Pour pousser le HTTPS, Google devient une autorité de certification racine

Après avoir incité les acteurs du Web à migrer vers le HTTPS – en favorisant le ranking des sites employant ce protocole -, Google met la main à la pâte. Mountain View ouvre en effet sa propre autorité de certification racine, conçue pour authentifier l'identité des sites Web et gérer les exigences des produits Google en matière de certificats SSL/TLS.

Depuis quelque temps déjà, Google gère sa propre autorité de certification subordonnée (GIAG2). Mais, afin de pousser l'adoption du protocole HTTPS plus sécurisé que l'ancien HTTP, Google étend ses efforts pour renforcer la sécurité du Web avec la nouvelle autorité de certification racine, qui sera gérée par sa nouvelle division Google Trust Services.

« *Comme nous attendons avec impatience l'évolution du Web et de nos propres produits, il est clair que HTTPS continuera à être une technologie fondamentale. C'est pourquoi nous avons pris la décision d'élargir nos efforts actuels autour de l'autorité de certification pour inclure l'exploitation de notre propre autorité de certification racine* », a déclaré Ryan Hurst de la division sécurité et protection de la vie privée de Google.

Rachat de deux autorités de certification

« *Le processus d'intégration des certificats racines dans les produits et le délai avant que ces versions des produits soient largement déployées peuvent être longs. Pour cette raison, nous avons également acheté deux autorités de certification racines existantes, GlobalSign R2 et R4. Ces certificats racines nous permettront de commencer l'émission de certificats indépendants plus tôt* », ajoute Ryan Hurst.

Pour les utilisateurs des services Google et de son navigateur Chrome, la mise en œuvre des nouveaux certificats n'entraîne pas beaucoup de perturbations. Les développeurs Web et logiciels, en revanche, devront travailler pour répondre aux normes des certificats de Google, ce qui pourrait ralentir la vitesse à laquelle ils sortent de nouveaux produits et mises à jour.

Google semble avoir pris le parti d'adopter une approche sans concession en matière de sécurité Web ; la firme a récemment annoncé qu'elle bloquera les pièces jointes de fichiers JavaScript dans Gmail, et qu'elle déprécierait les sites utilisant le protocole web HTTP non sécurisé dans son moteur de recherche.

D'autres acteurs suivent cette voie, y compris Mozilla dont le navigateur Firefox 51 mettra en garde les utilisateurs visitant les sites Web HTTP contre les risques qu'ils encourent en consultant de telles pages.

A lire aussi :

Chiffrement : Symantec a émis des certificats HTTPS illégitimes

HTTPS : Google bannit les certificats Symantec de Chrome et Android

OVH propose gratuitement les certificats SSL de Let’s Encrypt

Crédit photo : isak55 / Shutterstock