Chiffrement : Zoom a du mal à placer le curseur

Où en est Zoom avec le chiffrement de bout en bout ?

Le chantier est prioritaire, mais le travail à accomplir est immense.

Il y a, d'une part, les enjeux technologiques, synthétisés dans un livre blanc. Entre autres, le maintien de la compatibilité avec des services tiers (RTC, systèmes de visioconférence SIP, diffusion sur YouTube…).

De l'autre, se pose la question de la protection des utilisateurs.

Les propos d'Alex Stamos* résument le dilemme qui se pose en la matière.

L'ancien directeur technique de Facebook accompagne aujourd'hui Zoom – en tant que consultant – dans sa stratégie d'implémentation du chiffrement de bout en bout.

Il évoque un « exercice difficile » marqué par la nécessité de trouver un équilibre entre deux aspects : la protection des utilisateurs et celle de leur vie privée.

Or, les deux notions ne sont pas forcément compatibles. La première implique la possibilité de surveiller les communications, tandis que la seconde induit leur verrouillage complet.

> *So this creates a difficult balancing act for Zoom, which is trying to both improve the privacy guarantees it can provide while reducing the human impact of the abuse of its product.*
>
> *— Alex Stamos (@alexstamos) June 3, 2020*

La crainte d'un précédent

Si Alex Stamos se montre ainsi mesuré, Eric Yuan a fait preuve de moins de précautions.

Le patron de Zoom est allé droit au but mardi 2 juin, lors de la conférence téléphonique faisant suite à la présentation des résultats trimestriels l'entreprise.
Il a affirmé que les utilisateurs de la version gratuite n'auraient pas accès au chiffrement de bout en bout. La raison : cela compliquerait les relations avec les forces de l'ordre en cas d'usage abusif de la plate-forme.

Ces propos lui ont valu des critiques de la part d'associations de défense des libertés civiles à l'ère numérique. Leur craintes : que Zoom établisse un précédent en mettant la confidentialité hors de portée de ceux qui en auraient le plus besoin.

La réaction dans ce milieu n'a cependant pas été unanime. Certains se sont montrés moins incisifs, à l'image de Jon Callas, de l'ACLU (American Civil Liberties Union). D'après lui, faire payer l'accès au chiffrement de bout de bout est l'idéal pour dissuader les « prédateurs sexuels et autres criminels »

qui s'en servent à de mauvaises fins.

Payer pour chiffrer ?

Un porte-parole est intervenu à la suite des déclarations d'Eric Yuan, pour apporter des clarifications.
Zoom est conscient de la fragilité de certains publics (enfants, personnes ciblées par des discours haineux…) et prendra des mesures en conséquence. Ce qui se traduira par l'ouverture du chiffrement de bout en bout aux utilisateurs « dont on aura pu vérifier l'identité ».

C'est moins évident dans le discours d'Alex Stamos. À l'en croire, les forfaits Affaires et Entreprise seront les premiers à bénéficier du chiffrement de bout en bout. Bénéficieront du même traitement les organisations qui utilisent la version gratuite en vertu d'une offre spéciale (les écoles par exemple).

Si l'implémentation se fait correctement, même les équipes de Zoom ne pourront plus intervenir dans des réunions (elles le font actuellement lorsqu'elles le considèrent comme nécessaire pour protéger les utilisateurs).

***** « Les forces de l'ordre voient la suppression du chiffrement comme la solution à tous les problèmes. Les défenseurs de la vie privée ne perçoivent que les atteintes à la vie privée et écartent les autres types d'abus *», glisse Alex Stamos*.

> *Many voices in law enforcement want no E2EE, because they see access to plaintext as the solution to all problems and believe the privacy harms are massively overblown. Privacy advocates only see privacy harms, and dismiss other abuses as overblown.*
>
> *— Alex Stamos (@alexstamos) June 3, 2020*

Illustration principale © Den Rise – shutterstock.com