Heartbleed : un an après, la faille est tombée dans l'oubli

Un cœur qui saigne. Le logo était choc pour que le grand public comprenne que la faille Heartbleed avait un impact direct sur la façon d'utiliser Internet. Le 9 avril 2014, un éditeur Codenomicon Defensics annonçait la découverte d'une vulnérabilité dans le logiciel OpenSSL chargé de protéger login de connexion, mot de passe, numéro de carte bancaire et autres données depuis le serveur qui héberge la transaction en cryptant la communication réalisée depuis le terminal (PC, tablette, smartphone…) sous protocole SSL/TLS. Au total, plusieurs millions de sites web étaient touchés et la couverture médiatique de ce trou de sécurité a été très importante.

Certes la faille a été corrigée pour la plupart des sites touchés, mais il restait en mai 2014 encore plus de 320 000 serveurs vulnérables. Et en septembre 2014 soit 5 mois après la divulgation, des chercheurs de 4 universités américaines ont dressé un bilan sur l'impact de Heartbleed.

La mémoire courte des américains

Mais qu'en est-il quasiment un an après ? Avec une telle médiatisation, on pouvait s'attendre à une prise de conscience de la part du grand public sur les questions de sécurité. Que nenni rétorque Dashlane qui vient de publier les résultats d'une étude. Le spécialiste de la gestion des mots de passe a interrogé plus de 2000 américains et à la question « *Avez-vous entendu parler de Heartbleed ?* », 86% des sondés ont répondu non. L'oubli médiatique a été rapide et les répercussions aussi. A la question « *Si vous avez entendu parler de Heartbleed, quelles sont les mesures de sécurité avez-vous prises pendant les 30 jours suivant l'annonce de la faille ?* », 49% ont changé au moins 1 mot de passe.

Emmanuel Shalit, CEO de Dashlane explique à nos confrères de *VentureBeat* : « *Le résultat le plus surprenant est que près de 9 américains sur 10 n'aient aucun souvenir de Heartbleed qui était sans doute la faille de sécurité la plus dangereuse de l'ère numérique moderne.* » Surtout que Heartbleed a ouvert la voie à d'autres menaces comme Shellshock ou Poddle, etc.

Dans son étude, l'éditeur démontre aussi que les gens se considèrent comme les plus à même de se protéger du piratage et des vols de données. La perception des données importantes selon les personnes interrogées est aussi surprenante. Ils sont plus sensibles à leurs informations de sécurité sociale et données bancaires. Par contre, ils sont 1% à considérer l'e-mail comme un sujet de préoccupation majeur en termes de sécurité. Un comble quand on sait que la messagerie recèle de multiples données sensibles.

A lire aussi :

Piratage de l'hôpital US : Heartbleed fait des millions de victimes
Shell Shock : une faille dans Bash à la hauteur de Heartbleed