12/04/2013

EPR05/2013

www.enisa.europa.eu

Agence européenne ENISA : les fournisseurs de services Internet ne parviennent pas à mettre en place des filtres contre les grandes cyber-attaques

Dans son analyse d'une cyber-attaque massive récente, l'agence de cyber-sécurité de l'Union européenne ENISA souligne aujourd'hui que les fournisseurs d'accès Internet ont échoué dans la mise en place de mesures de sécurité connues déjà depuis plus d'une décennie. Cette erreur est aussi un facteur clé de l'échec de la lutte contre les cyber-attaques majeures, souligne l'Agence dans sa note d'information urgente : « Les cyber-attaques récentes peuvent-elles réellement menacer la disponibilité d'Internet ? »

La note d'information urgente se concentre sur la cyber-attaque à grande échelle organisée en mars contre l'organisation à but non lucratif Spamhaus qui a des bureaux à Genève et à Londres. L'assaut numérique a provoqué des retards notables pour les internautes, principalement au Royaume-Uni, en Allemagne ainsi que dans d'autres pays d'Europe occidentale. Selon les médias en ligne, l'attaque contre Spamhaus, qui a commencé le 16 mars, est le plus grand déni de service distribué (DDoS) dans l'histoire d'Internet. Les attaques DDoS fonctionnent par «surcharge» de la capacité du trafic entrant d'un site. L'attaque contre Spamhaus a duré plus d'une semaine. Dans sa phase finale, l'énorme quantité de trafic généré a causé des problèmes au London InterNet exchange.

L'ENISA souligne que la technique utilisée pour l'attaque DDoS est loin d'être nouvelle. Pourtant, aujourd'hui encore, de nombreux fournisseurs d'accès n'utilisent pas l'ensemble de recommandations, connu sous le nom Best Current Practice 38 (BCP38), qui existe depuis près de 13 ans. Un ensemble similaire de recommandations pour les opérateurs de serveur DNS (BCP140, publié en 2008) aurait réduit le nombre de serveurs pouvant être détournés par attaques par amplification DNS. Si ces recommandations avaient été mises en œuvre par tous les opérateurs, le filtrage du trafic aurait pu bloquer ces attaques.

Il y a, selon l'ENISA, un certain nombre de leçons qui peuvent être tirées de la crise, y compris :

- Les attaques ont de plus en plus d'ampleur. L'attaque de mars 2013 contre Spamhaus a atteint une taille de plus de 300 gigabits de données par seconde tandis que la plus grande attaque DDoS déclarée en 2012 était de 100 gigabits de données par seconde.
- La taille compte. Lors d'une attaque de telle envergure, même les points d'échanges commerciaux d'Internet, qui bénéficient normalement d'infrastructures de très grandes capacités, peuvent être compromis.

L'Agence émet trois recommandations techniques :

- Les opérateurs de services pertinents devraient mettre en œuvre le BCP38 ;
- Les opérateurs de serveurs DNS doivent vérifier si leurs serveurs peuvent être détournés, et mettre en œuvre BCP 140 le cas échéant ;
- Les points d'échange des opérateurs Internet doivent s'assurer qu'ils sont protégés contre les attaques directes.

Le directeur exécutif de l'ENISA, le Professeur Udo Helmbrecht, a déclaré : *« Il est clair que les fournisseurs d'accès Internet ont encore beaucoup à apprendre en ce qui concerne la protection contre les cyber-attaques. La prévention est la clé pour lutter efficacement contre les cyber-attaques. Nous nous félicitons de la stratégie de cyber-sécurité de l'UE, qui propose un renforcement du rôle de l'ENISA, avec des ressources suffisantes en vue d'aider à protéger la société et l'économie numériques de l'Europe. »*

Pour la note d'information urgente ENISA
Contexte : La **stratégie sur la cybersecurité** de l'UE
Pour toute demande d'interview : Ulf Bergstrom, Porte-parole, press@enisa.europa.eu, téléphone : +30 6948 460 143, ou Dr. Louis Marinos, louis.marinos@enisa.europa.eu

Veuillez noter: traduction. La version anglaise est la seule version officielle
www.enisa.europa.eu/media/enisa-en-francais/
www.enisa.europa.eu