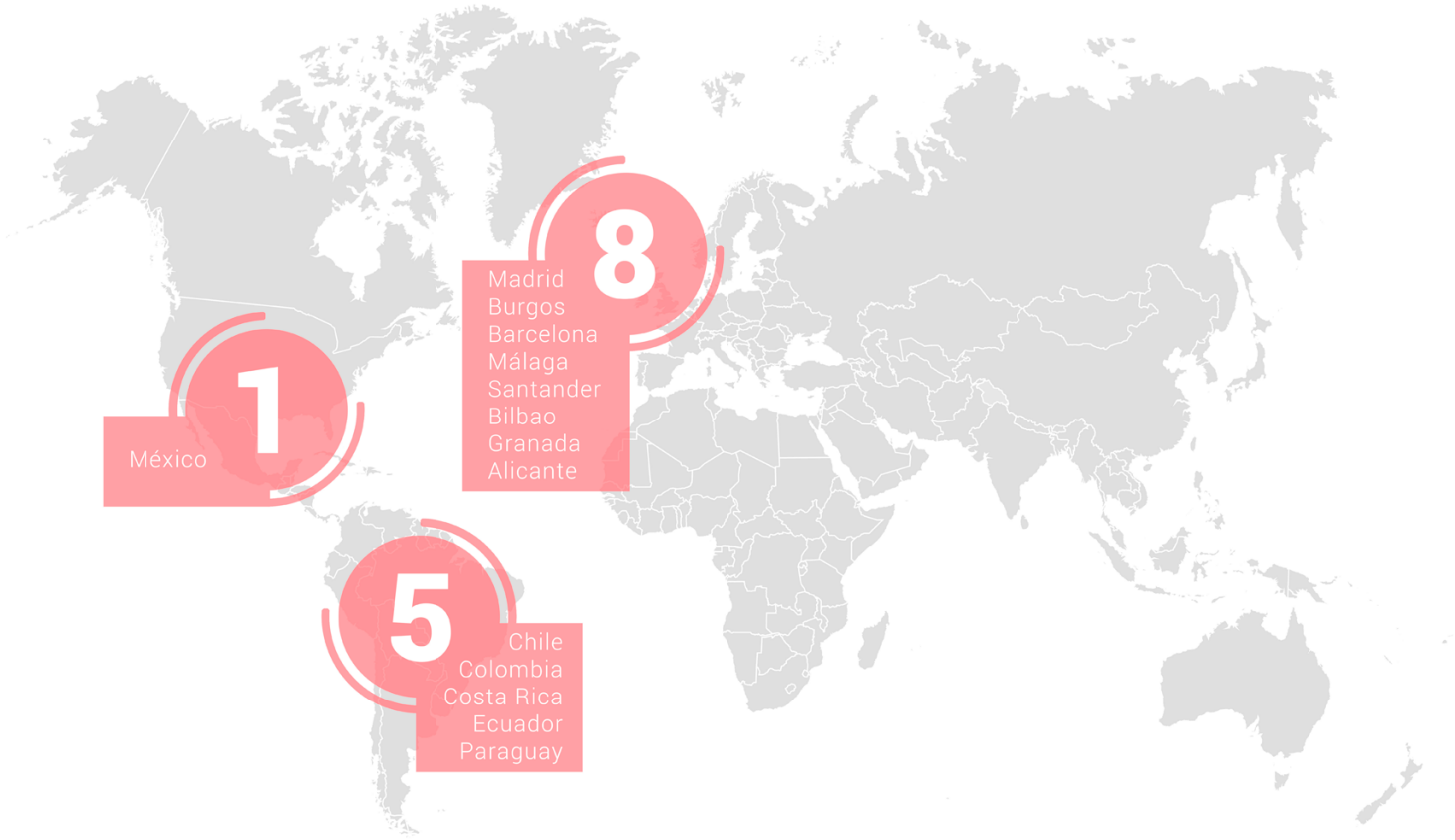
GrupoACMS
CONSULTORES

GRUPO ACMS Consultores

7 consejos sencillos de protección en Internet



AENOR
ER
Empresa Registrada
ISO 9001

(ER-0772/2013)

Alcance ISO 9001

Diseño, desarrollo, implantación, formación y mantenimiento de sistemas de gestión de la calidad, medioambiental, de la prevención de riesgos laborales, protección de datos, seguridad alimentaria y de la calidad y competencia técnica en laboratorios clínicos.

Alcance ISO 27001

Los sistemas de información que dan soporte a las actividades de diseño, desarrollo, implantación, formación y mantenimiento de sistemas de gestión y el diseño, desarrollo y comercialización de software de sistemas de gestión de acuerdo con la declaración de aplicabilidad vigente.

AENOR
ER
Seguridad Información
ISO/IEC 27001

(SI-0021/2020)

Publicada el 14/06/2019

7 consejos sencillos de protección en Internet

- Los secuestros de BGP (Border Gateway Protocol), la piratería del mapa de ruta de Internet, continúan sucediendo. A pesar de años de advertencias por parte de expertos en seguridad.

- Esto supone un peligro para la seguridad nacional, la privacidad de los ciudadanos y la resistencia de Internet, tanto en Europa como a nivel mundial.

- El año pasado ENISA encuestó a una gama de proveedores grandes y pequeños en toda la UE, confirmando que los secuestros de BGP también son un problema en la UE: el 44% de los encuestados dijo que el impacto de los incidentes de BGP es alto, que afecta a un gran número de usuarios y que dura muchos Horas, y el 93% dice que necesita una solución urgente.

- El protocolo Border Gateway, es como un mapa de ruta dinámico de Internet, utilizado por los operadores de red para encontrar la mejor ruta de una computadora a otra, en todo el mundo. Pero tiene 25 años y no fue diseñado pensando en la seguridad. La buena noticia es que existen soluciones, pero desafortunadamente no todos los operadores de red están implementando.

Casos recientes

En 2008, un operador en Pakistán, famoso por BGP, secuestró todo el tráfico de Youtube del mundo, por accidente. Aquí hay tres ejemplos muy recientes de casos de alto perfil y alto impacto:

- En 2018, el tráfico de Google, desde personas del oeste de los EE. UU., Fue secuestrado por BPG para viajar a través de Rusia a China. Al parecer, esto se hizo intencionalmente y con fines de espionaje.

- En 2017, el tráfico de Internet a 80 sitios web de alto perfil (Google, Apple, Facebook, Microsoft, etc.) fue secuestrado por BGP por una red rusa (anteriormente inactiva).

- En 2018, el tráfico de la nube de Amazon de varios clientes de Ethereum cryptocoin fue secuestrado por BGP. El objetivo era robar miles de euros en criptomoneda.

Muchos ataques de BGP no hacen titulares de noticias. Y existe el riesgo de que los atacantes utilicen las vulnerabilidades de BGP no solo para el espionaje o el crimen financiero, sino para deshabilitar completamente las conexiones de Internet, para interrumpir a la sociedad.

¿Cuáles son los riesgos?

Los ataques de BGP se usan para diferentes propósitos, desde delitos financieros dirigidos a unos pocos usuarios por robo de monedas criptográficas, hasta espionaje a gran escala e incluso se pueden usar para causar paralizantes cortes de Internet. Nuestra dependencia de Internet, un mayor uso y un aumento en la cantidad y la sofisticación de los ataques cibernéticos, significa que los riesgos de dejar el BGP sin garantía son muy altos.

Recomendaciones de ENISA para la seguridad de BGP.

En el seguimiento de la encuesta de seguridad BGP de 2018, ENISA discutió con expertos en el sector de las telecomunicaciones en los últimos meses, para compilar una lista corta de medidas de seguridad básicas:

- Monitoreo y detección: controle las rutas utilizadas por su tráfico de Internet para detectar anomalías, no solo para garantizar la capacidad de recuperación sino también para la privacidad y seguridad de los suscriptores;

- Coordinación: Es crucial coordinar con pares, publicando políticas de ruta y participando en bases de datos de peering;

- Filtrado de prefijos: es importante filtrar los prefijos que nunca deben anunciarse o reenviarse en su red, tanto en el tráfico de entrada como en el de salida de la red;

- Filtrado de ruta: es importante filtrar los atributos de ruta de BGP AS para los elementos que no deberían estar permitidos en los anuncios de ruta de BGP hacia dentro o fuera de su red;

- Filtrado de Bogon: es importante filtrar los prefijos falsos (también llamados bogones), ya que estos prefijos nunca deben aparecer en los anuncios de BGP;

- Tiempo de vida segura (GTSM): es importante implementar la seguridad TTL, lo que hace que sea más difícil atacar las sesiones BGP;

- Infraestructura de clave pública de recursos (RPKI): es importante implementar RPKI y firmar digitalmente los anuncios de ruta para que los compañeros puedan verificar que los anuncios sean auténticos y estén autorizados.

Estos 7 pasos son relativamente simples y efectivos para apuntalar BGP.

Los proveedores de comunicaciones electrónicas, pero también todas las demás organizaciones que administran el llamado Sistema Autónomo (que implementa BGP) deben adoptar e implementar estas 7 medidas como mínimo.

Información histórica

- BGP tiene 25 años y no fue diseñado teniendo en cuenta la seguridad, es decir, confía intrínsecamente en que cada operador de red tenga buenas intenciones y no cometa errores. Cada operador puede simplemente anunciar que tiene una ruta rápida y corta. Las implementaciones ingenuas de BGP simplemente aceptan tales anuncios. Los secuestros de BGP, tanto intencionales como no intencionados, han estado ocurriendo durante años. Hay varios esfuerzos de la industria que abogan por una seguridad adicional, pero la implementación no se produce de forma generalizada y los ataques cibernéticos dirigidos a las vulnerabilidades de BGP continúan ocurriendo.

- Este trabajo sobre seguridad de BGP se realizó en el contexto del artículo 13a de la directiva marco, que solicita a los Estados miembros de la UE que se aseguren de que los proveedores tomen las medidas de seguridad adecuadas para proteger sus redes y servicios.

- En los últimos 10 años, ENISA colaboró estrechamente con los Estados miembros de la UE y expertos de las autoridades nacionales de reglamentación de las telecomunicaciones (ANR) que supervisan esta parte de la legislación de la UE, en el marco del Grupo de Expertos del Artículo 13a de ENISA. El grupo de expertos del Artículo 13a de ENISA se reúne 3 veces al año para discutir e intercambiar información sobre seguridad en el sector de las comunicaciones electrónicas.

Nos definimos como una compañía consultora independiente cuyo objetivo fundamental es suministrar servicios de consultoría en las áreas de Gestión empresarial, que representen para el cliente una solución excelente, que satisfaga sus necesidades explícitas o implícitas, tenga en cuenta las regulaciones y normas aplicables, y cumpla los objetivos de plazo y coste establecidos.

Madrid

C/ Campezo 3, nave 5 28022 Madrid

Tfno.: (+34) 91 375 06 80

Burgos

Centro de Empresas, 73 09007 Burgos

Tfno.: (+34) 947 041 645

Barcelona

C/ Plaça Universitat 3 08007 Barcelona

Tfno.: (+34) 93 013 19 49

Málaga

C/ Alejandro Dumas 17 29004 Málaga

Tfno.: (+34) 95 113 69 04

México

José González Varela 15 14700 Tlalpan

Tfno.: (+52) 5513 39 96 22

www.grupoacms.com
informacion@grupoacms.com