Von Whatsapp auf Signal umsteigen!

#tldr: Es ist höchste Zeit zu hinterfragen, ob Whatsapp nicht mehr aus unserem Leben wegzudenken ist. Hinter der Kommunikations-Plattform Whatsapp steckt Facebook, ein IT-Konzern, dessen Geschäftsmodell darin besteht, mit den Daten seiner Nutzerinnen zu handeln. Der Datenskandal bei Facebook erschüttert das Vertrauen in Technologie-Giganten insgesamt und nachhaltig. Der Messenger Whatsapp ist schon wegen ihrer Besitzerin nicht mehr über alle Zweifel erhaben. Im Vergleich zu anderen Chat-Apps schneidet Whatsapp zudem nicht rosig ab. Vor allem eine App erweist sich im Bezug auf Sicherheit und Privatsphäre als überlegen: Der kostenlose Messenger «Signal».

Logo by Whatsapp, Facebook Inc.

Der von 1.3 Miliarden Menschen genutzte Messenger Whatsapp hat im Jahre 2016 Ende-zu-Ende-Verschlüsselung implementiert. Das bedeutet, dass nur Chat-Teilnehmerinnen die Inhalte der übermittelten Nachrichten sehen können. Selbst die Server von Whatsapp können die Nachrichten weder entschlüsseln noch mitlesen. Die Verschlüsselung beruht auf dem Verfahren von Open Whisper Systems. Dieses Verfahren gilt in der Sicherheits-Branche als äusserst sicher. Leider weist Whatsapp, welche von Facebook für 16 Milliarden Dollar aufgekauft wurde, beim Design wesentliche Schwachstellen auf, welche die Sicherheit der Nutzerinnen gefährden können.

Zum einen speichert Whatsapp (Facebook) auf ihren Servern die Metadaten der Chats. Somit kann weiterhin nachvollzogen werden, wer mit wem zu welchem Zeitpunkt kommuniziert hat. Diese Metadaten können mehr über die Nutzerinnen verraten, als wir auf den ersten Blick vermuten würden. Facebook ist eine gewinnorientiertes Unternehmen, welches von der Aus- und Verwertung von Daten lebt. Deshalb ist damit zu rechnen, dass sie diese Metadaten auswerten. Sie haben sich zwar durch die Implementierung von starker Verschlüsselung selber der Möglichkeit beraubt, auf die Inhalte der Whatsapp-Chats zuzugreifen. Dieser Umstand verdient angesichts der Tatsache, dass selbst Google bis heute keine sichere E-Mail-Kommunikation anbietet, eine gewisse Anerkennung. Google will konsequent mitlesen, auslesen, einordnen.

> *Das Leben und die Gesundheit sehr vieler Menschen hängt von sicherer Kommunikation ab.*

Zum anderen legt Whatsapp beim Konkurrenten Google optional ein verschlüsseltes Backup an. Einen eigenen Server für die Sicherung zu verwenden, gehört nicht zum Funktionsumfang. Dieses Backup kann vorerst nicht ohne Weiteres entschlüsselt und verwertet werden. Wer direkten, physischen Zugang zu einem Smartphone hat, kann dieses Backup jedoch mittels einer Spezial-Software entschlüsseln. Womöglich genügt es bereits, ein Smartphone mittels Schadsoftware zu übernehmen und fernzusteuern. Geheimdienste und Hacker reiben sich die Hände. Wer sich denkt, er habe wieder einmal nichts zu verlieren, versetze sich kurz in die Lage von Regime-Kritikerinnnen in totalitären Regimen! Unter solchen Bedingungen ist sichere Kommunikation eine Frage von Leben und Tod, Freiheit oder Gefangenschaft. Das Leben und die Gesundheit sehr vieler Menschen hängt von sicherer Kommunikation ab. Angehörige westlicher Demokratien ignorieren diese überlebenswichtige Notwendigkeit allzu leichtfertig.

> *Wer Whatsapp weiterhin nutzen will, ist gut beraten, die Einstellung "zuletzt*

> *online" zu deaktivieren.*

Eine weitere Schwachstelle von Whatsapp ist die Möglichkeit, die Aktivitäten von Nutzerinnen anhand der Information, wann eine Nutzerin "zuletzt online" war, auszulesen und mit den Aktivitäten anderer Teilnehmerinnen des Telefonbuches in Verbindung zu bringen. War das bislang nur mit aktiven Nachforschungen möglich, so existiert mittlerweile eine dreiste Stalking-App, welche diese Verfolgung von Freunden und Bekannten automatisiert. Daraus lassen sich Rückschlüsse auf das Privatleben und die Kommunkation anderer ziehen. Geht eine Beziehung gerade in die Brüche? Wer chattet mit wem zu später Stunde? Die Informationen, die man aus solchen Verknüpfungen ableiten kann, verletzen die Privatsphäre der Nutzerinnen erheblich. Obwohl auch diese Stalking-App nicht in der Lage ist, Inhalte von Chats mitzulesen, lassen sich aus diesen Metadaten sehr persönliche Informationen über die Beziehungen zwischen Freunden und Bekannten oder deren Gewohnheiten ableiten. Wer Whatsapp weiterhin nutzen will, ist gut beraten, die Einstellung "zuletzt online" zu deaktivieren. Doch Whatsapp kann problemlos durch sicherere Messenger-Apps ersetzt werden.

> *Signal bietet das eindrückliche Feature, dass sich Nachrichten nach einer vom Sender festgelegten Zeitdauer selber löschen.*

Logo by Signal, Open Whisper Systems

Jene Organisation, welche die Verschlüsselungs-Technologie für Whatsapp entwickelt hat, bietet selber einen kostenlos verfügbaren Messenger an, der vieles besser macht als Whatsapp. Open Whisper Systems entwickelte den Messenger «Signal». Dieser Nachrichten-App verzichtet auf die Weitergabe und Speicherung von Metadaten. Telefonummern aus dem Adressbuch werden nicht an Server weitergegeben. Einzig für die Registrierung ist die einmalige Angabe der eigenen Nummer erforderlich. Die Verschlüsselung und der Programm-Code wurde in einem Peer-Review-Verfahren überprüft und gilt als sicher. Ein externes Backup der Chats gibt es nicht. Sollte das Telefon verloren gehen oder ersetzt werden müssen, können die Chatverläufe nicht wiederhergestellt werden. Aus Sicherheitsüberlegungen ist dieser Verzicht sinnvoll. Ferner bietet Signal das eindrückliche Feature, dass sich Nachrichten nach einer vom Sender festgelegten Zeitdauer selber löschen. Diese Nachrichten verbleiben lediglich im Gedächtnis des Empfängers. Hochsensible Informationen lassen sich somit weder von Hackern noch von Geheimdiensten rekonstruieren. Ja, auch die Strafverfolgungsbehörden bleiben aufgrund dieses «Killer-Features» aussen vor. Wie damit umzugehen ist, muss in separaten philosophischen Betrachtungen diskutiert werden.

https://brain-rain.ch/wp-content/uploads/2018/04/InfatuatedMeaslyBittern.mp4

Selbstvernichtendes Tape aus «Mission Impossible».

Signal bietet ferner verschlüsselte Telefonie an. Die App ist für alle grossen Mobil- und Desktop-Plattformen verfügbar und unmittelbar einsetzbar. Sie steht allen Interessenten als Open Source zur Verfügung, kann also von allen Experten eingesehen und auf Sicherheitslücken überprüft werden. Ein solches Sicherheits-Audit wurde durchgeführt mit dem Ergebnis, dass Signal aussergewöhnlich gut und sicher programmiert wurde. Renommierte Experten wie der Sicherheits-Forscher Bruce Schneier oder der Whistleblower Edward Snowden bürgen für die Sicherheit dieser App. Es gibt gute Gründe, diesen Menschen zu vertrauen. Einerseits wissen sie, wovon sie sprechen, andrerseits sind sie auf absolut sichere Kommunikation angewiesen.

> *Als Maxime der Technologie-Sicherheit gilt: Die Methoden und Algorithmen müssen offen, einsehbar und überprüfbar sein.*

Der Fakt, dass Signal als offener Quelltext angeboten wird, wirkt einer feindlichen Übernahme oder Unterwanderung der ursprünglichen Programmierer entgegen. Sollte sich die Ausrichtung von Open Whisper Systems zum Nachteil der Nutzerinnen ändern, können andere den sicheren Entwicklungszweig weiterführen. Ferner fallen absichtlich im Quellcode eingebaute Fehler aufgrund des offenen Entwicklungsmodelles schneller auf. Als Maxime der Technologie-Sicherheit gilt: Die Methoden und Algorithmen müssen offen, einsehbar und überprüfbar sein. Proprietäre, nicht einsehbare Verschlüsselungs-Software gilt als Schlangenöl, ein Wundermittel, welches keine nachweisbare oder sogar eine schädliche Wirkung hat.

> *Werbung und Verschlüsselung schliessen sich aus.*

Wenn sich hingegen bei Facebook das Geschäftsmodell ändert, könnte die Verschlüsselung von Whatsapp sehr schnell aufgeweicht werden. Dass genau dies eintreffen wird, ist gar nicht einmal so abwegig, denn schon lange herrscht bei Facebook Ratlosigkeit darüber, wie man die Millarden-Investition in Whatsapp endlich in klingende Münze verwandeln kann. Es wurde schon darüber nachgedacht, Whatsapp-Nutzerinnen personalisierte Werbung in die Chats auszuspielen. Wenn sich jedoch Facebook in verschlüsselte Chats einklinken will, muss die Verschlüsselung aufgehoben oder relativiert werden. Ein Festhalten an Verschlüsselung in Kombination mit Werbung kann nämlich nur bedeuten, dass diese zwischengeschalteten Werbe-Botschaften als kontextlos, absurd, aberwitzig bis beleidigend empfunden werden. Werbung und Verschlüsselung schliessen sich aus. Die Zukunft wird zeigen, wie Facebook Whatsapp ausserhalb der Verwertung von Metadaten zu monetarisieren gedenkt.

> *Der Umstieg auf Signal ist das Gebot der Stunde.*

Es hat sich gezeigt, dass es auch abgesehen vom mangelnden Vertrauen in Facebook unzählige Gründe gibt, von Whatsapp auf Signal umzusteigen. Erschwerend bei diesem Umstieg kommt anfänglich hinzu, dass Signal noch nicht über die kritische Masse von Nutzerinnnen verfügt. Wer mit seinen Freundinnen sicher kommunizieren will, muss diese zuerst davon überzeugen, Signal zu installieren. Eine Möglichkeit ist, dieses Plädoyer für Signal zu teilen. Ferner sind alle aufgerufen, in ihrem nächsten Umfeld Überzeugunsarbeit für Signal zu leisten. Ein breiter Einsatz von Signal schenkt uns nicht nur mehr Sicherheit und Privatsphäre, sondern mindert unsere grosse Abhängigkeit von unberechenbaren US-Konzernen, welche mehr an Geld als am Wohl ihrer Kundschaft interessiert sind. Der Umstieg auf Signal ist das Gebot der Stunde.