# Comment les décideurs peuvent-ils améliorer la sécurité du routage mondial ?

*Informations destinées aux décideurs des secteurs des TIC et des télécommunications*

Aujourd'hui, Internet joue un rôle essentiel dans la majorité des sociétés du monde. De la banque à l'éducation, de la santé à la logistique, presque tous les secteurs s'appuient sur des applications et des services basés sur Internet pour fonctionner.

Notre dépendance accrue à l'égard des technologies numériques s'accompagne de préoccupations croissantes concernant la sécurité sur Internet. Si celle-ci comporte de nombreuses dimensions, il est essentiel de sécuriser les principaux éléments constitutifs de l'infrastructure Internet.

Le système de routage d'Internet permet aux données de circuler d'un point à un autre. La sécurité du réseau Internet repose sur la circulation correcte de ces données vers leur destinataire.

Des milliers d'incidents de routage Internet se produisent chaque année, entraînant des dommages économiques :

- en rendant des services clés inaccessibles ;
- en perturbant le commerce électronique ;
- en permettant à des acteurs malveillants d'espionner les utilisateurs et, ce faisant, de compromettre les systèmes.

Si les mesures de sécurité existantes peuvent contribuer à résoudre bon nombre de ces incidents de routage, les solutions qu'elles apportent sont souvent limitées. Compte tenu de l'interconnexion des réseaux, de nombreuses solutions ne fonctionnent que si d'autres réseaux procèdent aux mêmes améliorations. **Pour changer réellement les choses, nous avons besoin d'une action collective.**

À l'appui du programme plus vaste de sécurité sur Internet, nous encourageons les décideurs à travailler avec, entre autres, les opérateurs réseau et infrastructure, les agences de protection des infrastructures critiques et les organismes de normalisation afin d'améliorer la sécurité du routage mondial tout en préservant les aspects vitaux du système qui ont permis à Internet d'être ouvert et universel.

## Qu'est-ce que le MANRS ?

Les Normes pour la sécurisation du routage mutuellement agréées (MANRS) sont un ensemble de meilleures pratiques basées sur des normes existantes. Ces pratiques aident les opérateurs réseau à améliorer la sécurité du système de routage mondial d'Internet.

Le MANRS définit quatre actions simples mais concrètes que les opérateurs réseau peuvent mettre en œuvre pour améliorer considérablement la sécurité et la fiabilité d'Internet. Entre autres :

1. **Filtrage** – définition d'une politique de routage claire et mise en place d'un système permettant de garantir que les annonces aux réseaux adjacents sont correctes.
2. **Anti-usurpation** – activation de la validation de l'adresse source (SAV) et mise en œuvre de l'anti-usurpation pour empêcher les paquets ayant une adresse IP source incorrecte d'entrer et de sortir du réseau.

3. **Coordination** – maintien d'informations de contact actualisées et accessibles dans le monde entier pour faciliter la réponse aux incidents.
4. **Validation mondiale** – publication de données permettant à d'autres parties prenantes de valider les informations de routage à l'échelle mondiale.

Les deux premiers, le filtrage et la validation de la source IP, s'attaquent aux causes profondes des incidents de routage courants. Les deux autres, la coordination et la validation mondiale, permettent de limiter l'impact des incidents et de réduire la probabilité de nouveaux incidents.

Les actions MANRS définissent des résultats plutôt que des méthodes spécifiques. Cela permet à la mise en œuvre d'évoluer avec la technologie et contribue à faire des actions MANRS une meilleure pratique.

**Outre les incidents de routage, le MANRS cherche à relever les défis de l'écosystème dans le système de routage mondial.**

Le MANRS améliore les incitations économiques à la sécurité du routage en permettant aux opérateurs réseau de démontrer leur engagement envers :

- la sécurité - en sécurisant l'infrastructure Internet de base pour une plus grande sécurité sur Internet au niveau mondial ;
- les clients - en garantissant que les services qu'ils fournissent respectent les meilleures pratiques de sécurité en matière de routage ;
- les concurrents - en veillant à ce que les incidents de sécurité liés au routage n'aient pas d'effet en cascade sur les autres opérateurs réseau ;
- les décideurs - en garantissant une infrastructure Internet nationale solide et résiliente à l'appui du programme plus vaste de sécurité sur Internet.

Une étude indépendante réalisée par 451 Research[1] à la demande de l'Internet Society a révélé que le routage, le détournement et l'interception du trafic étaient, en matière de sécurité, la principale préoccupation des entreprises. Les attaques par déni de service distribué (DDoS) et l'usurpation d'adresse arrivent en deuxième position.

## 94 % des entreprises se sont déclarées prêtes, dans une situation de concurrence, à payer plus pour un fournisseur membre du MANRS.

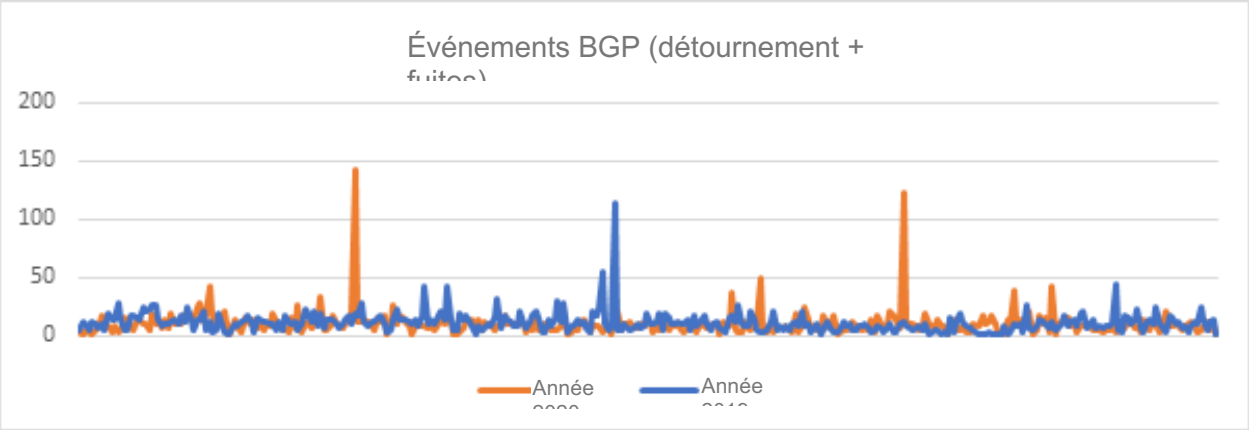
Cela souligne l'importance de la mise en œuvre du MANRS comme indicateur des bonnes pratiques de sécurité d'un opérateur réseau.

En tant que décideur, vous pouvez vous en servir pour encourager l'adoption du MANRS parmi les fournisseurs de réseaux tout en améliorant la sensibilisation à la sécurité du routage pour les utilisateurs, y compris les entreprises.

[1] Rapport d'étude du projet MANRS : https://www.manrs.org/wp-content/uploads/2017/10/MANRS-451-Study-Report.pdf

## Pourquoi le MANRS est-il important pour la sécurité sur Internet ?

En 2020, le réseau a connu un total de 3 873 incidents majeurs impliquant des attaques liées au BGP (Border Gateway Protocol). Parmi ceux-ci, 64 % étaient des détournements et le reste des fuites de route.




En 2019, 4 232 incidents réseau majeurs ont impliqué le BGP, ce qui a permis de constater les faits suivants :

- 3,8 % de la totalité des réseaux ont été affectés par un incident de routage ;
- 2 % de la totalité des réseaux ont été à l'origine des 4 232 incidents de sécurité liés au routage.

Ces incidents peuvent :

- créer une forte pression sur les infrastructures ;
- entraîner des pertes de trafic ;
- permettre l'inspection non autorisée du trafic ;
- servir à réaliser des attaques par déni de service (DoS).

En juillet 2020, deux incidents de routage importants se sont produits dans le système de routage BGP mondial[2], impactant plus de 1 500 réseaux dans le monde. Cela a mis en évidence la nécessité pour les opérateurs réseau de mettre en œuvre de bonnes pratiques en matière de sécurité du routage. Ces incidents ont touché des fournisseurs de réseaux nord-américains de premier plan, notamment TWC, Rogers et Charter[3].

Aucune organisation ni aucun groupe ne pouvant faire face seul aux menaces qui pèsent sur la sécurité liée au routage, le seul moyen efficace d'y parvenir est une action collective à l'échelle mondiale. **Les gouvernements et les décideurs peuvent jouer un rôle clé en facilitant une telle action collective.**

2. Une importante fuite de routes montre la nécessité de sécuriser le routage https://www.manrs.org/2020/07/big-route-leak-shows-need-for-routing-security/

3 .Un nouvel incident lié au Border Gateway Protocol affecte TWC, Rogers, Charter et d'autres https://www.manrs.org/2020/07/another-bgp-incident-impacts-twc-rogers-charter-and-others/

## En tant que décideur, quel rôle pouvez-vous jouer ?

1. **Évitez les barrières réglementaires :** contribuez à améliorer les incitations du marché pour une meilleure sécurité du routage en évitant toute barrière réglementaire et en facilitant la coopération et la collaboration.

2. **Encouragez les bonnes pratiques :** encouragez et facilitez les initiatives de manière à préserver les points forts du système de routage mondial, notamment sa résilience globale, sa facilité d'utilisation, sa flexibilité et son évolutivité.

3. **Favorisez l'adoption de lignes directrices communes :** vous êtes particulièrement bien placé pour favoriser l'adoption de lignes directrices communes aux opérateurs réseau, pour faciliter les meilleures pratiques du secteur en matière de sécurité du routage et pour promouvoir leur mise en œuvre.

4. **Octroyez des incitations :** lorsque cela est possible, facilitez le processus par des incitations telles que des subventions et des abattements fiscaux.

5. **Éliminez les obstacles juridiques :** aidez à identifier et à éliminer les obstacles juridiques au partage d'informations et aux réponses aux incidents de routage. Les opérateurs réseau et infrastructure, ainsi que les chercheurs en sécurité, peuvent craindre que la divulgation d'incidents ou de menaces de sécurité liés au routage ne les mette en danger sur le plan juridique. En leur offrant des garanties, vous pouvez contribuer à apaiser ces inquiétudes.

6. **Donnez l'exemple :** les gouvernements gérant en général leurs propres réseaux de grande taille, ils peuvent donner l'exemple en améliorant la fiabilité et la sécurité de l'infrastructure Internet à l'aide des meilleures pratiques du MANRS.

Compte tenu de l'impact considérable des incidents de routage sur les réseaux critiques, nous devons accorder une priorité élevée à la protection et à l'amélioration de notre infrastructure de réseau. Cependant, selon certaines études, la capacité de mesures simples à réduire considérablement ces incidents est généralement méconnue.

Certaines des mesures décrites ci-dessus ne sont pas entièrement nouvelles et des organisations pourraient s'efforcer de les intégrer dans un avenir proche. Pour garantir une infrastructure réseau plus saine et plus robuste, nous devons donner la priorité aux mesures mises en évidence dans ce document et soutenir leur mise en œuvre par des ressources adéquates.

- Pour en savoir plus sur le MANRS : manrs.org
- Découvrez le travail de l'Internet Society : internetsociety.org