Pentesting: ¿Cómo funciona el ‘hackeo ético’? 5 claves para entenderlo

CIUDAD DE MÉXICO. 21 de septiembre de 2022.- Cuando pensamos en *hackers* generalmente nos imaginamos a piratas informáticos que intentan entrar a los sistemas de las compañías para robar información y causar daños.

Pero lo que muchas compañías no saben es que para prevenir la llegada de estos cibercriminales antes descritos, es fundamental pensar como ellos y actuar de forma anticipada. Contratar un *hacker* en la actualidad es clave para procurar la seguridad de las compañías.

Sobre todo actualmente cuando en México se presentaron el año pasado 156 mil millones de intentos de ciberataques, mientras que en Colombia esa cifra es de 11.2 mil millones; ambos se posicionan como los países de Latinoamérica con mayor incidencia.

¿Cómo protegerse? Strike, compañía global de ciberseguridad, explica en 5 puntos la forma en la que funciona el *hacking* ético:

1. ¿Que es un Pentesting o Penetration Test?

Strike explica que se trata del proceso en el que un ‘*hacker* ético’ entra a los sistemas de una compañía, tal y como lo haría un cibercriminal, pero con el objetivo de encontrar posibles vulnerabilidades que un pirata informático podría explotar.

2. ¿Quiénes lo hacen?

Este proceso está a cargo de *hackers* éticos llamados ‘Strikers’, que realizan el *pentesting* de forma 100% manual, utilizando sus habilidades de *hacking* y conocimientos técnicos de distintos ámbitos e industrias como *crypto*, *e-commerce*, *healthtech* y *fintech*.

Los Strikers trabajaban de forma descentralizada y en diferentes partes del mundo. Durante todo el proceso, están en constante comunicación con la empresa mediante un chat y un *dashboard* en el que se carga la información a detalle para dar seguimiento puntual de las vulnerabilidades a la empresa.

3. ¿Qué sucede tras el análisis?

Como resultado, confeccionan un reporte que se va actualizando continuamente con todas las vulnerabilidades halladas las cuales son categorizadas por criticidad para que la empresa que contrató el *pentest* pueda arreglarlas en el periodo que consideren apropiado.

Las vulnerabilidades que se encuentran durante un *pentest* se utilizan para modificar las políticas de seguridad existentes e identificar debilidades comunes en todo el sistema, entre otros aspectos importantes.

4. ¿Cuántos tipos de *pentesting* existen?

No hay una forma única de realizar una prueba de *pentesting*. Hoy en día hay tres principales métodos:

- Black Box Testing: esta es la forma más sencilla de iniciar un proceso de *pentesting*. En el mismo se ponen a prueba las funcionalidades del sistema pero sin mirar la estructura del código interno.

- White Box Testing: es una forma más sofisticada y completa. Los Strikers inspeccionan el código, la infraestructura e integraciones con sistemas externos de la compañía, como por ejemplo el *software* de áreas específicas como contabilidad y ventas.

- Grey Box Testing: es una combinación de las dos anteriores en la cual el Striker realiza pruebas en los sistemas con un conocimiento parcial de las funciones internas del mismo.

5. ¿Cada cuanto debo hacer un *pentesting*?

Todo depende de las intenciones que tenga la compañía. Strike recomienda realizarlo mediante dos esquemas principalmente:

- One-Shot Pentesting: Orientado a startups que no tengan un equipo de ciberseguridad o no el mismo no está aún consolidado. Es ideal para aquellas compañías que buscan reportes de Compliance o necesiten hacer pruebas puntuales en su producto o plataformas.

- Pentesting Continuo: está orientado a grandes empresas que buscan una solución completa de *pentesting* que se realice de forma periódica. Tal y como visitar al doctor por chequeos de salud constantes, este plan busca acompañar a la compañía en todo su ciclo de desarrollo.

-o0o-

Sobre Strike

Strike es la 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 estanco 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