Die Manipulation der Massen

Facebook wird WhatsApp massenhaft zur Überwachung einsetzen und dabei auch die Verschlüsselung knacken.

*Von **Jens Bernert.***

> Hinweis zum Rubikon-Beitrag: Der nachfolgende Text erschien zuerst im „Rubikon – Magazin für die kritische Masse“, in dessen Beirat unter anderem Daniele Ganser und Rainer Mausfeld aktiv sind. Da die Veröffentlichung unter freier Lizenz (Creative Commons) erfolgte, übernimmt KenFM diesen Text in der Zweitverwertung und weist explizit darauf hin, dass auch der Rubikon auf Spenden angewiesen ist und Unterstützung braucht. Wir brauchen viele alternative Medien!

Der US-Internetgigant Facebook hat die Massenüberwachung aller WhatsApp-Inhalte beschlossen und führt bei der Gelegenheit gleich noch eine Zensur mit ein (1). Dies berichtete das US-Wirtschaftsmagazin Forbes (2). Der Bruch der Privatsphäre ist allumfassend, Kryptografie wird ignoriert: Betroffen sind auch die verschlüsselte Kommunikation und sonstige Inhalte. Die abgehörten Daten wandern, wie bei den US-Giganten üblich — da gesetzlich vorgeschrieben — auch an die US-Behörden, die ein Treiber dieser „Innovation“ sein dürften.

Facebook will bei den Überwachungs- und Zensurmaßnahmen direkt in den Kommunikationsanwendungen ansetzen — vor allem bei WhatsApp. Dadurch entfällt für die US-Behörden — wie auch für Facebook — das aufwendige Suchen nach Sicherheitslücken in Geräten und Software, die es erlauben, Schadcodes oder eben Überwachungssoftware einzuschleusen. Zudem werden Sicherheitslücken in der Regel nach einiger Zeit gepatcht. Letzteres ist nun nicht mehr relevant und damit auch keine Hilfe mehr, da die neue Vorgehensweise eine völlig andere ist.

In dem Forbes-Bericht des AI- und Big-Data-Spezialisten Kalev Leetaru mit dem Titel „Die Verschlüsselungsdebatte ist vorbei — Tot in den Händen von Facebook“ heißt es unter anderem zu dem Vorstoß des US-Internetkonzerns (1):

„Historisch war das Kompromittieren von Endgeräten ein teurer und komplexer Prozess, getrieben von einem Katz- und Maus-Spiel mit Hardware- und Software-Herstellern, um Schwachstellen zu finden, die genutzt werden konnten, um sie (Überwachungs- und Schadprogramme, Anmerkung des Übersetzers) aus der Ferne zu installieren und die notwendigen Privilegien auf dem Gerät zu erhalten.

Solche Versuche sind schwer zu skalieren, und je mehr Geräte infiziert sind, desto wahrscheinlicher ist es, dass die Schwachstelle entdeckt und gepatcht wird.

Als Problemlösung stellte Facebook Anfang des Jahres erste Ergebnisse seiner Bemühungen, eine globale Massenüberwachungsinfrastruktur direkt auf die Geräte der Nutzer zu bringen, wo diese die Schutzmechanismen einer Ende-zu-Ende-Verschlüsselung umgehen kann, vor.

In Facebooks Vision soll der tatsächliche Ende-zu-Ende-Verschlüsselungsclient — wie WhatsApp — eingebettete Content-Moderation und Blacklist-Filteralgorithmen enthalten. Diese Algorithmen werden kontinuierlich von einem zentralen Cloud-Service upgedatet, die aber lokal auf dem Gerät des Nutzers laufen. Sie scannen jede Klartext-Nachricht, bevor sie gesendet wird und jede verschlüsselte Nachricht, nachdem sie entschlüsselt wurde.

Das Unternehmen wies sogar darauf hin, dass es, wenn es Verstöße (von Facebook oder den Behörden definierte Inhalte, Anmerkung des Übersetzers) entdeckt, eine Kopie des zuvor verschlüsselten Inhalts unbemerkt kopieren und zu zentralen Servern für eine weitere Analyse senden wird, auch wenn der Nutzer dem widersprochen hat — was es zu einem richtigen Telekommunikationsüberwachungsdienst macht.“

Der Forbes-Artikel spricht in diesem Zusammenhang von „maschinenbasierter Überwachung von Milliarden Nutzern gleichzeitig“. Die Ausweitung der Überwachung auf andere Apps und das ganze Telefon — „Smartphone“ — kommt dann mit an Sicherheit grenzender Wahrscheinlichkeit als nächster Schritt, so die Prognose des Forbes-Berichts:

„Während sich einige Telefonhersteller davon distanzieren konnten, indem sie maßgeschneiderte Telefone samt Betriebssystemen anbieten, die ein solches Scanning nicht beinhalten, werden solche Geräte wahrscheinlich selten sein — nur benutzt von denen, die gewillt sind, weite Wege zu gehen, um der Überwachung durch die Regierung zu entgehen, und so automatisch große Aufmerksamkeit auf sich zu ziehen. Es ist wahrscheinlich, dass viele Regierungen mit der Zeit einfach Gesetze verabschieden, welche den Besitz und die Nutzung solcher Geräte verbieten, genauso wie viele Gerichtsbarkeiten Geräte verbieten, die Temposündern Strafzettel ersparen wollen.“

Quellen und Anmerkungen:

(1) https://blog.fdik.org/2019-07/s1564510212.html
(2) https://www.forbes.com/sites/kalevleetaru/2019/07/26/the-encryption-debate-is-over-dead-at-the-hands-of-facebook/

+++

Dieser Beitrag erschien am 31.07.2019 bei Rubikon – Magazin für die kritische Masse.

+++

Danke an den Autor für das Recht zur Veröffentlichung.

+++

Bildhinweis: monte_a / Shutterstock

+++

KenFM bemüht sich um ein breites Meinungsspektrum. Meinungsartikel und Gastbeiträge müssen nicht die Sichtweise der Redaktion widerspiegeln.

+++

KenFM jetzt auch als kostenlose App für Android- und iOS-Geräte verfügbar! Über unsere Homepage kommt Ihr zu den Stores von Apple und Google. Hier der Link: https://kenfm.de/kenfm-app/

+++

Dir gefällt unser Programm? Informationen zu Unterstützungsmöglichkeiten hier: https://kenfm.de/support/kenfm-unterstuetzen/

+++

Jetzt kannst Du uns auch mit Bitcoins unterstützen.