Tenga en cuenta la brecha:

cómo garantizar que sus métodos de detección de vulnerabilidades estén a la altura

Dado que se espera que los costos globales del cibercrimen alcancen los $ 10.5 billones anuales para 2025, según estudio, no es de extrañar que el riesgo de ataque sea la mayor preocupación de las empresas a nivel mundial. Para ayudar a las empresas a descubrir y corregir las vulnerabilidades y configuraciones erróneas que afectan a sus sistemas, hay diversas soluciones disponibles.

Pero tenga cuidado, es posible que no le den una visión completa y continua de sus debilidades si se usan de forma aislada. Con enormes ganancias financieras que se obtienen de cada violación exitosa, los piratas informáticos no descansan en su búsqueda de fallas y utilizan una amplia gama de herramientas y escáneres para ayudarlos en su búsqueda. Vencer a estos delincuentes significa mantenerse un paso por delante y utilizar el soporte de detección de vulnerabilidades más completo y receptivo que pueda.

Revisaremos cada solución y explicaremos cómo puede mantener su vigilancia. Por supuesto, la gestión de vulnerabilidades es solo un paso que las empresas deben tomar para prevenir una violación; también hay que tener en cuenta la gestión adecuada de activos, la capacitación de los empleados y la respuesta a incidentes, pero este artículo cubrirá específicamente el escaneo y las pruebas de penetración.

Análisis de vulnerabilidades.

Un escáner de vulnerabilidades comprueba sus sistemas en busca de fallas de seguridad que puedan usarse para robar datos o información confidencial o, en general, causar interrupciones en su negocio. En función de sus necesidades, puede implementar analizadores para vigilar cualquier área de su sistema, desde su infraestructura externa o interna hasta sus aplicaciones web y puntos finales, así como cualquier área autenticada o no autenticada de su sitio web.

Es por eso que es importante asegurarse de tener una solución de administración de vulnerabilidades que pueda brindarle visibilidad continua de sus sistemas y ayudarlo a priorizar y solucionar cualquier problema de seguridad.

Pruebas de penetración.

Una prueba de penetración (también conocida como prueba de lápiz) es un ataque cibernético simulado llevado a cabo por hackers éticos en sus sistemas para identificar vulnerabilidades que podrían ser explotadas por atacantes maliciosos. Esto le ayuda a comprender no solo lo que debe solucionarse, sino también el impacto potencial de un ataque en su negocio.

Con los hackers encontrando métodos más sofisticados para irrumpir en sus sistemas, ¿cuál es la mejor solución moderna para mantenerlo un paso por delante?

Un híbrido de escaneo de vulnerabilidades y pruebas de penetración.

Para obtener la imagen más completa de su postura de seguridad, debe combinar el escaneo automatizado de vulnerabilidades y las pruebas de penetración dirigidas por humanos.

Con los principales profesionales de seguridad del mundo a mano, investigarán más profundamente, encontrarán más vulnerabilidades y proporcionarán avisos sobre su impacto directo en su negocio para ayudarlo a mantener a raya a los atacantes.

La amenaza de ataque está aumentando, no te dejes vulnerable. Elija una cobertura continua y completa, contacte a nuestros especialistas para más información.

Fuente de información: thehackernews.com