Fiche d'Information à l'Intention des Décideurs:
6 Moyens par Lesquels « l'Accès Légal » au Cryptage Compromet la Sécurité

Le Cryptage – Quésaco?

Le cryptage est un processus qui consiste à brouiller ou à cacher des informations afin qu'elles ne puissent être lues que par une personne disposant du moyen (ou la clé) de les restituer à leur état initial. **Le chiffrement de bout** en bout offre le niveau de sécurité et de confiance le plus élevé, car idéalement, seul le destinataire souhaité dispose de la clé pour déchiffrer le message. Aucune autre partie n'est censée avoir de clé.

Les technologies de chiffrement sont des outils qui aident les personnes en ligne à protéger l'intégrité et la confidentialité de leurs données et de leurs communications numériques. Elles sécurisent la navigation sur le Web, les services bancaires en ligne et les services publics critiques tels que l'électricité, les élections, les hôpitaux et les transports, auprès desquels les citoyens accordent leur confiance. En 2018, plus de 1,7 milliard d'utilisateurs ont utilisé des services de messagerie cryptés E2E pour protéger leurs communications.[1]

Certains gouvernements craignent que le cryptage rende plus difficile la collecte d'informations pour prévenir ou punir les terroristes et les criminels. Ainsi, Ils se sont empressés d'adopter des **mandats « d'accès légal »** pour donner aux forces de l'ordre le pouvoir d'intercepter et d'accéder aux communications cryptées, ou de demander aux entreprises de le faire à leur place. Or, ces mesures mettent en danger l'ensemble des individus en ligne.

Bien qu'il soit souvent avancé que ces mandats n'affecteront pas le chiffrement mais utiliseraient d'autres moyens permettant de fournir un accès, la sécurité des utilisateurs est toujours menacée. En effet, tout point d'entrée dans un service sécurisé peut constituer une faille.

Les mesures « d'accès légal » affaiblissent la sécurité de l'Internet et mettent non seulement en péril l'économie mondiale, mais aussi les services essentiels auprès desquels nous dépendons et in fine la vie de l'ensemble des citoyens. Explications :

[1] https://telegram.org/blog/200-million; https://techcrunch.com/2018/01/31/whatsapp-hits-1-5-billion-monthly-users-19b-not-so-bad

1 **Un accès contraint affaiblit tout le monde:**
Il n'existe pas de verrou numérique pouvant être ouverts uniquement par les « bons » acteurs. Un accès légal facilitera automatiquement l'accès à des données sensibles à d'autres individus, tels que des criminels ou encore des gouvernements hostiles.

2 **Présence de risques pour la sécurité nationale et individuelle:**
En diminuant la sécurité des informations personnelles, des données bancaires et des informations gouvernementales, l'ouverture d'un accès légal pourrait involontairement faciliter l'espionnage, le vol d'identité, le chantage, la manipulation du marché et plus encore.

3 **Les terroristes trouveront de nouveaux moyens de dissimulation:**
Si les terroristes et les criminels ont connaissance de l'accès aux services de messagerie cryptés par les forces de l'ordre, ils utiliseront d'autres alternatives. Les communications des criminels pourraient alors être à l'abri des regards tandis que celles des utilisateurs journaliers seraient plus vulnérables.

4 **Existence de menaces sur la vie des personnes:**
Les communications cryptées de bout en bout protègent l'identité des journalistes, des activistes, des témoins protégés, de la police secrète et celle de bien d'autres individus. Or, La vulnérabilité des communications mettent ces vies en danger.

5 **Des risques pesant sur l'infrastructure de l'Internet:**
Des mesures d'accès légal menacent des éléments de sécurité essentiels de l'infrastructure même de l'Internet, tels que les mécanismes d'authentification garantissant la sécurité de tous en ligne.

6 **Un impact sur le commerce et l'investissement:**
Un tel accès peut significativement impacter l'économie mondiale. En effet, pour la plupart des multinationales, une part importante de leurs revenus provient des marchés actuels et émergents à l'étranger. Or, les consommateurs peuvent être réticents à acheter des produits ou à utiliser des services de pays où les gouvernements pourraient avoir accès à leurs informations et communications privées.

Chaque pays a le droit et le devoir de protéger ses citoyens. Cependant, les tentatives hâtives de faciliter l'accès au cryptage, même bien intentionnées, constituent un risque majeur pour la sécurité des citoyens respectueux de la loi et pour l'Internet en général.

A cet égard, nous recommandons de conserver les outils numériques existants qui sont assez puissants pour protéger nos territoires, nos économies et nos concitoyens. Il est essentiel que les dirigeants internationaux soutiennent le maintien d'un cryptage fort et applicable à tous.

Internet Society internetsociety.org