DAILY SCIENCE
DÉCOUVREZ LA SCIENCE, LA RECHERCHE ET L'INNOVATION "MADE IN BELGIUM"

CONFIDENTIALITÉ SUR LE WEB : UNE QUESTION DE TECHNIQUE ET DE COMPORTEMENT

Publié le 9 février 2015

Quatre médias francophones viennent de mettre en ligne un site web commun destiné à recueillir toutes les confidences que leurs lecteurs voudront bien leur transmettre. Le but ? « Etablir un contact direct et sécurisé entre des journalistes et des personnes souhaitant révéler des actes illégaux ou immoraux dont ils ont eu connaissance », précise « Sourcesure ».

Avant Internet, les informations (in)discrètes qui arrivaient sous les yeux des journalistes atterrissaient sur leur bureau sous la forme de lettres anonymes envoyées par la poste, par un pli déposé dans une boîte aux lettres. Les bouleversements digitaux ont changé les habitudes des informateurs. Place au click, à la pièce jointe, au courrier « forwardé ».

Au-delà de la pertinence de cette initiative, que nous n'examinerons pas ici, se pose la question de la sécurisation de ce mode de communication.

Des outils publics bien rodés

« Dans le cadre des communications sur internet, nous disposons aujourd'hui de mécanismes de chiffrement, souvent bien rodés et reconnus depuis parfois 30 ans, permettant de garantir la sécurité des transmissions face à quelqu'un qui les écoute. Et depuis les révélations de Snowden, ceux-ci sont utilisés de plus en plus systématiquement », explique le Pr Olivier Pereira (UCL), du Laboratoire de cryptographie. Le Pr Pereira a notamment participé à l'élaboration de systèmes de

vote électronique en Belgique et aux Etats-Unis.

Aux yeux du spécialiste, les outils mis en place sur le site des quatre médias francophones (La Libre Belgique, Le Monde, RTBF.be et Le Soir) destiné à recueillir les informations envoyées par les « lanceurs d'alerte », sont pertinents. « Les outils publics de cryptage et librement accessibles sur le web sont bien choisis », dit-il. « Cela me semble être ce qui se fait de mieux aujourd'hui, tout en restant utilisables par les internautes ».

« Sourcesure » préconise l'utilisation de la suite logicielle Tor. Elle fonctionne grâce à deux logiciels-serveurs: GlobaLeaks et Tor2Web et a également recours à « TAILS ».

TAILS permet de minimiser les traces que l'on laisse dans son ordinateur. « C'est une distribution Linux », explique le Pr Pereira. « Cela fonctionne comme Windows, mais cela remplace temporairement ce système d'exploitation. Tout est fait pour que chaque donnée envoyée ou reçue est instantanément effacée. De sorte qu'il ne reste pas de trace de la communication », souligne-t-il.

Une série de relais pour brouiller les pistes

« Le réseau TOR est également intéressant », estime le scientifique. « Au départ, il s'agissait d'un réseau développé par l'armée américaine afin de protéger l'anonymat des communications de ses membres. Il fonctionne par nœuds, par relais. L'utilisateur envoie ses informations à un premier nœud. La communication est bien entendu chiffrée, tant pour sa destination que son contenu. »

« Le premier nœud envoie le message à un second nœud en ajoutant un complément de chiffrement. Le second nœud ne sait rien de la personne à l'origine du message ni de son contenu. Il se borne à faire suivre ce message à un troisième nœud, lequel est capable de déchiffrer l'adresse du destinataire final. Pour la réponse, éventuelle cela fonctionne dans l'autre sens. En plaçant ces intermédiaires en cascade qui ne connaissent que le maillon précédent ou suivant dans la chaine, on augmente la confidentialité des communications. Surtout si chacun des nœuds utilisés se situe dans un pays différent, aux législations en matière de protection de données et de la vie privée différentes ».

L'armée américaine s'est aussi rendu compte que pour assurer le plus grand anonymat possible à ses utilisateurs, il ne fallait pas cantonner le système aux seuls militaires… Elle a dès lors mis TOR dans le domaine public.

Métadonnées et discipline personnelle

Voilà pour les outils techniques. Il reste encore à faire attention au comportement des « informateurs » et de la nature des fichiers qu'ils envoient. Si l'informateur est le seul à avoir accès

aux informations qu'il transmet, il risque par ce simple fait d'être identifiable comme source de la fuite. De même, les fichiers informatiques (textes, photos, tableaux…) sont souvent accompagnés de métadonnées (date de la prise de vue d'une photo par exemple, l'heure, voire la localisation, l'identification de l'auteur d'un fichier texte…). « Un nettoyage de ces données s'impose avant leur transmission, » estime le chercheur.

Le système est-il infaillible? « Non, certainement pas, mais il faudra aux indiscrets beaucoup de moyens et beaucoup d'énergies pour contourner les mesures techniques mises en place. Je pense qu'on peut difficilement faire beaucoup mieux à l'heure actuelle », conclut Olivier Pereira.