Cisco lance un programme de vérification anti-NSA des équipements

Les révélations du lanceur d'alerte Edward Snowden sur les méthodes mondiales d'espionnage de la NSA (National Security Agency) ont porté un coup aux affaires de Cisco. En mai 2014, on apprenait ainsi que l'agence américaine injectait des backdoors dans du matériel informatique destiné à l'export. Serveurs, routeurs et autres équipements réseau étaient ainsi «□modifiés□» permettant à la NSA d'écouter les données de clients internationaux qui installent ces matériels.

Les pratiques de la NSA, qui remontent au moins à 2010 (comme le montre ce document extirpé par Snowden), n'ont certainement pas arrangé les résultats commerciaux de Cisco à l'export. Particulièrement en Chine, pays régulièrement accusé par les Américains de mener des cyber-attaques sur son territoire. Suite aux révélations de l'ancien consultant de l'agence de sécurité, le gouvernement chinois avait encouragé les entreprises locales à privilégier les solutions des fournisseurs locaux (Lenovo, Huawei, ZTE…). S'il est difficile de mesurer l'impact de cet appel, Cisco a affiché des résultats en recul de 21% sur la région en 2015 par rapport à 2014, selon son rapport annuel.

Vérifier le code

Une tendance que l'équipementier américain entend corriger au regard de la taille du marché chinois stratégique pour les fournisseurs IT mondiaux et plus globalement. Cisco a toujours nié collaborer directement avec la NSA. Et son CEO de l'époque, John Chambers (aujourd'hui président du conseil d'administration), s'était fendu d'une lettre à Barack Obama pour alerter des risques de pertes de confiance qu'entraînent les pratiques d'espionnage informatique. Mais les paroles et démarches d'influence ne suffisent pas. Pour restaurer cette confiance, Cisco passe aux actes.

L'équipementier a lancé le programme **Technology Verification Service**. En phase beta pour l'heure, il permet aux clients de vérifier les équipements avant de les acheter. Le service, qui sera payant, *« aide les clients à tester et se faire une idée de la technologie Cisco, y compris sur le matériel, les logiciels et le firmware*, indique l'équipementier sur son site. *Vous pouvez accéder, examiner, tester le code source et autre propriété intellectuelle au sein d'une installation spécialisée, dans un site hautement sécurisé. »* Celui-ci doit s'ouvrir début 2016 au Research Triangle Park en Caroline du Nord. Les premiers tests avec des clients triés sur le volet ont démarré en octobre.

184 points de contrôle

Cisco a également renforcé ses exigences en matière de sécurité auprès de ses quelque 25□000 fournisseurs (rappelons que l'entreprise ne dispose d'aucune usine de production). Ces derniers subissent aujourd'hui jusqu'à 184 points de contrôle en fonction de leurs spécificités couvrant des domaines tels que la fabrication, la gouvernance et la gestion d'actifs, pour vérifier l'intégrité de leurs actions.

Il n'en reste pas moins que, si tant est qu'il soit possible d'examiner de manière absolument fiable les millions de lignes de code d'un routeur, le problème demeure entre le moment où Cisco expédie ses produits aux clients et celui où ils le reçoivent (dans le cas où la NSA poursuivrait ses pratiques d'implantation de portes dérobées après sa réforme). D'autre part, les entreprises ont aujourd'hui probablement d'autres chats à fouetter, comme les groupes de cybercriminels ou d'activistes, pour assurer la sécurité de leur réseau que de s'inquiéter de pratiques d'espionnage sponsorisées par des Etats à des fins de sécurité nationale essentiellement.

Le long chemin du retour de la confiance

Enfin, plus qu'un problème de sécurité, Cisco paye peut-être commercialement, en Chine au moins, le boycott indirect que subissent ses concurrents chinois. Soupçonnés d'être à la solde du gouvernement chinois, Huawei et ZTE, ne peuvent accéder au marché américain des équipements de cœur de réseau. En 2012, le gouvernement australien a banni les équipements Huawei du projet de réseau très haut débit national. En France, toujours en 2012, le rapport Jean-Marie Bockel préconisait également d'écarter les routeurs chinois des cœurs de réseau.

Cisco n'est pas le seul fournisseur américain à subir les conséquences des révélations d'Edward Snowden. Selon les différents analystes, l'impact de la perte de confiance générée par les pratiques de la NSA s'élèvera entre 22 et 35 milliards de dollars de manque à gagner en 2016 pour l'industrie américaine IT. Le chemin du retour de la confiance sera long…

Lire également
Washington n'impose pas de backdoor légale à l'industrie IT
Chiffrement : comment échapper à la curiosité de la NSA
La politique biaisée de divulgation des zero day de la NSA