Comment les équipes de réponse aux incidents de sécurité informatique peuvent-elles améliorer la sécurité du routage mondial ?

Informations destinées aux CSIRT

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.

Internet est constitué de dizaines de milliers de réseaux interconnectés utilisant les protocoles TCP/IP (72 000 en juin 2021). Ces réseaux sont connectés les uns aux autres à l'aide du protocole BGP (Border Gateway Protocol). Le BGP est le seul protocole de passerelle actuellement disponible.

Le problème du BGP est qu'il a été conçu pour un environnement essentiellement universitaire. La sécurité n'était pas une considération importante, car les réseaux participants étaient censés coopérer pour maintenir le réseau en bonne santé. Le BGP est donc entièrement basé sur une confiance non vérifiée entre les réseaux.

Malheureusement, cela rend le système de routage mondial d'Internet intrinsèquement peu sûr. Il est de plus en plus souvent attaqué, soit par des criminels organisés qui voient l'occasion de voler des données et de causer des perturbations, soit en raison d'une mauvaise configuration et d'erreurs.

Quel est le rapport entre les CSIRT et la sécurité du routage ?

En tant que membre d'une équipe de réponse aux incidents de sécurité informatique (CSIRT), vous participez à l'élaboration de mesures de sensibilisation et d'atténuation de la sécurité pour vos utilisateurs finaux. Pourtant, la plupart des CSIRT n'incluent pas la sécurité du routage dans la sécurité des infrastructures au sein de leurs portefeuilles de services. Et ce, bien que le système de routage soit un élément clé des infrastructures nationales et internationales critiques.

Si les CSIRT ne gèrent généralement pas de réseaux, vous possédez néanmoins des connaissances spécialisées sur les attaques et les menaces, ainsi que sur les stratégies d'atténuation et de résolution. Vous êtes également chargé de recommander les meilleures pratiques en matière de sécurisation des systèmes, des réseaux, des données et des actifs critiques, ainsi que d'autres mesures de prévention des incidents.

Pour soutenir le portefeuille de la sécurité sur Internet, nous vous encourageons, en tant que membre d'un CSIRT, à travailler avec d'autres pour améliorer la sécurité du routage mondial, tout en adoptant une vision globale de l'écosystème de la sécurité sur Internet. C'est là que le MANRS intervient.

Qu'est-ce que le MANRS ?

Le MANRS (Normes pour la sécurisation du routage mutuellement agréées) est soutenu par l'Internet Society. Il s'agit d'une communauté d'opérateurs réseau, de fournisseurs de contenu et d'IXP responsables qui s'engagent à améliorer la sécurité et la résilience d'Internet. Il 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, les organisations peuvent à la fois contribuer à améliorer leur réseau et encourager les autres fournisseurs à améliorer leur infrastructure.

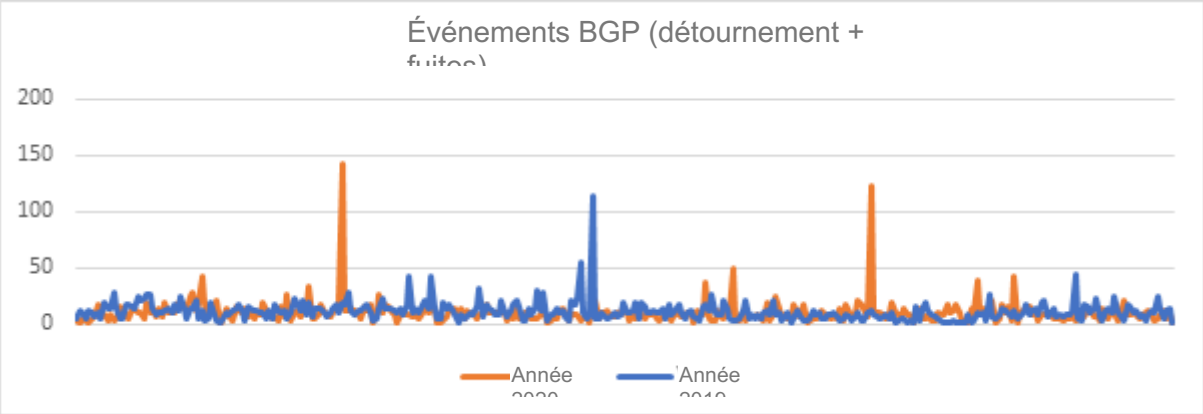
Le MANRS définit quatre actions simples mais concrètes que les opérateurs réseau peuvent mettre en œuvre pour améliorer considérablement la sécurité et la fiabilité d'Internet. Entre autres :

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 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.

Pourquoi le MANRS est-il important ?

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).

Les incidents de routage posent des problèmes concrets

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 dehors de ces cas marquants, des incidents de routage se produisent tous les jours, menaçant la stabilité et la sécurité du système de routage d'Internet.

Une étude indépendante réalisée par 451 Research à la demande de l'Internet Society[1] 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 montre que la mise en œuvre du MANRS est un indicateur fiable des bonnes pratiques de sécurité d'un opérateur réseau. Cependant, également selon cette recherche, le fait que des mesures simples peuvent réduire considérablement ces incidents est généralement mal compris.

Comment le MANRS peut-il aider les CSIRT ?

Dans le cadre des initiatives de renforcement des capacités et d'engagement communautaire du MANRS, nous souhaitons soutenir les communautés CSIRT dans les domaines suivants :

- la sensibilisation aux questions de sécurité du routage au sein de vos communautés ;
- l'encouragement d'autres CSIRT à ajouter la surveillance des incidents de sécurité de routage et le traitement des incidents à leur portefeuille de services ;
- l'encouragement des CSIRT à adopter l'outil de surveillance de l'Observatoire du MANRS pour fournir une connaissance situationnelle de la sécurité du routage ;
- l'extension de la portée de l'initiative MANRS dans les groupes CSIRT, ainsi que dans les initiatives nationales en matière d'infrastructures critiques ;
- l'organisation d'ateliers pratiques sur la sécurité du routage ou le co-développement d'un cursus sur la sécurité du routage dans le cadre de programmes de formation des formateurs et/ou de renforcement des capacités en matière de criminalistique des réseaux ;
- l'ajout de la sécurité du routage aux programmes d'audit de la sécurité du réseau.

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

De leur côté, les CSIRT peuvent :

- contribuer à encourager leurs organisations mères ou leurs membres à prendre plus au sérieux les questions de sécurité du routage ;
- sensibiliser les gouvernements à l'impact des problèmes de sécurité du routage sur les infrastructures critiques ;
- encourager l'adoption de recommandations en matière de sécurité du routage (telles que les normes NIST).

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.

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