L'Enisa très critique sur les contournements du chiffrement

On ne l'avait pas entendu lors du débat en Angleterre sur le chiffrement, ni en écho des discussions aux Etats-Unis sur ce sujet. L'Enisa (agence européenne pour la sécurité des réseaux et des systèmes d'information) vient donc de s'inviter dans le concert d'avis sur la réglementation de l'usage de la cryptographie des communications, en publiant un rapport sur le sujet.

Pour l'organisme, nous vivons dans un monde paradoxal. D'un côté, la confiance, et donc la sécurité des communications, est un élément essentiel du développement de l'économie numérique. « *Aujourd'hui, la communication non chiffrée est une menace* », avoue le rapport. De l'autre, les risques et les enquêtes nécessitent des outils pour contrecarrer, découvrir et arrêter des cybercriminels ou des terroristes.

Mais c'est bien sur le principe de la confiance que l'Enisa se positionne et s'appuie pour considérer que la mise en place de portes dérobées dans les outils de chiffrement serait un mauvais choix. Pour l'agence, ces backdoors risquent de « *créer des vulnérabilités qui peuvent être à leur tour utilisées par les cybercriminels et les terroristes* ».

Séquestre des clés ou interdisant le chiffrement ?

D'autres solutions, tel le séquestre des clés par un tiers, ne sont pas considérées comme une alternative fiable. « *Actuellement, il n'y a aucune implémentation qui fonctionne et l'appel à un tiers de confiance implique un changement fondamental dans l'infrastructure des télécommunications. Cette dernière deviendrait alors plus complexe et donc plus vulnérable aux intrusions et aux pannes* », souligne l'Enisa. Avant d'ajouter « *que ce service est également une menace pour la collecte de preuve : si un attaquant obtient la clé privée de quelqu'un, il peut parfaitement se faire passer pour cet individu* ».

Autre alerte de l'agence, reprise par de nombreux cryptographes, dont Guillaume Poupard, directeur général de l'Anssi : les lois interdisant le chiffrement sont aisément contournables. Il existe déjà une « *grande quantité d'outils* » et les algorithmes sont accessibles au public. L'organisme considère « *qu'un programmeur disposant de compétences moyennes pourrait les mettre en œuvre* ».

Au final, l'Enisa aligne les critiques plus simplement que les propositions. Elle considère que le chiffrement fournit aux télécommunications « *à la fois l'enveloppe, le sceau ou le tampon et la signature* », et que ces outils électroniques sont « *nécessaires pour protéger nos biens dans un monde hautement informatisé* ». Pour l'instant, toutes les mesures de contournement proposées sont des remèdes pires que le mal.

A lire aussi :

Après les attentats : faut-il mieux encadrer le chiffrement ?

Querelles juridiques américaines sur le déchiffrement d'iOS

Crédit Photo : Den Rise-Shutterstock