10 cosas principales que debe saber sobre VAPT

2020, el año de la pandemia, también trajo una ciberpandemia. La cantidad de ataques y amenazas aumentaron significativamente y se volvieron más sofisticados. Con un ataque cada 39 segundos y, en promedio, 2.244 veces cada día, la seguridad se convierte en una gran preocupación para las empresas grandes y pequeñas.

Aquí es donde entra en juego el VAPT. Si no está familiarizado con este acrónimo, no le culpamos: es un concepto relativamente nuevo en un mundo en el que parece aparecer un acrónimo nuevo cada día. Sin embargo, las estadísticas anteriores demuestran que deberías familiarizarte con el VAPT antes de que tus activos digitales sean atacados.

Vamos a profundizar en ello.

10 cosas que deberías saber sobre el VAPT

1. ¿Qué es el VAPT?

VAPT significa Vulnerability Assessment and Penetration Testing (Evaluación de Vulnerabilidad y Pruebas de Penetración). VAPT es un término que describe las pruebas de seguridad diseñadas para identificar y ayudar a abordar las vulnerabilidades.

VAPT es un término que puede incluir varias técnicas de pruebas como la evaluación automatizada de la vulnerabilidad.

evaluación, pruebas de penetración realizadas por ingenieros humanos cualificados, e incluso operaciones de equipo rojo.

2. VAPT es una solución de pruebas más completa

La evaluación automatizada de la vulnerabilidad es un gran comienzo. Las pruebas de penetración son también una importante medida de seguridad. Pero VAPT reúne estas dos técnicas y otras bajo el mismo techo virtual para ofrecer a las empresas una visión más completa de sus problemas de seguridad.

Con VAPT, es más fácil descubrir y mitigar las vulnerabilidades críticas en todas las plataformas y tipos de software, incluso de terceros.

3. VAPT puede ayudarle a descubrir las lagunas entre varias herramientas de seguridad

Si es un habitual de nuestro blog, ya sabe que abogamos por una combinación de pruebas y evaluaciones automatizadas y manuales. Sin embargo, incluso la combinación entre la evaluación automatizada de evaluación automatizada de la vulnerabilidad y pentests manuales le deja abierto a algunas vulnerabilidades.

Por ejemplo, si ejecuta dos herramientas de evaluación de vulnerabilidad diferentes para la misma aplicación, los resultados pueden ser completamente diferentes. ¿Cómo puede saber en cuál confiar?

VAPT añade una nueva capa (a menudo manual) a todo esto. Este enfoque integrador de las pruebas de seguridad está diseñado para salvar las diferencias entre las herramientas automatizadas y crear una perspectiva unificada sobre las vulnerabilidades de seguridad.

4. VAPT le ayuda a priorizar los riesgos

Incluso algunas de las empresas más conscientes de los riesgos se olvidan de este paso crucial. Encuentran y recopilan las vulnerabilidades pero simplemente renuncian a la priorización de los riesgos, el paso más importante.

En el panorama actual de la ciberseguridad, donde las amenazas son cada vez más diversas y sofisticadas, la priorización de los riesgos es una necesidad absoluta. De lo contrario, puede acabar dedicando mucho tiempo a los riesgos triviales, mientras que los más graves quedan desatendidos. A su vez, esto expone a su organización a graves amenazas que podrían haberse mitigado fácilmente.

La priorización de los riesgos es una parte integral del VAPT. Una buena estrategia VAPT aborda y enfatiza este paso marcando claramente qué amenazas y qué riesgos deben abordarse en primer lugar.

Para saber más sobre nuestro servicio VAPT y nuestras otras soluciones, envíenos un correo electrónico a sales@bluedogsec.com o visite bluedog-security.com.

5. VAPT descubre errores de configuración y lagunas en varias aplicaciones

La razón número uno del éxito de los ciberataques es el error humano. Las aplicaciones web, las redes, las aplicaciones móviles... todas ellas están escritas por humanos y, por tanto, son propensas a cometer errores. Esto es exactamente lo que los atacantes buscan explotar.

La mayoría de las vulnerabilidades explotables se deben a errores de configuración o a prácticas de codificación incorrectas. Ambas cosas pueden estar presentes en sus propias aplicaciones o en las de terceros.

El VAPT gestionado por una empresa de terceros es la forma más fácil de detectarlas y abordarlas antes de que se conviertan en problemas crónicos o, peor aún, antes de que un atacante tenga éxito. Sin embargo, hay que elegir con cuidado al proveedor de VAPT. Debe trabajar con una empresa que no escatime en los conocimientos de los ingenieros que contrata.

6. VAPT mejora su proceso de SDLC

El SDLC (ciclo de vida del desarrollo de software) es una metodología que siguen las empresas de TI. Como ocurre con todas las metodologías, el SDLC necesita evolucionar constantemente para responder a las nuevas demandas del mercado e incluso a las nuevas ciberamenazas.

La realización periódica de pruebas de penetración como parte de su proceso VAPT alineado con el proceso SDLC es la forma casi perfecta de garantizar una gran seguridad. De esta manera, tu código, junto con todos los cambios que se realicen en él, pasan por numerosas comprobaciones de seguridad que son capaces de detectar vulnerabilidades desde el principio, mucho antes de que lances tu producto.

7. VAPT tiene un excelente retorno de la inversión

¿Sabe qué ocurre con el dinero que invierte en ciberseguridad? Probablemente no. De hecho, es uno de los campos que tiene fama de tener un ROI difícil de precisar. Mientras no se produzcan ataques, usted considera que es dinero bien invertido.

Y no se equivoca.

Pero, gracias a su enfoque integral, VAPT puede decirle exactamente cuánto dinero ha ahorrado al elegir un enfoque integrador en lugar de métodos de prueba dispares, por ejemplo. O cuánto, de media, le podría haber costado un ataque exitoso.

8. Un concepto, múltiples aplicaciones

VAPT no sólo es ideal para las aplicaciones web. También puede utilizarse con éxito para aplicaciones móviles o para redes. De hecho, cualquier activo orientado a Internet puede utilizar VAPT.

Por supuesto, el término es el mismo, pero el enfoque difiere de un activo a otro. Por eso el componente humano es esencial en el proceso VAPT. Un enfoque dirigido por humanos ayuda a elegir las herramientas y los procesos adecuados para identificar las vulnerabilidades más frecuentes para cada tipo de activo.

9. No hay una talla única en el VAPT

Sí, hay numerosas herramientas que pueden utilizarse para diversas aplicaciones. Y sí, el proceso VAPT tiene unos pocos componentes básicos que serán los mismos en todos los activos que se prueben.

Pero en general, el proceso VAPT será diferente de una empresa a otra. El enfoque y la duración dependen del tamaño de la empresa, de la cantidad de datos y del número de dispositivos y activos que deben ser probados y escaneados.

10. El VAPT ayuda a cumplir la normativa

Un número cada vez mayor de empresas utilizan VAPT como la forma más segura y rápida de lograr el cumplimiento de diversas normas como GDPR, ISO 27001 y PCI DSS. Incluso si se lleva a cabo únicamente con fines de cumplimiento, VAPT seguirá detectando las principales vulnerabilidades y puede ayudarle a mantener sus activos seguros.

Reflexiones finales

El VAPT es, irónicamente, una de las últimas cosas en las que piensan los directivos. Es decir, hasta que el primer ataque tiene éxito.

Con un ataque medio que cuesta más de 2 millones de dólares, ¿realmente quieres esperar tanto tiempo? Le prometemos que VAPT es menos costoso y menos doloroso que un ataque exitoso.

En Bluedog tenemos un conjunto de servicios VAPT, desde escaneos automatizados mensuales de bajo coste hasta pruebas de penetración manuales en profundidad, contacte con uno de nuestros distribuidores hoy mismo sobre VAPT; no espere a ser atacado.