



Kill the Messenger

Viele löschen Whatsapp und zügeln zu Telegram, Threema und Co., wo ihre Daten besser geschützt sind. Schön! Doch eigentlich wäre es Zeit, die Messenger-Welt komplett umzukrempeln.

Von [Olivier Baumann](#), [Patrick Venetz](#) (Text) und Quickhoney (Illustration), 24.02.2021

Nach drei Tagen sind alle migriert – auch der Schwager hat sich schliesslich durchgerungen. Der Familien-Chat ist neu auf Signal.

Animierte Lamas ersetzen jetzt das Spiegelei, es gibt neue Stickerbildchen. Doch am Inhalt ändert sich nichts: Fotos von Winterspaziergängen, Links zur Impfanmeldung, Memes, Emojis.

Whatsapp ist gelöscht.

Ende gut, alles gut.

Was ist geschehen?

Exodus

Im Januar 2021 hat Whatsapp neue Datenschutzrichtlinien veröffentlicht. Per Pop-up hat es die User darüber informiert, dass der Dienst ohne die Zustimmung zu den neuen Datenschutzrichtlinien bald nicht mehr genutzt werden könne: Es entfällt die Option, den Datenaustausch zwischen Whatsapp und dem Mutterkonzern Facebook zu unterbinden. (Eine Option, die eigentlich sowieso nur jene Whatsapp-Nutzerinnen hatten, die sich vor 2016 angemeldet hatten.)

Prompt – und ironischerweise auf Whatsapp und Facebook selbst – gingen daraufhin Posts über die neuen Nutzungsbedingungen viral. Seither spricht alle Welt über Privatsphäre und Datenschutz. Und man erinnert sich wieder daran, warum Facebook 2014 so viel Geld für die Übernahme von Whatsapp bezahlt hat: 22 Milliarden Dollar.

Logisch: Es sind die Daten.

Nicht die wörtlichen Inhalte der Chats, nein, die Metadaten: Abermilliarden von Datenpunkten über die Beziehungen zwischen den Nutzern. Sie sind wertvoll im Online-Werbemarkt, dem Kerngeschäft von Facebook.

Denn so gerne sich Menschen als Individuen betrachten – statistisch gesehen mögen sie, was ihre Freunde mögen. Und sie kaufen, was ihre Freunde kaufen. Ja, auch Sie.

Deshalb ist Facebook stets darauf erpicht, dass soziale Interaktionen auf seinen Plattformen stattfinden – nicht auf jenen der Konkurrenz: damit der Konzern den Werbeumsatz pro Nutzerin maximieren kann.

Weil das vielen nicht gefällt (oder sie fälschlicherweise glauben, Facebook erhalte neu Zugriff auf alle verschlüsselten Whatsapp-Nachrichten), kommt es nun also zum Exodus.

Und in den Medien läuft das grosse Vergleichen. Welcher andere Messenger ist der beste?

- Für **Threema** spricht die Ende-zu-Ende-Verschlüsselung. Doch der Quellcode ist nicht vollständig offen, und auch bei der Verbreitung hapert es noch.
- Auch **Signal** gehört bei der Verbreitung nicht zu den Spitzenreitern. Doch es punktet beim Verschlüsselungsprotokoll und mit der Finanzierung über eine gemeinnützige Stiftung.
- Dagegen ist **Telegram** populär. Doch sowohl der Quellcode als auch die Finanzierung der App sind intransparent.

Der «K-Tipp» empfiehlt Signal, «Watson» kürt Threema zum klaren Gewinner, und die NZZ kann sich nicht entscheiden. Einig ist man sich über Whatsapp: Die Nachrichten sind sicher, persönliche Nutzerdaten aber sind Freiwild.

Signal verzeichnete im Januar fast 10 Millionen neue Nutzer, die Server brauchen einen ganzen Tag lang zusammen. Telegram hat nun 25 Millionen zusätzliche Nutzerinnen.

Die Schwiegermutter teilt ihre Witz-Comic-Trouvaillen neu statt über die grüne App über die blaue mit gestrichelter Sprechblase. Videos und Sprachnachrichten der Nichte kommen via iMessage. Die Lesegruppe bleibt vorerst auf Telegram, die Fahrlehrerin auf Whatsapp, die Rollenspiel-Gruppe kommuniziert auf Discord und die Arbeitskollegen auf Slack. Ein paar Freunde sind nur via Threema erreichbar, andere nur per SMS. Vielfalt!

Ende gut, alles gut?

Nun ja.

Cappuccino

Stellen Sie sich vor, Sie müssten für jeden E-Mail-Anbieter eine eigene App installieren, um Nachrichten an Adressen dieses Anbieters zu schicken.

Eine Hotmail-App für Nachrichten an Hotmail-Adressen.

Eine Gmail-App für Nachrichten an Gmail-Adressen.

Eine GMX-App für Nachrichten an GMX-Adressen.

So absurd das klingen mag, genau diese Situation hat sich bei den Messaging-Apps etabliert. Die Apps, die uns vor einem Jahrzehnt aus der SMS-Hölle erlösten – der auf 160 Zeichen beschränkte, ehemalige Goldesel der Telecom-Unternehmen –, sind zu ihrer eigenen Hölle verkommen.

Telegram, Signal, Threema und Whatsapp unterscheiden sich zwar bezüglich Datenschutz, Funktionsumfang und Nutzererfahrung. Eines haben sie aber alle gemeinsam: Es sind Datensilos, geschlossene Systeme.

Das bedeutet: Die jeweiligen Anbieter kontrollieren nicht etwa einen kleinen Teil, sondern die gesamte Kommunikation (aufgrund von Verschlüsselung erfahren sie allerdings oft nur, wer mit wem wann interagiert). Nichts hält sie davon ab, Zugänge zu unterbinden oder Daten zweckzuentfremden.

Silos sind zudem anfälliger für Zensur. Eine Nachrichtenplattform wie Telegram oder Whatsapp zu blockieren, kann für Regierungen technisch einfacher sein als ein System mit vielen unabhängigen Anbietern.

E-Mails funktionieren anders.

Die Anbieter bilden hier kein geschlossenes, sondern ein offenes System. Basierend auf einem offenen Protokoll, das fast so alt ist wie das Internet.

1971 wurde es entwickelt, von Nerds für Nerds. Die Entwickler – Frauen in diesem Fall nicht mitgemeint – wollten sich gegenseitig elektronische Nachrichten zum Stand der Entwicklung des Arpanets (so hiess der Vorläufer des Internets) schicken. Early Adopter waren Behörden und Universitäten.

Okay, sehr wahrscheinlich mögen Sie E-Mails nicht.

Weil es immer fünf Anläufe braucht, bis das alte Konto aufs neue Handy migriert ist. Weil zeitweise 90 Prozent der Nachrichten in Ihrem Posteingang Spam sind – Werbung für Potenzpillen, Viren, Trojaner, Newsletter, die Sie nie abonniert haben. Oder, wenn Sie sich im Datenschutz auskennen: weil E-Mails üblicherweise nicht Ende-zu-Ende-verschlüsselt sind.

Doch wie auch immer Sie dazu stehen: Dass wir uns auch 50 Jahre nach ihrer Erfindung noch immer täglich mit «diesen verdammten E-Mails» herumschlagen, weist auf etwas Besonderes hin.

Darauf, wo die Zukunft von Kurznachrichten liegen könnte.

Das Stichwort dazu heisst «Föderation».

In einem föderierten System einigen sich die Teilnehmenden auf gemeinsame Regeln und Standards. Kein einzelner Akteur kontrolliert das System. Das Internet an sich ist ein föderiertes System: Es gibt viele Millionen Server, die alle die gleiche Sprache sprechen.

E-Mails haben auch deshalb universelle Verbreitung gefunden (und sind auch darum nicht totzukriegen), weil E-Mail keine Plattform – kein Silo –, sondern ein offener Standard ist.

Der Unterschied? Stellen Sie sich vor, Sie machen Cappuccino.

Cappuccino ist ein offener Standard. Das Rezept ist allgemein bekannt: Kaffee und Milch, geschäumt, je nach Wunsch etwas Zucker, Kakaopulver zum Bestäuben. Jede kann Cappuccino machen. Sie müssen nur die richtige Software (Kaffee und Milch) und Hardware (Kaffeemaschine) organisieren und etwas Zeit investieren.

Ähnlich verhält es sich bei E-Mails. Die Software, um einen E-Mail-Server zu betreiben, ist frei verfügbar. Jeder kann einen Server aufsetzen, dafür braucht es nur einen Rechner mit Internetzugang.

Ein E-Mail-Anbieter kann niemals die ganze Kommunikation, die über den E-Mail-Standard stattfindet, kontrollieren. Es gibt Hunderte E-Mail-Anbieter und Millionen E-Mail-Server. Die Daten, die ein Anbieter besitzt, sind lediglich ein Ausschnitt. Nutzerinnen auszuschliessen, ist unmöglich.

Whatsapp und Co. sind kein Cappuccino, sondern Nespresso. Die Kapseln funktionieren nur mit der entsprechenden Maschine. Die Nachrichten nur innerhalb der jeweiligen App.

Fair enough. Cappuccino statt Nespresso.

Doch wie?

Roulette

Von einem föderierten Instant-Messaging-Standard haben Sie wahrscheinlich noch nie gehört. Verständlich, denn Messenger, die auf offene Standards setzen, sind erst eine Nische.

Doch mit jedem Shitstorm wachsen sie. Element zum Beispiel – ein Messenger, der auf dem sogenannten Matrix-Protokoll basiert – registrierte nach dem Fauxpas von Whatsapp eine Verhundertfachung der Downloads.

Das Matrix-Protokoll ist nur einer von mehreren offenen Messenger-Standards. Aufmerksamkeit erregte es 2018, als die französische Regierung ankündigte, für ihre interne Kommunikation künftig darauf zu setzen.

Geleitet vom strategischen Ziel der digitalen Souveränität – und getrieben vom Unbehagen über die vermehrte Nutzung von Whatsapp, Telegram und Co. für Staatsgeschäfte –, veranlasste Frankreich die Entwicklung von Tchap: einer Messaging-App, die auf dem Matrix-Protokoll basiert.

Schleswig-Holstein, Hamburg und die deutsche Bundeswehr wollen derzeit ähnliche Lösungen implementieren.

Für staatliche Akteure hat das Matrix-Protokoll einen entscheidenden Vorteil: Es ist wie E-Mail, also Cappuccino. Matrix-Server lassen sich selbst betreiben, die Hoheit über die Daten ist somit – im Unterschied zu geschlossenen Silos – gewährleistet.

Ich will es genauer wissen: Wie sieht die Matrix-Adresse aus?

Eine Matrix-Adresse sieht einer E-Mail-Adresse ähnlich. Das @-Zeichen rückt an den Anfang, Name und Server werden mit Doppelpunkt getrennt. Aus name@republik.ch wird so @name:republik.ch.

Föderation ist ein Prinzip, das vielfältig einsetzbar ist. Twitter hat 2019 etwa angekündigt, die Entwicklung eines dezentralen Protokolls für Microblogging zu unterstützen. Daraus entstand das Projekt «Bluesky».

André Staltz, Mitautor des ersten Berichts von Bluesky, glaubt, dass offene Standards – die meist als Open-Source-Projekte vorangetrieben werden – den längeren Atem haben. Zu Beginn hinken sie zwar der Unternehmenssoftware hinterher. Doch wenn sie erst einmal genauso gut oder besser sind, bleiben sie dauerhaft etabliert. Beispiele sind das Betriebssystem Linux oder die Online-Enzyklopädie Wikipedia.

Doch die Zukunft von föderierten Instant-Messengern ist nicht nur wegen der Nutzerfreundlichkeit ungewiss. Sie können auch Behörden ein Dorn im Auge sein, da sie sich schlechter überwachen lassen. Und föderierte Systeme sind anfällig für Teilnehmerinnen mit schlechten Absichten, die dann beispielsweise Spam verbreiten. Sie zu blockieren, fällt in geschlossenen Systemen leichter.

Damit sich längerfristig ein offenes Protokoll wie Matrix durchsetzt, braucht es also noch einige Shitstorms. Aber mit jedem weiteren Messenger-Roulette wird ein Protokoll, das nicht auf kurzfristige Trends, sondern auf die Dauer ausgelegt ist, attraktiver.

Damit zurück zu Whatsapp. Beziehungsweise zurück zu Telegram, dem neuen Whatsapp. In der Spaziergang-Telegram-Gruppe beginnt nämlich die Diskussion schon wieder aufs Neue.

Die Frage diesmal: «Threema oder Signal?»

Der Erste spricht sich für Threema aus, weil die Daten in der Schweiz liegen und kein grosser Konzern dahinterstehe. Eine andere Person wendet ein, dass das in Bezug auf Datenschutz nur Swissness-Hype sei, denn das «uralte Schweizer Datenschutzgesetz» von 1993 (VDSG) hinke der europäischen Datenschutz-Grundverordnung (DSGVO) hinterher. (Diese Person ist übrigens nicht up to date, das neue DSG ist revidiert, vom Parlament abgesegnet und wird 2022 in Kraft sein.) Jemand hält fest, dass hinter Signal eine Stiftung stehe. Das Fazit: Wir werden wohl doch mehrere Apps benutzen müssen.

Lohnt es sich also wirklich, von Whatsapp in ein anderes Silo zu wechseln?

Wenn Ihnen Datenschutz und Privatsphäre egal sind: nicht unbedingt.

Wenn Ihnen nicht egal ist, was mit Ihren Daten passiert, dann ist die Antwort ganz klar: Ja, Sie sollten wechseln. Sie entziehen sich damit, zumindest teilweise, dem Geschäftsmodell des Überwachungskapitalismus. Jeder Schritt weg davon ist ein Schritt in die richtige Richtung. Nutzen Sie Signal oder Threema. Bewegen Sie andere dazu. Aber wo auch immer Sie landen, machen Sie es sich nicht zu gemütlich.

Und wenn Sie ganz mutig sein wollen: Installieren Sie Element.

Willkommen in der Matrix.

Zur Debatte: Sehen wir uns in der Matrix?

Diskutieren Sie mit uns via Matrix – über Matrix. Alles, was Sie dazu brauchen, ist ein Messenger (zum Beispiel Element – für Smartphone oder Computer) und den folgenden Link. Wir treffen uns im Channel #republik:matrix.org, zusätzlich erreichen Sie die Autoren unter @iovi:matrix.org und @paeve:matrix.org.

In einer früheren Version waren wir beim neuen Schweizer Datenschutzgesetz nicht ganz präzise, es wird 2022 in Kraft treten – wir haben dies im Beitrag ergänzt.