08/01/2013

EPR01/2013
www.enisa.europa.eu

Nuevo informe sobre las principales tendencias en el primer panorama de ciberamenazas elaborado por la agencia ENISA de la UE

ENISA, la agencia de ciberseguridad de la UE, ha publicado el primer y más completo análisis del panorama de ciberamenazas de 2012, donde se recogen más de 120 informes de amenazas. En el informe se identifican y enumeran las principales, así como sus tendencias, y se concluye que los "drive-by exploits" se han convertido en la amenaza número uno en la web.

El informe "Panorama de amenazas" de ENISA recoge 120 informes recientes procedentes de la industria de la seguridad, redes de excelencia, organismos de normalización y otros terceros independientes entre 2011 y 2012, lo que lo convierte en la síntesis más exhaustiva actualmente disponible a nivel mundial. El informe proporciona una visión de conjunto independiente de las amenazas y fuentes de amenaza observadas, junto a las que actualmente son las más importantes, así como las tendencias emergentes en este ámbito. Además, el informe "Panorama de amenazas" se dedica a analizar al ciberenemigo, y se identifican las diez (de un total de dieciséis) principales amenazas en áreas de tecnología emergentes, junto a un listado de las mismas. Las áreas consideradas han sido informática móvil, medios sociales, infraestructuras críticas, infraestructuras de confianza, informática en la nube y "big data". Las diez principales amenazas identificadas son:

1. "Drive-by exploits" (inyecciones de código malicioso para aprovecharse de vulnerabilidades en navegadores web)
2. Gusanos/troyanos
3. Ataques de inyección de código
4. "Exploit kits" (paquetes de software listos para usar, con los que se automatiza el cibercrimen)
5. "Botnets" (equipos zombis controlados de forma remota)
6. Ataques (distribuidos) de denegación de servicio (DDoS/Dos)
7. "Phishing" (correos y sitios web fraudulentos)
8. Vulneración de información confidencial (violaciones de datos)
9. "Rogueware"/"scareware"
10. Correo basura

Por último, la agencia propone varias conclusiones a la industria y grupos interesados sobre cómo combatir de forma más efectiva ciberamenazas a negocios, población y economía digital en general:

- Usar una terminología unificada en los informes de amenazas.
- Tener en cuenta la perspectiva del usuario final.
- Crear casos de uso para escenarios de amenazas.
- Reunir datos de seguridad de las incidencias, incluidos el punto de inicio y el objetivo del ataque.

- Modificar los controles de seguridad para adaptarlos a las tendencias de amenazas emergentes.
- Reunir y desarrollar mejores pruebas sobre vectores de ataque (métodos) para comprender las dinámicas de los ataques.
- Reunir y desarrollar mejores pruebas sobre el impacto logrado por los atacantes.
- Reunir y mantener información de mayor calidad sobre fuentes de amenazas.

El director ejecutivo de ENISA, el profesor Udo Helmbrecht, afirmó:

"Me enorgullece que la Agencia asuma esta importante tarea para lograr una mejor comprensión de las actuales ciberamenazas. Se trata del primer y más completo análisis de ciberamenazas disponible hasta la fecha y de un punto de referencia para todos los responsables de políticas de ciberseguridad, así como partes interesadas".

Para el **informe** completo, con un listado detallado de todas las amenazas y conclusiones detalladas.

Para entrevistas: Graeme Cooper, director de asuntos públicos, móvil: +30 6951 782 268, o Ulf Bergstrom, portavoz, + 30 6948 460 143, press@enisa.europa.eu o Dr. Louis Marinos, louis.marinos@enisa.europa.eu

.

www.enisa.europa.eu