¿Cómo pueden mejorar las personas formuladoras de políticas la seguridad del enrutamiento global?

Información para personas formuladoras de políticas de telecomunicaciones y TIC

Hoy en día, Internet juega un papel fundamental en la mayoría de sociedades del mundo. Desde la banca hasta la educación, la salud y la logística, casi todos los sectores dependen de aplicaciones y servicios basados en Internet para funcionar.

Nuestra mayor dependencia de las tecnologías digitales trae consigo una creciente preocupación por la seguridad de Internet. Si bien la seguridad de Internet tiene muchas dimensiones, es fundamental proteger los componentes básicos de la infraestructura de Internet.

El sistema de enrutamiento de Internet permite que los datos fluyan de un punto a otro. Garantizar que estos datos fluyan correctamente a su destinatario previsto, es la base de la seguridad de de Internet.

Cada año se producen miles de incidentes de enrutamiento de Internet que provocan daños económicos y sociales de la siguiente manera:

- haciendo que servicios clave sean inaccesibles;
- interrumpiendo el comercio electrónico;
- permitiendo que los agentes malintencionados espíen a los usuarios y, con ello, el potencial de comprometer los sistemas.

Si bien las medidas de seguridad existentes pueden ayudar a abordar muchos de estos incidentes de enrutamiento, las soluciones que brindan suelen ser limitadas. La naturaleza interconectada de las redes implica que muchas soluciones solo funcionan cuando otras redes realizan las mismas mejoras. **Necesitamos de acciones colectivas para lograr un cambio verdadero.**

En apoyo de la agenda más amplia de seguridad de Internet, alentamos a las personas formuladoras de políticas a trabajar con operadores de redes e infraestructura, agencias de protección de infraestructura crítica y organismos de estándares, entre otros, para mejorar la seguridad del enrutamiento global y al mismo tiempo preservar los aspectos vitales del sistema que han permitido que Internet sea abierta y universal.

¿Qué es MANRS?

Las Normas Mutuamente Acordadas para la Seguridad del Enrutamiento (MANRS, por sus siglas en inglés) es un conjunto de mejores prácticas basadas en normas existentes. Estas prácticas ayudan a los operadores de redes a mejorar la seguridad del sistema global de enrutamiento de Internet.

MANRS define cuatro acciones simples pero concretas que los operadores de red deben implementar para mejorar en gran medida la seguridad y confiabilidad de Internet. Entre estas se incluyen:

1. **Filtrado**: definir una política de enrutamiento clara e implementar un sistema para garantizar que los anuncios a las redes adyacentes sean correctos.

2. **Antisuplantación**: habilitar la validación de la dirección de origen e implementa la antisuplantación para evitar que paquetes con direcciones IP de origen incorrectas entren y salgan de la red.
3. **Coordinación**: mantener información de contacto actualizada y accesible a nivel mundial para ayudar con la respuesta a incidentes.
4. **Validación global**: publicar datos que permitan a otros agentes validar la información de enrutamiento a escala global.

Las dos primeras (el filtrado y la antisuplantación de direcciones IP) abordan las causas raíz de los incidentes comunes de enrutamiento. Las siguientes dos (coordinación y validación global) ayudan a limitar el impacto de los incidentes y a disminuir la posibilidad de incidentes futuros.

Las acciones de MANRS definen los resultados en lugar de métodos específicos. Esto permite que la implementación cambie con la tecnología y ayuda a establecer las acciones de MANRS como mejores prácticas.

Junto con los incidentes de enrutamiento, MANRS busca abordar los desafíos del ecosistema en el sistema de enrutamiento global.

MANRS mejora los incentivos económicos para la seguridad del enrutamiento al permitir que los operadores de redes demuestren su compromiso con:

- La seguridad: asegurando la infraestructura básica de Internet para una mayor seguridad global en Internet.
- Los clientes: asegurándose de que los servicios que brindan se adhieran a las mejores prácticas de seguridad de enrutamiento.
- La competencia: al garantizar que los incidentes de seguridad de enrutamiento no tengan un efecto en cascada sobre otros operadores de red.
- Personas formuladoras de políticas: asegurando una infraestructura nacional de Internet sólida y resiliente en apoyo de la agenda más amplia de la seguridad de Internet.

Un estudio independiente de 451 Research[1], encargado por Internet Society, descubrió que el enrutamiento, el secuestro y la interceptación del tráfico eran la principal preocupación de seguridad para las empresas. Los ataques de denegación de servicio distribuido (DDoS) y la suplantación de direcciones IP ocuparon el segundo lugar.

El 94% de las empresas dijeron que, en una situación competitiva, estarían dispuestas a pagar más por un proveedor que fuera participante de MANRS.

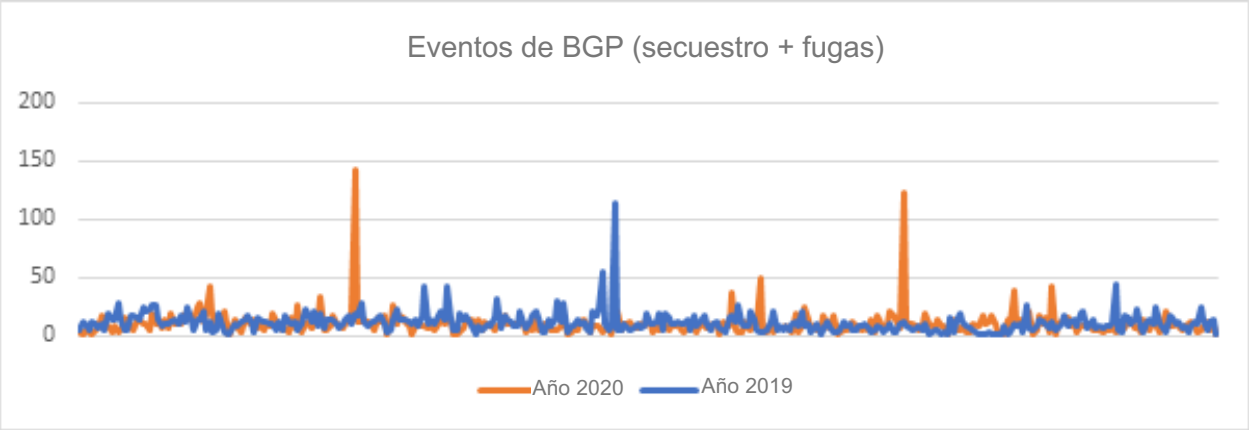
Esto destaca la importancia de la implementación de MANRS como indicador de las sólidas prácticas de seguridad de un operador de red.

Como responsable de la formulación de políticas, usted puede utilizar esto para fomentar la adopción de MANRS entre los proveedores de red al tiempo que mejora la conciencia sobre la seguridad del enrutamiento para las personas usuarias, incluidas las empresas.

[1] Informe de estudio del proyecto MANRS: https://www.manrs.org/wp-content/uploads/2017/10/MANRS-451-Study-Report.pdf

¿Por qué MANRS es importante para la seguridad de Internet?

En 2020, hubo un total de 3,873 incidentes de red importantes que involucraron ataques relacionados con Border Gateway Protocol (BGP). De estos, el 64% fueron secuestros y el resto fueron fugas de ruta.



En 2019, hubo 4,232 incidentes importantes en la red que involucraron a BGP, de los cuales:

- el 3.8% de todas las redes fueron afectadas por un incidente de enrutamiento
- el 2% de todas las redes fueron responsables de los 4,232 incidentes de seguridad de enrutamiento.

Estos incidentes pueden:

- causar estragos graves en la infraestructura;
- conllevar la caída del tráfico;
- permitir la inspección no autorizada del tráfico;
- utilizarse para realizar ataques de denegación de servicio (DoS).

En julio de 2020, hubo dos incidentes de enrutamiento importantes en el sistema de enrutamiento global BGP[2], que afectaron a más de 1,500 redes en todo el mundo. Esto destacó la necesidad de que los operadores de redes implementen buenas prácticas de seguridad de enrutamiento. Estos incidentes afectaron a los principales proveedores de la red de América del Norte, incluidos TWC, Rogers y Charter, entre otros[3].

La única forma eficaz de abordar las amenazas de seguridad de enrutamiento es mediante la acción colectiva global, ya que ninguna organización o grupo puede hacerlo solo. **Los gobiernos y las personas formuladoras de políticas pueden desempeñar roles clave en facilitar dicha acción colectiva.**

2. La gran fuga de ruta demuestra la necesidad de seguridad en el enrutamiento https://www.manrs.org/2020/07/big-route-leak-shows-need-for-routing-security/

3 .Otro incidente de Border Gateway Protocol afecta a TWC, Rogers, Charter y otros https://www.manrs.org/2020/07/another-bgp-incident-impacts-twc-rogers-charter-and-others/

¿Qué papel puede desempeñar como formulador de políticas?

1. **Evite las barreras reglamentarias:** ayude a mejorar los incentivos del mercado para mejorar la seguridad del enrutamiento evitando las barreras reglamentarias y facilitando la cooperación y la colaboración.

2. **Fomente las buenas prácticas:** fomente y facilite iniciativas de forma que preserve las fortalezas del sistema de enrutamiento global, incluida su resiliencia general, facilidad de uso, flexibilidad y escalabilidad.

3. **Promocionar pautas comunes:** se encuentra en una posición única para promover pautas comunes para los operadores de red, ayudar a facilitar las mejores prácticas de la industria para la seguridad del enrutamiento y promover su implementación.

4. **Incentivos de subvenciones:** cuando sea posible, habilite el proceso mediante incentivos como subvenciones y bonificaciones fiscales.

5. **Elimine las barreras legales:** ayude a identificar y eliminar las barreras legales en el intercambio de información y las respuestas a los incidentes de enrutamiento. Los operadores de redes e infraestructura y los investigadores de seguridad pueden preocuparse de que la divulgación de incidentes o amenazas de seguridad de enrutamiento puede ponerlos en peligro legal. Proporcionar salvaguardias para ellos puede ayudar a mitigar tales preocupaciones.

6. **Liderar con el ejemplo:** dado que los gobiernos suelen administrar grandes redes propias, pueden predicar con el ejemplo mejorando la confiabilidad y seguridad de la infraestructura de Internet utilizando las mejores prácticas de MANRS.

Dado el impacto significativo de los incidentes de enrutamiento en redes críticas, debemos dar una alta prioridad a la protección y mejora de nuestra infraestructura de red. Sin embargo, las investigaciones muestran una falta de comprensión general sobre el hecho de que medidas sencillas pueden reducir de manera dramática dichos incidentes.

Algunas medidas descritas anteriormente no son completamente nuevas y algunas organizaciones pueden estar trabajando para integrar dichas medidas en el futuro cercano. Para garantizar una infraestructura de red más saludable y sólida, debemos dar prioridad a las medidas destacadas en este documento, y respaldar su implementación con recursos adecuados.

- Obtenga más información sobre MANRS: manrs.org
- Lea sobre el trabajo de Internet Society: internetsociety.org