RFC 4778 : Operational Security Current Practices

Stéphane Bortzmeyer
<stephane+blog@bortzmeyer.org>

Première rédaction de cet article le 8 juin 2007

Date de publication du RFC : Janvier 2007

https://www.bortzmeyer.org/4778.html

La sécurité est désormais omniprésente sur Internet et d'innombrables RFC en parlent. Celui-ci liste les pratiques de sécurité actuellement mises en œuvre par les opérateurs réseau et les FAI.

C'est donc plutôt un reportage qu'un RFC normatif. Après avoir revu les menaces existant sur les réseaux, et les différents types d'attaque, notre RFC cite les contre-mesures adoptées. Pour chaque grande fonction, le RFC explique les attaques possibles sur cette fonction et les contre-mesures spécifiques. Les fonctions sont :

- La protection physique des équipements, placés dans des locaux fermés, à accès contrôlé. Même dans ces locaux, l'utilisation de mots de passe sur les équipements est systématique, souvent avec déconnexion automatique au bout de N minutes,
- La gestion à distance des équipements, typiquement via SSH (plus une base d'authentification, par exemple avec Radius), SNMP n'étant en général utilisé qu'en lecture et HTTP semblant souvent neutralisé. La plupart des acteurs enregistrent toutes les actions ainsi effectuées.
- L'acheminement des paquets IP ("*forwarding*"). Certains opérateurs, mais pas tous, mettent en œuvre les méthodes de filtrage décrites dans le RFC 2827 [1] ou bien le RFC 3704. Le filtrage par adresse MAC est très rare.
- Les protocoles de routage ("*routing*"). Ceux-ci peuvent faire l'objet d'attaques spécifiques (RFC 4593). L'authentification dite MD5 est largement utilisée, ainsi que le GTSM (RFC 3682). Diverses règles contrôlent le nombre maximum de préfixes envoyés par un pair, mais rares sont les opérateurs qui filtrent selon le contenu des IRR ("*Internet Routing Registry*").
- DoS. Ce phénomène, plaie de l'Internet, est une des plus grosses préoccupations des opérateurs. Parmi les contre-mesures, l'établissement de routes spéciales pour faire disparaitre le trafic non désiré dans un trou noir, routes souvent injectées dans BGP pour assurer leur transport rapide dans tout le réseau.

1. Pour voir le RFC de numéro NNN, https://www.ietf.org/rfc/rfcNNN.txt, par exemple https://www.ietf.org/rfc/rfc2827.txt