Karl-Friedrich-Gymnasium Mannheim

ElternMedienMentoren am KFG

Smartphone-Sicherheit:
WhatsApp und die Alternativen

Über 50 Milliarden Nachrichten werden täglich über die *WhatsApp*-Server verschickt.
Gerade aber wegen dieser Popularität wird *WhatsApp* immer häufiger von Betrügern missbraucht, die gefälschte Zahlungsaufforderungen, Spam-Kettenbriefe u. ä. versenden. In letzter Zeit werden auch Abzock-Abos in Apps untergebracht, zum Beispiel als Werbebanner in Handy-Games. „Sie befinden sich meist am oberen oder unteren Bildschirmrand. Beim Spielen fallen sie meist nicht auf, klickt man diese aber aus Versehen an, kann es bei Abzocker-Apps sein, dass auch hier automatisch ein Abo-Vertrag geschlossen wird. Sie bekommen davon nichts mit, da dieser Vorgang komplett im Hintergrund läuft. Niemand, nicht einmal Ihr Netzanbieter kann Ihnen dann sagen, wann, wie, wo oder mit wem Sie diesen Vertrag geschlossen haben.“ [1]
Vor Abzock-Fallen können Sie sich schützen, indem Sie bei Ihrem Netzbetreiber eine Sperrung von Drittanbieterdiensten beantragen.

Ein großes Problem bei *WhatsApp* ist nach wie vor die sichere Verschlüsselung. Immer wieder wird von außen auf Sicherheitslücken aufmerksam gemacht und immer wieder wird bei *WhatsApp* nachgebessert. Ein „Katz-und-Maus-Spiel“ nennen es die Experten.[2]
Edward Snowden bezeichnete *WhatsApp* als wahrscheinlich spionageanfälligste Software, weil das Programm auf sämtliche Adressbuchkontakte zugreift.
Ende letzten Jahres nun führte *WhatsApp* endlich eine End-to-End Verschlüsselung für die Kommunikation zwischen Android-Geräten ein. Diese ist allerdings auf Einzelnachrichten beschränkt. Gruppen-Chats und verschickte Medien werden noch nicht verschlüsselt, ebensowenig die Kommunikation zwischen iOS-Geräten.
Das neueste Problem: Durch eine Sicherheitslücke in der neuen Telefonfunktion „WhatsApp Calls“ kann das Smartphone auch als Wanze fungieren. Denn mit der alten Android-Version 2.12.45 nimmt der Messenger heimlich alle *WhatsApp*-Telefonate auf. Auch in den Tests der Chip-Redaktion[3] wurden alle *WhatsApp*-Anrufe automatisch mitgeschnitten und im internen Speicher unter **WhatsApp -> Media -> WhatsApp Calls** hinterlegt. Nach dem Entpacken lassen sich alle Anrufe abspielen - dies gelingt aber nur mit der alten *WhatsApp*-Version 2.12.45. Ein Update beseitigt das Problem.

Außerdem lässt sich *WhatsApp* von seinen Nutzern bei der Installation weitreichende Befugnisse einräumen. So hat *WhatsApp* Zugriff auf Mikrofon, Fotos und Standortdaten und

[1] http://www.chip.de/news/Drittanbieter-sperren-und-Handy-Abo-Fallen-vermeiden_57745308.html
[2] www.datenschutzbeauftragter-info.de/whatsapp-und-datenschutz-antworten-auf-die-wichtigsten-fragen/
[3] http://business.chip.de/news/WhatsApp-warnt-vor-eigener-App-Android-Version-belauscht-Anrufe_73303306.html

überträgt diese Informationen an amerikanische Server. Damit trägt jeder *WhatsApp*-Nutzer eine potentielle Wanze mit sich herum, ohne zu wissen wann genau welche Daten zu welchen konkreten Zwecken übermittelt und wie lange sie gespeichert werden.
Daher wanderten seit der *WhatsApp*-Übernahme durch Facebook bereits viele Nutzer zu anderen Chat-Anbietern ab, die höhere Sicherheitsstandards versprechen; denn Facebook-Chef Mark Zuckerberg eignete sich mit der Übernahme von *WhatsApp* auch Daten wie Mobilnummern von mehr als 450 Millionen *WhatsApp*-Nutzern an.

Darüber hinaus können die Privatsphäre-Einstellungen mit wenig Aufwand von Dritten umgangen werden, so dass die eigenen *WhatsApp*-Aktivitäten offengelegt werden, selbst wenn man bei allen Optionen die strengsten Einstellungen auswählt. Um dies zu demonstrieren, veröffentlichte ein Open-Source-Entwickler im Februar die Software *WhatsSpy Public*:[4] Sie deckt den Online/Offline Status, das Profilbild, Statusupdates und Privatsphäre-Einstellungen auf. All diese Daten stellt das Tool für jede beliebige Telefonnummer, die zu einem *WhatsApp*-Account gehört, dar.

Fragwürdige Klauseln in der *WhatsApp* AGB
Laut AGB behält sich *WhatsApp* das Recht vor, alle im eigenen Profil mitgeteilten Daten zu nutzen. Der Haken hierbei: Alle Urheberrechte verbleiben trotzdem bei den App-Nutzern. Wird beispielsweise ein Bild versandt, an dem eigentlich Drittanbieter die Rechte besitzen, muss der Nutzer mit möglichen rechtlichen Folgen rechnen. Die Verbraucherschutzzentrale (VZBV) will laut Handelsblatt nun gegen diese umstrittene Klausel klagen. Allein die Tatsache, dass die Allgemeinen Geschäftsbedingungen eines in Deutschland tätigen Unternehmens nur in englischer Sprache vorliegen, sei gesetzeswidrig.
Die SHZ geht noch einen Schritt weiter und spricht von einer “digitalen Enteignung”:[5] Denn wer bei *WhatsApp* Bilder oder Texte verschicke, trete nach Auslegung der SHZ seine Rechte daran vollständig ab. Alles, was ein Nutzer poste, dürfe von *WhatsApp* ohne Einschränkungen weiterverbreitet werden, kostenlos in Werbeanzeigen genutzt oder weiterverkauft werden.

Daher warnen auch die Datenschützer: Wem die Vertraulichkeit der eigenen Kommunikation etwas wert ist, der sollte auf vertrauenswürdigere Dienste zurückgreifen.

Alternative Messenger

1. Threema

Der Schweizer Messenger *Threema* hat vor allem einen großen Vorteil: Seine Server stehen ausschließlich auf Schweizer Boden. Damit greift für den Anbieter das strenge europäische Datenschutzrecht und US-Geheimdienste können nicht einfach auf Nachrichten und Nutzerdaten zugreifen. Selbst wenn die NSA Zugriff auf die Daten bekäme, wären sie für die Beamten kaum von Nutzen. Grund: *Threema* nutzt eine sogenannte **End-to-End-Verschlüsselung**. Das bedeutet, dass Nachrichten, Bilder und andere Daten auf dem Gerät des Absenders verschlüsselt und erst auf dem Empfänger-Gerät entschlüsselt werden. Diese sogenannte „asymmetrische Kryptografie“ garantiert, dass nur der vorgesehene Empfänger Ihre Nachrichten lesen kann (zur Verschlüsselung setzt *Threema* auf die asymmetrische ECC-Chiffre mit einer Schlüsselstärke von 255 Bit). Das bedeutet:

[4] http://www.freeware.de/download/whatsspy-public/
[5] http://www.shz.de/nachrichten/deutschland-welt/netzwelt/whatsapp-wer-bilder-verschickt-tritt-rechte-ab-id6638266.html

Die App chiffriert jede Nachricht mit einem neuen Schlüssel, der ausschließlich auf dem verwendeten Gerät vorliegt. **Im Unterschied zu anderen populären Messaging-Apps (einschließlich derer, die Verschlüsselungen einsetzen), hat bei *Threema* selbst der Serverbetreiber absolut keine Möglichkeit, die Nachrichten mitzulesen.** Die kostenpflichtige App ist für iOS (1,79 Euro) und Android (1,60 Euro) verfügbar. [6]

2. Line

***Line* ist eine kostenlose Messenger-App der japanischen Firma Line Corporation, mit der man nicht nur chatten kann, denn zu den Stärken von *Line* zählen auch die kostenlosen Internet-Telefonate, die sich mit dieser App führen lassen.** Die Chatnachrichten lassen sich mit außergewöhnlichen Emoticons, Bildern und Videos erweitern. Mit der sogenannten „Timeline" lässt sich *Line* auch zum sozialen Netzwerk ausbauen. (In der neuen Version 4.3 wurde das Teilnehmerlimit in Gruppen auf 200 erhöht und eine Stickervorschau hinzugefügt.)
Sicherheit: Im Gegensatz zu *WhatsApp* verschlüsselt *Line* zwar alle Inhalte für den Transfer gut und sicher, doch benutzt es keine End-to-End-Verschlüsselung. Und noch eine Sicherheitslücke: Werden bei *WhatsApp* Telefonnummern unverschlüsselt für Dritte einsehbar, so ist es bei *Line* die Seriennummer des Smartphones.

3. Telegram

Diese App wirbt zu Recht mit ihrer sicheren Verschlüsselung: Zu Beginn des Jahres boten ihre Entwickler in einem Wettbewerb 200.000 Dollar demjenigen, dem es gelänge, eine abgefangene *Telegram*-Nachricht zu entschlüsseln. Bis Ablauf der Wettbewerbsfrist jedoch ist dies niemandem gelungen. Inzwischen wurde die Summe sogar auf 300.000 Dollar erhöht.
Auch *Telegram* operiert mit End-to-end-Verschlüsselung und ist zu Recht stolz auf seine unschlagbare Sicherheit.
Die Verschlüsselung erfolgt jedoch nicht automatisch, sondern muss vom Nutzer über die Option „Secret Chats" gewählt werden. Mit der Option „Self-Destruction" kann man einstellen, nach welcher Zeit ein Chat auf Sender- und Empfängerseite gelöscht werden soll.
Der russische Anbieter verkündete am 9.12. 2014 die Überschreitung der Rekordmarke von einer Milliarde versandter Nachrichten pro Tag. Für Datenschützer weniger erfreulich ist, dass *Telegram* die Adressbucheinträge seiner Nutzer speichert.

Die App ist für Android und iOS erhältlich, beide Versionen sind vollkommen kostenlos.

4. Tango

Der *WhatsApp*-Konkurrent *Tango* hat von Investoren 280 Millionen US-Dollar erhalten, davon allein 215 Millionen vom chinesischen Internetriesen Alibaba. Bereits 70 Millionen aktive Nutzer verwenden den Messenger, **der für Android und iOS erhältlich ist und sogar über eine Anruffunktion verfügt. Besonders zeichnet *Tango* die Möglichkeit aus, über das Programm Videoanrufe führen zu können – komplett kostenlos über 3G, 4G oder WLAN.** Sprachanrufe sind selbstverständlich ebenfalls möglich, jedoch ausschließlich zu anderen *Tango*-Nutzern. Gruppenchats sind mit bis zu 50 Personen möglich. *Tango* verfügt im Gegensatz zu *WhatsApp* über einen News-Feed, der Neuigkeiten von Freunden anzeigt. So können Fotos geteilt werden, die von Freunden mit einem lächelnden Smiley, ähnlich dem *Gefällt mir*-Button von Facebook, versehen werden können. Darüber hinaus besitzt *Tango* eine Spiele- und Musikplattform. [7]

---

6 http://beste-apps.chip.de/android/app/threema-android-app,ch.threema.app/

7 **http://www.smartphone-tarif-checker.de/apps/tango-gute-messenger-app-oder-nur-eine-weitere-whatsapp-alternative_1202.html**