¿Cómo pueden los equipos de respuesta a incidentes de seguridad informática mejorar la seguridad del enrutamiento global?

Información para los Equipos de Respuesta ante Emergencias Informáticas (CSIRT, por sus siglas en inglés)

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.

Internet está formada por miles de redes interconectadas que ejecutan los protocolos TCP / IP (72,000 en junio de 2021). Estas redes están conectadas entre sí mediante el protocolo Border Gateway Protocol (BGP). BGP es el único protocolo de gateway disponible actualmente.

El problema con BGP es que fue diseñado para un entorno predominantemente académico. La seguridad no era una consideración importante, ya que se podía esperar que las redes participantes cooperaran para mantener la red en buen estado. Por lo tanto, BGP se basa completamente en la confianza no verificada entre redes.

Desafortunadamente, esto hace que el sistema de enrutamiento global de Internet sea intrínsecamente inseguro. Cada vez más, es objeto de ataques, ya sea por parte de delincuentes organizados que ven la oportunidad de robar datos y causar interrupciones, o debido a errores de configuración.

¿Qué tienen que ver los CSIRT con la seguridad del enrutamiento?

Como miembro de un equipo de respuesta a incidentes de seguridad informática (CSIRT), usted participa en el desarrollo de medidas de mitigación y concientización sobre la seguridad para sus usuarios finales. Sin embargo, la mayoría de los CSIRT no incluyen la seguridad del enrutamiento como parte de la seguridad de la infraestructura dentro de sus carteras de servicios. Esto es así a pesar de que el sistema de enrutamiento es un elemento clave de la infraestructura crítica nacional e internacional.

Si bien los CSIRT generalmente no administran redes, usted posee conocimientos especializados sobre ataques y amenazas, así como estrategias de mitigación y resolución. También es responsable de recomendar las mejores prácticas para proteger los sistemas, las redes y los datos y activos críticos, junto con otros mecanismos de prevención de incidentes.

En apoyo de la cartera de seguridad de Internet, como parte de un CSIRT, lo alentamos a trabajar con otros actores para mejorar la seguridad de enrutamiento global, a la vez que adopta una visión integral del ecosistema de seguridad de Internet. Aquí es donde entra MANRS.

¿Qué es MANRS?

Internet Society apoya las Normas Mutuamente Acordadas para la Seguridad del Enrutamiento (MANRS, por sus siglas en inglés). Es una comunidad de operadores de redes responsables, proveedores de contenido e IXP comprometidos con mejorar la seguridad y la resiliencia de Internet. Ofrece un conjunto de mejores prácticas basadas en las normas existentes para que los operadores de redes mejoren la seguridad del sistema global de enrutamiento de Internet.

Al elegir proveedores de servicios que cumplan con MANRS, las organizaciones pueden ayudar a mejorar su red y alentar a otros proveedores a mejorar su infraestructura.

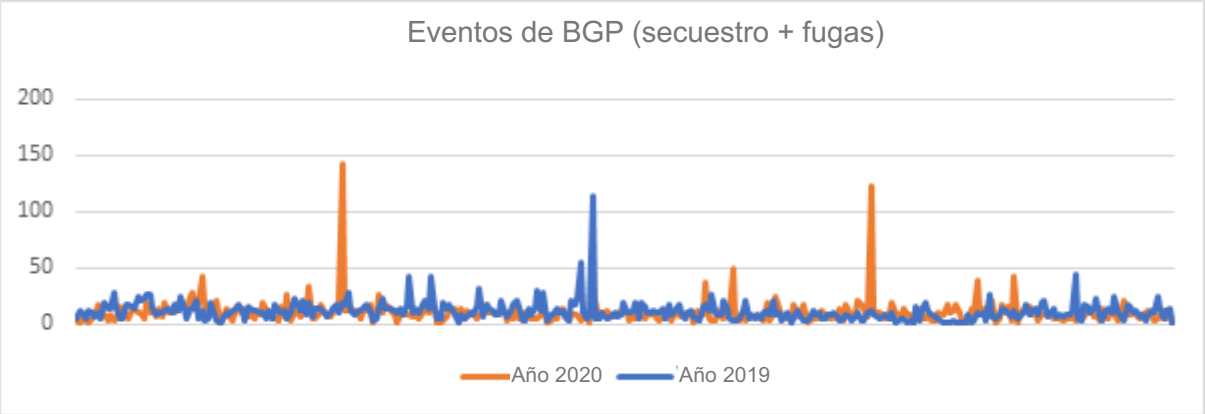
MANRS define cuatro acciones simples pero concretas que los operadores de red deben implementar para mejorar en gran medida la seguridad y confiabilidad de Internet. Entre estas se incluyen:

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 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.

¿Por qué es importante MANRS?

En 2020, hubo un total de 3,873 incidentes de red importantes que involucraron ataques relacionados con 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; y
- utilizarse para realizar ataques de denegación de servicio (DoS).

Los incidentes de enrutamiento causan problemas en el mundo real

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 red de América del Norte, incluidos TWC, Rogers y Charter, entre otros[3].

Aparte de estos casos bien conocidos, los incidentes de enrutamiento ocurren todos los días y la estabilidad y seguridad del sistema de enrutamiento de Internet corre un riesgo significativo.

Un estudio independiente de 451 Research, encargado por Internet Society,[1] 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 muestra que la implementación de MANRS es un buen indicador de las prácticas de seguridad sólidas de un operador de red. Sin embargo, esta investigación también mostró que existe una falta general de comprensión de que las medidas sencillas pueden reducir drásticamente dichos incidentes.

¿Cómo puede ayudar MANRS a los CSIRT?

Como parte de las iniciativas de desarrollo de capacidades y participación comunitaria de MANRS, nos gustaría apoyar a las comunidades CSIRT en las siguientes áreas:

- crear conciencia sobre los problemas de seguridad de enrutamiento dentro de sus comunidades;
- alentar a otros CSIRT a agregar el monitoreo de incidentes de seguridad de enrutamiento y el manejo de incidentes a sus carteras de servicios;
- alentar a los CSIRT a adoptar la herramienta de monitoreo del Observatorio MANRS para proporcionar conocimiento de la situación de la seguridad del enrutamiento;
- extender el alcance de la iniciativa MANRS dentro de las circunscripciones del CSIRT, así como en iniciativas nacionales de infraestructura crítica;
- realizar talleres prácticos de seguridad de enrutamiento o desarrollo conjunto de un plan de estudios de seguridad de enrutamiento en el contexto de la formación de instructores y/o programas de desarrollo de capacidades de análisis forense de redes; y
- agregar seguridad de enrutamiento a los programas de auditoría de seguridad de la red.

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

A su vez, los CSIRT pueden:

- ayudar a alentar a sus respectivas organizaciones o integrantes a tomar más en serio los asuntos de seguridad de enrutamiento;
- sensibilizar a los gobiernos sobre cómo los asuntos de seguridad del enrutamiento pueden afectar la infraestructura crítica; y
- fomentar la adopción de recomendaciones de seguridad de enrutamiento (como los estándares NIST).

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.

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