SALTO BASE

Hackers, ¡búsquense!

Andaba yo corriendo por el Hotel Auditorium, cerca de Madrid, en 2014, para cubrir un congreso de drones cuando me paré, a la puerta de una sala, a ver una mesa plagada de folletos y se me acercó un tipo sonriendo y me dijo: ¿Conoces RootedCON? Uno, que no tenía tiempo, miró a ambos lados buscando escapatoria… pero fruto de la curiosidad periodística no pude sino echarle un vistazo al primer programa que me daba en mano: "Los hackers son de Marte, los jueces son de Venus", decía una ponencia que daba un tal Jorge Bermúdez, fiscal. "Pues sí, me dijo un tal Román: este es un congreso de hackers: ¿te apuntas?". Y ahí que me fui al día siguiente.

Su trabajo y su curiosidad son críticos ante el abrumador despliegue de normativas concernidas –ENS, DORA, CER...– y, sobre todo, la Ley Ciberresiliencia (CRA), que exigirá en la UE implementar ciberprotección en el ciclo de vida de cualquier producto conectado, incluyendo la detección y solución de vulnerabilidades.

Desde entonces y a las puertas ya de celebrarse su XV edición madrileña, conviene poner en valor que en él se han reportado algunas de las más notables vulnerabilidades descubiertas por investigadores españoles (hackers). Son muchas, y entre ellas figuran algunas muy fascinantes, como las descubiertas en **Whatsapp** por **Pablo San Emeterio** y **Jaime Sánchez** –las presentaron porque ""llevamos dos años comunicando errores a WhatsApp y no nos contestan"–, hasta 'Dirty Tooth', la mostrada por el equipo de 'Ideas Locas'; de **Chema Alonso**, –por entonces en **Eleven Paths**–, que permitía almacenar los contactos y el registro de llamadas de un usuario de **Apple** iPhone, a través de un fallo en la conexión *bluetooth;* los posibles fallos en los contadores inteligentes de la red eléctrica, mostrados por investigadores de **Tarlogic** –que llegó a presentar una herramienta para auditar y hacer más seguras estas redes–, o la última sonada: el fallo que podría permitir el ataque a cierta parte de la infraestructura ferroviaria en España, según mostraron en 2024, **David Meléndez** y **Gabriela García.** Pero se cuentan a decenas. Y todas tienen algo en común: la responsabilidad de los ponentes para informar de ellas sin incrementar el riesgo y reportar a quien proceda para ponerle solución. Lógico: se visibiliza para que se corrijan las cosas.

Fruto de su sensibilidad por los hackers –y de congresos como RootedCON–, en Alemania se ha presentado un proyecto de Ley –nos hacemos eco en esta edición–, para proteger a los investigadores de ciberseguridad de ser procesados en caso de descubrir vulnerabilidades. Por lo mismo, en 2021, la ya ex directora la **Agencia de Seguridad Cibernética y de Infraestructura (CISA)** de EE.UU., **Jen Easterly**, destacó en una entrevista su apuesta porque "la comunidad de hackers privados desempeñe un papel importante y ayude a fortalecer las iniciativas de ciberdefensa de Estados Unidos".

Y es que dar a conocer vulnerabilidades, ya sea en congresos técnicos, de forma directa a las empresas, a las Fuerzas y Cuerpos de Seguridad, al **CCN**... o a través de los denominados 'Programas de *Bug Bounty*' –programas de recompensas–, se ha convertido en una imperiosa necesidad, más si cabe con la acuciante ciberseguridad que demanda el uso intensivo que de la IA está haciendo el cibercrimen. Incluso la **Fuerza Aérea** estadounidense organiza, desde 2017, un programa para este colectivo en el que 'abre' sus servidores y sitios web, bajo el lema 'Hack the Air Force' para comprobar que son seguros, de verdad.

En definitiva, ser maduro en este ámbito, en lo corporativo, es también entender –empezando por la alta dirección– que siempre y cuando no haya mala fe y se colabore en pro de solventar el problema, los investigadores de ciberseguridad –*aka* hackers–, son más necesarios que nunca. Al fin y al cabo, su trabajo y su curiosidad se tornan aún más críticos ante el despliegue de cada vez más normativas concernidas –desde el ENS, hasta NIS2, DORA, CER, etc.– y, sobre todo, la Ley Ciberresiliencia (CRA) que exigirá en la UE implementar ciberprotección en el ciclo de vida de cualquier producto conectado, incluyendo la detección y solución de vulnerabilidades. Tener una línea de comunicación con cualquier hacker que avise de un fallo, no conocido, supone trabajar en equipo frente a la industria que ya lo hace: la del cibercrimen, patrocinado, incluso, por estados. Dicen que la curiosidad mató al gato... esperemos que no ocurra igual con los hackers.

José Manuel Vera
Redactor
Revista SIC