Tu empresa necesita un 'Hacker Ético' y estos son los motivos

CIUDAD DE MÉXICO. 06 de septiembre de 2022.- El cibercrimen le cuesta, y mucho, a las empresas. De acuerdo con datos del Internet Crime Complaint Center (IC3) las pérdidas a nivel global por ciberataques en 2021 ascendieron a USD $6,900 millones, una cifra que crece exponencialmente cada año y que se prevé que continúe al alza.

Por eso Strike, plataforma de ciberseguridad en Latinoamérica, señala que las empresas deben prevenir vulnerabilidades en sus sistemas mediante procesos periódicos de ciberseguridad como el 'hacking ético'. Sí, tal y como ir al doctor y realizarse chequeos de salud.

"Un error que suelen cometer las empresas es acudir a soluciones de ciberseguridad únicamente por necesidad: es decir, cuando requieren una certificación, cuando una auditoría les exige el testigo de un tercero, o incluso cuando ya fueron víctimas de amenazas como el ransomware y quieren saber por qué sucedió", explica Santiago Rosenblatt, CEO de Strike.

Por el contrario, el especialista sostiene que para detener a los hackers, es importante poder pensar como ellos. Esto se logra mediante técnicas de hacking ético.

- ¿Qué es el hacking ético?

Se trata del uso de técnicas como las que emplean los hackers maliciosos, pero con el objetivo de investigar, detectar vulnerabilidades, y proteger a las compañías. Es decir, el hacker se adentra al sistema y de forma pasiva "lo ataca", pero una vez dentro, en lugar de robar información o cifrar datos para extorsionar a la compañía, le ayuda a prevenir los escenarios negativos y entrega un diagnóstico de las debilidades y/o vulnerabilidades que existen en el sistema.

Strike, por ejemplo, emplea la técnica del *pentesting (penetration testing)*, que consiste en la realización de pruebas de penetración de sistemas para poner a prueba las vulnerabilidades del mismo.

- ¿Cómo funciona el pentesting?

1. **Detectar las necesidades:** Esta técnica que hace uso del hacking ético comienza con un formulario para determinar el objetivo con el que se realizará la prueba. En el mismo se indica si se busca el *pentesting* por prevención, por la exigencia de una certificación en particular, o incluso porque ya fueron víctimas de ciberataques en el pasado y no saben cómo fue que los atacaron.

2. **El hacker ideal:** Con esa información se determina qué 'Striker', será el encargado de realizar el *pentesting* correspondiente. "*No todos los Strikers son iguales, existen desde los especialistas en lenguaje JavaScript, por mencionar un ejemplo, hasta los que se especializan en hackear un sistema operativo determinado. Ahí es en donde debemos buscar al mejor 'Hacker ético' que nos haga match con la necesidad de la compañía",* explica el experto.

Por ejemplo, Strike cuenta con 'Hackers éticos' en diversas partes del mundo que trabajan de forma descentralizada y que se especializan en distintas industrias como *crypto*, *e-commerce*, *healthtech* y *fintech*. Esto permite contar con experiencias y métodos muy variados para atender a todo tipo de compañías.

3. **Seguimiento:** el Striker se adentra al sistema y está en constante comunicación con la empresa mediante un chat y un tablero en el que se carga la información a detalle para así poder realizar un seguimiento puntual.

Ahí las compañías pueden saber qué vulnerabilidades existen, el nivel de riesgo que implican y las recomendaciones que el 'hacker ético' emite para resolverlas, ya sea en ese preciso momento si el cliente lo decide, o posteriormente cuando se trata de vulnerabilidades de bajo riesgo.

4. **Reporte:** El *pentesting* concluye con un reporte en el que detallan todas las vulnerabilidades, la forma de resolverlas y las recomendaciones pertinentes, así como el impacto que pueden tener y el diagnóstico de la empresa.

"El hacking ético y las técnicas como el pentesting son una necesidad de mercado que debe tomarse con seriedad. Aunque el usuario final y las empresas no lo noten, los fabricantes de software y los sistemas están en constante cambio y evolucionan casi a diario. Todos los updates y cambios de código que se ejecutan abren nuevas vulnerabilidades y es complicado atenderlas cuando se realiza un escaneo de ciberseguridad anual. Hacer de la ciberseguridad un hábito es necesario hoy en día: tan solo en Latinoamérica, se generan más de 289 mil millones de intentos de ciberataques al año", concluye el especialista.

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