diverse Einstellungen, um den Datenfluss zu reduzieren, diese müssen aber von den Nutzern nachträglich selbst durchgeführt werden.

Die sichereren Alternativen

Kommen wir zu jenen Messengern, die auch hinsichtlich des Datenschutzes empfehlenswerte Alternativen zu WhatsApp darstellen. Da ist etwa **Wire**, ein Schweizer Dienst auf Basis von Open-Source-Software. Ähnlich wie bei Telegram ist eine geräteübergreifende Nutzung möglich, weshalb die Daten verschlüsselt auf einem Server zwischengespeichert werden. So wie bei den übrigen bisher genannten Messengern muss man sich bei Wire persönlich registrieren, kann aber alternativ zur Handynummer eine E-Mail-Adresse angeben. Der Abgleich der Kontakte erfolgt verschlüsselt und sie werden nicht bei Wire gespeichert. Alternativ kann man den Dienst auch dann nutzen, wenn man ihm den Zugriff auf die Kontakte verweigert. In diesem Fall muss man mit jedem Kommunikationspartner die Kontaktdaten austauschen und verifizieren. Auch Wire speichert persönliche Daten sowie Gerätedaten und gibt sie fallweise an Anbieter in der EU oder der Schweiz weiter. Das dient eigenen Angaben zufolge zur Bereitstellung des Service bzw. zum Schutz der unternehmenseigenen Rechte. Zudem wird darauf hingewiesen, dass diese Daten im Fall eines Verkaufs des Messengers an ein anderes Unternehmen übertragen werden können (was ja auf die Konkurrenz ebenso zutrifft). Die Übermittlung anonymisierter Nutzungsstatistiken kann man deaktivieren.

Ein Name, der häufig fällt, ist **Threema** – ein Dienst, der gleichfalls in der Schweiz angesiedelt ist. Als Minuspunkt wird oft angemerkt, dass die App kostenpflichtig ist. Einmalige 2,99 Euro sollten aber nicht das Hindernis sein; eher schon die Tatsache, dass es sich in diesem Fall bei der App nicht

Rat und Hilfe für Verbraucher in Europa ECC-Net
Finanziell unterstützt durch die Europäische Union

Dieser Artikel wurde aus den Mitteln des Verbraucherprogramms der Europäischen Union (2014 – 2020) gefördert.

um Open Source handelt (beim Verschlüsselungsstandard hingegen schon). Threema ist jedenfalls der einzige Messenger, der auf Wunsch größtmögliche Anonymität bietet. Die Registrierung mit Handynummer oder E-Mail-Adresse ist ebenso optional wie der anonymisierte Abgleich der Kontakte (so wie bei Wire kann man alternativ eine persönliche Verifizierung mittels QR-Code vornehmen). So oder so erhält jeder Nutzer eine zufallsgenerierte Threema-ID. Der Dienst betont, dass keinerlei persönliche Daten bzw. Nutzungsdaten gespeichert werden. Auch die Threema-ID ist dem Anbieter nicht bekannt. Achtung! Auf die Option, den eigenen Standort zu übermitteln, sollten Sie besser verzichten, da hier die Google-Standortdienste zum Einsatz kommen.

Bleibt noch der unter anderen vom ehemaligen CIA-Mitarbeiter und Auslöser der NSA-Affäre Edward Snowden empfohlene Messenger **Signal**. Das allein ist natürlich noch kein ausreichender Grund, diesen Dienst als das Nonplusultra anzupreisen. Das tun wir auch nicht, denn wie in den anderen Fällen gibt es Pros und Kontras. Zu Letzteren zählt etwa, dass das Unternehmen in den USA sitzt und der dortigen Rechtsprechung unterliegt. Anders als bei Threema ist es nicht möglich, vollständig anonym zu bleiben, weil man eine Telefonnummer angeben muss. Der Benutzername hingegen ist frei wählbar und wird auch nicht an Signal übertragen. Der Ablgleich der Kontaktdaten erfolgt verschlüsselt und ebenfalls ohne Datenspeicherung. Verschlüsselte Nachrichten werden nur dann zwischengespeichert, wenn das Gerät des Empfängers gerade offline ist. Sonst gibt es kein Backup, die Nachrichten sind ausschließlich auf den jeweiligen Endgeräten gespeichert. Die App ist Open Source, so wie auch die verwendete Verschlüsselungstechnologie (die übrigens auch bei WhatsApp zum Einsatz kommt). In den Grundeinstellungen ist Signal einfach gehalten, diverse Komfortfunktionen, die man von anderen Messengern kennt, können freigeschaltet werden (z.B. Lesebestätigungen).

Eine Frage des Vertrauens

Fest steht: Wer absolut sicher kommunizieren möchte, wählt das persönliche Gespräch unter vier Augen. Bei einer Smartphone-App ist Sicherheit relativ und auch eine Frage des Vertrauens in den Anbieter. Die Ende-zu-Ende-Verschlüsselung der Inhalte sollte eigentlich selbstverständlich sein. Der Umgang mit den Kundendaten trennt dann die Spreu vom Weizen, wobei es in der Natur der Sache liegt, dass es den einen, uneingeschränkt empfehlenswerten Messenger gar nicht geben kann. Es gibt jene, die man halt verwendet, weil „der Rest der Welt" es auch tut, jene, von denen man eher die Finger lassen sollte, und zwischendrin jene, zu denen man aus der Überzeugung heraus greift, dort als Kunde besser aufgehoben zu sein.

Handbuch Datenschutz

Flexcover, 204 Seiten, € 19,90, www.konsument.at/hb-datenschutz

Viele Aktionen im Alltag sind mit dem Austausch und der Preisgabe persönlicher Daten verbunden. Dieses Buch gibt Einblick in dieses Big-Data-Business und motiviert zu einem sparsamen Umgang mit den eigenen Daten. Es zeigt, wo die Datenkraken in unseren Alltag eingreifen und was man tun kann, um Privatsphäre möglichst zu bewahren.

Bestellungen

Tel. 01 588 774 | Fax 01 588 77-72 | E-Mail: kundenservice@konsument.at
Onlineshop www.konsument.at/shop