¿Cómo pueden mejorar las empresas la seguridad del enrutamiento global?

Información para directivos empresariales

Hoy en día, Internet juega un papel esencial en nuestras sociedades cada vez más digitales en todo el 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 que protejamos 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 Internet.

Cada año se producen miles de incidentes de enrutamiento de Internet que provocan daños económicos 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.**

Para contribuir a los esfuerzos para proteger Internet, las empresas deben trabajar con operadores de redes e infraestructura, agencias de protección de infraestructura crítica, entre otros, para garantizar que sus proveedores implementen las mejores prácticas de seguridad del enrutamiento y, al mismo tiempo, preserven 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 una iniciativa impulsada por la comunidad respaldada por Internet Society. MANRS proporciona un conjunto de mejores prácticas basadas en las normas existentes para que los operadores de red mejoren la seguridad del sistema global de enrutamiento de Internet.

Al elegir proveedores de servicios que cumplan con MANRS (y unirse a MANRS si usted opera una red), su empresa puede mejorar su seguridad y alentar a otros proveedores a mejorar su infraestructura.

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 estos 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 actores validar la información de enrutamiento a escala global.

Las dos primeras acciones (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 ocuparon el segundo lugar.

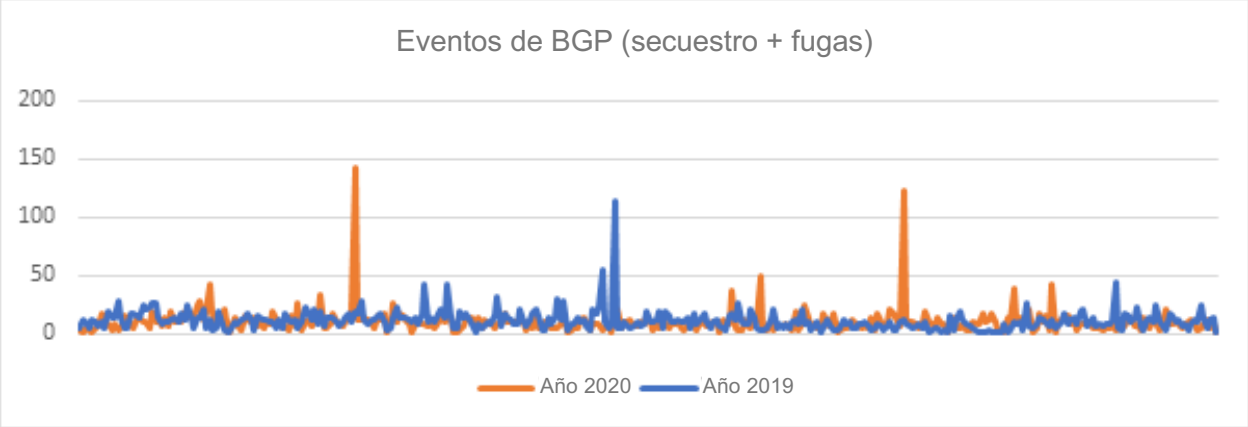
El 94% de las empresas dijeron que estaban dispuestas a pagar más por un proveedor que fuera participante de MANRS en una situación competitiva.

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

[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 las empresas?

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

- crear una tensión grave en la infraestructura;
- conllevar la caída del tráfico;
- permitir la inspección no autorizada del tráfico;
- ser utilizados para realizar ataques de denegación de servicio (DoS), que amenazan la continuidad comercial.

En julio de 2020, hubo dos incidentes de enrutamiento importantes en el sistema de enrutamiento global de BGP[2]. 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 en que su empresa puede abordar las amenazas de seguridad de enrutamiento es eligiendo proveedores de servicios que sigan un conjunto establecido de pautas, como MANRS. Al elegir proveedores que adopten estas medidas, puede impulsar el mercado para construir redes más resistentes que, a su vez, hacen que la infraestructura de red global sea más segura.

---

[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/

¿Cómo puede MANRS ayudar a su organización?

1. **Garantice la continuidad comercial y evite daños a la reputación:** Toda empresa debe saber si sus proveedores implementan las mejores prácticas de enrutamiento de Internet como parte de su programa de continuidad comercial. Las acciones de MANRS ofrecen a su empresa una forma eficaz de evitar contratiempos de seguridad de la red que pueden causar un daño significativo a la reputación de cualquier negocio.

2. **Califique a los proveedores o socios:** MANRS puede ayudar a los líderes de su empresa a elegir una red adecuada o un socio de operaciones en la nube sin tener que realizar un proceso de evaluación extenso o complejo. Varios proveedores clave ya cumplen con MANRS, lo que simplifica significativamente el proceso de auditoría de sus capacidades de seguridad.

3. **La seguridad como diferenciador:** si opera redes, implementar las acciones de MANRS permite que su empresa comunique a sus clientes que se toma en serio la seguridad de su infraestructura de red. Esto puede servir como un diferenciador fundamental para su organización.

4. **Resolución de incidentes de seguridad de la red:** la adopción de las acciones de MANRS en sus redes ayuda a su organización a mitigar los impactos inmediatos y severos de los incidentes de seguridad de la red. Si no se resuelven, estos pueden afectar su capacidad para operar y dañar la confianza del cliente en su negocio.

5. **Inteligencia de amenazas:** es posible que desee mejorar el conocimiento de la situación de su empresa y esté interesado en incorporar fuentes de inteligencia en sus operaciones. La información y los flujos de eventos que pueden generar las acciones de MANRS tendrán valor para su empresa.

6. **Una lista de verificación para auditar la solidez de la infraestructura:** las acciones destacadas por MANRS pueden servirle como una lista de verificación útil para garantizar la solidez de su infraestructura de TI interna. La incorporación de las acciones de MANRS en las operaciones internas de TI puede ayudarlo a aumentar la eficiencia operativa.

7. **Apoyo de la comunidad para los asuntos de seguridad:** unirse a la iniciativa MANRS le brinda a su empresa acceso a una comunidad más grande que se preocupa por la seguridad y aborda los problemas que la rodean. La comunidad también puede servir como una forma de identificar socios dentro del ecosistema con quienes unir fuerzas para crear una base más sólida para la seguridad.

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 las medidas sencillas pueden reducir de manera dramática dichos incidentes.

Algunas de las 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