L’UE doit-elle obliger les géants de l’Internet à céder leurs clés de chiffrement ?

Council of the European Union
General Secretariat

Brussels, 17 January 2015
(OR. en)

DS 1035/15

LIMITE

MEETING DOCUMENT

From: EU Counter-Terrorism Coordinator
To: Delegations
Subject: EU CTC input for the preparation of the informal meeting of Justice and Home Affairs Ministers in Riga on 29 January 2015

This is a first paper for discussion in COSI on 20 January 2015. It does not yet include the Commission's proposals which will be discussed in the College on 21 January, nor the contributions from the Member States. The document which will be submitted to the informal meeting of JHA ministers in Riga on 29/30 January will be shorter, include the outcome of the COSI discussions as well as contributions from the Member States and the Commission.

Europe is facing an unprecedented, diverse and serious terrorist threat. The horrific attacks that took

L’UE doit-elle obliger les géants de l’Internet à céder leurs clés de chiffrement ?

La montée en puissance du terrorisme en Europe relance le débat sur le chiffrement des communications et la création de backdoors réservés aux forces de l’ordre européenne. Le coordinateur antiterrorisme de l’UE, Gilles de Kerchove, demande sans détour un accès aux clefs de chiffrement des géants de l’Internet.

Les géants de l’Internet vont-ils bientôt être obligés de partager leurs clés de chiffrement avec la police et les agences de renseignement européennes pour les aider à lutter contre le terrorisme ? C’est en tout cas une recommandation ferme de Gilles de Kerchove, le coordinateur antiterrorisme de l’Union Européenne. C’est une suggestion étonnante quand on se souvient que les entreprises comme Google ou Facebook ont commencé à chiffrer leurs communications pour lutter contre la curiosité des agences de renseignement chinoises mais aussi américaines, anglaises, allemandes, hollandaises et françaises comme l’ont indiqué les documents révélés par Edward Snowden.

L’association de protection des droits civils Statewatch
a divulgué un document rédigé par le coordinateur
antiterroriste Gilles de Kerchove.

Gilles de Kerchove suggère que la Commission européenne « devrait revoir ses règles pour obliger les entreprises de l’Internet et des télécommunications opérant dans l’UE à fournir … aux autorités nationales compétentes un accès à leurs communications [c’est à dire leurs clefs de chiffrement] », selon un document divulgué par l’association de protection des droits civils Statewatch. Dans ce document, M. de Kerchove expose ses vues sur les mesures anti-terrorisme à prendre dans l’UE en vue d’une réunion des ministres de la Justice et de l’Intérieur de l’UE à Riga, la semaine prochaine.

Des keyloggers pour suivre les échanges

Cette proposition est controversée parce que, comme le note le coordinateur, la généralisation du chiffrement pour les échanges sur Internet rend très difficile, voire impossible, les interceptions légales par les autorités nationales compétentes. Nous avons discuté de ces questions avec les cybergendarmes de Paris (Section de recherche de Paris et ses spécialistes N-Tech) et de Rosny Sous Bois (C3N). Sans coopération des fournisseurs de services (Whatsapp, Skype ou encore iMessage), il est très difficile de lire les messages échangés. La solution la plus facile – pour les forces de l’ordre – est aujourd’hui l’installation d’un cheval de Troie ou keylogger (un enregistreur de frappes) sur les terminaux des suspects, smartphones, tablettes ou PC. Une opération toujours délicate puisqu’elle doit être effectuée à l’insu des utilisateurs.
« Whatsapp ou Viber commencent à être très utilisés par les criminels avec des mobiles jetables », nous avait confié le major Etienne Neff de la section de Paris. « Les criminels sont aujourd’hui plus sophistiqués et utilisent également des solutions payantes ». Les forces de l’ordre peuvent toujours accéder aux métadonnées fournies par les opérateurs mais il faut séparer le flux et le reconditionner pour le traiter.

Les entreprises également sous surveillance

L’appel à plus de surveillance des échanges sur Internet est revenu sur le devant de la scène en Europe suite aux assassinats perpétués dans les bureaux du magazine satirique Charlie Hebdo et à l’épicerie HyperCacher à Paris. Après les deux attentats, les ministres de la Justice et de l’Intérieur de l’UE avaient publié une déclaration commune dans laquelle ils soulignaient qu’il est essentiel « d’entretenir une étroite collaboration avec les FAI pour endiguer la propagande terroriste en ligne ».
Si la Commission a refusé de commenter les plans anti-chiffrement de M. de Kerchove, le document fuité contient des détails supplémentaires comme le contrôle du « chiffrement décentralisé » des entreprises. Cela pourrait être une référence au chiffrement de bout-en-bout utilisé par certaines entreprises sensibles pour verrouiller leurs communications.

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://www.lemondeinformatique.fr/actualites/lire-l-ue-doit-elle-obliger-les-geants-de-l-internet-a-ceder-leurs-cles-de-chiffrement-59993.html
Par Serge Leblal