MANRS

Mutually Agreed Norms for Routing Security

Comment les Décideurs Politiques Peuvent-ils Améliorer la Sécurité du Routage Mondial ?

INFORMATIONS DESTINEES AUX DECIDEURS DES SECTEURS DES TIC ET DES TELECOMMUNICATIONS

Plusieurs incidents récents de routage Internet ont provoqué des problèmes concrets, notamment la perte de recettes commerciales, le détournement de trafic Internet et des attaques par déni de service (DDoS). En conséquence, de plus en plus de gouvernements étudient comment sécuriser leurs réseaux et le système de routage mondial

Internet étant un ensemble de réseaux interdépendants, la résolution de problèmes systémiques tels que la sécurité du routage nécessite une action collective mondiale, telle que les actions préconisées dans les normes pour la sécurisation du routage mutuellement agréées (MANRS), une initiative menée par le secteur pour atténuer les menaces de sécurité de routage les plus courantes. Les gouvernements et les décideurs politiques peuvent contribuer à encourager les bonnes pratiques préconisées par MANRS dans leurs propres réseaux et dans leurs régions.

Les décideurs politiques doivent travailler avec les opérateurs de réseaux et d'infrastructures, les agences de protection des infrastructures critiques et les organismes de normalisation, entre autres, pour améliorer la sécurité du routage mondial tout en préservant les aspects vitaux du système qui ont permis à Internet d'être ouvert et universel.

Quel Rôle les Décideurs Politiques Peuvent-ils Jouer ?

Que ce soit par le biais de politiques de marchés publics ou en travaillant avec le secteur privé pour améliorer la sécurité du routage, les gouvernements ont un rôle crucial à jouer dans la création d'un écosystème de routage Internet plus sûr.

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

Encourager les bonnes pratiques : faciliter les initiatives de manière à préserver les atouts d'Internet, notamment sa résilience globale, sa facilité d'utilisation, sa flexibilité et son évolutivité.

Promouvoir des directives communes : soutenir l'utilisation de directives communes qui facilitent les bonnes pratiques actuelles du secteur en matière de sécurité du routage.

Incitations sous forme de subventions : motiver les opérateurs locaux à adopter les bonnes pratiques en matière de sécurité du routage grâce à des incitations telles que des subventions et des réductions d'impôts.

Encourager le partage d'informations : identifier et éliminer les obstacles juridiques au partage d'informations et aux réponses aux incidents de routage. Les opérateurs de réseaux et d'infrastructures et les chercheurs en sécurité doivent pouvoir travailler ensemble pour divulguer les incidents et les menaces qui pèsent sur la sécurité du routage. Leur offrir des garanties peut contribuer à apaiser ces inquiétudes.

Montrer l'exemple : investir, améliorer et assurer la fiabilité et la sécurité de l'infrastructure Internet de vos propres réseaux gouvernementaux en adoptant les bonnes pratiques de MANRS.

Les Gouvernements Passent à L'action

Les États-Unis et les Pays-Bas sont deux exemples récents de gouvernements soucieux de la sécurité du routage.

Le 31 juillet 2023, la Federal Communications Commission des États-Unis a organisé un atelier sur la sécurité du protocole BGP (Border Gateway Protocol) soulignant l'importance de remédier aux vulnérabilités du BGP et de sécuriser le routage Internet.

En juillet également, l'administration Biden-Harris a publié le plan de mise en œuvre de la stratégie nationale de cybersécurité, qui identifie « la collaboration avec les principales parties prenantes pour assurer un routage Internet sécurisé » comme une mesure essentielle.

Le gouvernement fédéral américain réfléchit également aux moyens d'améliorer la sécurité du routage de ses propres réseaux.

Aux Pays-Bas, l'initiative « se conformer ou expliquer » du gouvernement néerlandais exige que les services gouvernementaux déploient une bonne pratique de sécurité de routage appelée RPKI (soit l'acronyme de Resource Public Key Infrastructure, s'agissant d'un cadre d'infrastructure à clé publique de ressource), ou expliquent de manière satisfaisante pourquoi ils ne peuvent pas s'y conformer.

De même, un partenariat public-privé néerlandais a développé un programme Gold Star, qui fournit un service (internet.nl) aux opérateurs de réseaux du secteur privé pour montrer qu'ils respectent les bonnes pratiques en matière de sécurité de routage.

Équilibrer les Intérêts du Gouvernement est un Défi

Alors que les gouvernements tentent d'améliorer la sécurité du routage, ils doivent respecter la nature décentralisée et distribuée à l'échelle mondiale d'Internet.

Il n'y a pas de point de défaillance unique ni de contrôleur unique, le système de routage est donc difficile à contourner au niveau mondial. En fait, l'architecture du système de routage contribue à la résilience, à l'évolutivité et à la facilité d'adoption d'Internet.

Mutually Agreed Norms for Routing Security (MANRS)

Les efforts des dirigeants visant à centraliser le système de routage sapent les qualités qui ont fait le succès d'Internet et augmentent le risque d'attaques. Le gouvernement et le secteur doivent travailler ensemble sur des solutions qui donnent la priorité à la nature distribuée du système de routage Internet tout en renforçant l'adoption des bonnes pratiques. Les participants à l'initiative MANRS sont bien placés pour conseiller les gouvernements qui tentent de résoudre ce problème.

POUR EN SAVOIR PLUS SUR MANRS.ORG