HTTPS sera déployé sur tous les sites du gouvernement US

Washington a récemment déploré le piratage des données de 4 millions de fonctionnaires fédéraux et mis temporairement hors service le site de l'armée américaine – army.mil – compromis par une attaque revendiquée par un groupe se faisant appeler « Armée syrienne électronique », lundi 8 juin. Ce même jour, l'administration Obama a annoncé que tous les sites web du gouvernement des États-Unis auront adopté HTTPS (**HyperText Transfer Protocol Secure**) d'ici le 31 décembre 2016.

Le Bureau de gestion et du budget (OMB) de la Maison Blanche indique dans sa directive du 8 juin 2015 que *« **tous les sites et services Web fédéraux** accessibles au public fourniront des services par le biais d'une connexion sécurisée »* à l'avenir. Et ce par le biais du protocole de transfert hypertexte sécurisé HTTPS, *« la plus forte protection des connexions Web publiques à l'heure actuelle »*.

Cette note fait suite à l'ouverture d'une consultation publique sur la stratégie « **HTTPS-Only Standard** » présentée en mars dernier par l'administration américaine. L'initiative a fait l'objet de nombreux commentaires deux ans après les premières révélations d'Edward Snowden sur les pratiques du renseignement américain, la NSA en particulier, dont l'utilisation de portes dérobées (backdoors).

La migration vers le tout HTTPS

Utilisé par les sites d'établissements bancaires et financiers depuis des années et proposé aux internautes sous la forme d'une extension de navigateurs – HTTPS Everywhere – née d'une collaboration entre le projet Tor et l'Electronic Frontier Foundation, HTTPS est désormais privilégié par de grands noms du numérique, de Google à Mozilla. Le gouvernement américain veut faire de même. Son action vise à rendre plus difficile l'**interception de communications par des tiers**, à conserver la confiance des usagers des sites web fédéraux et à moderniser ses services en ligne.

Pour accompagner cette migration vers le tout HTTPS, Washington propose un tableau de bord des déploiements ainsi qu'un guide de bonnes pratiques sur le site cio.gov ouvert aux contributions techniques internationales. On peut notamment y lire que *« toute activité de navigation doit être considérée comme privée et sensible »*. **Double discours** ? La NSA, dont les pouvoirs de collecte viennent d'être limités aux États-Unis, a réaffirmé le mois dernier la nécessité d'un cadre légal permettant de contourner le chiffrement… tout en le présentant comme une technologie d'avenir.

Mais attention, prévient dans un communiqué **Tony Scott**, DSI de la Maison Blanche, *« HTTPS garantit uniquement l'intégrité de la connexion entre deux systèmes, et non l'intégrité des systèmes eux-mêmes. HTTPS n'a pas été conçu pour protéger un serveur Web du piratage ou pour empêcher le service Web d'exposer des informations de l'utilisateur durant le fonctionnement normal du service. »* Malgré tout, ajoute-t-il, l'initiative HTTPS-Only *« permettra d'éliminer des décisions incohérentes et subjectives concernant les contenus ou les activités de navigation qui sont sensibles par nature, et de créer un standard de confidentialité plus élevé à l'échelle gouvernementale. »* Un pas que n'a pas encore franchi la France.

Lire aussi :
Pour la NSA, le chiffrement c'est le futur mais avec des ouvertures
Des chercheurs évaluent les conséquences du « S » dans HTTPS

crédit photo © Pavel Ignatov – Schuttersock