Sécurité : 85 % des VPN SSL sont des passoires

Les VPN (réseaux privés virtuels) exploitant le protocole de chiffrement SSL/TLS sont souvent insuffisamment sécurisés, faute d'exploiter des technologies à jour. C'est le constat dressé par la société High-Tech Bridge après avoir étudié un peu plus de 10 000 de ces VPN SSL accessibles publiquement et fournis par les principaux acteurs du marché (Cisco, Dell, Fortinet…).

La société de services IT basée entre la Suisse et les États-Unis constate que plus des trois quarts des serveurs testés exploitent encore SSLv3, une version aujourd'hui considérée obsolète environ vingt ans après sa sortie. De nombreux standards et normes interdisent formellement son implémentation ; les principaux navigateurs Web en ont désactivé, par défaut, la prise en charge.

Quelques dizaines de VPN utilisent même encore SSLv2, sur lequel Internet Explorer avait pourtant fait l'impasse… dès 2005.

Autre point commun à de nombreux VPN (76 % d'entre eux en l'occurrence) : l'utilisation d'un certificat non approuvé ; c'est-à-dire que l'autorité qui (auto)signe ledit certificat est inconnue du navigateur Web. Assez pour permettre à un tiers de s'intercaler sur la connexion et d'intercepter des données, sur le principe d'une attaque « Man-in-the-Middle », comme le relèvent nos confrères de *ITespresso*.

SHA-1, clef de 1 024 bits, Heartbleed

Toujours sur le volet des certificats, 74 % ont une signature SHA-1, un format insuffisamment sécurisé qui doit – théoriquement – être abandonné par l'industrie des navigateurs Web d'ici au 1er janvier 2017.

Sa vulnérabilité a été démontrée à plusieurs reprises, notamment dans le cadre d'un travail de recherche mené par plusieurs organismes dont l'Inria. Les ressources informatiques nécessaires pour craquer SHA-1 sont devenues plus accessibles financièrement : quelques dizaines de milliers de dollars suffisent désormais pour venir à bout de l'algorithme.

Dans le même ordre d'idée, le format des clés de chiffrement associées aux VPN pose également problème : 41 % d'entre elles exploitent un algorithme RSA-1024, alors qu'on considère aujourd'hui que le minimum pour garantir la sécurité est 2048 bits (voir la FAQ de Symantec sur ce sujet et une démonstration de l'Université du Michigan remontant à 2010).

A ce florilège de technologies dépassées, s'ajoute les vulnérabilités laissées par les failles non patchées. Ainsi, parmi les VPN basés sur la librairie Open Source OpenSSL, 10 % sont encore vulnérables à la faille Heartbleed, faute de mise à jour.

Au global, 85 % des VPN mis à l'épreuve héritent de la note la plus basse en matière de sécurité. High-Tech Bridge note aussi que seulement 3 % d'entre eux sont conformes à la norme PCI DSS (Payment Card Industry Data Security Standard)… et qu'aucun ne l'est vis-à-vis des

recommandations du NIST (National Institute of Standards and Technology), agence américaine qui définit des bonnes pratiques pour l'implémentation et l'exploitation de SSL/TLS.

A lire aussi :

Le chiffrement par TLS victime de… la paresse

Juniper : une backdoor made in NSA… récupérée par une organisation inconnue

SHA-1 : Google, Microsoft et Firefox font le ménage dans le HTTPS

Crédit Photo : Isak55-Shutterstock