Chiffrement : WhatsApp complètement motus et bouche cousue

WhatsApp avait initié le déploiement du chiffrement de bout en bout des messages de type texte envoyés via son service dès novembre 2014 sur la mouture Android de son application. La société annonce maintenant avoir finalisé ce processus sur l'intégralité de son service, « *faisant de WhatsApp un leader pour protéger vos communications privées* », peut-on lire dans une contribution de blog.

Le maître-mot est également la simplicité d'usage : « *L'idée est simple : lorsque vous envoyez un message, la seule personne qui peut le lire est celle ou le groupe de chat auquel vous avez envoyé ce message.* » Ce chiffrement concerne toujours les messages texte mais s'étend désormais aussi aux appels vocaux, aux chats de groupe, aux envois de photos, vidéos et messages vocaux.

Toutes les plates-formes mobiles (iOS et Android, mais également Windows Phone, BlackBerry, BB10, Nokia S40 et Nokia S60), sur lesquelles WhatsApp est disponible, sont concernées avec une mise à jour des applications idoines.

Pour rappel, Facebook avait jeté son dévolu sur WhatsApp en 2014 pour quelques 19 milliards de dollars. Si sa base d'utilisateurs était à l'époque de 450 millions de mobinautes, elle a désormais passé la barre du milliard de personnes.

Appui d'Open Whisper Systems

Cette nouvelle composante relative à la confidentialité des données (chemin emprunté par d'autres services de messagerie tels que Telegram) devrait séduire de nouveaux mobinautes. Dans sa communication, la société n'hésite d'ailleurs pas à déclarer que la sécurité des données a toujours été son cheval de bataille : « *WhatsApp a toujours eu pour priorité de rendre vos données et communications aussi sécurisées que possible.* »

Pour y parvenir, WhatsApp s'est appuyé sur la technologie développée par Open Whisper Systems, un groupe à but non lucratif qui développe des logiciels en mode Open Source. Avec comme leitmotiv de « *rendre les communications privées simples* », le groupe s'est déjà illustré avec sa propre application baptisée Signal (d'appels en VoIP et de messagerie) qui bénéficie d'un tel chiffrement de bout en bout.

Autre témoignage de sa crédibilité : Edward Snowden avait lui-même fait l'article des applications TextSecure et RedPhone (adossées elles aussi à la technologie de chiffrement de bout en bout de Open Whisper Systems). Le groupe veut aller plus loin et pousser son protocole Open Source dans d'autres services de messagerie (que WhatsApp).

Afin de bénéficier de cette technologie implémentée dans les dernières moutures des applications mobiles de WhatsApp, il est nécessaire (pour le mobinaute et ses contacts) d'utiliser ces versions mises à jour, précise *ITespresso*.

Une activation du chiffrement par défaut et transparente

Pour l'utilisateur, les processus de chiffrement et de déchiffrement se font de manière automatique. Ils sont activés par défaut tout le temps. Lorsqu'un mobinaute dispose de la mouture de WhatsApp avec chiffrement, le service ne lui permettra d'ailleurs plus de transmettre des données non chiffrées (si jamais il tentait de revenir à une version antérieure de l'application par exemple).

Le billet de blog prend également des airs de manifeste contre les atteintes à la vie privée « *dans un monde où nos données sont plus que jamais numérisées* ». WhatsApp se targue également d'avoir mis en œuvre le seul processus de chiffrement qui vaille, soulignant que de nombreuses applications de messagerie « *chiffrent seulement les messages entre elles et leurs utilisateurs alors que le chiffrement de bout en bout de WhatsApp garantit que seule la personne avec qui vous communiquez peut lire ce qui est envoyé et qu'il n'y a pas d'intermédiaires, pas même WhatsApp* ».

S'il s'agit de parer aux hackers et aux régimes autoritaires. On peut y voir également un pied de nez aux institutions gouvernementales (telles que le FBI aux Etats-Unis).

A lire aussi :

WhatsApp prochaine cible de la justice US sur le chiffrement
Chiffrement : Google et WhatsApp soutiennent Apple

Crédit Photo : Imilian-Shutterstock