Ataques API: Un blanco común en un mundo de *apps*

CIUDAD DE MÉXICO. 20 de junio de 2023.- En el vertiginoso mundo digital en el que vivimos, la interconexión de aplicaciones y servicios se ha vuelto omnipresente. Detrás de cada interacción en línea, ya sea al enviar un mensaje, realizar una compra o compartir información, se encuentran las interfaces de programación de aplicaciones, más conocidas como API por sus siglas en inglés.

Estas API permiten a diferentes aplicaciones comunicarse entre sí y compartir datos y funcionalidades, lo que ha impulsado la innovación y la comodidad en nuestras vidas digitales. Pero esta dependencia de las API también ha llevado a un aumento alarmante en los ataques dirigidos a estas interfaces.

Los ciberdelincuentes encontraron un blanco fácil en las vulnerabilidades de las API para obtener acceso no autorizado a datos sensibles, llevar a cabo ataques de denegación de servicio o incluso secuestrar cuentas de usuario en diferentes plataformas basadas en aplicaciones, como son incluso las redes sociales

- ¿Qué es un ataque API?

Consiste en el uso abusivo o manipulador de una API, generalmente empleada para violar datos o influir en una solución de comercio. Estos pueden adoptar diferentes formas, como la explotación de vulnerabilidades o el uso de técnicas para descubrir contraseñas débiles. Además, los ataques de denegación de servicio (DoS) también pueden dirigirse a las API, sobre cargándolas con una gran cantidad de tráfico inusual, lo que puede afectar la disponibilidad de un servicio o incluso causar un colapso completo.

- ¿De qué tamaño es el riesgo?

El problema radica en que existe una amplia adopción de servicios y aplicaciones que dependen de la ejecución de sus sistemas en estas interfaces. Desde aplicaciones de banca móvil hasta redes sociales y servicios de entrega de alimentos, cientos de miles de *apps* que utilizamos a diario se basan en la interacción con las API.

De hecho, en 2022 el uso indebido de API se convirtió en el vector de ataque más común contra las aplicaciones; según Vaadata, estas interfaces representan el 90% de la superficie de ataque en los atentados contra apps, que hoy son mucho más atacadas que otras plataformas como los sitios *web* tradicionales.

Lo anterior deriva en filtraciones de datos de múltiples empresas en el mundo ya que las API acceden directamente a datos y servicios críticos.

- ¿Qué hacer al respecto?

Para mitigar los riesgos asociados con los ataques API, es fundamental implementar medidas sólidas de seguridad. Esto implica asegurarlas mediante autenticación y autorización adecuadas, además de implementar cifrado sólido para proteger los datos en tránsito entre *app* y usuario.

También es importante establecer un monitoreo constante de las actividades en las API para detectar comportamientos sospechosos o anormales. Implementar sistemas de registro y monitoreo centralizados que permitan una rápida respuesta a incidentes de seguridad es una opción viable.

Otro consejo es el de aplicar el principio del menor privilegio. Es decir, limitar los permisos de acceso de las API al interior de las empresas a solo aquellos colaboradores que realmente lo necesitan.

Finalmente es importante realizar pruebas de seguridad periódicas, en las que el *pentesting* destaca como una opción ideal, para identificar y abordar posibles vulnerabilidades en las API. Esto ayudará a descubrir debilidades y brindará la oportunidad de corregirlas antes de que los atacantes las aprovechen.

En conclusión, los ataques a las API representan una amenaza cada vez mayor en un mundo debido a lo atractivas que son estas interfaces para los ciberdelincuentes, quienes buscan aprovechar las vulnerabilidades y obtener acceso no autorizado a información sensible.

Con una sólida estrategia de seguridad, la implementación de buenas prácticas, y desde luego tomando en cuenta que la seguridad debe ser un proceso continuo, las empresas pueden proteger sus API y mitigar los riesgos asociados, salvaguardando la confidencialidad, integridad y disponibilidad de sus servicios digitales.

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