Google veut chiffrer pour éviter la surveillance sauvage des données

Google est gêné aux entournures. Le groupe américain, dont l'activité est largement liée à l'exploitation des données personnelles des utilisateurs de ses services, se trouve aujourd'hui sous le feu des critiques, suite à la découverte de l'affaire Prism.

La firme avait déjà indiqué en juin ne pas donner accès à ses serveurs au gouvernement américain, ni de façon directe, ni via une porte dérobée (voir « Surveillance "Made in NSA" : Google monte au créneau »).

C'est une question de réputation : Google n'aime pas qu'on l'accuse de collaboration ouverte avec les autorités pour faciliter l'accès aux échanges interpersonnels, explique *ITespresso.fr*. À charge pour la justice d'émettre des injonctions dans ce sens.

Pour les requêtes encore plus sensibles émanant de la part des agences de renseignement (américaines ou étrangères), la direction juridique de la firme Internet de Mountain View semble filtrer les demandes au cas par cas.

Car, ce que Google redoute par-dessus tout, c'est la défiance des utilisateurs finaux et la suspicion permanente des associations de défense des droits civils sur Internet.

Selon le *Washington Post*, Google accélère depuis le mois de juin le déploiement d'un programme renforcé de chiffrement qui avait été validé fin 2012.

Une course aux armements

Mais le dispositif a ses limites : cela n'empêchera pas les agences de renseignement d'espionner les utilisateurs de Google. Et le groupe Internet devra toujours répondre aux injonctions judiciaires.

Néanmoins, Google et les experts en sécurité IT considèrent qu'en multipliant les initiatives de chiffrement renforcé, la surveillance de masse est beaucoup plus compliquée à instaurer.

« *C'est une course aux armements*, déclare **Eric Grosse**, vice-président en charge de la sécurité ingénierie chez Google. *Nous considérons ces organismes gouvernementaux parmi les joueurs les plus talentueux dans cette partie.* »

En effet, les États comme la Chine, la Russie, le Royaume-Uni, mais aussi Israël recrutent des hackers très qualifiés.

Des services de renseignement comme la NSA (USA) ou le GCHQ (UK) sont en mesure de casser les codes de la plupart des messages chiffrés qui passent sur le Net.

Selon l'Office of the Director of National Intelligence (organisme de supervision du renseignement aux États-Unis), les programmes de surveillance du Net sont légitimes.

« À travers l'Histoire, les nations ont utilisé le chiffrement pour protéger leurs secrets. Et aujourd'hui, les terroristes, les cybercriminels et les trafiquants spécialistes de la traite des êtres humains exploitent le chiffrement pour camoufler leurs activités. Notre communauté du renseignement ne ferait pas son métier si elle n'essayait pas de combattre cela. »

Crédit photo : © John Lee – Fotolia.com

Voir aussi

Quiz Silicon.fr – 10 questions sur Google