NO TODOS LOS *HACKERS* SON ENEMIGOS

La palabra suele tener una acepción negativa, pero a nivel empresarial se requiere este tipo de perfiles para apuntalar los sistemas de seguridad de las compañías.

POR: *Fernando Guarneros*

Javier Bernardo es un experimentado *hacker.* Su trabajo es poner a prueba los sistemas de ciberseguridad de las empresas hasta encontrar un punto vulnerable de acceso. A diferencia de lo que se cree, él no trabaja desde la clandestinidad y tampoco esconde su identidad. Su oficina es colorida, está bien iluminada y reúne a talentosos *hackers* que someten a las compañías a duros procesos para comprobar si en realidad son seguras.

Bernardo es el líder de *hackers* éticos en Strike, una empresa de ciberseguridad fundada en Uruguay con presencia en Latinoamérica, Estados Unidos, Europa y Asia, por lo que es consciente del estereotipo alrededor de la palabra *hacker,* que dicta que las personas dedicadas a esta actividad son criminales en internet buscando un beneficio económico.

Pero *hacking* también tiene una acepción positiva, pues es cuando se prueban los sistemas de seguridad con el consentimiento de las empresas con el objetivo de identificar brechas, reportarlas y solucionarlas antes de que un ente malicioso se aproveche.

"Buscamos técnicas de ciberseguridad defensiva para identificar vulnerabilidades, remediarlas o mitigarlas. La idea es utilizar todas las habilidades de un *hacker* en la detección de fallas o errores", comenta Bernardo.

El primer paso en el trabajo de un *hacker* de sombrero blanco, como también son

FOTO: ANYLÚ HINOJOSA-PEÑA

conocidos, es tener claros sus objetivos; es decir, qué área se va a analizar para saber cómo atacar y encontrar las brechas para acceder a la información.

Luego del acceso, comienza la etapa de escaneo de los posibles puntos de ataque. Para ello, los *hackers* deben saber qué tecnologías usan las empresas, con qué lenguaje de programación trabajan, los sistemas operativos o los servidores donde se aloja su información.

Con esa información, detalla Bernardo, aunado a la experiencia del *hacker* y la lógica del negocio en cuestión, se emplean técnicas para atacar a través de diferentes vectores y, aunque pueda parecer sencillo, es una labor que requiere constancia, creatividad y saber manejar la frustración, ya que para lograr una sola vulnerabilidad se requieren miles de intentos.

UN ARMA DE DOBLE FILO

Las técnicas que usan un *hacker* ético y uno malicioso son las mismas: ingeniería social, pruebas de penetración, investigación, programación de sistemas señuelo o herramientas físicas y digitales. Estas son algunas de las formas en que atacan ambos lados.

Por ello, pueden considerarse como espadas de doble filo; sin embargo, se requiere mayor apertura de las empresas para recibir y recompensar a quienes entregan reportes de fallas de seguridad.

"En el pasado, lamentablemente, se solía elegir las actividades de sombrero negro porque la respuesta de las empresas no era muy buena, no se les recompensaba económicamente ni se reconocía el trabajo de los *hackers",* dice Bernardo.

Pero como su nombre lo indica, la visión de estos expertos es cada vez más ética y entre sus características destaca la confidencialidad, pues, en ocasiones, las empresas temen compartir elementos, como su código fuente, ante el riesgo de una filtración. No obstante, el acceso a este elemento permite hallar problemas de mayor impacto.

Esto ha producido un cambio de enfoque en las compañías, donde atender este asunto es una inversión en vez de un gasto. Por un lado, aminora el interés por actividades maliciosas y, por el otro, previene situaciones críticas en las que se podría gastar más dinero.

El reporte 'Estado del *ransomware* 2022', elaborado por la firma de ciberseguridad Sophos, detalla que de 200 organizaciones que se consultaron en México, el 74% fue víctima de *ransomware* (secuestro de información) y por cada caso se desembolsaron, en promedio, 482,466 dólares. Si bien el dinero no se usó para pagar el rescate, sí fue necesario para la reactivación de las operaciones.

"La tentación del lado oscuro del *hacking* no va a dejar de existir por cuestiones de capital", resalta Bernardo. "Pero profesionalizar esta disciplina y que las empresas tengan sus propios equipos de seguridad da pie a que más especialistas decidan ir por el lado ético, pues su recompensa, salario y reputación van a crecer".

> **LA TENTACIÓN DEL LADO OSCURO DEL *HACKING* NO VA A DEJAR DE EXISTIR POR CUESTIONES DE CAPITAL.**
> Javier Bernardo, líder de *hackers* éticos de Strike.

200

organizaciones fueron consultadas por Sophos, de las cuales, el 74% fue víctima de *ransomware* en 2022.

UN TRABAJO DE ACTUALIZACIÓN Y CREATIVIDAD

Una vez que se detecta la brecha, el trabajo del *hacker* es reportar todos los detalles al respecto, como su severidad o qué tan expuesta está. Asimismo, documenta todos los pasos con el fin de que el responsable de seguridad de la empresa pueda reproducir la vulnerabilidad y es cuando se define el impacto que tiene la brecha, además de una sugerencia de cómo remediarlo.

Aunque parece un proceso apartado del usuario, es necesario para que este cuente con equipos funcionales. Se emplea, por ejemplo, cuando se va a lanzar un nuevo sistema operativo para *smartphones,* pues antes de publicarse, empresas como Android o Apple comparten sus sistemas a expertos en seguridad.

Una vez en sus manos, los someten a diferentes amenazas para detallar vulnerabilidades. Al reportarlas, las empresas las validan, revisan y comprueban que existan para solucionarlas. Este proceso, detalla Bernardo, puede durar semanas o meses, por ello, las versiones beta suelen salir mucho antes que la final.

EL *HACKING* COMO CARRERA

Andrew Wilson, director general de Bishop Fox para Latinoamérica, repara en la necesidad de crear más especialistas de 'hackeo' ético, pues es un sector en donde se pueden crear carreras firmes y bien remuneradas. Si bien es un campo donde la experiencia es un elemento importante, los empleos para jóvenes recién egresados suelen iniciar en 20,000 pesos mensuales, por lo que un problema común es enfrentar los salarios que da el cibercrimen. Con base en un estudio de Kaspersky al mercado laboral en la Darkweb, los especialistas son buscados para crear *malware* o páginas de *phishing* con promesas de entre 23,000 y 26,000 pesos.

Sin embargo, el salario de un especialista con mayor trayectoria puede alcanzar hasta los 40,000 pesos mensuales. Además, existen *hackers* 'freelance', quienes se dedican a notificar de vulnerabilidades a empresas en busca de recompensas y, mientras más complejas sean, la paga es más alta.

Javier Bernardo supo que quería ser *hacker* ético gracias a un acercamiento temprano con la tecnología, y aunque antes las carreras no eran tan frecuentes, reconoce que ahora el panorama académico favorece más a los jóvenes, además de los salarios.

Destaca la necesidad de ser autodidacta y buscar apoyo en comunidades de desarrolladores, pues es donde nacen nuevas metodologías y se comparte el conocimiento que no se da en las aulas. "Es una de las formas más vanguardistas que tenemos para intentar estar un paso adelante de los cibercriminales", indica.