MANRS

Mutually Agreed Norms for Routing Security

Comment la Sécurité du Routage Améliore la Confidentialité en Ligne

INFORMATIONS DESTINEES AUX DEFENSEURS DE LA CONFIDENTIALITE EN LIGNE

La confidentialité en ligne est la liberté de ne pas être observé en ligne à son insu et sans y consentir. L'amélioration et la sécurisation de la manière dont le trafic circule sur Internet via le routage contribuent à améliorer la confidentialité en ligne en réduisant la possibilité que les données soient interceptées, collectées ou observées par des parties non autorisées.

Sécuriser un Système Basé sur une Confiance non Vérifiée

Internet est composé de plus de 74 000 réseaux indépendants, notamment ceux gérés par des entreprises, des universités et des écoles, des agences gouvernementales, des fournisseurs d'accès à Internet à haut débit et mobile, ainsi que des fournisseurs de connectivité qui assurent des services de transit pour leurs clients.

Chaque réseau échange des informations de routage sur la manière dont il se connecte aux réseaux voisins. Ces informations permettent à votre routeur de sélectionner le meilleur itinéraire (route) pour atteindre le réseau auquel vous devez vous connecter.

Le partage d'informations de routage repose sur la confiance et n'a pas été conçu dans un souci de sécurité. Le routage peut donc être exploité de manière abusive en partageant délibérément ou par erreur des informations incorrectes, ce qui peut faciliter des activités malveillantes sur Internet et entraîner :

- La suppression du trafic
- L'inspection et/ou la collecte non autorisée du trafic
- Des attaques par déni de service (DoS)
- La déconnexion d'Internet de pays entiers

Comment l'initiative MANRS Peut-elle Améliorer la Confidentialité en Ligne?

La sécurité sur Internet et la confidentialité en ligne peuvent être considérablement améliorées si les opérateurs de réseau (tels que les fournisseurs de services Internet - FAI), les points d'échange Internet (IXP), les réseaux de diffusion de contenu (CDN), les fournisseurs de cloud et les fournisseurs d'équipement mettent en œuvre les bonnes pratiques actuelles de routage sécurisé telles que celles définies par les Normes pour la sécurisation du routage mutuellement agréées (MANRS).

Mutually Agreed Norms for Routing Security (MANRS)

L'initiative MANRS définit des actions spécifiques qui aident à éliminer les malfaiteurs et les mauvaises configurations accidentelles qui nuisent à la sécurité sur Internet. Ces actions comprennent :

- Filtrer les informations de routage incorrectes
- Rendre plus difficiles à usurper l'identité des services Internet authentiques
- Tenir à jour les coordonnées actuelles exactes pour aider les opérateurs de réseaux à contacter les bonnes personnes si un réseau est compromis, piraté ou partage des informations de routage incorrectes
- La validation cryptographique des informations de routage

Comment Puis-je Participer à l'initiative MANRS ?

Vous n'avez pas besoin d'avoir des connaissances techniques pour participer à l'initiative MANRS. Vous pouvez :

- Promouvoir le programme MANRS au sein de votre chapitre de l'Internet Society ou de votre communauté technique
- Parler de la sécurité du routage et de MANRS avec votre organisme de réglementation ou votre FAI
- Suivre le blog de MANRS et les médias sociaux pour rester informé des développements récents
- Promouvoir l'initiative MANRS auprès d'autres organisations impliquées dans la confidentialité en ligne
- Si vous dirigez un réseau ou gérez une entreprise qui le fait, prenez les mesures préconisées et rejoignez l'initiative MANRS

EN SAVOIR PLUS SUR MANRS.ORG