Gartner : le SDN est un paradis pour hackers

Au centre de la stratégie de tous les grands équipementiers réseau, le Software-Defined Network est « *une véritable mine d'or pour les pirates informatiques* ». C'est en tout cas l'opinion de **Greg Young, analyste en chef de la sécurité réseau du cabinet Gartner**, qui pointe des lacunes dans la sécurité des architectures SDN, provenant tant de l'interopérabilité des consoles d'administration entre elles, que de leur compatibilité avec certains équipements de sécurité ou des protocoles SDN eux-mêmes.

Pour le Gartner, ce constat ne remet pas en cause le développement futur du SDN qui, en centralisant les données sur une plateforme unique pour les redistribuer ensuite sur les switchs appropriés, doit aboutir à une **gestion simplifiée du réseau**. Mais il doit pousser les fournisseurs à travailler différemment. Pour Greg Young, le contrôleur SDN devenant un point central de régulation, il doit devenir un élément actif de la politique de sécurité. En servant notamment à détecter et contrer les attaques. Au sein des entreprises, l'arrivée du SDN doit également se traduire par **un rapprochement entre les administrateurs réseau et les RSSI**. « *L'utilisation de solutions de sécurité interopérables avec le SDN peut contribuer à réconcilier les sceptiques avec ce concept et simplifier la gestion des flux sur les réseaux sans compromettre les données* », assure de son côté Trevor Dearing, directeur marketing EMEA de Gigamon, un fournisseur spécialisé dans la gestion du trafic réseau.

Contrôleurs SDN : la cible rêvée de la NSA ?

De facto, les révélations d'Edward Snowden sur les écoutes massives de la NSA, dont le tout récent programme Hacienda de scan des ports TCP, doivent pousser l'industrie à s'interroger. Car, dans une architecture SDN, **les contrôleurs deviennent une cible de choix** pour des espions ou n'importe quelle organisation cyber-criminelle. De nombreux experts en sécurité ont souligné les risques inhérents à cette architecture centralisée. « *Il existe tant de moyens pour un assaillant de modifier les fondations même de votre trafic réseau en agissant sur le contrôleur. Nous n'avons jamais connu cela auparavant. Même les outils de management réseau traditionnels ne donnent pas ce niveau de flexibilité permettant de changer dynamiquement le comportement d'un réseau nœud par nœud* », expliquait en février dernier Dave Shackleford, un consultant de Voodoo Security, à nos confrères de SearchSDN.

En octobre dernier, la Open Networking Foundation, qui pilote le protocole Open Flow, publiait une analyse qui pointait les deux risques majeurs du SDN : sa console centralisée donc – cible de choix pour tout hacker cherchant à soutirer de l'information – mais aussi **le protocole de communication entre le contrôleur et les switch**, qui pourrait être visé notamment dans le cadre d'attaques en déni de service.

Crédit photo : © Sergej Khackimullin – Fotolia.com

A lire aussi :

Le marché du SDN estimé à 3,52 milliards dollars en 2018
Virtualisation du réseau : l’adoption du SDN prendra du temps