Messenger-dämmerung

Sichere Messenger: WhatsApp und Alternativen im Test

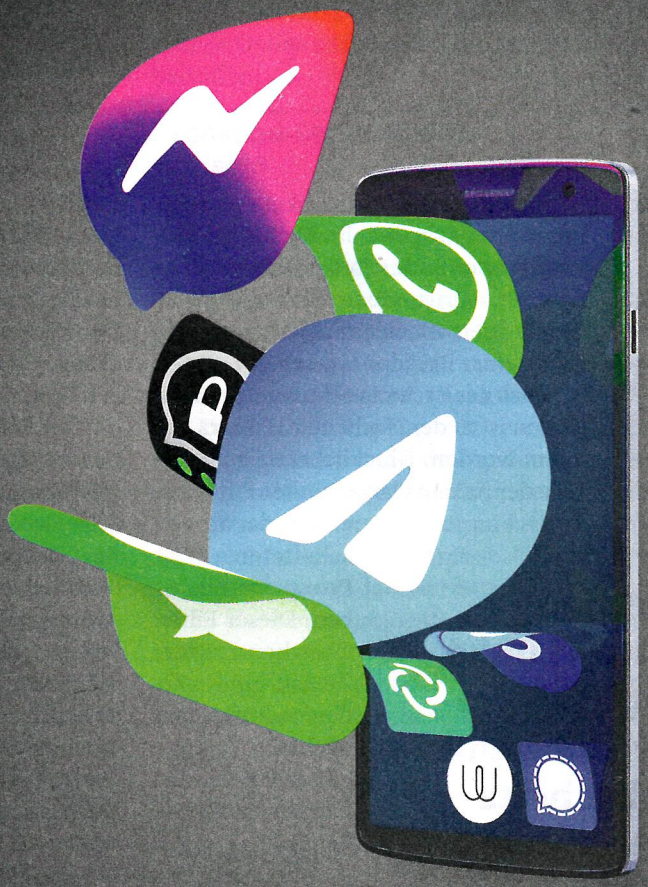


Bild: Andreas Martini

WhatsApps Status als De-facto-Standard bröckelt: Immer mehr Menschen mögen ihre Daten nicht dem Facebook-Konzern überlassen. Glücklicherweise gibt es Alternativen, die nicht nur sicherer, sondern auch mindestens so komfortabel sind. Fünf haben wir getestet.

Von Jan-Keno Janssen, Sylvester Tremmel und Sebastian Trepesch

Was ein kleines Info-Fenster anrichten kann: Als der populäre Messenger WhatsApp Anfang des Jahres darum bat, neuen Nutzungsbedingungen zuzustimmen, hat er damit eine wahre Wechsel-Welle ausgelöst. Laut der App-Analysefirma Sensor Tower wurde beispielsweise Signal zwischen dem 6. und 10. Januar 7,5 Millionen Mal installiert – über 40 Mal mehr als in der Vorwoche. Telegram meldete 25 Millionen neue User in drei Tagen.

Was ist da los?

Facebook setzt der WhatsApp-Kundschaft die Pistole auf die Brust: Wer den Änderungen der Nutzungsbedingungen nicht zustimmt, kann keine Nachrichten mehr lesen und schreiben. Als Frist galt zuerst der 8. Februar, Facebook hat die Einführung aber, vermutlich als Reaktion auf die Messenger-Wechsel-Welle, auf den 15. Mai verschoben.

Aber was ändert sich denn nun eigentlich? Bei Nachrichten zwischen Privatnutzern laut Facebook nichts, die sind und bleiben für den Konzern nicht lesbar. Betroffen sind vielmehr Chats zwischen Privatnutzern und Unternehmen. Letztere sollen künftig Dienstleister beauftragen dürfen, die Chats in ihrem Namen abzuwickeln. Auch Facebook selbst will diese Dienstleistung seinen Firmenkunden anbieten, hätte in bestimmten Fällen also ebenfalls Zugriff auf die WhatsApp-Chats und könnte sie im Auftrag des Kunden auch für dessen Werbezwecke auswerten. Facebook erhofft sich davon offenbar einen Schub für die Nutzung der Business-Funktionen von WhatsApp. Wie das künftig aussehen könnte, sieht man in China, dort kann man nämlich mit der WeChat-App zum Beispiel eine Pizza oder ein Taxi bestellen und direkt bezahlen. Insgesamt betreffen die Änderungen bei WhatsApp vor allem die Kundschaft außerhalb der EU, hierzulande schützt die DSGVO davor, dass Facebook zu viele Daten für Werbung auswerten darf. Klar ist auf alle Fälle: Facebook will WhatsApp endlich das Geldverdienen beibringen – ob man das in Einklang mit einer sicheren und datensparsamen Kommunikationsumgebung bringen kann, scheint mindestens fraglich.

Doch wo kann man denn überhaupt sicher kommunizieren und muss dennoch nicht auf den von WhatsApp gewohnten Komfort verzichten? Für diesen Test haben wir fünf WhatsApp-Alternativen ausgewählt: Element, Signal, Telegram, Threema und Wire. Die Auswahl fiel uns nicht leicht, denn eigentlich wäre unser Mindeststandard an Sicherheit der gleiche gewesen, den auch WhatsApp bietet, nämlich voreingestellte Ende-zu-Ende-Verschlüsselung (end-to-end encryption, E2EE). Sprich: Die Nachrichten werden nicht nur zum und vom Server verschlüsselt (Transportverschlüsselung), sondern permanent verschlüsselt gehalten und erst beim Empfänger entschlüsselt. Das macht WhatsApp seit 2016, und zwar mit dem in der Cryptoszene geachteten Double-Ratchet-Verfahren.

Dieses – von Signal erfundene – System ist gut für die asynchrone Kommunikation von Messengern geeignet und bietet wichtige Eigenschaften wie Forward Secrecy [1]. Aufgrund solcher Vorteile wird das Verfahren auch von diversen anderen Messengern eingesetzt, im Testfeld neben Signal und WhatsApp auch von Element und Wire.

Den sehr populären Facebook Messenger haben wir nicht mit aufgenommen – er nutzt standardmäßig keine E2EE, und vor allem: Wer von WhatsApp wegen der neuen Facebook-Nutzungsbedingungen weg will, wechselt nicht zum Facebook-Messenger. Wegen unvollständiger E2EE haben wir Skype und Snapchat ebenfalls nicht getestet. Das ansonsten ordentliche iMessage fiel raus, weil es ausschließlich auf Apple-Geräten läuft.

Eine Ausnahme haben wir bei Telegram gemacht, die App umgibt kurioserweise eine Aura der Sicherheit. Der Messenger verschlüsselt standardmäßig nicht Ende-zu-Ende, es lassen sich lediglich manuell „geheime Chats“ starten, die etliche Nachteile haben. So funktionieren sie nur als Einzelchat, nicht in Gruppen. Außerdem sind die verschlüsselten Chats nur auf dem Haupt-Mobilgerät sichtbar, nicht auf dem Desktop-Client. Trotz allem gilt Telegram als sicherere WhatsApp-Alternative, weshalb wir es in den Test aufgenommen haben.

Unabhängig von der Verschlüsselung der Inhalte fallen beim Versand von Nachrichten Metadaten an. Diese Problematik – mit der Messenger unterschiedlich umgehen – beleuchten wir in einem separaten Artikel auf S. 24.

Geschäftsmodelle

Interessant sind die völlig unterschiedlichen Geschäftsmodelle der sechs Testkandidaten. Während sich bei WhatsApp erst diffus abzeichnet, wie Facebook mit dem Messenger Geld verdienen will (Werbung und Messaging mit Firmen), sind die Geschäftsmodelle von Threema und Wire

Bei Signal kann man jede einzelne Nachricht mit einem Emoji kommentieren.

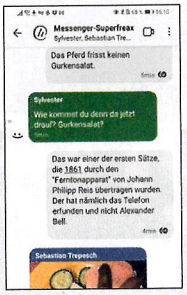
Element

Element ist laut Play-Store-Downloadzahlen der bislang unpopulärste Messenger dieses Tests – dafür aber auch der mit dem größten Nerd-Faktor. Die Software hieß bis vor einigen Monaten noch „Riot.im“ und setzt den offenen Standard Matrix um. Das ist ein Application-Layer-Kommunikationsprotokoll mit föderierenden Servern, ähnlich dem E-Mail-Standard SMTP. Chatpartner müssen also nicht beim selben Server registriert sein – oder denselben Client nutzen –, um miteinander zu reden.

Matrix schickt sich zumindest an, erfolgreicher zu werden als bisherige offene Instant-Messaging-Protokolle wie XMPP und IRCv3; unter anderem will die französische Regierung langfristig alle Ministerien auf Matrix-Kommunikation umstellen. Das deutsche Verteidigungsministerium testet seit Ende 2019 den „BwMessenger“ auf dienstlichen und privaten Geräten, der ebenfalls auf Matrix basiert.

Element kann als einziger Testkandidat die Kommunikation über einen selbst gehosteten Server laufen lassen. Ansonsten ist die Software eher rudimentär: Es gibt keine GIF-Bibliothek, keine Standort-Übermittlung und keine Sprachnachrichten, obwohl die für viele lebenswichtig sind.

- gute Verschlüsselung
- föderierende, offene Server
- erfordert Technikaffinität
- keine Sprachnachrichten



Signal

Das wohl anschaulichste Argument für Signal lieferte der im Exil lebende US-Whistleblower Edward Snowden vor Kurzem auf Twitter: „Ich benutze es jeden Tag und bin trotzdem noch nicht tot.“ Der Messenger hat sich seit seinen frickeligen Anfängen als „TextSecure“ in den letzten zehn Jahren erstaunlich entwickelt. Inzwischen kann man die App auch Technik-Laien empfehlen; wer mit WhatsApp klarkommt, bedient auch Signal. Dem Konkurrenten hat Signal sogar einiges voraus: So funktioniert der Desktop-Client auch dann, wenn das Handy ausgeschaltet ist – bei WhatsApp muss es zwingend aktiv und mit dem Netz verbunden sein. Außerdem kann man bei Signal einzelne Nachrichten mit Emojis versehen, was die Kommunikation effizienter macht. Die Stabilität der App hat sich vor allem mit den letzten Updates stark verbessert – hakte es zu Anfang des Tests noch mit zu spät übertragenen Nachrichten, klappt inzwischen alles zuverlässig.

In Sachen Sicherheit ist Signal quasi der Goldstandard. Die App hat das Double-Ratchet-Verfahren erfunden und vermeidet mehr Metadaten als die Konkurrenz. Einziges Manko: Zur Registrierung und als Nutzer-ID ist die Telefonnummer verpflichtend, eine anonyme Nutzung ist nicht möglich.

- beste Verschlüsselung
- einfache Handhabung
- Non-Profit-Entwickler
- Telefonnummern-Zwang

Telegram

Das hat Pavel Durov clever eingefädelt: Durch sein Leben als Exilant – er kehrte Russland 2014 den Rücken – lud er seinen Messenger Telegram mit viel Freiheitskämpfer-Image auf. In letzter Zeit fiel Telegram allerdings vor allem dadurch auf, dass etliche Quer- und Wirrköpfe hier ihre Verschwörungsmythen publizieren – oft nachdem YouTube und Co. ihnen deswegen den Zugang gesperrt hatten. Dabei arbeitet Telegram durchaus mit Regierungen zusammen und wird beispielsweise vom europäischen Polizeiamt gelobt für das „Fördern enger Partnerschaften mit Organisationen wie Europol“.

Telegrams Ende-zu-Ende-Verschlüsselung ist der Double-Ratchet-Konkurrenz technisch unterlegen. Viel schlimmer ist aber, dass Telegram standardmäßig gar keine Ende-zu-Ende-Verschlüsselung nutzt. Der Messenger ist damit klar unsicherer als die anderen Testkandidaten. Außerdem werden die Inhalte normaler Chats auf den Servern des Anbieters gespeichert, wobei unklar ist, wer darauf Zugriff nehmen könnte. In Sachen Komfort und Geschwindigkeit ist Telegram dagegen ganz weit vorne. Außerdem bemerkenswert: Die fantastische Exportfunktion (siehe S. 22), die liebevollen Stickerpacks und die praktischen Bots.

- stabil, schnell, viele Funktionen
- Cloud praktisch, aber unsicher
- nicht vollständig E2E-verschlüsselt
- Geschäftsmodell unklar

deutlich greifbarer: Threema verkauft die Privatkunden-Version der App für rund vier Euro und lizenziert die Geschäftskunden-Variante Threema Work an Unternehmen. Letzteres bietet auch Wire mit Wire Pro und Enterprise an; die Privatkundenvariante ist kostenlos.

Signal muss gar keinen Profit erwirtschaften, sondern wird von einer US-amerikanischen Non-Profit-Stiftung finanziert. Das Anschubkapital von 50 Millionen US-Dollar kam von WhatsApp-Mitgründer Brian Acton. Außerdem wirbt Signal um Spenden. Bei Element handelt es sich um die Referenzimplementierung des freien Protokolls Matrix, Geld soll mit Support und Beratung sowie mit der Lizenzierung von Apps an Firmen und Behörden verdient werden. Unter anderem setzen die Bundeswehr und die französische Regierung Matrix-Messenger ein.

Und dann ist da noch Telegram: Die Entwicklung wird vor allem vom Milliardär Pavel Durov finanziert, der Russlands populärstes soziales Netzwerk vk.com aufgebaut und 2014 für viel Geld verkauft hat. Laut der Telegram-FAQ soll in diesem Jahr mit der

Threema

Weil der Name „End-to-End-Encrypting Messaging Application" (EEEMA) nicht ganz so geschmeidig über die Lippen geht, hat der Schweizer Entwickler Manuel Kasper kurzerhand „Threema" daraus gemacht. Das war vor neun Jahren – und der Messenger behauptet sich immer noch gegen die Konkurrenz aus dem Silicon Valley. Vor Kurzem haben die Macher sich getraut, den Quellcode der Client-Software offenzulegen – den Servercode allerdings nicht.

In Sachen Funktionen ähnelt Threema stark WhatsApp, bietet aber auch Eigenständiges, zum Beispiel das Erstellen von Umfragen. Threema kostet als einzige getestete Software auch für Privatpersonen Geld, je nach Store knapp vier Euro. Für Unternehmen gibt es „Threema Work", das Mobile Device Management (MDM) unterstützt. Unter anderem wird die Software von der Schweizer Regierung und Daimler verwendet.

Die Verschlüsselung hält nicht mit dem Double-Ratchet-Verfahren mit. Sehr schön ist dagegen, dass der Betreiber seine Software schon mehrfach von Dritten auditieren ließ und sehr offen mit den Ergebnissen umgeht. Ebenfalls ein Plus: Threemas IDs sind anonym und werden nur auf Wunsch mit Telefonnummern oder Mailadressen verknüpft.

- Server in EU
- anonymer Betrieb möglich
- keine Sticker und GIFs
- keine kostenlose Version

WhatsApp

WhatsApp war lange Zeit das Tempo-Taschentuch der Messenger: Seit Jahren kommt fast keine Junggesellinnen-Vorbereitung oder Kindergeburtstags-Organisation ohne die grüne App aus, zumindest hierzulande. Außer in deutschsprachigen Ländern ist WhatsApp in ganz Europa, Nordamerika, Russland und Indien populär – lediglich in Ostasien nutzen Menschen häufig andere Messenger. Laut Statista verwenden 2 Milliarden Menschen regelmäßig WhatsApp, es ist damit der meistgenutzte Messenger der Welt.

Doch spätestens seit den neuen Nutzungsbedingungen denken immer mehr Leute darüber nach, ob WhatsApp wirklich die beste Wahl ist. Zwar verschlüsselt der Messenger brav Ende zu Ende, aber was ist mit den Metadaten (siehe Artikel auf S. 24), fließen die womöglich doch in Facebooks Datensammlung?

Auch fernab von Sicherheitsbedenken spricht vieles gegen WhatsApp. Ganz grundlegend nervt zum Beispiel, dass der Desktop-Client nur läuft, wenn das Mobilgerät mit dem Netz verbunden ist. Außerdem ist ein Datenexport, um ohne WhatsApp-Client auf seine Chats zuzugreifen, sehr umständlich (siehe Artikel auf S. 20).

- gute Verschlüsselung
- einfach zu bedienen
- kaum Schutz von Metadaten
- Telefonnummern-Zwang

Wire

Wire wird häufig vergessen, wenn es um sichere Messenger geht – dabei hat die Software durchaus ihre Fans. Die Wire Swiss GmbH sitzt in der Schweiz, entwickelt wird die Software in Berlin, die Server befinden sich in der EU.

Die Wire-Clients wirken nicht ganz so stromlinienförmig wie die Konkurrenz, funktionieren generell aber ordentlich. Etwas nervig ist, dass der App-Start nach dem Tipp auf eine Benachrichtigung häufig mehrere Sekunden dauert. An einigen Stellen versucht Wire, Dinge anders zu machen, zum Beispiel mit einer netten Kritzeln-Funktion.

Zur Verschlüsselung setzt Wire auf eine Variante des Double-Ratchet-Verfahrens. Wer einen Chat als sicher markieren will, muss allerdings alle Geräte seines Gegenübers einzeln verifizieren. Nur dann bekommt man auch angezeigt, wenn sich neue Geräte in einen Chat einklinken. In unverifizierte Chats könnte der Betreiber theoretisch eigene Geräte einschleusen und mitlesen, weil der Wire-Server das dafür nötige Passwort kennt. In Zukunft will Wire diese Lücke durch den Umstieg auf Messaging Layer Security (MLS) schließen, einen Standard für sichere Chatsysteme, an dessen Entwicklung sich Wire beteiligt.

- Server in EU
- gute Verschlüsselung
- App manchmal schwerfällig
- E2EE-Lücke in unverifizierten Chats

Monetarisierung gestartet werden, um Infrastruktur und Gehälter zu finanzieren. Durov habe eine Strategie entwickelt, um Telegram „langfristig zu sichern". Das soll so unauffällig passieren, dass „die meisten Nutzer fast keine Veränderung" feststellen.

Neben einem nachvollziehbaren Geschäftsmodell sorgt ein offener Quellcode für Vertrauen – schließlich kann man im Zweifel nachschauen, was App und Server so machen. Von unseren Testkandidaten sind Element, Signal und Wire komplett quelloffen, also sowohl die Clients als auch die Server-Software – allerdings ist der von Signal veröffentlichte Servercode veraltet. Bei Telegram und neuerdings auch bei Threema kann man sich nur den Client-Code anschauen. Was auf den Servern passiert, bleibt Betriebsgeheimnis. WhatsApp ist vollständig closed-source.

Fazit

Ginge es ausschließlich um Komfort und Funktionsvielfalt, würde Telegram diesen Test mit Pauken und Trompeten gewinnen: Dank Cloud-Speicherung muss man bei Telegram nie nervige Backups machen,

außerdem bietet die App etliche Features, die die Konkurrenz nicht hat, zum Beispiel das Hinzufügen von Kontakten nur über den Standort („Leute in der Nähe“) und einen superschnellen Browser-Client. Betrachtet man jedoch die Sicherheit, fällt Telegram durch: Die Cloud-Speicherung ist hochproblematisch, schließlich weiß niemand, wer wie, wann und wo Zugriff auf die Daten hat. Außerdem muss man die Ende-zu-Ende-Verschlüsselung umständlich manuell einschalten und sie hat auch noch etliche Nachteile, zum Beispiel dass man die „geheimen Chats“ nur auf dem Haupt-Mobilgerät abrufen kann. Die anderen Messenger beherrschen saubere Ende-zu-Ende-Verschlüsselung auf mehreren Geräten gleichzeitig.

Ausnahme ist dabei Threema, das keine Kopplung mehrerer Geräte unterstützt. Die Entwickler arbeiten aber schon dran. Auch bei der Ende-zu-Ende-Verschlüsselung geht Threema eigene Wege und bietet Eigenschaften wie Forward- und Future-Secrecy nicht. Element, Signal, WhatsApp und Wire nutzen dagegen das Double-Ratchet-Verfahren. Unterschiede zeigen sie unter anderem in Gruppenchats – wo manche Kandidaten etwa Forward-Secrecy fallen lassen – und beim „Wartungsaufwand“. Im Test machte besonders Element Probleme; manche Räume mussten wir neu anlegen, damit alle Teilnehmer mitlesen konnten. Bei Wire hakelte die Einbindung zusätzlicher Clients, Logout und Re-Login halfen aber. WhatsApp stiehlt sich hier aus der Verantwortung: Der Desktop-Client funktioniert nur in Kombination mit dem Handy.

Das größte WhatsApp-Ablöse-Potenzial hat Signal: Es ist einfach zu bedienen, kostet nichts und bietet fast die gleiche Funktionsvielfalt wie die grüne App vom Facebook-Konzern. Allerdings befinden sich die Signal-Server nicht in Europa, weshalb der DSGVO-Status unklar bleibt. Zweifelsfrei nachweisen, ob ein Messenger DSGVO-konform ist, könnte man ohnehin nur mit einer Zertifizierung – die es zurzeit auf dem Markt noch nicht gibt. Am weitesten lehnt sich zu diesem Thema Threema aus dem Fenster, das Unternehmen schreibt auf seiner Website klipp und klar: „Threema ist DSGVO-konform“.

(jkj@ct.de) c't

Literatur

[1] Sylvester Tremmel, Für immer unlesbar, Wie moderne Kommunikationsverschlüsselung funktioniert, c't 03/2021, S. 60

Sichere Messenger

Name	Element	Signal
URL	https://element.io	https://signal.org
Hersteller	New Vector Ltd., künftig Element	Signal Messenger LLC
Mobil-Clients für	Android ab 5.0, iOS ab 11.0	Android ab 4.4, iOS ab 11.0
Desktop-Clients für	Browser, Windows, macOS, Linux	Windows, macOS, Linux
Desktop-Clients ohne aktives Mobilgerät nutzbar	✓	✓
mehrere Mobilgeräte je Konto	✓	✓[1]
mehrere Konten je Gerät	–	–
deutsche Version verfügbar	✓	✓
Kontakte		
Anmeldung / anonyme Nutzung möglich	Matrix-ID, Mailadresse, Telefonnummer, Drittanbieter-Accounts (Google, Facebook etc.) /✓(mit anonymer Mailadresse)	Telefonnummer / –
Adressbuchabgleich	–	✓
neue Kontakte hinzufügen	Matrix-ID, QR-Code, optional über Identity-Server (Mailadresse, Telefonnummer)	Telefonnummer, Einladung
Gruppenchat (maximale Größe)	✓ (unbegrenzt, evtl. Server-limitiert)	✓ (1000)
Online-Status (abschaltbar)	– (eigentlich möglich, zurzeit auf matrix.org deaktiviert)	–
Inhalte		
fernlöschbare / selbstlöschende Nachrichten	✓ / –	✓ / ✓
Text nachträglich editierbar	✓	–
Textnachrichten zitieren / weiterleiten	✓ / ✓	✓ / ✓
Nachrichten liken	✓ (beliebige Emojis)	✓ (beliebige Emojis)
SMS verwalten	–	✓
Emojis / Sticker / GIF-Suche	✓ / ✓ / –	✓ / ✓ / ✓
Bilder / Videos / Dateien senden	✓ / ✓ / ✓	✓ / ✓ / ✓
Sprachnachrichten	–	✓
Telefonie / Videocalls	✓ / ✓	✓ / ✓
Standort: fix / live	– / –	✓ / –
Umfrage erstellen	–	–
Info zugest. / gelesen (abschaltbar)	✓ / ✓ (–)	✓ / ✓ (✓)
Suchfunktion Global / Einzelchat	✓ / ✓ (im Test unzuverlässig)	✓ / ✓
Besonderheiten	föderiert, offener Standard (Matrix), öffentliche Gruppen, über Bridges Interoperabilität mit über 20 anderen Messengern	Gesichter blurren in Fotos, Vermeidung von Metadaten
Sicherheit & Privatsphäre		
Geschäftsmodell Anbieter	optionale Abomodelle, Lizenzierung/Support	Non-profit (spendenfinanziert)
Firmenstandort	UK / Frankreich	USA
Serverstandort	Europa	USA
Open-Source (Client/Server)	✓ / ✓	✓ / –[4]
Reproducible Builds möglich	✓ (nur Android)[5]	✓ (nur Android)
Chats Ende-zu-Ende-verschlüsselt	✓	✓
Chat-Verschlüsselungsprotokoll	Olm[7]/Megolm	Signal[7]
Forward Secrecy / Future Secrecy / Deniability [8]	✓[2] / ✓[2] / ✓	✓ / ✓ / ✓
Server speichert Chat-Verläufe	✓	–
Backup	nutzerseitig verschlüsselt, auf Anbieter-Server	nutzerseitig verschlüsselt, lokal
Export von Chat-Verläufen	–	–
Kontakt-Verifizierung	QR-Code, Emoji-Code	manuell, QR-Code
Profilinformat. E2E-verschlüsselt	–	✓
Kontakt blockieren	✓	✓
App mit PIN- oder Biometrie-Sperre	✓	✓
Bewertung		
Verbreitung	⊖	○
Funktionsumfang	○	⊕
Bedienung	⊖	⊕
Sicherheit und Privacy	○	⊕
Preis	kostenlos	kostenlos

[1] nur ein Smartphone [2] nur in 1:1-Chats [3] für EU-Nutzer [4] veröffentlichter Server-Code veraltet [5] vom Anbieter nicht beworben
⊕⊕ sehr gut ⊕ gut ○ zufriedenstellend ⊖ schlecht ✓ vorhanden – nicht vorhanden

	Telegram	Threema	WhatsApp	Wire
	https://telegram.org	https://threema.ch	https://www.whatsapp.com	https://wire.com
	Telegram Messenger LLP	Threema GmbH	WhatsApp Ireland Limited[3]	Wire Swiss GmbH
	Android ab 4.1, iOS ab 9.0	Android ab 4.4, iOS ab 10.0	Android ab 4.03, iOS ab 9.0 (nur iPhone, nicht iPad)	Android ab 7.0, iOS ab 10.0
	Browser, Chrome-App, Windows, macOS, Linux	Browser	Browser, Windows, macOS	Browser, Windows, macOS, Linux
	✓	–	–	✓
	✓	–	–	✓
	✓	–	–	✓
	✓	✓	✓	✓
	Telefonnummer / –	Threema-ID / ✓	Telefonnummer / –	Telefonnummer oder Mailadresse / ✓ (mit anonymer Mailadresse)
	✓ (optional)	✓ (optional)	✓	–
	Telefonnummer, „Kontakte in der Nähe", optionaler Username	Threema-ID, QR-Code	Telefonnummer, QR-Code	Mailadresse, Telefonnummer, Username
	✓ (200.000, „Broadcast"-Gruppen unlimitiert)	✓ (256)	✓ (256)	✓ (500)
	✓ (✓)	–	✓ (✓)	–
	✓ (ohne Hinweis) / ✓	– / –	✓ / ✓	✓ (ohne Hinweis) / ✓
	✓	–	–	✓
	✓ / ✓	✓ / ✓	✓ / ✓	✓ / ✓ (ohne Hinweis)
	–	✓[2]	–	✓
	–	–	–	–
	✓ / ✓ / ✓	✓ / – / –	✓ / ✓ / ✓	✓ / – / ✓
	✓ / ✓ / ✓	✓ / ✓ / ✓	✓ / ✓ / ✓	✓ / ✓ / ✓
	✓	✓	✓	✓
	✓ / ✓[2]	✓[2] / ✓[2]	✓ / ✓	✓ / ✓
	✓ / ✓	✓ / –	✓ / ✓	✓ / –
	✓	✓	–	–
	✓ / ✓ (–)	✓ / ✓ (✓)	✓ / ✓ (✓)	✓ / ✓ (✓)
	✓ / ✓	✓ (nur Android) / ✓	✓ / ✓	– / ✓
	Video-„Sprachnachrichten" als Kreisvideo, „In der Nähe"-Funktion, öffentliche Gruppen, praktische Bots, WhatsApp-Import	Vertrauensstufen für Kontakte	Mitteilungs-Feed („Status") für Kontakte, Nachricht-an-alle-Kontakte-Funktion („Broadcast")	„Ping", Zeichnen-Funktion, Soundeffekte bei Sprachnachrichten
	privatfinanziert, geplant: Werbe- und Premium-Features (keine Werbung in Privatchats).	Bezahlapp, Variante für Unternehmen („Threema Work")	Werbung, Funktionen für Unternehmen (geplant)	optionale Abomodelle
	VAE	Schweiz	Irland[3]	Schweiz
	verteilt	Schweiz	verteilt	EU
	✓ / –	✓ / –	– / –	✓ / ✓
	✓	✓ (nur Android)	–	–
	–[6]	✓	✓	✓
	MTProto v2	NaCl crypto_box	Signal[7]	Proteus[7]
	✓ / – / ✓	–[9] / – / ✓	✓ / ✓[2] / ✓	✓ / ✓ / ✓
	✓	–	–	–
	serverseitig verschlüsselt, auf Anbieter-Server (ohne E2EE-Chats)	nutzerseitig verschlüsselt, lokal (Android); Systembackup (iOS)	serverseitig verschlüsselt, auf Google- bzw. Apple-Servern	nutzerseitig verschlüsselt, lokal
	✓[10]	✓	✓	–
	manuell, visueller Vergleich	QR-Code	manuell, QR-Code	manuell
	–	✓	–	–
	✓	✓	✓	✓
	✓	✓	✓	✓
	⊕	○	⊕⊕	○
	⊕⊕	○	⊕	○
	⊕⊕	⊕	⊕	⊖
	⊖	⊕	○	⊕
	kostenlos	3,99 € (Apple App Store, Google PlayStore), 3,60 € (Android-APK über shop.threema.ch)	kostenlos	kostenlos

[6] optional in 1:1-Chats möglich [7] Double-Ratchet-Variante [8] in Chats, Erläuterungen in c't 3/2021, S. 60 [9] nur in Transportverschlüsselung [10] über Desktop-App

Nichts zurücklassen

WhatsApp-Chats archivieren

Wer sich von WhatsApp verabschiedet, will nicht auch alle alten Chats über Bord werfen. Zum Glück lassen sich die Nachrichten auch ohne WhatsApp-Account erhalten. Wir haben uns mehrere Methoden angeschaut und zeigen, was sich lohnt und was nicht.

Von Stefan Porteck

Sobald man Freunde und Verwandte davon überzeugt hat, WhatsApp den Rücken zuzukehren, zeigt sich ein weiteres Problem: Die alten WhatsApp-Chats sind verloren, sobald man sein Nutzerkonto löscht. Kein leichter Abschied, denn jeder hat den einen oder anderen Chat, an dem schöne Erinnerungen hängen.

Glücklicherweise gibt es mehrere Wege, die alten Chats, Sprachnachrichten, Bilder und Videos zu sichern, um später jederzeit darin herumstöbern zu können. Wir haben uns Tools und Wege angeschaut, die ein Backup der Nachrichten versprechen – mit gemischten Ergebnissen.

Für die meisten Nutzer reichen die Backups völlig aus, die sich unter Android und iOS mit WhatsApp-Bordmitteln erledigen lassen – die WhatsApp aber gut versteckt: Für den Export öffnet man zunächst den gewünschten Chat und tippt dort oben rechts auf das Dreipunktemenü und wählt dort „Mehr" und dann „Chat exportieren".

Das folgende Dialogfenster erfragt, ob der Export auch gesendete und empfangene Medien – also Bilder, Videos und Sprachnachrichten – enthalten soll. Hier wählt man die Option mit Medien. Im folgenden Dialog speichert man die Dateien entweder lokal oder in einem Cloud-Speicher wie Dropbox oder Google Drive.

Der Export erhält eine Textdatei, die die einzelnen Nachrichten nebst Namen der Verfasser sowie Zeitstempeln und Verweisen auf die mitgeschickten Medien enthält. Sie lässt sich mit jedem Texteditor öffnen und durchsuchen. Das ist effizient, aber nicht besonders schön – doch dazu später mehr. Darüber hinaus landen im Export die im Chat enthaltenen Fotos, Sticker, Videos und Sprachnachrichten.

Bei Chats mit sehr vielen Nachrichten oder Medien erlebt man aber eine Enttäuschung, denn sie sind nicht vollständig – sie beginnen nicht am Tag 1 der Unterhaltung, sondern mitunter erst Jahre später. Das liegt daran, dass WhatsApp pro Chat maximal 40.000 Einträge exportiert. „Diese Einschränkungen sind auf die maximale E-Mail-Größe zurückzuführen", schreibt das Unternehmen auf seiner Webseite. Gemeint sind nicht nur die angehängten Medien, sondern auch die Anzahl der Nachrichten innerhalb der Textdatei.

Das ergibt aus mehreren Gründen keinen Sinn: Erstens ist es ohnehin keine gute Idee, den Export per Mail vom Handy zu schicken, weil die meisten Provider Mails mit ein paar hundert angehängten Bildern ablehnen dürften, und zweitens ist es völlig unklar, warum die Nachrichten innerhalb der Textdatei in die Rechnung eingehen.

Um das beschnittene Backup zu erweitern, exportiert man denselben Chat direkt ein zweites Mal und wählt dabei die Option ohne Medien aus. Im zweiten Backup befindet sich nun eine neue Textdatei, die hoffentlich den gesamten Chatverlauf enthält. Diese kopiert man zum ursprünglichen Export und erhält einen Chat-Verlauf

mit Medien und allen Nachrichten. Wer sichergehen will, dass kein Bild fehlt, greift unter Android einfach zu einem Dateimanager wie dem Total Commander und sichert die Medien von Hand. Sie liegen im sogenannten internen gemeinsamen Speicher, der den Pfad /storage/emulated/WhatsApp/Media hat. Dort finden sich in separaten Unterordnern sortiert nach Audio, Video, Dokumenten und Bildern alle Medien aller Chats und lassen sich einfach per USB auf den PC oder aufs Notebook kopieren.

Schöner aufbereiten

Das mit der Exportfunktion erzeugte Backup zeigt mehrere Schönheitsfehler. Der offensichtlichste: Das Lesen der Nachrichten ist in Textdateien ohne Einrückungen ziemlich anstrengend. Für eine ansprechende Aufbereitung der Chats gibt es verschiedene Tools. So stellt der Open-Source-Webdienst WA-Reader die Konversationen deutlich gefälliger und im Look des WhatsApp-Chatfensters dar. Dafür lädt man die Textdatei auf der Webseite https://whatsapp-reader.herokuapp.com hoch und bekommt den Chart inklusive Emojis präsentiert. Da die Verarbeitung auf dem Server des Anbieters stattfindet, ist es keine gute Idee, sich damit Chats mit sensiblen Inhalten anzuschauen. Wer seine Privatsphäre schützen will, lädt den WA-Reader von der Github-Seite des Anbieters herunter und lässt ihn in einer Python-Umgebung lokal auf dem eigenen Rechner laufen.

Der Wermutstropfen: Die Bilder werden nicht in die grafische Aufbereitung des Chats eingebunden. Trotzdem reicht der Textexport in den meisten Fällen zum Schwelgen in Erinnerungen aus – schließlich weiß man ja, dass man sich alle zugehörigen Bilder im entsprechend mitgesicherten Ordner separat anschauen könnte.

Mitgeschnitten

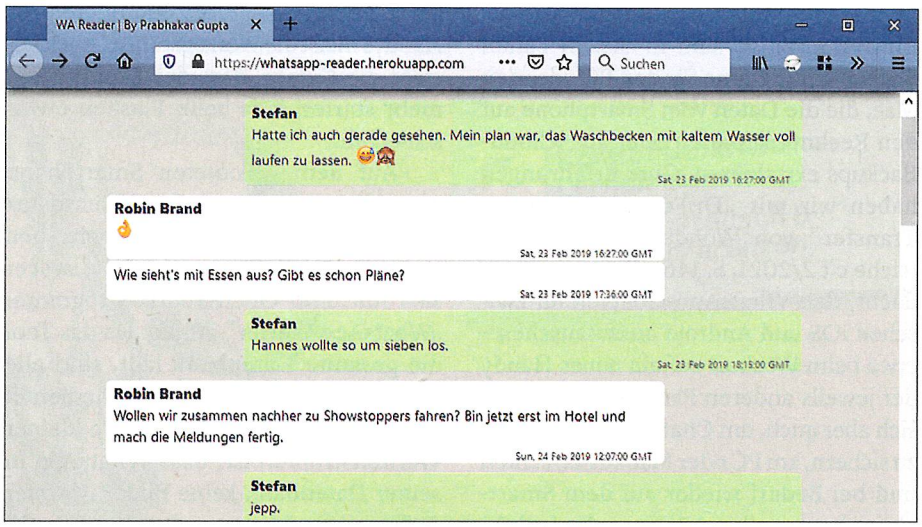
Ist es zu mühsam, alle erhaltenswerten Chats einzeln anzufassen, müssen zusätzliche Tools her. Das clevere Chrome-Browser-Add-On „Backup WhatsApp Chats" macht sich zunutze, dass sich WhatsApp außer auf dem Smartphone auch im Browser verwenden lässt. Dafür ruft man die URL https://web.whatsapp.com auf und scannt mit der WhatsApp-App auf dem Smartphone den auf der Webseite angezeigten QR-Code, worauf der eigene WhatsApp-Account mit dem Browser verknüpft wird. Das Add-On lädt dann einfach die gewünschten Chats im Browser, greift dabei die Nachrichten ab und speichert sie als CSV- oder HTML-Datei auf der Festplatte. Sofern die Bilder und Videos des Chats sich noch auf dem Handy befinden, werden sie auch in der Webansicht dargestellt und landen ebenfalls im vom Add-On angelegten Backup. Hat man sie zwischenzeitlich vom Smartphone gelöscht, zeigt auch die Web-Ansicht von WhatsApp nur Platzhalter an.

Zumindest laut den Bewertungen im Chrome-Web-Store und unseren Versuchen mit einem Testaccount mit wenigen Chats und Medien scheint das Tool zu funktionieren. Mit jahrelang gewachsenen Konten haben wir es aber aus gutem Grund nicht ausprobiert: Bei der Nutzung gewährt man dem Tool den Vollzugriff auf alle Chats und zugehörige Medien. Wahrscheinlich hat nahezu jeder mindestens einen Chat mit sensiblen Inhalten wie Bankdaten, Adressen oder Ähnlichem, und in so manchem Gruppenchat finden sich unvorteilhafte Fotos der letzten Geburtstagsfeier. Alle diese Daten könnte das Browser-Add-On theoretisch abgreifen. Ob man dem Anbieter vertrauen will, muss jeder für sich selbst entscheiden.

Gute Tools, schlechte Tools

Darüber hinaus versprechen diverse Android-Apps, ein vollständiges Backup der Chats aus dem internen Speicher des Handys zu ziehen. Viele von ihnen kosten ein paar Euro. Die meisten Nutzer werden nicht glücklich mit den Apps – beispielsweise, weil sie moderne Android-Geräte haben. Einige solcher Lösungen für Android versuchen, mit Hilfe der Android-Debug-Bridge (adb) einen Dump des internen WhatsApp-Speichers anzulegen und so dessen Datenbank nebst der nötigen kryptografischen Schlüssel zu kopieren. Doch dem hat Google schon mit Android 10 einen Riegel vorgeschoben, um zu verhindern, dass Malware Daten aus Banking-Apps oder eben auch aus verschlüsselnden Messengern abgreift. Backup-Apps, die direkt auf dem Smartphone laufen, scheitern auf neueren Geräten ebenfalls, da aktuelle Versionen von Android ihnen nur noch Zugriff auf ihre eigenen internen Speicher und den gemeinsam genutzten Speicher geben, nicht aber auf die Bereiche anderer Apps.

Wer noch einen Uralt-Knochen besitzt, schafft es mit solchen Apps und Programmen mitunter schon, eine Kopie der WhatsApp-Datenbank und der internen Schlüsseldateien zu erstellen, dennoch scheitern die Tools nicht selten an deren Verschlüsselung. Sie wurde in der Vergangenheit immer wieder angepasst. Unter Android zeigt sich mit einem Blick auf die Dateien der Datenbank, womit man es zu tun hat: Dateien mit dem Namen msgstore.db.crypt12 identifizieren die aktuelle Ausbaustufe. Manche Backup-Tools können trotz vorhandenem Keyfile mit crypt12 nicht umgehen. Statt ihre Entschlüsselungsroutinen an das neue Format anzupassen, setzen sie deshalb auf gepatchte oder ältere WhatsApp-Versionen, die die älteren Varianten db.crypt5 oder db.crypt7 nutzen. Einige Backuptools empfehlen deshalb, sich eine alte WhatsApp-Version zu besorgen. Sofern man sie von Diensten wie APK-Mirror herunterlädt, ist das kein Problem. Andere Tools bringen eigene



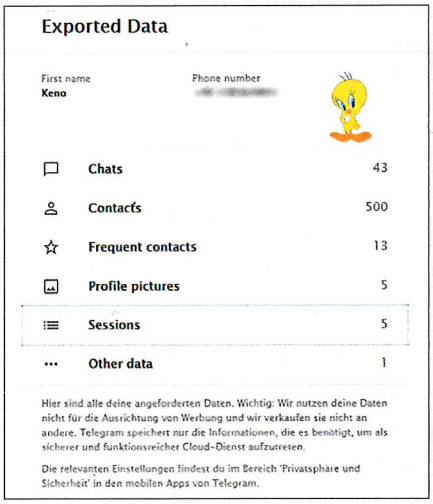
Die als Textdatei exportierten Chats lassen sich mit dem WA-Reader entweder im Web oder lokal in der gewohnten Form betrachten.

Vorbildlich: So funktionieren Datenexport und Backup bei Telegram

Telegram ist schnell, komfortabel und hat sehr viele Funktionen – nur leider ist der Messenger nicht sonderlich sicher (siehe Test auf S. 14). Vor allem die Speicherung jeglicher Inhalte in der Cloud ist problematisch; schließlich kann niemand wissen, wer Zugriff auf die Telegram-Server hat.

Wer deshalb auf einen sichereren Messenger wechselt, aber Chats, Fotos, Videos und Sprachnachrichten von Telegram sichern will, hat es deutlich leichter als beispielsweise bei WhatsApp – Telegram bringt nämlich eine sehr komfortable Exportfunktion mit. Diese findet man zurzeit ausschließlich im Desktop-Client, der für Windows, macOS und Linux erhältlich ist. Die Funktion verbirgt sich unter Einstellungen/Erweitert/Daten Exportieren. Achtung: Bei „Privaten Gruppen" ist „Nur meine Nachrichten" voreingestellt, wenn die Chat-Backups also inhaltlich Sinn ergeben sollen, muss man das Häkchen wegklicken.

Außerdem lässt sich auswählen, ob das Backup im HTML- oder JSON-Format gespeichert werden soll. Als Datenhalde zum einfachen späteren Nachlesen im Browser eignet sich das HTML-Format am besten. Um aufs Backup zuzugreifen, muss man lediglich die Datei „export_results.html" im Hauptverzeichnis des Backup-Download-Verzeichnisses anklicken, schon kann man sich komfortabel durch die gespeicherten Chats hangeln. Schön: Es werden nicht nur die in den Chats geposteten Fotos, Videos und Sprachnachrichten gespeichert, sondern auch Sticker und GIFs. *(jkj@ct.de)*



Einfach durchklicken durchs Backup: Telegram exportiert alle Daten vorbildlich im HTML-Format.

WhatsApp-Apps gleich mit. Aus Sicherheitsgründen sollte man davon bei kostenlosen Tools aber eher die Finger lassen.

Wegen der schieren Menge weiterer Backup-Tools ist es kaum möglich, vorab herauszufinden, welches Tool wirklich zuverlässig die alten WhatsApp-Chats retten kann. Einen Hinweis geben die Bewertungen im jeweiligen App-Store, doch mit jedem WhatsApp- oder Firmware-Update mag sich die Situation ändern. Zusammenfassend lässt sich sagen: Sowohl unter Android als auch unter iOS funktionierten Backup-Apps, die auf dem Smartphone laufen, in der Regel nicht mehr.

Generalschlüssel

Eine Alternative sind in diesen Fällen Backup-Programme für den PC oder den Mac, die die Daten vom Smartphone auf den Rechner kopieren oder aus iCloud-Backups extrahieren. Gute Erfahrungen haben wir mit „Dr.Fone – WhatsApp Transfer" von Wondershare gemacht (siehe c't 2/2021, S. 146). Es ist dafür gedacht, den WhatsApp-Chatverlauf zwischen iOS und Android auszutauschen – etwa beim Wechsel auf ein neues Handy der jeweils anderen Plattform. Es eignet sich aber auch, um Chats unverschlüsselt zu sichern, am PC oder Mac zu betrachten und bei Bedarf wieder auf dem Smartphone herzustellen. Mit einem Preis ab 29 Euro ist WhatsApp Transfer aber nicht gerade die billigste Lösung.

Wirklich zuverlässig klappt das volle Backup der kompletten Datenbank auf Android-Geräten mit Root-Zugriff – also solchen, bei denen man mit Administratorrechten auf das gesamte Dateisystem zugreifen kann. Dafür finden sich in einschlägigen Webforen wie XDA-Developer für praktisch jedes Gerät passende Anleitungen.

Beim Entsperren des Bootloaders wird allerdings aus Sicherheitsgründen das Handy auf Werkseinstellungen zurückgesetzt – es gehen alle Nutzerdaten verloren. Vorher sollte man also eine Sicherung aller Daten (inklusive denen von WhatsApp) vorgenommen haben. Zudem verfällt beim Entsperren und Rooten des Handys meist die Werksgarantie. Auch besteht die Gefahr, dass das Handy nicht mehr startet, falls beim Flashen etwas schiefgeht.

Auf dem gerooteten Smartphone navigiert man in den Ordner /data/data/com.whatsapp/databases und kopiert den gesamten Inhalt auf den PC. Dort lässt er sich mit dem Open-Source-Programm „WhatsApp Viewer" öffnen. Da das Tool die gesamte Datenbank lädt, sind alle Chats mit ihren zugehörigen Medien in einer Oberfläche zu finden. Ein kleiner Wermutstropfen ist, dass WhatsApp in seiner Datenbank keine Bilder in voller Auflösung speichert, sondern nur Thumbnails. Beim Durchscrollen der alten Chats stört das nicht, wer aber Bilder und Videos in voller Auflösung behalten möchte, muss sie wie oben beschrieben gesondert auf den PC kopieren.

Fazit

WhatsApp bietet immerhin eine rudimentäre Exportfunktion, die trotz einiger Nachteile in den meisten Fällen völlig ausreichen dürfte. Wer sich bequemere und weniger sperrig aufbereitete Archive wünscht, greift zu generischen Smartphone-Backup-Tools oder WhatsApp-Spezialisten. Hierfür muss man aber ein paar Euro investieren, und nach unseren Erfahrungen funktionieren viele Tools unter aktuellen Betriebssystemen nicht mehr. Auf der sicheren Seite ist man mit einem gerooteten Android-Telefon: Man kopiert einfach die interne WhatsApp-Datenbank auf den PC und öffnet sie mit einem Viewer-Tool – ratsam ist das aber nur für Frickler, die bereits Erfahrungen mit dem Flashen alternativer Android-ROMs besitzen.

WhatsApp macht es einem also nicht gerade leicht, einzelne oder alle Chats für die Ewigkeit zu sichern und ohne die Smartphone-App zu betrachten. Wie es besser geht, zeigt ausgerechnet Telegram (siehe Kasten). Vielleicht nimmt man aber auch den Wechsel zu einem neuen Messenger zum Anlass, einen digitalen Hausputz vorzunehmen und Ballast über Bord zu werfen. *(spo@ct.de)* c't

Weitere Infos: ct.de/yune

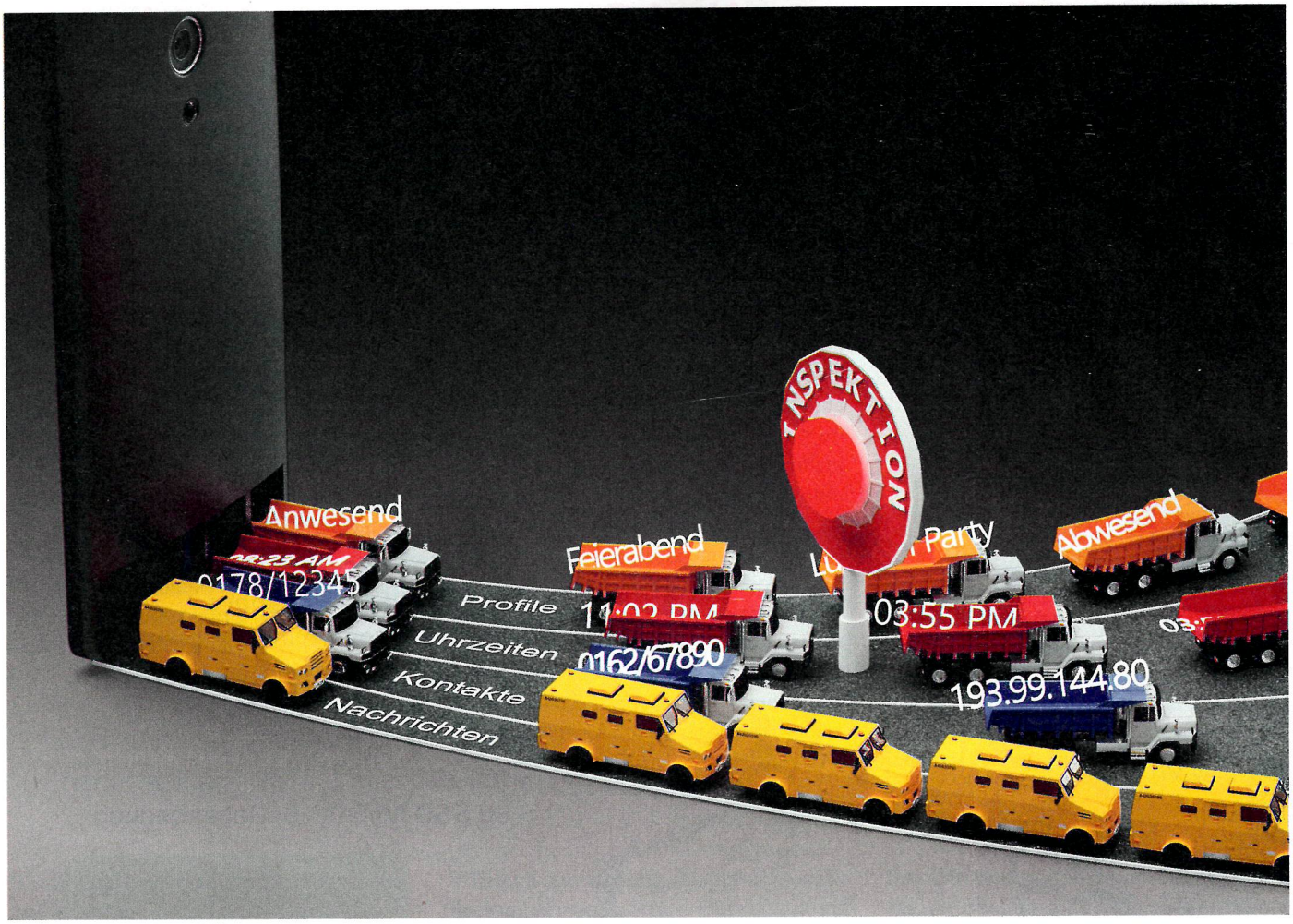


Bild: Andreas Martini

Ohne Sendungsverfolgung

Wie Messenger versuchen, Metadaten zu vermeiden

Seit immer mehr Messenger Ende-zu-Ende-verschlüsseln, rücken die sogenannten Metadaten in den Fokus. Aus ihnen lassen sich viele Schlüsse ziehen – kein Wunder, dass WhatsApp mit Metadaten eher indiskret umgeht. Andere Messenger machen das besser.

Von Sylvester Tremmel

Metadaten sind Daten über Daten. Im Kontext von Messengern gehören dazu zum Beispiel die Accounts von an einem Chat beteiligten Personen, Informationen über die Mitglieder einer Gruppe, Versand- und Empfangszeitpunkte und so weiter – Informationen, die zwar zur Kommunikation gehören, aber nicht selbst Inhalt der Kommunikation sind. Gängige Ende-zu-Ende-Verschlüsselungen erfassen Metadaten nicht, weshalb Chat-Betreiber und teilweise auch Dritte sie auswerten können.

Aus solchen Auswertungen lassen sich vielfältige Schlüsse ziehen. Neben den Freundes- und Bekanntenkreisen – die viel verraten – kann man zum Beispiel auch Tagesabläufe rekonstruieren: Die erste Reaktion auf eine Nachricht vom Vorabend schränkt den Zeitpunkt des Aufstehens ein. Eine Messenger-App, die sich werktäglich unter der IP-Adresse eines Unternehmens meldet, lässt auf den eigenen Arbeitgeber schließen. Ulmer Forscher konnten allein aus dem Anwesenheitsstatus bei WhatsApp zum Beispiel Tagesabläufe und Abweichungen davon rekonstruieren sowie herausfinden, wer mit wem sprach [1].

Aber wie verhindert man solche Rückschlüsse? Nachrichten haben nun mal notwendigerweise einen Absender, eine Reihe von Empfängern und werden zu bestimmten Zeitpunkten versendet und empfangen. Metadaten gänzlich zu vermeiden ist tatsächlich nicht möglich. Aber man kann sie reduzieren, Zugriffe auf sie beschränken und vermeiden, dass Metadaten miteinander oder mit anderen Daten korreliert werden.

Es lässt sich zum Beispiel nicht verhindern, dass Sende- und Empfangszeitpunkte existieren. Man kann sich zwar einen Messagingdienst suchen, der solche Daten angeblich nicht speichert, aber kontrollieren kann man das nicht. Wer dem Versprechen nicht traut, muss eigene Server betreiben: Der Messenger Element nutzt zum Beispiel Matrix, ein offenes Chatprotokoll. Wer will, kann selbst einen Matrix-Server aufsetzen und darüber zum Beispiel mit der eigenen Familie chatten. Um Metadaten muss man sich dann keine Sorgen machen. Neben Matrix ist auch das offene Chatprotokoll XMPP verbreitet. Beide Protokolle „föderieren", man kann also auch mit Leuten chatten, die sich bei anderen Servern angemeldet haben – dann muss man sich aber wieder um Metadaten sorgen und den Betreibern dieser Server vertrauen.

Schutz durch Pseudonyme

Der Messenger Threema geht das Problem anders an. Er versucht zu verhindern, dass entstehende Metadaten aufschlussreich sind: Threema kann zwar sehen, dass Account X Nachrichten mit Account Y austauscht, aber Accounts werden bei Threema über bedeutungslose Nummern identifiziert. Mit der Information, dass „UVB8A8CN" mit „63IMJ3F7" chattet, lässt sich – egal ob mit oder ohne Uhrzeit – wenig anfangen. Ähnliches lässt sich bei Messengern wie Element oder Wire erreichen. Sie erlauben, Benutzernamen frei zu wählen – wer sich eine sinnlose Zeichenkette als Name ausdenkt, chattet unerkannt.

Bei Messengern, die stattdessen E-Mail-Adressen oder Telefonnummern als IDs nutzen, können die Accounts deutlich leichter Personen zugeordnet werden. Schlimmstenfalls ist die Telefonnummer öffentlich verzeichnet und die E-Mail-Adresse enthält den vollen Namen. Trotzdem gehen auch datenschutzfreundliche Messenger diesen Weg, weil dadurch Gesprächspartner einander viel leichter finden – wer kennt schon die Threema-ID jedes Arbeitskollegen. In [2] haben wir ausführlich erklärt, wie Messenger versuchen, mit dieser Problematik umzugehen.

Damit pseudonyme Adressen wirklich schützen, dürfen Nutzer sie natürlich nicht mit anderen identifizierenden Daten verknüpfen. Wenn „UVB8A8CN" als E-Mail-Adresse „max-mustermann@firma.de" im Account hinterlegt hat, ist zumindest für den Dienstbetreiber klar, mit wem „63IMJ3F7" chattet. Aber auch ohne solche Fehler können pseudonyme Adressen nicht verhindern, dass Netzwerke entstehen. A redet mit B und C, C antwortet B nur selten, chattet aber viel mit D und so weiter. Solche Netzwerke lassen sich – zumindest theoretisch – mit anderen bekannten sozialen Graphen vergleichen, um herauszufinden, wer A, B, C und D sind. Und bekannte soziale Graphen stehen von Google über Facebook zu Twitter vielfach zur Verfügung.

Von der Post lernen

Um solche Vergleiche unmöglich zu machen, wissen Messenger-Anbieter idealerweise gar nichts über die Bekanntschaftsnetzwerke. Aber wie soll Alice Bob eine Nachricht schicken, ohne dem Dienstbetreiber zu offenbaren, dass Alice und Bob sich kennen? Dass das möglich ist, zeigt ein analoges Beispiel: Die Post stellt einen Brief von Alice an Bob auch dann zu, wenn Alice nicht als Absender auf dem Brief vermerkt ist.

Damit das praktisch funktioniert – und auch wirklich die Kommunikation zwischen Alice und Bob verschleiert –, müssen aber zwei Voraussetzungen erfüllt sein. Erstens muss es eine Art Briefkasten geben, der anonym Briefe annimmt. Wenn Alice mit ihrem Brief zum Postamt geht, ist es unerheblich, ob sie einen Absender notiert; die Post sieht ja, wer den Brief aufgibt. Zweitens muss man solche Briefkästen irgendwie vor Spam schützen. Wenn jeder und jede unerkannt Briefe einwerfen darf, wäre unerwünschte Post sonst kaum zu vermeiden. Bei der realen Post schützen die Kosten für eine Briefmarke – bedingt – vor Spam.

Der einzige Messenger im Test auf Seite 14, der so ein System tatsächlich umsetzt, ist Signal. Die App nennt das Feature „Sealed Sender" (siehe ct.de/y5rr). Es ist für Nachrichten von bekannten Kontakten immer aktiv und funktioniert im Prinzip wie das Beispiel mit der Post: Statt sich am Server anzumelden und eine Nachricht samt Adressat abzugeben, kontaktiert die App den Server anonym und übergibt die Nachricht. Der Server stellt sie dann zu, ohne zu wissen, von wem sie stammt.

Damit man Nachrichten nicht unter falschem Namen versenden kann, ist eine Sealed-Sender-Mitteilung zweifach verschlüsselt. Der Empfänger B entfernt die erste Verschlüsselung und findet darin die eigentliche Nachricht und eine Art Unterschrift des Absenders. So überprüft er, dass die Nachricht von A kommt, was der Server ja nicht weiß. Wenn die Nachricht authentisch ist, entfernt B auch die innere Verschlüsselung und liest die Nachricht.

Das Spam-Problem umgeht Signal, indem es Sealed-Sender-Nachrichten nur von Kontakten erlaubt, die der Empfänger bereits kennt. Wer solchen Missbrauch nicht fürchtet, kann die Beschränkung in den Einstellungen der App aufheben.

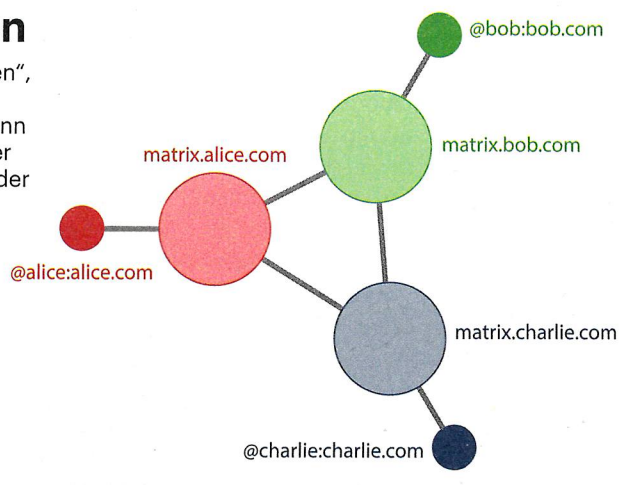
Verkehrsüberwachung

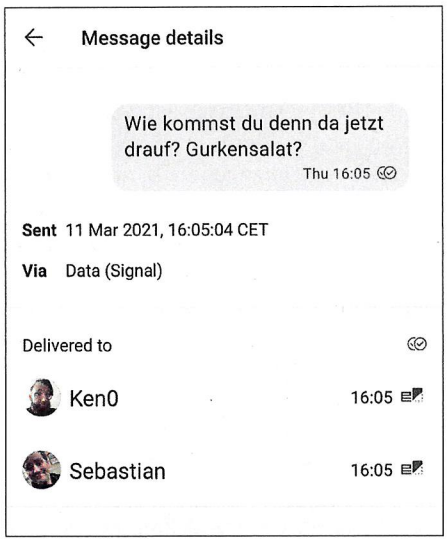
Sealed-Sender verhindern auf der Ebene des Messenger-Protokolls, dass bekannt wird, wer mit wem redet. Hundertprozentigen Schutz bieten sie aber nicht. Zum Beispiel lassen sich Sender und Empfänger von Nachrichten auch auf Ebene der IP-Adressen korrelieren. Wenn IP X 3412 Bytes an einen Messenger-Server schickt und der gleich darauf 3412 Bytes an IP Y, dann liegt der Schluss nahe, dass X mit Y chattet.

Solche Traffic-Analysen kann nicht nur der Messagingdienst selbst anstellen, sondern auch ein Lauscher auf der Leitung oder der Server- beziehungsweise Rechen-

Föderationen

Matrix-Server „föderieren", sodass es viele Server (große Kreise) geben kann und trotzdem alle Nutzer (kleine Kreise) miteinander chatten können. Wer einen eigenen Server aufsetzt und keine Unterhaltung über Servergrenzen hinweg führt, muss sich um Metadaten kaum Sorgen machen.





Auf Wunsch zeigt Signal den Sealed-Sender-Status an (kleine Icons rechts unten): Die Nachricht wurde an beide Gesprächspartner übermittelt, ohne dass der Server wusste, von wem sie stammt.

zentrums-Dienstleister. Traffic-Analysen sind aber, zumindest bei einigermaßen rege genutzten Messengern sehr aufwendig. Systeme wie Sealed Sender bieten daher durchaus einen echten Nutzen – ganz besonders für Dienste wie Signal, die Telefonnummern als Adressen verwenden. Wem das nicht reicht, der muss zu extremeren Maßnahmen wie dem dezentralen Messenger Briar greifen: Der nutzt das Tor-Netzwerk, um Nachrichten auszutauschen und dabei die beteiligten IP-Adressen zu verschleiern. Aber auch Tor garantiert keine absolute Sicherheit, und Briars kompromissloser Fokus auf Datenschutz schränkt die Benutzerfreundlichkeit durchaus ein. Zum Beispiel müssen Kommunikationspartner gleichzeitig online sein, um chatten zu können.

IP-Adressen sind nicht nur problematisch, weil sie eventuell verraten, wer mit wem redet. Sie lassen sich oft auch einem geografischen Gebiet zuordnen und verraten damit den ungefähren Aufenthaltsort. Messenger tun das einerseits gegenüber dem Chat-Anbieter und eventuellen Dienstleistern – ungut, aber ein ganz allgemeines Problem: Jeder Webseitenaufruf verrät dem Webseitenbetreiber dieselbe Information (und noch viel mehr).

Problematisch wird die Geolokalisierung von IP-Adressen auch an anderer Stelle, nämlich wenn Chatpartner Sprach- oder Videoanrufe tätigen. In gängigen Implementierungen tauschen die beteiligten Apps dabei direkt Daten aus und leiten sie nicht über Server des Anbieters. Das verrät den Gesprächsparteien die IP-Adressen ihrer Gegenüber. Wer das ist, wissen sie meist ohnehin, aber die IPs erlauben eben auch eine Einschränkung des Standorts, was eventuell nicht gewünscht ist. Manche Messenger erlauben daher, auch Sprach- und Videodaten über den Anbieterserver zu leiten. Je nach Standort und Auslastung des Servers kann das aber die Performance beeinträchtigen.

Members only

Neben dem eigentlichen Nachrichtenaustausch können Messagingdienste auch noch durch eine andere verbreitete Funktion erfahren, wer wen kennt – durch Gruppen. Auf den ersten Blick mag das überraschen: Gruppenmitglieder kennen einander natürlich, aber wieso muss der Dienstanbieter wissen, wer in welcher Gruppe ist? Tatsächlich muss er das an sich nicht. Damit Alice, Bob und Charlie eine Gruppe bilden, reicht es im Prinzip, wenn die drei sich darauf einigen. Nachrichten an so eine „Gruppe" sind ganz normale Nachrichten, nur sendet jeder eben immer zwei Stück gleichzeitig. Alice sendet an Bob und Charlie, Bob an Alice und Charlie und Charlie an Alice und Bob. Für den Anbieterserver ist nichts besonderes zu erkennen, er weiß nicht mal, dass eine Gruppe existiert.

Tatsächlich hat Signal seine Gruppen früher so organisiert, aber dieser naive Ansatz hat erhebliche Probleme. In modernen Messengern sind Gruppen nämlich nicht nur eine Ansammlung von Nutzern. Sie haben einen Namen und eventuell ein Bild oder eine Beschreibung – alles schützenswerte Metadaten. Außerdem sollen gelegentlich neue Mitglieder aufgenommen oder alte entfernt werden. All das muss man bei diesem Ansatz über Nachrichten zwischen den Gruppenmitgliedern lösen, der Anbieter weiß schließlich nicht mal, dass eine Gruppe existiert.

Solche Verwaltungsnachrichten, die Gruppeninformationen ändern und Mitglieder bearbeiten, können sich aber überschneiden, wenn mehrere Gruppenmitglieder sie parallel versenden. Diese Race-Conditions treten bei Messengern leicht auf: Gruppenmitglieder sind oft nicht gleichzeitig online und es dauert dadurch lange, bis Nachrichten alle Mitglieder erreicht haben.

Vollends an seine Grenzen stößt der Ansatz, wenn Gruppenmitglieder unterschiedliche Rechte haben sollen. Welche Instanz kontrolliert, wer was darf? Was, wenn sich eine Nachricht zum Entzug eines Rechts mit einer anderen Nachricht, die dieses Recht ausübt, überschneidet? Letztlich ist auch Signal wegen solcher Beschränkungen von dem System abgerückt und speichert Gruppeninformationen mittlerweile auf dem Server. Andere Messenger machen das seit jeher so; die Betreiber wissen also, wer in welchen Gruppen ist, wie Gruppen heißen et cetera.

Um diesen Preis nicht zu zahlen, verschlüsselt Signal die Gruppeninformationen so, dass der Server sie nicht lesen kann. Das ist alles andere als trivial, schließlich soll der Server das Rechtesystem durchsetzen. Er muss also entscheiden, ob ein Nutzer die Informationen ändern darf, ohne zu erfahren, wer dieser Nutzer ist. Die Signal-Entwickler haben sich dafür mit Kryptografie-Forschern von Microsoft zusammengetan und ein mathematisch ausgefeiltes System von „anonymous credentials" – anonymen Legitimationen – erarbeitet (siehe ct.de/y5rr).

Fazit

Ganz ohne Metadatenspuren kann man nicht chatten. Manche Informationen lassen sich kaum vermeiden und manche Einschränkungen führen zu weit. Man kann es aber zumindest besser machen als WhatsApp. Dieser Messenger nutzt nämlich (anders als Threema) keine pseudonymen IDs, erlaubt (im Gegensatz zu Element) keine eigenen Server und versucht nicht (wie Signal) Kontakte und Gruppenmitgliedschaften zu verschleiern. Rigorose Versprechen, Metadaten nicht zu speichern oder weiterzugeben, findet man bei WhatsApp ebenso wenig. Alle genannten Alternativen bieten also Vorteile gegenüber WhatsApp, am weitesten treibt Signal die Metadatenvermeidung. Die ideale Schnittmenge – verschleierte Absender und Gruppen, eigene Server und pseudonyme IDs – bietet aktuell allerdings kein Messenger. *(syt@ct.de)* c't

Literatur

[1] Andreas Buchenscheit et al, Privacy Implications of Presence Sharing in Mobile Messaging Applications: https://dl.acm.org/doi/10.1145/2677972.2677980

[2] Sylvester Tremmel, Zeigt her Eure Kontakte, Warum Messenger nach Ihrer Telefonnummer fragen, c't 06/2021, S. 118

Informationen zu Sealed Sender und anonymen Gruppen: **ct.de/y5rr**