Normas mutuamente acordadas para la seguridad de las rutas (MANRS)

Introducción

La seguridad, en general, es un área difícil cuando se trata de incentivos. La seguridad de la infraestructura mundial de Internet, ya sea el DNS o el enrutamiento, conlleva retos adicionales: la utilidad de las medidas de seguridad depende de las acciones coordinadas de muchas otras partes.

A lo largo de la historia de Internet, la colaboración entre los participantes y la responsabilidad compartida por su buen funcionamiento han sido dos de los pilares que han sustentado el enorme crecimiento y éxito de Internet, así como su seguridad y resistencia. Las soluciones tecnológicas son un elemento esencial en este caso, pero la tecnología por sí sola no es suficiente. Para estimular mejoras visibles en esta esfera, es necesario un mayor cambio hacia la cultura de la responsabilidad colectiva.

El presente documento tiene por objeto captar este espíritu de colaboración y proporcionar orientación a los operadores de redes para abordar las cuestiones de seguridad y resistencia del sistema mundial de enrutamiento de la Internet. Otro objetivo importante es documentar el compromiso de los líderes de la industria para abordar estas cuestiones, lo que debería amplificar el impacto a medida que se unan más partidarios.

Objetivos

1. Sensibilizar y fomentar las acciones demostrando el compromiso del creciente grupo de partidarios
2. Promover la cultura de la responsabilidad colectiva para la resistencia y la seguridad del sistema de enrutamiento mundial de Internet
3. Demostrar la capacidad de la industria para abordar las cuestiones de resistencia y seguridad del sistema de enrutamiento mundial de Internet en el espíritu de la responsabilidad colectiva
4. Proporcionar un marco para que los proveedores de servicios de Internet comprendan mejor y ayuden a abordar las cuestiones relacionadas con la resistencia y la seguridad del sistema de encaminamiento mundial de la Internet

Alcance

Existen muchas recomendaciones diferentes para mejorar la seguridad y la resistencia del sistema de rutas entre dominios. Algunos de los consejos pueden parecer incluso algo contradictorios y a menudo la decisión clave puede consistir en comprender qué es lo más importante o apropiado para una red determinada, teniendo en cuenta su tamaño y recursos, el número de conexiones externas, los clientes y usuarios finales con que cuenta, el tamaño y la experiencia de su personal, etc.

Las medidas previstas y avanzadas que figuran a continuación subrayan un conjunto de recomendaciones que son definitivamente valiosas para la seguridad y la capacidad de recuperación generales del sistema de encaminamiento mundial, así como para el propio operador de la red. Se refieren a tres clases principales de problemas:

- Problemas relacionados con la información de ruta incorrecta;
- Problemas relacionados con el tráfico con direcciones IP de fuentes falsas; y
- Problemas relacionados con la coordinación y la colaboración entre los operadores de la red.

Las acciones previstas definen un "paquete" mínimo, un conjunto de recomendaciones que deben ser definitivamente implementadas por los operadores que apoyan este documento del MANRS. Este paquete no es exhaustivo y se espera que muchos operadores de redes estén implementando medidas y controles aún más fuertes ya, o planeen hacerlo en el futuro. Las Acciones Avanzadas que figuran más adelante en este documento amplían aún más el paquete mínimo.

Somos conscientes del hecho de que cualquier acción en particular no es una solución integral a los problemas señalados. Pero cada una es un pequeño paso que, si se multiplica por un gran número de partidarios, puede convertirse en una mejora significativa de la resistencia del sistema de enrutamiento mundial de Internet. Por consiguiente, la selección de las medidas se basó en una evaluación del equilibrio entre los pequeños costos individuales incrementales y el posible beneficio común.

Definiciones

Para articular los detalles de las medidas previstas y las medidas avanzadas, es necesario definir explícitamente una serie de términos, para relacionarlos con su uso general en la industria de la Internet.

- Infraestructura - Las redes internas del operador, a las que se debe poder llegar a través de Internet.
- Usuario final - Redes dentro del dominio administrativo y de enrutamiento de un operador.
- Red de compañeros - Una red externa con la que se intercambia tráfico relacionado tanto con su respectiva infraestructura, como con las redes

de los clientes.

- Red de tránsito - Una red externa a la que se envía el tráfico relacionado con su infraestructura y redes de clientes, pero de la que se recibe el tráfico de Internet en general.
- Red de clientes - Una red externa para la cual un operador proporciona servicios de tránsito.
- Single Homed ĸ Un único y sencillo enlace entre redes, o la conexión de un usuario final a la infraestructura. Esto representa un camino único por el que el tráfico puede fluir dentro de las redes o entre ellas.
- Multi Homed ĸ Múltiples caminos entre redes (incluso múltiples redes), o conexiones entre un usuario final y la infraestructura; esto puede crear múltiples caminos a través de la infraestructura y de Internet por los que el tráfico puede transitar.

Principios

1. La organización (proveedor de servicios de Internet/operador de la red) reconoce el carácter interdependiente del sistema de encaminamiento mundial y su propia función de contribuir a una Internet segura y resistente.
2. La organización integra las mejores prácticas actuales relacionadas con la seguridad y la resistencia del encaminamiento en sus procesos de gestión de la red, de conformidad con las Medidas.
3. La organización se ha comprometido a prevenir, detectar y mitigar los incidentes de enrutamiento mediante la colaboración y la coordinación con sus homólogos y otros proveedores de servicios de Internet, de conformidad con las Medidas.
4. La organización alienta a sus clientes y pares a adoptar estos Principios y Acciones.

Acciones esperadas

1. Evitar la propagación de información de ruta incorrecta.

- El operador de la red define una política de enrutamiento clara e implementa un sistema que asegura la corrección de sus propios anuncios y los anuncios de sus clientes a las redes adyacentes con el prefijo y la granularidad ASKpath.
- El operador de la red es capaz de comunicar a sus redes adyacentes qué anuncios son correctos.
- El operador de red aplica la debida diligencia al comprobar la corrección de los anuncios de su cliente, específicamente que el cliente tiene legítimamente el ASN y el espacio de dirección que anuncia.

2. Prevenir el tráfico con direcciones IP de origen falsas.

- El operador de la red implementa un sistema que permite la validación de la dirección de origen para al menos redes de clientes de talón de un solo domicilio, sus propios usuarios finales y su infraestructura. El operador de la red implementa el filtro antiK spoofing para evitar que los paquetes con una

dirección IP de origen incorrecta entren y salgan de la red.

3. **Facilitar la comunicación y la coordinación operativa mundial entre los operadores de la red.**

    - El operador de la red mantiene información de contacto actualizada y accesible a nivel mundial.

Acciones avanzadas

- 4. 4. Facilitar la validación de la información de ruta a escala mundial.
- El operador de la red ha documentado públicamente la política de enrutamiento, los ASN y los prefijos que se pretenden anunciar a partes externas.

Elaboración y referencias

Acción 1. Evitar la propagación de información de ruta incorrecta.

- El operador de la red define una política de enrutamiento clara e implementa un sistema que asegura la corrección de sus propios anuncios y los anuncios de sus clientes a las redes adyacentes con el prefijo y la granularidad del camino AS.
- El operador de la red es capaz de comunicar a sus redes adyacentes qué anuncios son correctos.
- El operador de red aplica la debida diligencia al comprobar la corrección de los anuncios de su cliente, específicamente que el cliente tiene legítimamente el ASN y el espacio de dirección que anuncia.

Discusión: Lo más importante es asegurar los anuncios de enrutamiento de entrada, en particular de las redes de clientes, mediante el uso de filtros *explícitos de* nivel de prefijo o mecanismos equivalentes. En segundo lugar, se podrían utilizar filtros de ruta AS para exigir que la red del cliente sea explícita acerca de qué sistemas autónomos (AS) se encuentran a continuación de ese cliente. Alternativamente, los filtros AS-path que bloquean los anuncios de los clientes de los A-es con los que el proveedor tiene una relación libre de acuerdos pueden prevenir algunos tipos de "fugas" de enrutamiento. El filtrado de los anuncios BGP de los clientes por los filtros AS-path por sí solo no es *suficiente* para prevenir problemas catastróficos de enrutamiento a nivel sistémico.

Referencias:

"Servicios y procedimientos de seguridad recomendados para los proveedores de servicios de Internet", Sección Infraestructura de la red, http://www.rfcKeditor.org/bcp/bcp46.txt

"Operaciones y seguridad de BGP", http://tools.ietf.org/html/draftKietfKopsecKbgpKsecurity

Seguridad del protocolo de la puerta fronteriza, NIST: Publicación especial SP 800K54, http://csrc.nist.gov/publications/nistpubs/800K54/SP800K54.pdf

"Requisitos de seguridad operacional para la infraestructura de la red IP de los grandes proveedores de servicios de Internet (ISP)", http://tools.ietf.org/html/rfc3871

"Using RPSL in Practice", http://tools.ietf.org/html/rfc2650

"Using the RIPE Database as an Internet Routing Registry", https://labs.ripe.net/Members/denis/usingKtheKripeKdatabaseKasKanKinternetKroutingKregistry

Mejores prácticas de seguridad de BGP, Informe final del GT4 del CSRIC III de la FCC, http://transition.fcc.gov/bureaus/pshs/advisory/csric3/CSRIC_III_WG4_Report_March_%202013.pdf

Acción 2. Evitar el tráfico con direcciones IP de origen falsas.

- El operador de la red implementa un sistema que permite la validación de la dirección de la fuente para, al menos, las redes de clientes de un solo domicilio, sus propios usuarios finales y la infraestructura. El operador de la red implementa un filtro anti-spoofing para evitar que los paquetes con una dirección IP de origen incorrecta entren y salgan de la red.
- Discusión: Los enfoques comunes de este problema han implicado características de software como la validación de la dirección de origen (SAV) en redes de cable-módem o la validación estricta de uRPF (unicast Reverse-Path Forwarding) en redes de enrutadores. Estos métodos pueden facilitar los gastos generales de administración en los casos en que el enrutamiento y la topología son menos relativamente dinámicos. Otro enfoque podría consistir en utilizar la información del filtro de prefijos de entrada para crear un filtro de paquetes, que permitiría sólo los paquetes con direcciones IP de origen para los que la red podría anunciar legítimamente la accesibilidad.

Referencias:

"Filtro de entrada a la red": Defating Denial of Service Attacks which employ IP Source Address Spoofing", http://tools.ietf.org/html/bcp38

"Filtrado de entrada para redes multihomed", http://tools.ietf.org/html/bcp84

"Asegurando el borde", http://www.icann.org/committees/security/sac004.txt

"RIPE AntiKSpoofing Task Force HOWKTO", http://www.ripe.net/ripe/docs/ripeK 431

Mejores prácticas de seguridad de BGP, Informe final del GT4 del CSRIC III de la FCC, http://transition.fcc.gov/bureaus/pshs/advisory/csric3/CSRIC_III_WG4_Report_March_%202013.pdf

Acción 3. Facilitar la comunicación y la coordinación operativa mundial entre los operadores de redes.

- El operador de la red mantiene información de contacto actualizada y accesible a nivel mundial.

Discusión: Los lugares comunes para mantener esa información son PeeringDB, las bases de datos whois de los RIR y los grandes IRR como RADB y RIPE. Un operador de red debería registrar y mantener información de contacto 24 horas al día, 7 días a la semana, en al menos una de estas bases de datos. Esta información de contacto debería incluir la información del punto de contacto actual del operador para el NOC del AS, todos los netblocks y los nombres de dominio. Se alienta a los operadores a que documenten sus políticas de enrutamiento de la red en una TIR. También se agradece información adicional, como por ejemplo, una URL de espejo en el campo apropiado en su registro PeeringDB.

Referencias:

"Uso de la RPSL en la práctica", http://tools.ietf.org/html/rfc2650

Peering DB, https://www.peeringdb.com RADB,

http://www.radb.net/

Acción 4. Facilitar la validación de la información de ruta a escala mundial.

- El operador de la red ha documentado públicamente la política de enrutamiento, los ASN y los prefijos que se pretenden anunciar a partes externas.

Discusión: Para facilitar la validación de la información de encaminamiento por otras redes a escala mundial, es necesario disponer de información sobre la política de encaminamiento, las notas de ruta y los prefijos que se pretende anunciar a partes externas.

Una de las formas de hacer pública la política es documentándola mediante el uso de la RPSL en uno de los Registros de Enrutamiento de Internet (IRR) reflejados por el RADB (por ejemplo, RIPE, ARIN, RADB, etc.). En este caso, los operadores deben registrar y mantener como mínimo uno (o más) objetos IRR "as-set" que contengan una lista de ASN destinados a ser anunciados a partes externas, y que podrían ser utilizados por herramientas automáticas para generar prefijos-filtros. Los operadores también deben mantener su información en la TIR para asegurarse de que esté actualizada.

Otro medio más seguro para facilitar la validación a escala mundial es el sistema RPKI. Los operadores podrían obtener certificados RPKI para sus propios prefijos de los RIR que les asignaron esos prefijos, y publicar y mantener los ROA correspondientes a los prefijos que anuncian.

Los operadores deben animar a los operadores de sus redes de clientes a que también lo hagan. Esto permitirá a otras redes validar los anuncios a escala mundial.

Referencias:

"Using RPSL in Practice", http://tools.ietf.org/html/rfc2650

"Using the RIPE Database as an Internet Routing Registry", https://labs.ripe.net/Members/denis/usingKtheKripeKdatabaseKasKanKinternetKroutingKregistry

"Operación de validación de origen basada en la infraestructura de clave pública de recursos (RPKI)", http://www.rfcKeditor.org/bcp/bcp185.txt