Dominique Loiselet, Blue Coat : « généraliser le HTTPS va rendre la sécurité aveugle »

La problématique n'est pas nouvelle. Les flux HTTPS représentent déjà une part significative du trafic Internet. Mais l'annonce faite récemment par Google, l'acteur leader du référencement surtout en Europe, de sa volonté de privilégier sur son moteur de recherche les sites proposant des connexions HTTPS (combinaison du HTTP avec une couche de chiffrement comme SSL ou TLS) risque de donner un sérieux coup d'accélérateur au phénomène. Avec des conséquences pour les webmasters, mais surtout pour les responsables sécurité (RSSI) des entreprises, comme l'explique Dominique Loiselet, directeur général del'éditeur américain Blue Coat pour la France.

Silicon.fr : Quelles sont les conséquences d'une généralisation des connexions HTTPS qui devrait découler de la récente annonce de Google :

Dominique Loiselet : Au fil des ans, les entreprises ont déployé de multiples solutions – contrôles sur les contenus, IPS, IDS, firewalls, gateway, etc. – pour apporter à leurs utilisateurs un certain niveau de confiance dans l'usage de la technologie. Or HTTPS rend ces technologies aveugles. Cet état de fait est d'ailleurs de mieux en mieux compris par les cybercriminels qui utilisent cette technique pour améliorer la dangerosité de leurs menaces ou faire sortir des données des entreprises. Le cabinet Gartner estime qu'en 2017, la moitié des attaques passeront par des flux chiffrés. Aujourd'hui, entre 20 et 40 % des flux sont déjà chiffrés. Sur cette part du trafic, qui va aller grandissante étant donné le positionnement de l'acteur dominant du référencement qu'est Google, les investissements des entreprises en matière de sécurité deviennent inutiles. Et maintenir le niveau de confiance offert aux utilisateurs sur les flux non cryptés sera difficile.

Pourquoi ?

Au moins pour trois raisons. D'abord parce que les solutions de sécurité présentes dans les entreprises sont déployées dans des silos qui ne communiquent pas entre eux. Il faut donc, en première approche, traiter la question du HTTPS sur chaque équipement. Ensuite, déchiffrer les

flux HTTPS au sein de ces équipements pour leur permettre d'inspecter le trafic – une option qui existe depuis des années sur des antivirus, firewalls, IDS, etc. – dégrade leurs performances de façon considérable. Dans une récente étude, NSS Labs estime ainsi que le déchiffrement se traduit par une dégradation de performances de 74 % sur les firewalls de nouvelle génération. Pour un RSSI, la conséquence est mathématique : si les flux HTTPS se généralisent, il lui faut 4 boîtiers là oà¹ auparavant un seul suffisait ! Enfin, il faut prendre en compte l'aspect légal. On ne peut pas tout déchiffrer, en particulier dans un pays comme la France. C'est donc une politique de déchiffrement qu'il faut mettre en place, conforme à la politique de sécurité de l'entreprise, en accord avec la législation du pays concerné et en concertation avec la DRH et les représentants du personnel.

##D'oà¹ l'approche centralisée que vous proposez à travers vos solutions SSL Visibility Appliance…

Ces boîtiers réseau, issus d'une technologie rachetée en 2013 à Netronome, déchiffrent le trafic crypté une seul fois et redirigent les flux vers les différents équipements. Cette approche décharge ces derniers d'une tà¢che pour laquelle ils ne sont pas conçus. Ces appliances intègrent également les connaissances issues de nos autres technologies. Ce qui nous permet de proposer des catégorisations de sites en fonction des URL, de la géolocalisation, etc. Associés à d'autres règles liées par exemple aux profils des utilisateurs, ces outils permettent de bà¢tir une politique de déchiffrement. Des boîtiers de ce type sont déjà déployés dans de très grandes entreprises en France.

Avec la généralisation des flux cryptés, on peut imaginer que les fabricants de firewalls, d'IDS ou de gateway proposent des composants dédiés afin d'assurer le déchiffrement sans dégrader les performances…

C'est possible. Mais deux problèmes subsisteront. Il faudra s'assurer que tous les équipements bénéficient de cette mise à jour. Et d'autre part, cette approche ne permet pas de mettre en place une politique centralisée qu'offre un hub de déchiffrement. Or, avec la généralisation annoncée du HTTPS, il y a fort à parier que les RSSI aient à mener pour le déchiffrement un travail identique à celui accompli pour le filtrage d'URL. Travail qui passera par une concertation avec les salariés et une négociation avec les représentants du personnel. Tant que le déchiffrement de flux par l'entreprise restait un épiphénomène, personne ne s'y intéressait vraiment. Très souvent, les entreprises limitent le déchiffrement à l'antivirus sans que personne ne s'y intéresse vraiment. Désormais, il va falloir l'étendre à des outils bien plus intrusifs, comme ceux de FireEye. Car, en plus d'assurer la sécurité des échanges, l'entreprise doit aussi veiller à sa conformité. Comment rester conforme à PCI DSS et garantir qu'aucun numéro de carte bleue n'a été exfiltré si on est aveugle sur 40 % du trafic ? Comment un OIV (Opérateur d'Importance Vitale) pourra-t-il savoir s'il est victime d'une attaque si cette dernière utilise le cryptage pour échapper à sa vigilance ?

Comprenez-vous la décision de Google, motivée, selon la société, par la volonté d'améliorer la sécurité sur le Web ?

Je ne comprends pas vraiment cet argument. Le SSL ne fait que garantir la confidentialité des informations véhiculées. Et n'est en rien une garantie contre la vulnérabilité des sites.

A lire aussi :

Sécurité de l’information : les entreprises dépensent toujours plus