Vers une sécurisation à marche forcée du Web collaboratif ?

- Informatique - Internet -

Date de mise en ligne : mercredi 17 juin 2009

Jusqu'à présent activé pour les services au contenu confidentiel comme Google Health, le protocole a de fortes chances d'être étendu aux autres outils bureautiques. Avant de s'étendre à l'ensemble du web 2.0 ?

Les données personnelles et les données des entreprises se multiplient sur les réseaux sociaux et les services en lignes. Pas étonnant que les attentes des utilisateurs soient plus grandes. En particulier d'un point de vue de la sécurité. Ainsi, le protocole de sécurité HTTPS était jusqu'à présent utilisé de manière automatique par Google pour des applications contenant des données privées : Google Voice, Health, AdSense et AdWords. La firme de Mountain View a de fortes chances de l'adopter de manière généralisée pour ses autres outils : l'entreprise a annoncé qu'elle s'apprêtait à lancer des tests utilisateurs, afin de rendre cette sécurité activée par défaut. Tout d'abord sur Gmail, puis sur les applications Google Docs et Google Calendar.

Une technologie déjà existante

Jusqu'à maintenant, l'utilisateur devait se frayer seul un chemin vers l'outil d'activation du protocole enfoui dans l'application. Cette décision fait suite à la demande d'une quarantaine de chercheurs et d'académiciens des secteurs des sciences de l'informatique, de la sécurité de l'information et du droit relatif aux données privées. Regroupé sous le groupe Consumer Watchdog, le collectif a envoyé à l'entreprise une lettre de six pages réclamant la généralisation du protocole. Ce, afin de prévenir les risques de vols d'informations ou d'espionnage.

Une adoption sous réserve

Sur son blog Public Policy, l'entreprise Google précise cependant que l'adoption du protocole se fera sous réserve qu'elle ne provoque pas d'effets négatifs sur l'expérience utilisateur, et que le système soit applicable. Selon Watchdog, cette formulation constitue pour Google un moyen de se retourner si la société décide finalement de ne pas réellement mettre en application sa promesse de généraliser le HTTPS. Pour rappel, ce protocole est présent dans tout navigateur web et est largement utilisé dans la finance et les industries de la santé. Son intérêt, c'est qu'il sécurise l'utilisation de ses applications sur des réseaux Wi-Fi à risques.

Post-scriptum :

http://www.atelier.fr/securite/10/1...