WhatsApp verschlüsselt konsequent

Privatsphäre für eine Milliarde Nutzer

WhatsApp führt hochmoderne, respektable Ende-zu-Ende-Verschlüsselung ein, die selbst den Facebook-Servern den Einblick in unsere Nachrichten verwehrt – kann man das allen Ernstes glauben? Die Ergebnisse unserer Untersuchung deuten darauf hin, dass WhatsApp am Ende eines mehrjährigen Prozesses nun tatsächlich ein vollwertiger Krypto-Messenger ist.

VON FABIAN A. SCHERSCHEL

WhatsApp verschlüsselt seit gut anderthalb Jahren Chat-Nachrichten und Anhänge nicht nur im Transport, sondern auch Ende-zu-Ende. Eine solche Ende-zu-Ende-Verschlüsselung ist ein essenzieller Schutz der Privatsphäre des Anwenders, da der Dienstanbieter – in diesem Fall Facebook – bei alleiniger Transportverschlüsselung immer noch alle Nachrichten auf dem Server mitlesen kann. In der Theorie war die Einführung von Ende-zu-Ende-Verschlüsselung also sehr löblich, in der Praxis konnte sich der Nutzer allerdings bis jetzt nicht darauf verlassen, dass seine Nachrichten auch wirklich sicher waren. Das hat WhatsApp nun endlich geändert.

Ab sofort werden laut WhatsApp alle Nachrichten mit dem Signal-, ehemals TextSecure-, Protokoll mit Axolotl Ratcheting von Krypto-Koryphäe Moxie Marlinspike verschlüsselt. Der ist in der Krypto-Szene hoch angesehen. Darüber hinaus engagiert er sich als Privacy-Aktivist, was es unwahrscheinlich macht, dass er seine Seele an Facebook verkauft und bewusst Hintertüren implementiert. Das von ihm entwickelte Protokoll kommt auch beim Open-Source-Messenger Signal zum Einsatz und ist dort bis aufs kleinste Detail prüf- und verifizierbar.

Vertrauen ist gut, Kontrolle ist besser

Wie auch schon im Rahmen des WhatsApp-Schwerpunktes in c't 11/2015 wollten wir WhatsApp allerdings nicht einfach glauben und haben der App erneut auf den Zahn gefühlt. Ziel unserer Tests war es, herauszufinden, ob Android- und iPhone-Smartphones auch wirklich immer die Ende-zu-Ende-Verschlüsselung einsetzen. In unseren Tests im vorherigen Jahr konnten wir beobachten, dass iPhones mit WhatsApp weiterhin im Klartext innerhalb der Transportverschlüsselung mit anderen Geräten kommunizierten. Mit anderen Worten: Diese Nachrichten kamen lesbar und unverschlüsselt an den WhatsApp-Servern vorbei und hätten dort mitgelesen werden können. Die neue Verschlüsselung hatte folglich einen Aus-Schalter, denn eine manipulierte App oder ein Man-in-the-Middle konnte jederzeit veranlassen, dass im Klartext kommuniziert wird.

Bei neuerlichen Tests bedienten wir uns wieder mehrerer Telefone mit beiden Betriebssystemen und eines Laptops mit einem Python-Tool namens yowsup, welches WhatsApp-Nachrichten direkt über das Internet ins WhatsApp-Netz senden und daraus empfangen kann. Da die Python-Bibliothek quelloffen ist, konnten wir den Code so anpassen, dass er zum Beispiel beim Empfang einer Nachricht direkt den rohen, hoffentlich verschlüsselt empfangenen Text ausspuckt, bevor dieser bei der Krypto-Routine ankommt, die ihn entschlüsseln soll. Zwar beobachteten wir auch jetzt wieder unverschlüsselte Nachrichten, sobald aber einer der Gesprächspartner anfing, verschlüsselt zu kommunizieren, merkten sich das beide Partner und ab diesem Zeitpunkt beobachteten wir nur noch Ende-zu-Ende verschlüsselte Nachrichten.

Außerdem konnten wir wiederholt nachstellen, dass ein Löschen der privaten Schlüssel eines Endgerätes eine Warnung beim Gegenüber auslöst. Das passiert zum Beispiel bei einer kompletten Neuinstallation der App ohne Backup. Chatpartner, mit denen zuvor schon einmal verschlüsselt kommuniziert wurde, erhalten dann die Warnung, dass sich die „Sicherheitsnummer“ des Kontos geändert habe. Dazu muss man allerdings in den WhatsApp-Einstellungen unter dem Punkt Sicherheit anwählen, dass Sicherheitswarnungen angezeigt werden sollen. Ab Werk ist das bei den Android- und iOS-Apps deaktiviert.

Wir haben mehrfach versucht, die Apps zum Versenden oder Empfangen von Klartext zu bewegen, was uns allerdings nicht gelang. Auch das manuelle Verschicken unverschlüsselter Botschaften per yowsup an Gesprächspartner, mit

denen wir zuvor verschlüsselt kommuniziert hatten, schlug fehl. Es scheint also ganz so, als ob WhatsApp sein Versprechen gehalten hat. Wer an den Details unserer Untersuchung interessiert ist, kann diese in einem Hintergrundartikel auf heise Security nachlesen (siehe c't-Link).

Die Metadaten bleiben

Allerdings sind durch die Ende-zu-Ende-Verschlüsselung natürlich nicht alle potenziellen Probleme aus der Welt geräumt. Der Quellcode von WhatsApp liegt nicht offen, Anwender müssen Facebook also nach wie vor ein gewisses Vertrauen einräumen. Zum Beispiel, dass der Anbieter die geheimen Schlüssel nicht auf einem Seitenkanal von ihrem Smartphone ableitet und so die Nachrichten auf dem Server doch wieder entschlüsseln kann. Auch das Metadaten-Problem bleibt bestehen. Die WhatsApp-Server sehen zwar nicht den Inhalt der Nachrichten, aber sie können nach wie vor beobachten, wer mit wem spricht. Und WhatsApp macht keinen Hehl daraus, dass diese Daten gespeichert werden. Das ist besonders interessant für Strafverfolgungsbehörden und Geheimdienste, die diesen Daten fast so viele Informationen entlocken können wie dem Inhalt der eigentlichen Nachrichten.

Ob WhatsApp jetzt sicher verschlüsselt oder nicht, vielen Nutzern stößt es unangenehm auf, dass der Dienst gezwungenermaßen die Telefonnummern im Adressbuch des Smartphones auf die Facebook-Server lädt. Besonders im deutschen Firmenumfeld macht es die App damit zu einem No-Go, denn dieses Verhalten kollidiert ziemlich direkt mit dem rechtlichen Verständnis von Datenschutz hierzulande. Für die sichere Firmenkommunikation ist WhatsApp also nach wie vor keine Alternative.

Wer Geschäftsgeheimnisse oder noch sensiblere Informationen besprechen will, greift nach wie vor lieber zur Open-Source-Alternative Signal oder einem Messenger wie Threema, dessen erklärtes Geschäftsziel die Privatsphäre der Nutzer ist. Zumal Threema zusätzlich die Schlüsselverwaltung und das damit verbundene Vertrauensverhältnis zum Gesprächspartner klarer in den Vordergrund rückt. In einem solchen Einsatzgebiet stellt es immerhin auch kein Problem dar, dass man erst einmal alle Gesprächspartner dazu überreden muss, einen neuen Messenger zu installieren. Der Kreis ist beim Besprechen solcher Themen da eher überschaubar.

Nichtsdestotrotz ist es ein bedeutender Schritt, dass nun über eine Milliarde Nutzer von Ende-zu-Ende-Verschlüsselung profitieren, ohne dass sie sich dessen überhaupt bewusst sein müssen. WhatsApp und Facebook verzichten im Unterschied zu Google und vielen anderen Chat-Diensten auf die Option, die Nachrichten der Nutzer für Data Mining auszuschlachten. Das erschwert die Totalüberwachung durch Datenkraken und andere Übeltäter und verdient Anerkennung.

(fab@ct.de)

Auch iPhones können nun verschlüsselt bei WhatsApp chatten. Hier hat zum ersten Mal der Schlüsselaustausch mit unserem Python-Bot stattgefunden.

Über einen QR-Code kann man sich versichern, dass der auf dem eigenen Gerät gespeicherte Schlüssel auch wirklich zum Gegenüber passt.

Das Python-Tool yowsup erlaubt es uns, die empfangene Nachricht vor und nach der Verschlüsselung sichtbar zu machen.

Untersuchungsergebnisse: ***ct.de/yyg6***