Let Encrypt, une autorité de certification gratuite pour chiffrer le Web

Différents acteurs de l'IT, comme **Cisco, Akamai, Mozilla, mais aussi l'Electronic Frontier Foundation**, Identrust et des chercheurs de l'Université du Michigan, ont annoncé la création d'une **autorité de certification alternative et gratuite**. L'initiative a été baptisée **Let Encrypt** et vise à encourager le chiffrement des connexions aux sites Web. Ce projet intervient en réaction à la surveillance massive de la NSA dévoilée par le lanceur d'alertes Edward Snowden. Après le choc de ces révélations – mettant au jour la complicité des industriels américains dans les écoutes des espions US -, les acteurs de l'IT tentent de regagner la confiance de leurs clients en brandissant l'arme du chiffrement.

La prochaine version du protocole http sera ainsi probablement chiffrée par défaut. Google a aussi récemment indiqué son intention de mieux référencer les sites qui utilisent le chiffrement SSL/TLS. Même dans le mobile, Android et iOS ont sauté le pas du chiffrement des contenus des terminaux mobiles, s'attirant l'ire du FBI.

Gratuit et transparent

De son côté, Let Encrypt veut démocratiser le chiffrement des sites Web avec des **certificats gratuits**. Ces derniers apporteront la preuve aux navigateurs des utilisateurs que la connexion est sécurisée et authentifiera le site Web. Josh Aas, directeur de l'Internet Security Research Group en charge de piloter le projet Let Encrypt, s'interroge : « pourquoi ne pas utiliser TLS (successeur de SSL, NDLR) partout ? L'ensemble des navigateurs sur chaque terminal le supporte. Idem pour les serveurs dans les datacenters. Pourquoi nous ne changerions pas simplement la manière de procéder ? ». Dans la ligne de mire de l'association d'intérêt général, **la réduction des coûts et de la complexité pour obtenir un certificat**, « *le défi est pour le certificat des serveurs. Le passage obligé pour toutes communications TLS est l'obtention d'une clé publique qui authentifie le serveur. Pour de nombreux opérateurs, cette demande de certification est source de tracas, de confusion et peut s'avérer coûteuse. Par ailleurs, le certificat peut-être difficile à installer et à mettre à jour* ».

Selon le site de Let Encrypt, l'autorité de certification sera **mise en ligne au deuxième trimestre 2015**. Elle assure que les certificats seront gratuits, automatisés (dans les tests, un développeur met en général 1 à 3 heures pour activer le chiffrement, là il devrait réduire ce temps à 20 ou 30 secondes). Le protocole utilisé entre les serveurs web et l'autorité de certification est connu sous le nom de ACME (Automated Certificates Management Environment).

La transparence sera assurée par la **publication de la délivrance et de la révocation des certificats**. Un point essentiel. On se souvient en effet de l'affaire DigiNotar ou celle de Comodo en 2011 montrant les faiblesses des certificats en cas de vol. A l'époque, certains voulaient mettre fin à ce système de certification comme l'initiative « Convergence » soutenue par Moxie Marlinspike, expert en sécurité. Let Encrypt reprend le flambeau avec, espérons-le, plus de succès dans le changement des mentalités.

A lire aussi :

5 questions pour comprendre le déchiffrement SSL

Plus de 100 000 sites en SSL RSA 1024 bits écartés des navigateurs