Instant-Messenger im Privatsphäre-Check

Florian Göhring

HTWK Leipzig

florian.goehring@htwk-leipzig.de

7. Dezember 2018

Zusammenfassung

In Zeiten des Instant-Messaging hat sich WhatsApp in der Breite etabliert, doch mit dem Nutzerwachstum hat sich auch die Skepsis verstärkt. Nach der Übernahme durch Facebook sind die Sicherheitsbedenken größer denn je. Nun hat WhatsApp angekündigt, zukünftig personalisierte Werbung anhand der Chatinhalte zu schalten, was einen Eingriff in die Privatsphäre der Nutzer bedeutet. Alternativen wie Signal oder XMPP sind vorhanden, doch werden sie trotz zahlreicher Vorteile von der Allgemeinheit kaum wahrgenommen. Die Monopolstellung ermöglicht die Fortführung von WhatsApps Handlungen.

I. Einführung

WhatsApp ist der verbreitetste Instant-Messenger[1], der auf Smartphones existiert. Die App hat mehr als eine Milliarde Nutzer weltweit, doch das muss nicht unbedingt heißen, dass es die beste Anwendung dieser Art ist.

Nachdem WhatsApp von Facebook gekauft wurde[2], prophezeiten viele einen bevorstehenden Datenmissbrauch. Nun, gut vier Jahre später, scheinen sich die Befürchtungen zu bewahrheiten. Nachdem sich die Blicke auf Facebook und den Cambridge-Analytica-Skandal richteten, wurde nun für WhatsApp angekündigt, 2019 personalisierte Werbung zu schalten, deren Inhalte auf Chatverläufe zurückzuführen sind, indem die Ende-zu-Ende-Verschlüsselung geöffnet wird.

Alternativen gibt es, doch nicht jede ist besser. Für die Nutzer ist der Umstieg schwer, denn „Jeder hat WhatsApp.“, „Das ist zu umständlich“ oder „Wir können nichts ändern“.

[1] vgl. https://www.statista.com/statistics/272014/, 07.12.2018

[2] siehe https://heise.de/-2118920, 07.12.2018

II. WhatsApp technisch erklärt

WhatsApp ist ein so genannter Walled Garden: eine geschlossene Plattform, die durch Restriktionen die Wahlmöglichkeiten des Nutzers einschränkt. Das bedeutet, WhatsApp funktioniert nur mit WhatsApp, die Applikation ist fest vorgegeben.

Mit der Verwendung stimmen die Nutzer den AGBs und der Rechteanforderung auf ihr Endgerät zu. Dazu zählt der Zugriff auf die Telefonnummer und das Telefonbuch, welche auf die Server von WhatsApp hochgeladen und synchronisiert werden. Der Nutzung von Telefonnummern für Werbezwecke wird damit zugestimmt.

Das verwendete Verschlüsselungsprotokoll ist nicht öffentlich. Die Ende-zu-Ende-Verschlüsselung (E2E) ist ein Feature, welches WhatsApp eingeführt hat und jederzeit nach eigenem Ermessen ändern kann. Es besteht keine Gewissheit, wie die Daten beim Empfänger ankommen. Ebenso ist der gesamte Quellcode von WhatsApp nicht frei zugänglich.[1]

Alle Daten liegen zentral auf den Firmen-

Servern und können beliebig genutzt werden. Aufgrund des Finanzierungsmodells - dem Handel mit Daten - ist es möglich, dass vorliegende Daten verwendet werden.[2, S. 181f.]

III. Die Alternativen

WhatsApp bietet nicht die notwendigen Bedingungen für eine private Kommunikation. Doch Alternativen gibt es viele, welche den Schutz der Daten und der Privatsphäre der Nutzer gewährleisten.[1]

Signal Signal ist ein stetig verbesserter Instant-Messenger mit einer sicherheitsbewussten Firmenphilosophie[3]. Im Gegensatz zu WhatsApp ist Signal Open-Source, sodass jeder Nutzer den Quellcode einsehen kann. Mit E2E-Verschlüsselung wird der Schutz der Daten gewährleistet und Telefonnummern werden nicht synchronisiert. Finanziert wird die Non-Profit-Organisation über eine Stiftung. Der Messenger wird u. a. vom Whistleblower Edward Snowden empfohlen.[3, S. 6]

Neben Vorteilen wie verschwindende Nachrichten oder bessere Foto- und Videoqualität gibt es auch negative Aspekte: Signal ist ebenso ein Walled Garden und zur Registrierung wird die Telefonnummer genutzt. Dabei ist es auch nur einer von vielen Messengern.[2, S. 185ff.]

XMPP/Jabber Bei XMPP (oder Jabber) handelt es sich um ein quelloffenes Nachrichtenübertragungsprotokoll mit dezentraler Infrastruktur. Das bedeutet, es gibt mehrere Dienstanbieter, aus denen Nutzer selbst wählen können. Die Wahl des verwendeten Messengers ist frei (kein Walled Garden), die Kompatibilität untereinander ist größtenteils vorhanden und zur Nutzung wird keine Telefonnummer benötigt. Die Verschlüsselung funktioniert E2E, ist Open Source und öffentlich. Zudem ist es möglich, mehrere Konten anzulegen und parallel in einer Anwendung zu benutzen. So ist es denkbar, beispielsweise eine Nutzung mit einem Arbeits- und Privatkonto zu realisieren.

[3] aktuelle Maßnahme: `https://heise.de/-4207859`, 07.12.2018

Doch die Einrichtung ist zeitaufwändiger und für die meisten Nutzer zu umständlich, obwohl sie der einer E-Mail-Adresse entspricht. Kontakte müssen manuell hinzugefügt werden, da weder auf das Telefonbuch noch auf die Telefonnummer zugegriffen wird. Das Fehlen zahlreicher Features dürfte aber das größte Hindernis sein. Wo es bei WhatsApp möglich ist, z.B. Sprachnachrichten oder Kontakte zu senden, ist bei XMPP nur die Übertragung von Video, Bild und Text möglich.[2, S. 164ff.]

IV. Fazit

Es gibt noch weitere Alternativen auf dem Markt, doch es fehlt an der Umsetzung durch die Nutzer. Zu groß ist die Bequemlichkeit, zu klein die Einigkeit, wohin man wechseln soll, denn die eierlegende Wollmilchsau gibt es nicht.

Signal bietet ein gutes Leitbild, doch ist es ebenso ein Walled Garden. XMPP bietet als Föderation einen großartigen Datenschutz, doch fehlen die Features. Zudem wollen die Nutzer keine komplizierte Kontaktaufnahme, da die Erkennung über das Telefonbuch leichter ist.

Die Machenschaften von WhatsApp sollten dennoch nicht widerstandslos hingenommen werden, da ein solcher Umgang mit der Privatsphäre nicht akzeptabel ist. Möglicherweise wird die Schaltung von Werbung der entscheidende Initiator zum Wechsel vieler Nutzer.

Literatur

[1] Systemvergleich - Vergleich von WhatsApp mit freien, dezentralen Systemen. `https://www.freie-messenger.de/systemvergleich/`. Besucht: 07.12.2018.

[2] Johanna C Czeschik. *Gut gerüstet gegen Überwachung im Web - wie Sie verschlüsselt mailen, chatten und surfen*. Sybex, Wiley-VCH, Weinheim, 1. aufl. edition, 2016.

[3] Paul Rösler, Christian Mainka, and Jorg Schwenk. More is less: On the end-to-end security of group chats in signal, whatsapp, and threema. 04 2018.