La ciberseguridad según Winnie the Pooh: un nuevo informe de la agencia de la UE ENISA sobre trampas digitales, o honeypots ("tarros de miel"), para detectar ciberataques

ENISA, la agencia de ciberseguridad de la EU, ha publicado un estudio en detalle de treinta trampas digitales diferentes, conocidas como *honeypots* ("tarros de miel"), que pueden utilizar los Equipos de Respuesta ante Emergencias Informáticas (CERT, del inglés Computer Emergency Response Team) para la detección preventiva de ciberataques. El estudio descubre barreras para la comprensión de los conceptos básicos de los *honeypots* y ofrece recomendaciones acerca de cuál utilizar.

El creciente número de ciberataques complejos hace que los CERT necesiten una mayor capacidad para alertar de estos de forma precoz. Los *honeypots* son, simplificando, trampas cuyo único propósito es atraer a los atacantes con un señuelo que imita un recurso informático real (por ejemplo, un servicio, una aplicación, un sistema o datos). Cualquier entidad que se conecta a un *honeypot* pasa a considerarse sospechosa y se controla su actividad en busca de actividad maliciosa.

Este estudio es la continuación de un reciente informe de ENISA sobre la Detección preventiva de incidencias de seguridad en redes. En el anterior informe se concluía que, aunque los CERT reconocían que los *honeypots* proporcionaban información crucial acerca de la actividad de *hackers*, su uso para detectar e investigar ataques aún no era tan extendido como cabría esperar. Esto denotaba obstáculos para su implementación.

Este nuevo estudio presenta estrategias de implementación prácticas y cuestiones críticas para los CERT. En total, se probaron y evaluaron treinta *honeypots* de diferentes categorías. El objetivo: proporcionar información acerca de qué soluciones de código abierto y tecnologías de *honeypots* son mejores para su implementación y uso. Dado que no existe una solución panacea, este nuevo estudio identifica algunas desventajas y obstáculos para la implementación de los *honeypots*: dificultad de uso, documentación insuficiente, falta de estabilidad del *software* y de asistencia de los desarrolladores, poca normalización de estándares y la necesidad de técnicos altamente capacitados, así como problemas para la comprensión de los conceptos básicos de los *honeypots*. El estudio incluye una clasificación y estudia el futuro de esta tecnología.

El director ejecutivo de ENISA, el Professor Udo Helmbrecht, ha comentado que:

"Los honeypots *ofrecen a los CERT una potente herramienta para obtener datos de amenazas, sin impacto alguno en la infraestructura de producción. Si se implementan correctamente, aportan ventajas considerables a los CERT: se pueden rastrear actividades maliciosas en la circunscripción del CERT para permitir alertas precoces de infecciones por* malware*, nuevas* brechas*, vulnerabilidades y actividades* malware*, además de suponer una oportunidad para aprender acerca de las tácticas de los atacantes. Por*

tanto, si los CERT en Europa valoran más los honeypots *como una solución atractiva, podrían defender mejor sus circunscripciones"*.

Para el informe completo
Más información: COM(2009)149 e Implicaciones legales de enfrentarse a *botnets* de la OTAN

Para entrevistas, contacte con: Ulf Bergstrom, portavoz, en press@enisa.europa.eu o teléfono móvil: +30 6948 460 143, o Cosmin Cioabanu, experto de ENISA, en opsec@enisa.europa.eu

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