

IPv6 : les FAI craignent pour la sécurité du réseau

Selon le rapport annuel Worldwide Infrastructure Security Report publié par [Arbor Networks](#), plus de la moitié des fournisseurs d'accès à Internet (FAI) estiment que de nouvelles menaces pourraient émerger avec le déploiement du nouveau protocole IPv6 (Internet Protocol version 6).

L'enquête, qui portait sur environ 70 opérateurs de réseaux IP dans le monde, révèle une hausse continue d'attaques à petite échelle et sophistiquées : attaques de niveau service (DoS) ou sur des applications, empoisonnement DNS (DNS poisoning) et d'usurpation BGP (BGP hijacking).

Seulement 8 % des acteurs télécoms interrogés ayant répondu estiment que les menaces vont baisser avec l'amélioration du déploiement de l'IPv6, alors que 55 % estiment que les menaces vont s'aggraver.

Daniel Karrenberg, en qualité de chief scientist chez le registre Internet RIPE NCC, a déclaré que l'IPv6 n'est ni plus ni moins sécurisé que l'IPv4. « *Les responsables Internet doivent s'assurer que les parties spécifiques liées à la défense du réseau fonctionnent au moins aussi bien pour l'IPv6 que pour l'IPv4* », déclare-t-il. « *Si un firewall est utilisé comme stratégie de défense, il semblerait vain de lui faire inspecter uniquement les paquets IPv4 et laisser passer les paquets IPv6.* »

Selon Craig Labovitz, chief scientist chez Arbor Networks, de nombreux FAI ne seront pas pris en charge par les éditeurs de solutions de sécurité en cas de migration. « *Ils ne disposent pas de l'équipement et du soutien des fabricants pour la prise en charge des menaces relatives à la sécurité IPv6* », déclare-t-il. « *Une large gamme de commutateurs d'accès ne sont actuellement pas compatibles IPv6, et c'est encore plus vrai pour le matériel dédié aux backbones* »

Le rapport d'Arbor Networks soulignent également le fait que les FAI disposent de ressources de plus en plus limitées et se tournent de plus en plus souvent vers des fournisseurs de services managés de sécurité.

Selon Matthew Tyler, directeur du cabinet consulting Evolution Security Systems, si l'IPv6 devrait être plus sécurisé une fois implémenté, il restera des problèmes de sécurité au cours de la période de migration. « *Le plus gros problème de la sécurité réside dans la gestion continue du changement, et il est impossible de gérer le changement dans un environnement de la taille d'Internet* », déclare-t-il.