MANRS

Mutually Agreed Norms for Routing Security

¿Cómo Pueden los Formuladores de Políticas Mejorar la Seguridad del Enrutamiento Global?

INFORMACIÓN PARA LOS FORMULADORES DE POLÍTICAS DE TIC Y DE TELECOMUNICACIONES

Recientemente, diferentes incidentes de enrutamiento de Internet han provocado problemas en el mundo real, entre ellos, pérdidas de ingresos comerciales, el desvío de tráfico de Internet y ataques DDoS. Como resultado, cada vez más gobiernos están investigando cómo pueden limpiar sus redes y el sistema de enrutamiento global.

Dado que Internet es un conjunto de redes interrelacionadas, resolver los problemas sistémicos como la seguridad del enrutamiento requiere una acción colectiva global, como las acciones indicadas en las Normas Mutuamente Acordadas para la Seguridad del Enrutamiento (MANRS), una iniciativa liderada por la industria para reducir las amenazas más comunes a la seguridad del enrutamiento. Los gobiernos y los formuladores de políticas pueden ayudar a facilitar las mejores prácticas de MANRS en sus propias redes y regiones.

Los formuladores de políticas deben trabajar con los operadores de redes e infraestructura, las agencias de protección de infraestructura crítica y los organismos de estandarización, entre otros, para mejorar la seguridad del enrutamiento global y al mismo tiempo preservar los aspectos fundamentales del sistema que han permitido que Internet sea abierta y universal.

¿Qué Papel Pueden Desempeñar los Formuladores de Políticas?

Ya sea a través de sus políticas de adquisición o trabajando junto con el sector privado para mejorar la seguridad del enrutamiento, los gobiernos desempeñan un papel fundamental en la creación de un ecosistema de enrutamiento de Internet más seguro.

Evitar las barreras regulatorias: Aumentar los incentivos del mercado para mejorar la seguridad del enrutamiento al evitar las barreras regulatorias y facilitar la cooperación y la colaboración.

Fomentar las buenas prácticas: Facilitar iniciativas de una manera que preserve las fortalezas de Internet, incluso su resiliencia general, facilidad de uso, flexibilidad y escalabilidad.

Promover lineamientos comunes: Apoyar el uso de lineamientos comunes que faciliten las mejores prácticas actuales de la industria para la seguridad del enrutamiento.

Otorgar incentivos: Motivar a los operadores locales a utilizar las mejores prácticas en materia de seguridad de enrutamiento mediante incentivos como subvenciones y devoluciones de impuestos.

Fomentar el intercambio de información: Identificar y eliminar las barreras legales para el intercambio de información y las respuestas a incidentes de enrutamiento. Los operadores de

redes e infraestructura y los investigadores en el área de la seguridad deben poder trabajar juntos para divulgar las amenazas y los incidentes de seguridad de enrutamiento. Proporcionarles salvaguardias puede ayudar a aliviar estas preocupaciones.

Predicar con el ejemplo: Invertir, mejorar y mantener la confiabilidad y la seguridad de la infraestructura de Internet de sus propias redes gubernamentales utilizando las mejores prácticas de MANRS.

Los Gobiernos Están Actuando

Estados Unidos y los Países Bajos son dos ejemplos recientes de gobiernos que están abordando la seguridad del enrutamiento.

El 31 de julio del 2023, la Comisión Federal de Comunicaciones de los Estados Unidos organizó un Taller de seguridad del protocolo BGP en el que se destacó la importancia de abordar las vulnerabilidades del BGP y proteger el enrutamiento de Internet.

También en julio, la administración Biden-Harris publicó el Plan de Implementación de la Estrategia Nacional de Ciberseguridad, que identifica “colaborar con partes interesadas clave para impulsar el enrutamiento seguro de Internet” como una acción crítica.

El gobierno federal de Estados Unidos también está considerando cómo mejorar la seguridad de enrutamiento de sus propias redes.

En los Países Bajos, la iniciativa gubernamental de “cumplir o explicar” exige que los departamentos del gobierno implementen una mejor práctica de seguridad de enrutamiento llamada RPKI, o que expliquen adecuadamente por qué no pueden cumplir con este requisito.

De manera similar, una asociación público-privada holandesa desarrolló un programa de “estrellas doradas” que les ofrece a los operadores de redes del sector privado un servicio (internet.nl) para mostrar que cumplen con las mejores prácticas en materia de seguridad del enrutamiento.

Equilibrar los Intereses Gubernamentales es un Desafío

A medida que los gobiernos intentan mejorar la seguridad del enrutamiento, deben defender la naturaleza descentralizada y globalmente distribuida de Internet.

No existe un único punto de falla ni un único controlador, por lo que el sistema de enrutamiento es difícil de romper a nivel global. De hecho, la arquitectura del sistema de enrutamiento contribuye a la resiliencia, la escalabilidad y la facilidad de adopción de Internet.

Los esfuerzos de arriba hacia abajo para centralizar el sistema de enrutamiento socavan las cualidades que han convertido a Internet en un éxito y aumentan el riesgo de ataques a la seguridad. Los gobiernos y la industria deben trabajar juntos en soluciones que prioricen la naturaleza distribuida del sistema de enrutamiento de Internet y que, al mismo tiempo, aumenten el uso de las mejores prácticas. Quienes participan en la iniciativa MANRS están bien posicionados para asesorar a los gobiernos que intentan abordar este problema.

MÁS INFORMACIÓN SOBRE MANRS: MANRS.ORG