12/04/2013

EPR05/2013

www.enisa.europa.eu

Agencia europea ENISA: los proveedores de servicios de Internet no aplican filtros contra los grandes ciberataques.

En su análisis de un reciente ciberataque masivo, ENISA, la agencia de ciberseguridad de la UE, señala que los proveedores de servicios de Internet (PSI) no han aplicado medidas de seguridad conocidas y accesibles desde hace más de una década. Este error es uno de los principales factores que explican la incapacidad de contrarrestar los ciberataques más importantes, según subraya la Agencia en su nota informativa «¿Los recientes ciberataques pueden realmente amenazar la disponibilidad de Internet?».

Esta nota informativa se centra en el ciberataque a gran escala que tuvo lugar el pasado mes de marzo contra la organización sin ánimo de lucro Spamhaus, con sede en Ginebra y Londres. Esta agresión digital provocó retrasos sensibles para los usuarios de Internet, principalmente en el Reino Unido, Alemania y otras partes de Europa occidental. Según los medios en línea, el ataque contra Spamhaus, que empezó el día 16 de marzo, fue el mayor ataque de denegación de servicio distribuido (DDoS, por sus siglas en inglés) de la historia de Internet. Los ataques DDoS "sobrecargan" la capacidad de un sitio web para gestionar el tráfico entrante. El ataque contra Spamhaus duró más de una semana. En su fase final, la enorme cantidad de tráfico generado causó problemas en el London Internet Exchange.

ENISA subraya que la técnica empleada en el ataque DDoS no supone ninguna novedad. Aún así, sigue habiendo muchos proveedores de servicios de red que no utilizan el conjunto de recomendaciones conocido como Mejores Prácticas Actuales 38 (BCP38, por sus siglas en inglés), disponible desde hace casi 13 años. Un conjunto de recomendaciones parecido para operadores de servidores DNS (BCP140, publicado en 2008) hubiera reducido el número de servidores usados de forma indebida para ataques de amplificación DNS. Si todos los operadores hubieran aplicado estas recomendaciones, el filtrado del tráfico habría bloqueado dichos ataques.

Según ENISA, este ataque nos ha permitido aprender varias cosas:

- La envergadura de los ataques es cada vez mayor. El ataque de marzo de 2013 contra Spamhaus alcanzó un volumen superior a los 300 Gigabits de datos por segundo, mientras que el mayor ataque DDoS observado en 2012 fue de 100 Gigabits de datos por segundo.
- El volumen es importante. Con ataques de este volumen, incluso los puntos de intercambio de Internet comerciales, que normalmente disponen de una infraestructura de alta capacidad, pueden verse comprometidos.

La Agencia ha emitido tres recomendaciones técnicas:

- Los operadores de servicios competentes deberían aplicar las recomendaciones BCP38.
- Los operadores de servidores DNS deberían comprobar si sus servidores pueden ser usados de forma indebida, y aplicar las recomendaciones BCP140.
- Los operadores de puntos de intercambio de Internet deberían asegurarse de que cuentan con la protección necesaria contra ataques directos.

El profesor Udo Helmbrecht, Director Ejecutivo de ENISA, afirmó: "*Los operadores de red que aún no hayan aplicado el BCP38 y el BCP140 deberían pensar en hacerlo cuanto antes, si no quieren que se vean afectados sus clientes y, por consiguiente, su reputación. La prevención es fundamental para luchar eficazmente contra los ciberataques. Por ello, valoramos muy positivamente la Estrategia de Ciberseguridad de la UE, que propone reforzar el papel de ENISA, dotándola de los recursos necesarios para ayudar a proteger la economía y la sociedad digital europeas*".

Nota informativa de ENISA completa
Contexto: la **Estrategia de Ciberseguridad** de la UE
Entrevistas: Ulf Bergstrom, portavoz, press@enisa.europa.eu, móvil: +30 6948 460.143, o Dr. Louis Marinos, louis.marinos@enisa.europa.eu

Traducción. La única versión oficial es la ingleesa.
www.enisa.europa.eu