Comment les responsables informatiques peuvent-ils améliorer la sécurité du routage mondial ?

Informations destinées aux CIO, CTO et CISO

Aujourd'hui, Internet joue un rôle essentiel dans nos sociétés de plus en plus numériques à travers le 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.**

En tant que dirigeant, vous êtes un décideur essentiel. Vous jouez un rôle important dans la mise en place d'un dispositif efficace de sécurité réseau qui renforce et protège votre entreprise ainsi qu'Internet lui-même.

Qu'est-ce que le MANRS ?

Le MANRS (Normes pour la sécurisation du routage mutuellement agréées) est une initiative communautaire soutenue par l'Internet Society. Le MANRS fournit aux opérateurs réseau un ensemble de meilleures pratiques basées sur les normes existantes qui visent à améliorer la sécurité du système de routage mondial d'Internet.

En choisissant des fournisseurs de services conformes au MANRS (et en adhérant au MANRS si vous exploitez un réseau), votre entreprise peut à la fois améliorer sa sécurité et encourager les autres fournisseurs à améliorer leur infrastructure.

Le MANRS définit quatre actions simples mais concrètes :

- Filtrage du protocole BGP (Border Gateway Protocol) ;
- Anti-usurpation ;
- Coordination ; et
- Validation mondiale.

En mettant en œuvre ces actions, les opérateurs réseau peuvent améliorer considérablement la sécurité et la fiabilité d'Internet. Deux de ces étapes sont préventives et permettent de traiter les causes techniques des incidents de routage courants. Les autres mesures tirent parti des informations accessibles à l'échelle mondiale pour contribuer à limiter l'impact de ces incidents et à réduire la probabilité que de nouveaux incidents se produisent.

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 politiques - 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.

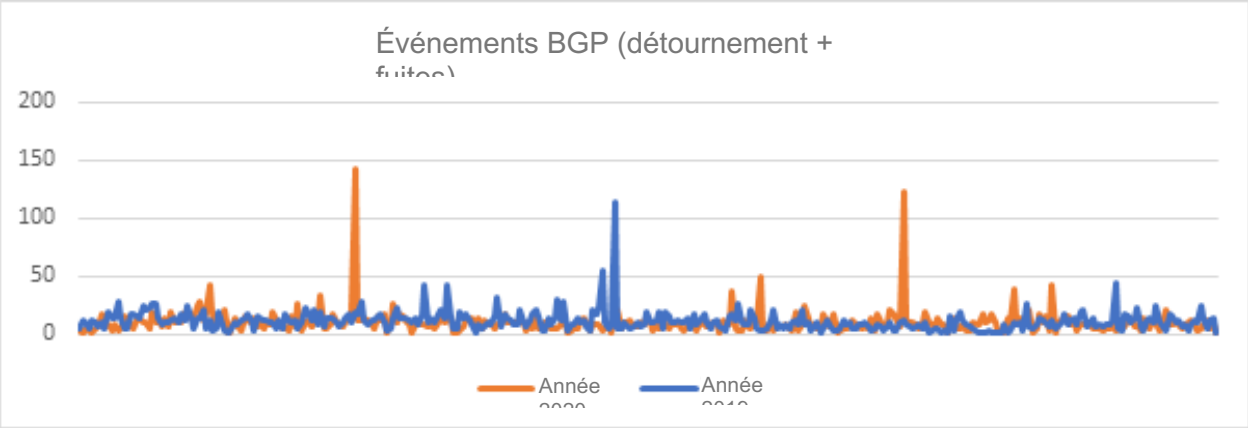
94 % des entreprises se sont déclarées prêtes, dans une situation de concurrence, à payer plus pour un fournisseur membre du MANRS.

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

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 les entreprises ?

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].

En tant que chef d'entreprise, vous pouvez aider votre entreprise à lutter efficacement contre les menaces de sécurité liées au routage en évaluant vos fournisseurs d'accès à l'Internet (FAI), vos réseaux de diffusion de contenu (CDN) et vos fournisseurs d'hébergement sur le cloud pour vous assurer de leur respect des meilleures pratiques en matière de sécurité.

Comment le MANRS peut-il aider votre organisation ?

1. **Assurez la continuité des activités et évitez les atteintes à la réputation :** Chaque entreprise devrait savoir si ses fournisseurs mettent en œuvre les meilleures pratiques de routage Internet dans le cadre de leur programme de continuité des activités. Les actions MANRS offrent à votre entreprise un moyen efficace de prévenir les incidents de sécurité réseau qui peuvent causer des dommages importants à la réputation de toute entreprise.

2. **La sécurité comme avantage concurrentiel :** La mise en œuvre d'actions MANRS permet à votre entreprise de communiquer auprès de ses clients sur son sérieux quant à la sécurité de son

infrastructure réseau. Cela peut constituer un facteur de différenciation essentiel pour votre organisation.

3. **Sélectionnez les vendeurs ou les partenaires :** Le MANRS peut aider les dirigeants de votre entreprise à choisir un partenaire approprié pour les opérations réseau ou cloud sans avoir à entreprendre un processus d'évaluation étendu ou complexe. Plusieurs fournisseurs clés sont déjà conformes au MANRS, ce qui simplifie considérablement le processus d'audit de leurs capacités de sécurité.

4. **Alignement des divisions sur la sécurité de l'infrastructure :** Les différents éléments de l'infrastructure informatique d'une entreprise peuvent avoir leurs propres pratiques de sécurité. La vulnérabilité de l'un d'entre eux peut représenter un risque sérieux pour votre entreprise. Les principes du MANRS peuvent servir de guide utile si vous cherchez à aligner toute votre infrastructure réseau sur des normes communes.

5. **Renseignement sur les menaces :** Votre entreprise peut chercher à améliorer sa connaissance de la situation et à s'intéresser par l'intégration de flux de renseignements à ses opérations. Les flux d'informations et d'événements que peuvent générer les actions MANRS auront donc de la valeur.

6. **Une liste de contrôle pour vérifier la robustesse de l'infrastructure :** Vous comprenez la menace que représentent les problèmes de sécurité réseau pour votre entreprise mais, en l'absence d'actions MANRS, vous ne disposez peut-être pas d'un moyen efficace et efficient de vérifier l'état de préparation de votre réseau central. La liste de contrôle du MANRS constitue un moyen simple d'évaluer la robustesse de l'infrastructure du réseau central de votre entreprise.

7. **Accès à une base de connaissances avancée :** Le MANRS vous donne accès à une vaste communauté qui se concentre sur les questions de sécurité. Cela peut aider votre organisation à établir une base plus solide pour la sécurité grâce à des collaborations.

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 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