SMTP STS : Google, Microsoft et Yahoo musclent le chiffrement des mails

Dans le monde du chiffrement, SMTP, le protocole de service de messagerie n'a jamais eu la cote. Né en 1982, ce protocole était loin d'imaginer la surveillance des quelques milliers d'ordinateurs connectés au PC à cette période. Avec le développement du web, des cyber-criminels et l'espionnage des Etats, les acteurs IT ont poussé l'extension STARTTLS à SMTP. Il s'agissait d'une méthode pour créer une connexion sécurisée pour envoyer des mails.

Malheureusement, STARTTLS a péché en matière de sécurité. En cause, une série de défauts de conception qui donnait la capacité à des attaquants d'usurper le serveur de réception et de leurrer l'expéditeur en lui laissant croire que le destinataire ne supporte pas le chiffrement et qu'il doit envoyer les données en clair.

Du HSTS adapté au SMTP

Pour combler ces défauts, des chercheurs indépendants, ainsi que plusieurs sociétés IT comme Yahoo, Facebook et Google, Microsoft ou Linkedin ont décidé de renforcer SMTP avec une nouvelle extension de chiffrement baptisé STS (Strict Transport Security). « *SMTP STS est au SMTP ce que le HSTS est au HTTPS* », tente de schématiser les spécialistes en sécurité dans le document remis à l'IETF.

L'analogie est pertinente, car tout comme HSTS, SMTP STS apporte la confidentialité des messages, l'authentification du serveur lors de l'initialisation d'un canal de communication chiffré, etc. L'objectif est d'éviter la dégradation du chiffrement en SSL/TLS plus vulnérable et aussi les attaques de type man in the middle. SMTP STS donnera la capacité à deux serveurs engagés dans un échange de mail de valider le chiffrement que chacun doit utiliser, si le cryptage est supporté et que faire s'il ne l'est pas.

Cette extension de protocole doit maintenant être regardée et analysée par l'IEEE avant d'être ratifiée. A noter que d'autres initiatives existent déjà pour sécuriser les emails comme DEEP (Deployable Enhanced Email Privacy).

A lire aussi :

Sécurité : 85 % des VPN SSL sont des passoires

Nogofail : Google traque les failles de SSL et TLS