Chiffrement des données sur iOS 8 : juste de la poudre aux yeux ?

Devant la presse américaine, le directeur du FBI a critiqué les **nouvelles fonctionnalités de cryptage** qu'introduisent **Apple et Google** dans leur système d'exploitation mobile, respectivement iOS et Android. Selon James B. Comey, ces nouvelles formes de chiffrement sont si sûres que les services de police ne pourront plus obtenir un accès facile aux informations stockées sur les smartphones et tablettes, même dans le cadre d'une écoute ordonnée par un juge lors d'une enquête officielle.

Les déclarations du directeur font écho aux inquiétudes exprimées par de nombreux services de police aux Etats-Unis, ces derniers soulignant l'importance des accès aux données stockées sur les smartphones (photos, messages, historique de navigation…) pour leurs enquêtes. « *Un jour viendra où la capacité à accéder à ces informations sera d'une importance vitale pour les gens*, a expliqué Comey à la presse américaine. *Je veux en discuter (avec les entreprises concernées, NDLR) avant que ce jour n'arrive* ». Et d'indiquer que le FBI a déjà pris contact avec Google et Apple, qui ont tous deux annoncé le renforcement du chiffrement dans leur OS mobile la semaine dernière.

Avant tout un argument marketing

Côté Android, la future version assurera le cryptage par défaut. Sur iOS 8, dévoilé en même temps que les iPhone 6, la firme à la pomme a, de côté, renforcé les options à disposition de ses utilisateurs, leur permettant de chiffrer la plupart de leurs données personnelles, protégées par un mot de passe de 4 chiffres. Sur le site de la société consacré à la confidentialité des données, Tim Cook, le Pdg, en fait d'ailleurs **un argument de vente**. « *Contrairement à ses concurrents, Apple ne peut pas bypasser votre mot de passe et accéder à vos données. Donc il est techniquement impossible pour nous de répondre aux requêtes du gouvernement visant à extraire des données de terminaux fonctionnant sous iOS 8* ». Tout simplement parce que **la clef de chiffrement réside sur les terminaux eux-mêmes**. Côté Android, le schéma est d'ailleurs identique, même si, en attendant la future version, le cryptage n'est accessible que via une option enfouie dans les menus de configuration de l'OS.

Rester que l'irruption de ces fonctions de cryptage relève largement de stratégies marketing, pensées pour **l'après-Snowden**. Rappelons que ces options ne changent rien aux capacités des services de police à intercepter les appels et à analyser les métadonnées de communication d'un individu (des informations que recueillent les opérateurs).

Les limites du cryptage d'iOS 8

Par ailleurs, le dispositif d'iOS 8 comporte plusieurs limites. D'abord, si la synchronisation avec iCloud est activée, les données seront **aussi stockées dans le Cloud d'Apple**. Non plus chiffrées par la clef présente sur le terminal, mais par une clef que détient Apple. La société peut alors très bien déchiffrer ces données de sauvegarde pour satisfaire les demandes d'accès des services gouvernementaux. Ensuite, la clef présente sur les terminaux iOS 8 est **protégée par un mot de**

passe de 4 chiffres, trop court pour résister à une attaque par force brute (consistant à essayer toutes les combinaisons possibles). Enfin, ce mot de passe n'est pas demandé quand l'iPhone ou l'iPad sous iOS 8 est **connecté à un Mac ou un PC auquel il est associé**, fonctionnalité laissée ouverte pour laisser iTunes échanger des données avec les terminaux iOS même quand ceux-ci sont verrouillés. Or, en cas d'arrestation, les services de police saisissent l'ensemble des appareils électroniques, et peuvent utiliser cette faille pour accéder aux données des terminaux mobiles, raconte Jonathan Zdziarski, un spécialiste de la sécurité d'iOS dans un billet de blog. A moins que l'iPhone ou l'iPad n'ait été éteint… Le conseil que le même Jonathan Zdziarski donne, in fine, à ses lecteurs pour se protéger, par exemple, de contrôles trop indiscrets aux aéroports…

A lire aussi :

Le système de reconnaissance faciale du FBI opérationnel

Données privées : Microsoft gagne une victoire contrastée contre le FBI