Comment les entreprises peuvent-elles améliorer la sécurité du routage mondial ?

Informations destinées aux dirigeants d'entreprise

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.**

Pour contribuer aux efforts visant à sécuriser le réseau Internet, les entreprises doivent travailler avec, entre autres, les opérateurs réseau et infrastructure et les agences de protection des infrastructures critiques, afin de garantir que vos fournisseurs mettent en œuvre les meilleures pratiques en matière de sécurité du routage tout en préservant les aspects vitaux du système qui ont permis à Internet d'être ouvert et universel.

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 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 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 du 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.

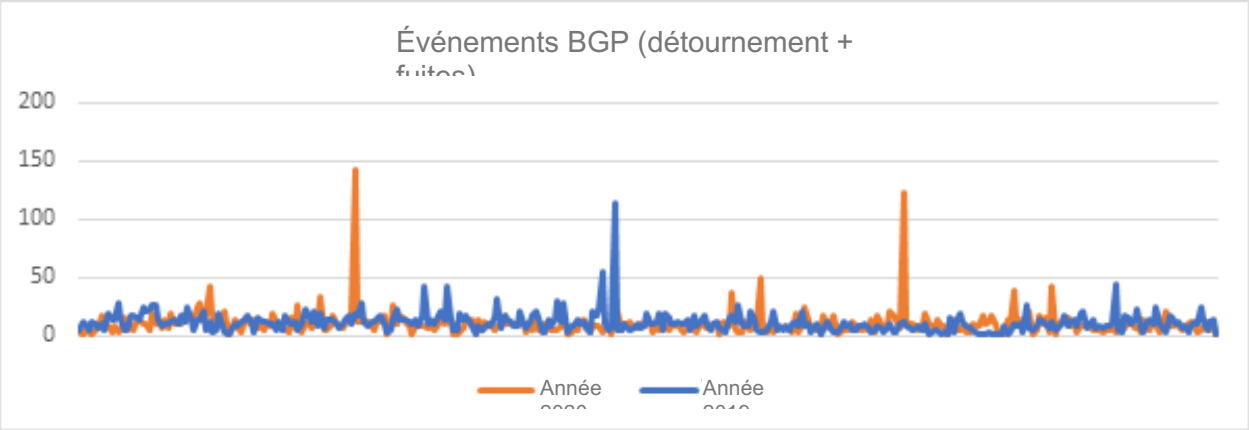
94 % des entreprises se sont déclarées prêtes, dans une situation de concurrence, à payer plus pour un fournisseur membre du MANRS.

Cela souligne l'importance de la mise en œuvre du MANRS comme indicateur de 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 protocole 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 ;
- être utilisés pour réaliser des attaques par déni de service (DoS), qui menacent la continuité des activités.

En juillet 2020, deux incidents de routage importants se sont produits dans le système de routage BGP mondial[2]. 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].

La seule façon efficace pour votre entreprise de lutter contre les menaces de sécurité liées au routage est de choisir des fournisseurs de services qui suivent un ensemble de directives établies, comme le MANRS. En choisissant des fournisseurs qui adoptent ces mesures, vous pouvez inciter le marché à construire des réseaux plus résilients qui, à leur tour, rendent l'infrastructure mondiale des réseaux plus sûre.

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

[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/

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. **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.

3. **La sécurité comme facteur de différenciation :** Si vous exploitez des réseaux, 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.

4. **Résoudre les incidents de sécurité réseau :** L'adoption d'actions MANRS sur vos réseaux aide votre organisation à atténuer les impacts immédiats et graves des incidents de sécurité réseau. S'ils ne sont pas résolus, ceux-ci peuvent perturber votre capacité à fonctionner et entamer la confiance des clients dans votre entreprise.

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 :** Les actions mises en évidence par le MANRS peuvent vous servir de liste de contrôle utile pour assurer la robustesse de votre infrastructure informatique interne. L'incorporation des actions MANRS aux opérations informatiques internes peut vous aider à accroître votre efficacité opérationnelle.

7. **Soutien communautaire pour les questions de sécurité :** En rejoignant l'initiative MANRS, votre entreprise a accès à une communauté plus large qui se préoccupe de la sécurité et des problèmes connexes. Cette communauté peut également servir à identifier les partenaires de l'écosystème avec lesquels votre entreprise peut unir ses forces pour créer une base de sécurité plus solide.

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