¿Cómo pueden los ejecutivos de TI mejorar la seguridad del enrutamiento global?

Información para las personas que ocupan los cargos de Dirección de Información (CIO), Dirección de Tecnología (CTO) y Dirección de Seguridad de la Información (CISO)

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 la red 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.**

Como persona en una posición ejecutiva, usted es fundamental. Usted tiene un papel importante que desempeñar en la adopción de una postura de seguridad de red eficaz que, en última instancia, fortalezca y proteja a su empresa, así como a Internet.

¿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 ayudar a alentar a otros proveedores a mejorar su infraestructura.

MANRS define cuatro acciones simples y concretas:

- Filtrado de Border Gateway Protocol (BGP);
- Antisuplantación;

- Coordinación; y,
- Validación global.

Al implementar estas acciones, los operadores de redes pueden mejorar enormemente la seguridad y confiabilidad de Internet. Dos de los pasos son preventivos y ayudan a abordar las causas técnicas detrás de los incidentes de enrutamiento comunes. Los otros pasos aprovechan la información accesible a nivel mundial para ayudar a limitar el impacto de tales incidentes y disminuir la probabilidad 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 del enrutamiento.
- La competencia: al garantizar que los incidentes de seguridad del 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 ciberseguridad.

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.

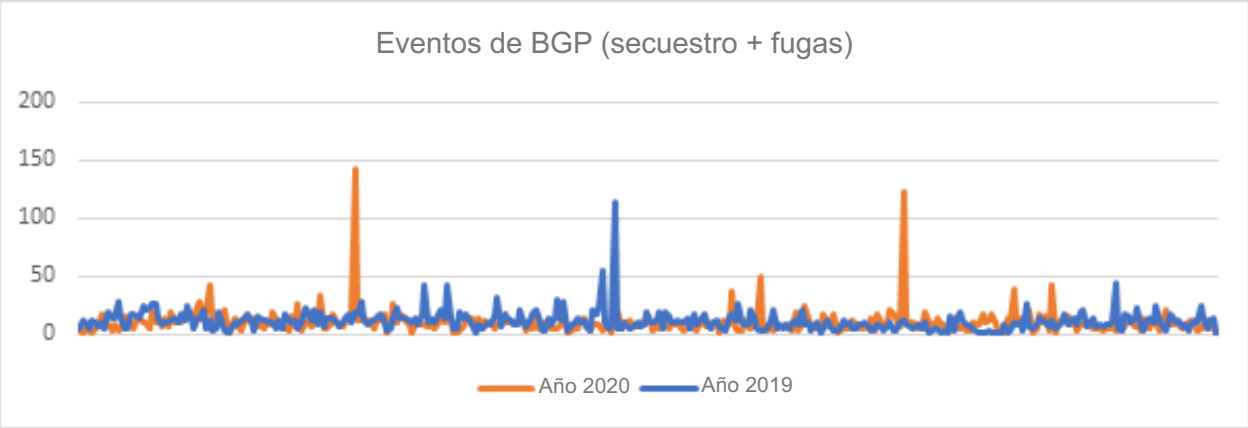
El 94% de las empresas dijeron que estaban dispuestas a pagar más por un proveedor que fuera participante de MANRS en una situación competitiva.

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 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:

- crear una tensión grave 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 del enrutamiento. Estos incidentes afectaron a los principales proveedores de la red de América del Norte, incluidos TWC, Rogers y Charter, entre otros[3].

Como líder en la compañía, puede ayudar a su empresa a abordar las amenazas de seguridad de enrutamiento de manera efectiva mediante la evaluación de sus proveedores de servicios de Internet (ISP), redes de entrega de contenido (CDN) y proveedores de alojamiento en la nube para asegurarse de que sigan las mejores prácticas de seguridad.

¿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. **La seguridad como ventaja competitiva:** la implementación de acciones de MANRS permite que su empresa comunique a los clientes que se toma en serio la seguridad de su infraestructura de red. Esto

puede servir como un diferenciador fundamental para su organización.

3. **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.

4. **Alineación de la seguridad de la infraestructura en todas las divisiones:** varios elementos de la infraestructura de TI de una empresa pueden tener sus propias prácticas de seguridad. La vulnerabilidad en cualquiera de ellos podría suponer un grave riesgo para su empresa. Los principios de MANRS pueden servir como una guía útil si está buscando alinear toda su infraestructura de red bajo estándares comunes.

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. Por lo tanto, 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:** reconoce la amenaza de los problemas de seguridad de la red para su empresa pero, sin las acciones MANRS implementadas, es posible que le falte una forma efectiva y eficiente de auditar la preparación de su red central. La lista de verificación de MANRS proporciona un medio sencillo para evaluar la solidez de la infraestructura de red central de su empresa.

7. **Acceso a una base de conocimientos avanzada:** MANRS le brinda acceso a una gran comunidad enfocada en abordar problemas de seguridad. Esto puede ayudar a su organización a construir una base más sólida para la seguridad a través de colaboraciones.

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 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