Nueva guía de buenas prácticas de ENISA sobre la revelación de vulnerabilidades

ENISA ha publicado una guía de buenas prácticas sobre la revelación de vulnerabilidades, con el objetivo de proporcionar una visión general de los desafíos a los que se enfrentan los investigadores en seguridad, los proveedores y otras partes interesadas implicadas en la revelación vulnerabilidades de software y hardware. El estudio permite entrever el complejo panorama relativo a la revelación de vulnerabilidades. Para ello realiza un balance de la situación actual e identifica retos y buenas prácticas, además de proponer recomendaciones concretas de mejora.

El núcleo del informe describe los conceptos principales sobre la revelación de vulnerabilidades junto con algunas cifras relativas a las vulnerabilidades que han sido reveladas en los últimos trece (13) años. A continuación se definen los actores clave implicados en el proceso de divulgación de vulnerabilidades y sus roles, y se exponen cuatro (4) casos de vulnerabilidades reveladas.

El *Prof. Udo Helmbrecht*, *Director Ejecutivo de ENISA, ha comentado: «Hoy en día la revelación de una vulnerabilidad implica una gran cantidad de complejas interdependencias que solo pueden abordarse de forma coordinada por las partes implicadas en el proceso». Este estudio es el primer intento de proporcionar una guía de referencia sobre el tema de la revelación de vulnerabilidades. ENISA acoge con satisfacción la oportunidad de seguir trabajando en esta área mediante la promoción de buenas prácticas, una mayor concienciación, la investigación y el desarrollo en este complejo campo.*

Las lagunas más comunes en la revelación de vulnerabilidades están relacionadas con implicaciones legales, el desconocimiento entre las partes interesadas y los diferentes niveles de madurez entre proveedores y entre investigadores. Las principales recomendaciones de mejora incluyen:

• La comunidad debe facilitar que mejore la madurez del proveedor.

• Internacionalización a través del aprendizaje de políticas, lo que implica que Internet necesita un enfoque más transnacional respecto a la revelación de vulnerabilidades; se pueden considerar también historias de éxito.

• Introducción de una tercera parte neutral o fortalecimiento de los centros de coordinación existentes.

• Los responsables políticos europeos y los Estados miembros deben mejorar el marco legal relativo a la revelación.

• Los proveedores deben facilitar la creación de confianza, transparencia y apertura.

• ENISA podría actuar y ofrecer asesoramiento para mejorar el panorama de la revelación de vulnerabilidades a la comunidad y la Comisión Europea.

Además, el informe ofrece una 'plantilla de política de revelación de vulnerabilidades' que proporciona las medidas procesales y la planificación temporal que la circunscripción puede seguir con el fin de implementar una política de divulgación de vulnerabilidades.

La conclusión general es que, a pesar de que hay muchos aspectos positivos en esta área, todavía hay margen de mejora, que se puede concretar en la creación de un panorama jurídico apropiado y en la generación de más

confianza y transparencia entre las partes implicadas.

Para acceder al informe completo
Para obtener información técnica: Cosmin Ciobanu, experto en NIS, **correo electrónico:** Cosmin.Ciobanu@enisa.europa.eu, **Tel:** +30 2814 409663
Para entrevistas y consultas de los medios por favor póngase en contacto con **press@enisa.europa.eu** , **Tel.** +30 2814 409576