5 buenas prácticas de seguridad necesarias en 2023

CIUDAD DE MÉXICO. XX de febrero de 2023.- La ciberseguridad ha pasado de ser un aspecto en el que se enfocaban los equipos de TI, CISOs, CTOs y profesionales de la seguridad informática a ser una de las prioridades corporativas de toda empresa.

Este año, derivado del notable incremento de ataques y de la diversificación de las amenazas, es importante que las empresas tengan muy claras las buenas prácticas que deben seguir, no solo para mitigar el riesgo financiero que los cibercriminales significan, sino el golpe en la reputación que un *hackeo* conlleva.

Es por eso que Strike, compañía líder en servicio de *hacking* ético para proteger a las empresas, destaca las siguientes 5 buenas prácticas que deben estar en los planes de toda compañía durante este 2023.

1. Enfoque 'Confianza Cero'

La 'Confianza Cero' (Zero Trust) no es una herramienta en particular, sino que es una actitud y un posicionamiento desde las compañías. El mantra de 'no confiar, siempre verificar' permite a las empresas anticiparse siempre a los ataques cibernéticos a través de soluciones y arquitectura centradas en la identidad y la autenticación.

Dicho lo anterior, las compañías requieren de una cuidadosa gestión de identidades y autenticación tanto de consumidores en sus plataformas como de colaboradores dentro del sistema interno, con métodos de doble factor, uso de biométricos en el acceso, microsegmentación, y la implementación de entornos seguros de comunicación.

2. Pentesting

Se trata de una prueba de penetración del sistema por parte de un experto en ciberseguridad y *hacking* ético, al cual la empresa contrata para que ponga a prueba sus sistemas, las medidas de seguridad implementadas, y se inmiscuya en el sistema. La diferencia es que lo hace con el objetivo de encontrar posibles vulnerabilidades y que éstas, en consecuencia, sean reparadas oportunamente.

Este experto en ciberseguridad usa sus habilidades en *hacking* para el bien. En lugar de ingresar a los sistemas para robar datos y hacer mal uso de ellos, los *hackers* éticos prueban las vulnerabilidades del sistema con tácticas creativas y contrarias a la intuición, del modo que lo haría un *hacker* malicioso, pero con fines de protección.

3. Honeypot

Se trata de la utilización de un activo digital falso que se asemeja a un objetivo valioso (como datos sensibles o información financiera de la empresa) y que tiene como objetivo atraer y engañar a los atacantes cibernéticos, desviando su atención de los activos esenciales y al mismo tiempo haciéndolos visibles para las empresas.

El *Honeypot* es sumamente utilizado cuando las organizaciones se encuentran haciendo investigaciones internas por sospechas de ciberataques, aunque debería ser una práctica implementada de forma más periódica para la creación de un ambiente más seguro.

4. Sistemas SOAR

Se trata de sistemas de orquestación, automatización y respuesta de ciberseguridad que deben ser adoptados para que las empresas puedan recopilar, de forma ágil y rápida, información como indicadores de riesgo, amenazas externas y otros datos.

Esa información permite realizar análisis de amenazas sofisticados y otorgar una clasificación de la gravedad de cada una de ellas, para actuar en consecuencia. También permite tener un panorama de seguridad más amplio ya que analiza fuentes externas a la red. De esta forma el sistema puede automatizar la respuesta a amenazas, resolver eventos de ciberseguridad y alertar al equipo de TI, todo con base en un análisis avanzado de información.

5. Seguridad enfocada en APIs

La comunicación entre sistemas a través de una API (app móvil o web conectada al servidor de una empresa) es una excelente forma de simplificar la interacción entre clientes y negocios, pero generalmente es sumamente vulnerable ya que estas se encuentran disponibles mediante redes públicas. Esto las pone en peligro de ser víctimas de ataques de denegación de servicios (DDoS) e interrupciones de servicios para realizar extorsiones, por mencionar ejemplos.

Por eso la seguridad de las API este año es clave para mantener seguro a cualquier sistema que recibe y envía datos a través de una red abierta entre clientes y servidores. De lo contrario la información de negocio está en riesgo y los atacantes podrían manipular los parámetros para realizar transacciones fraudulentas, por mencionar un ejemplo.

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