Pentest, Seguridad para tu Empresa

Pentest, la mejor práctica de seguridad para tu Empresa,

La realidad de los constantes ataques cibernéticos en el mundo obliga a las grandes y medianas compañías a realizar un completo y periódico análisis de la seguridad de sus sistemas, precisamente, a este tipo de evaluaciones le llamamos: Pentest o Penetration Testing.

La realidad de los constantes ataques cibernéticos en el mundo obliga a las grandes y medianas compañías a realizar un completo y periódico análisis de la seguridad de sus sistemas, precisamente, a este tipo de evaluaciones le llamamos: Pentest o Penetration Testing.

El objetivo principal de un pentest es detectar a través de un ataque simulado a nuestro sistema, los puntos débiles que puedan ser usados para violar cualquiera de las tres condiciones necesarias de la información: confidencialidad, integridad y disponibilidad.

Existen muchos casos donde las empresas sufren incidentes que podrían haberse evitado si los mecanismos de protección hubieran sido reforzados en su momento a través de un pentest, en la mayoría de los casos, el resultado de uno de estos ataques es la fuga de información, accesos no autorizados, pérdida de datos, entre muchos otros, pero para evitarnos dolores de cabeza, lo ideal es verificar que todos nuestros sistemas de seguridad están respaldados a través de este tipo de “auditorias” que permitirán brindar una solución oportuna

antes de que un ciberdelincuente descubra y aproveche las debilidades de nuestros sistemas.

Ahora, es fundamental decidir si quieres hacer un pentest de toda tu empresa, o solo de algún programa específico del cual necesitas mayor protección, para cualquiera de los dos casos se utiliza una metodología de evaluación de seguridad informática que incluye cuatro grandes etapas:

1) Descubrimiento

2) Exploración

3) Evaluación

4) Intrusión,

esta última etapa es fundamental debido a que se utiliza toda la información recolectada en las fases previas para evaluar las posibles alternativas que puedan permitir un ataque "exitoso" y evidenciar nuestras propias fallas.

Pentest y hackeo ¿es lo mismo?

Muchas personas confunden estos dos términos pero en realidad, la delgada línea que separa a una acción de la otra está en si estamos o no autorizados para hacer este "ataque" a un sistema, de no ser así sí que podríamos usar de forma correcta la terminología "hackear". Para ser más claros, en el pentest contamos con el permiso y aprobación del propietario del sistema a atacar, mientras que durante un ataque no consentido por el propietario estaríamos haciendo hacking, cosa que en la mayoría de países es un acto delictivo.

Ahora que ya conoces qué es un pentest, debes realizarlo antes de que un ciberdelincuente ejecute un ataque real y bloquee tu sitio web, ataque los correos electrónicos de tus clientes y usuarios o peor, puedas perder tus datos. Contacta a los asesores de Hostdime y podrás consultar sobre los mejores

planes de seguridad.

Nuestros clientes trabajan siempre con la tranquilidad de estar seguros frente a posibles amenazas de seguridad, concentrándose en expandir su negocio, desarrollar nuevas ideas y generas más ingresos.

Visítanos ya y descubre por qué en HostDime somos catalogados como la mejor empresa de servicios on line.