Hacking ético, ¿por qué es una necesidad básica de ciberseguridad en 2023?

CIUDAD DE MÉXICO. 16 de enero de 2023.- Los retos que las empresas enfrentarán a lo largo del 2023, que recién comienza, no son los mismos a los del año pasado en materia de seguridad cibernética.

Con cada vez más empleados trabajando de forma remota, sumado al incremento constante en la sofisticación de las técnicas que emplean los ciberdelincuentes y a la evolución de las amenazas más importantes, los encargados de TI y seguridad deben optar por métodos de protección más robustos y periódicos.

Es por eso que en 2023 las empresas deberán acudir a las soluciones y tendencias más importantes para proteger a sus sistemas, entre las que figura el *hacking* ético como uno de los métodos más necesarios para la protección de los sistemas.

Es decir, el *hacking* ético este año no debe ser considerado un lujo ni mucho menos debe haber temor sobre la apertura de los sistemas a especialistas en técnicas de *hacking*. Por el contrario, debe verse como uno de los procedimientos básicos que toda compañía debe emplear de forma frecuente, para asegurarse de que ningún cibercriminal encontrará vulnerabilidades y/o puertas abiertas que les permitan entrar y moverse libremente dentro de los servidores.

- ¿Por qué es una necesidad básica?

El primer punto que debemos destacar para saber que el *hacking* ético será un método necesario este año radica en hacerle saber a las empresas que es casi un hecho que los *hackers* malisiosos van a entrar a sus sistemas. De hecho, datos de Crowdstrike indican que al año los casos de filtraciones de ciberdelincuentes y robo de datos en empresas se incrementan a una tasa del 82%.

Dicho lo anterior, hay dos opciones a elegir: la entrada a los sistemas por parte de los *hackers* con fines maliciosos, o la práctica autorizada y controlada mediante la cual un experto en seguridad cibernética altamente calificado se inmiscuye en el sistema de la compañía para identificar sus vulnerabilidades.

El segundo aspecto que vuelve necesario al *hacking* ético es que permite anticiparse y actuar antes que cualquier cibercriminal, ya que los métodos y tácticas que utilizará el *hacker*, que en Strike es conocido como Striker, son los mismo y/o muy similares a los que emplean los entes malignos.

Esto da pie al tercer punto, que radica en que las tácticas utilizadas en el *hacking* ético evolucionan a la par que el cibercrimen.

Es decir, de la forma tradicional las compañías implementarían una solución con una forma única de actuar, que una vez descifrada por los ciberdelincuentes se vuelve obsoleta.

Por su parte, los *hackers* éticos pueden utilizar el método del *pentesting*, que es una penetración al sistema para la detección de vulnerabilidades periódicamente, para su reparación inmediata. De ese modo, aunque continúen apareciendo nuevas estrategias o métodos para vulnerar redes, siempre habrá un *hacker* como aliado de la compañía para anticiparse y protegerla de la ejecución de amenazas.

En conclusión, este año el involucramiento de los *hackers éticos* es más necesario que nunca. Si tomamos en cuenta que el cibercrimen no descansa y que, por el contrario, cada día se vuelve más complicado de detectar, es importante saber que los especialistas en seguridad cibernética pueden ser los principales aliados de las compañías, ya que, en el caso de los Strikers, son seleccionados por su experiencia y validaciones, que les permiten trabajar arduamente para brindar una experiencia de *pentesting* de alta calidad, con el objetivo de estar siempre un paso adelante de las amenazas.

-o0o-

Sobre Strike

Strike es una plataforma de ciberseguridad en Latinoamérica. Su principal misión es ayudar a que las compañías estén protegidas a través de la detección y resolución de vulnerabilidades en sus sistemas. Esto se realiza a través de tests de penetración - o *pentests* - llevados a cabo por su red global de hackers éticos, conocidos como “Strikers”, una comunidad global que reúne a los mejores expertos de ciberseguridad con reconocimientos y certificaciones internacionales. Su objetivo es impulsar una cultura de ciberseguridad de calidad y accesible, en la que la misma sea parte del ciclo de vida de las empresas y no algo ocasional o independiente. Más información en: https://strike.sh/

Síguenos en nuestras redes sociales:
Instagram - @strikesecurity
Twitter - @strike_secure
LinkedIn - Strike

Contacto para prensa México
another
Ahtziri Rangel | PR Expert
+ 52 1 55 1395 6970
ahtziri.rangel@another.co