L'Europe milite pour un certificat SSL europÃ©en normÃ©
Internet
PostÃ© par : JPilo
PubliÃ©e le : 18/5/2016 14:30:00

La fraude informatique, lâusurpation dâidentitÃ© numÃ©rique et plus gÃ©nÃ©ralement la cybersÃ©curitÃ© sont plus que jamais des sujets stratÃ©giques qui sâimposent aux entreprises, collectivitÃ©s et au grand public.

Â
Dans ce contexte grandissant, le passage des sites internet en HTTPS se dÃ©veloppe nÃ©cessairement. En effet, cette technologie, quand elle rÃ©pond Ã un process normÃ©, permet Ã lâinternaute dâune part de vÃ©rifier quâil est rÃ©ellement sur le site lÃ©gitime, et dâautre part de rendre confidentiels ses Ã©changes avec le site.

A lâorigine, le HTTPS concernait principalement les transactions financiÃ¨res, lâinternaute en acte dâachat est en effet basculÃ© au moment du paiement sur le site sÃ©curisÃ© dâune banque. Depuis, le piratage numÃ©rique sâest dÃ©veloppÃ©â¦ il est par exemple devenu courant pour un internaute de surfer sur un site e-commerce illÃ©gitime (alors quâil pense Ãªtre sur le site officiel), puis dâÃªtre dirigÃ© vers un paiement sÃ©curisÃ© mais sur le compte bancaire du hackerâ¦ Et il nây a pas que votre argent qui soit concernÃ©, mais Ã©galement toutes les donnÃ©es personnelles et sensibles que vous Ã©changez avec le site internet.

Il faut donc permettre Ã lâinternaute de vÃ©rifier, dÃ¨s sa connexion, quâil est rÃ©ellement sur le site concernÃ©. Câest pour cette raison que les sites de commerce, les sites rÃ¨glementaires et les portails sâÃ©quipent de plus en plus en HTTPS. Pour obtenir cette technologie, le propriÃ©taire dâun site doit sâÃ©quiper dâun certificat SSL. Mais ATTENTION, il existe en effet deux sortes de certificats SSL : les normÃ©s et les non normÃ©s. Et la diffÃ©rence est de tailleâ¦

En gÃ©nÃ©ral, le certificat SSL non normÃ© ne vÃ©rifie pas des informations vitales comme la vÃ©racitÃ© du propriÃ©taire du site, ce certificat est dâailleurs souvent gratuit. Ce HTTPS ne permet donc que de rendre confidentiels les Ã©changes avec le site sans savoir sâil sâagit du vrai siteâ¦ Alors que le certificat normÃ© est dÃ©livrÃ© selon un process rÃ¨glementaire par un prestataire de confiance habilitÃ© officiellement par un Etat ou assimilÃ©.

Ce prestataire va notamment vÃ©rifier lâexistence juridique du propriÃ©taire du site et vÃ©rifier si le nom de domaine lui appartient bien. En cliquant sur le cadenas prÃ©sent dans la barre de navigation, lâinternaute pourra accÃ©der Ã des informations garanties sur le prestataire et sur les informations prÃ©citÃ©es, il aura ainsi la sÃ©rÃ©nitÃ© dâÃªtre sur le site concernÃ©.

Il est essentiel pour les entreprises et collectivitÃ©s de sâÃ©quiper dâun certificat SSL normÃ©. Câest dans ce contexte que le certificat SSL normÃ© et europÃ©en a Ã©tÃ© intÃ©grÃ© au nouveau RÃ¨glement EuropÃ©en eIDAS qui entre en application le 1 juillet 2016. Pour une entitÃ© europÃ©enne, sâÃ©quiper dâun certificat adâhoc nâest que du bon sens ; en effet les donnÃ©es restent en Europe et la vÃ©rification sera rÃ©alisÃ©e selon des rÃ¨gles europÃ©ennes en conformitÃ© Ã©galement avec un autre nouveau RÃ¨glement EuropÃ©en sur la protection des donnÃ©es personnelles (GDPR).

En gÃ©nÃ©ralisant ces usages, lâ□□Europe devient garant dans la confiance numÃ©rique. Cette avancÃ©e est indiscutablement une nouvelle Ã©tape dans la lutte contre la cybercriminalitÃ©.

Enfin, on notera Ã©galement que la mise en place du protocole HTTPS est dorÃ©navant un Ã©lÃ©ment qui permet dâ□□amÃ©liorer son rÃ©fÃ©rencement sur les moteurs de recherche permettant de dÃ©velopper un avantage concurrentiel.

Arnauld Dubois, PDG de DHIMYOTIS