¿CON QUÉ FRECUENCIA DEBE DE HACERSE UNA PRUEBA DE PENETRACIÓN EN MI EMPRESA?

Hace apenas 5 años, las pruebas de penetración eran los temas de artículos en revistas de seguridad de la información, y se sometía a discusión si eran necesarios o no. Esto ha cambiado en la actualidad.

En un mundo que cambia constantemente, y con un mercado negro de hackers que vale millones, si esperas a una prueba de penetración, tal vez sea demasiado tarde. Sin embargo, algunas compañías hacen una prueba de penetración sólo cuando tienen que hacerlo, cuando necesitan comprobar que son seguras o cuando tienen que cumplir con ciertas regulaciones.

Tristemente, muchas empresas hacen estas pruebas una vez que han sido atacados, cuando los hackers han logrado entrar a la organización, llevándose registros, nombres de clientes, IP´s, etcétera, costándole a la compañía más de lo que puedan imaginar o calcular.

Algunos datos duros:

• Las cuentas robadas de twitter tienen más valor en el mercado negro que las tarjetas de crédito

• El hackeo es más redituable que la venta de drogas

• La venta de vulnerabilidades de programación en el mercado negro se ha vuelto común

La prueba de penetración debe ser realizada por un equipo de los mejores atacantes que tu organización pueda pagar, solicitándoles que ataquen y exploten tus defensas lo más profundamente posible. Las empresas están buscando ver el "lado malicioso" de su organización, procesos de negocios, la custodia de la

información, así como los sistemas principales o las infraestructura que están más expuestos a los ataques.

Antes de contestar la pregunta de "¿qué tan seguido debe ser realizada una prueba de penetración?", toma en cuenta los siguientes puntos:

1. Entre más alto sea el nivel de seguridad en la parte interna de la Red, pasará más tiempo antes de que se necesiten pruebas que muestren la vulnerabilidad desde el exterior de la misma;
2. No todos los sectores de la industria son iguales. Algunos requieren ser más estrictos con las pruebas que otros (por ejemplo: el financiero y el gubernamental);

3. Cuando la infraestructura de una empresa se compone de más Servidores que de otro tipo de dispositivos, será necesario recortar los tiempos entre las pruebas. La diversidad de sistemas operativos y aplicativos hacen más compleja la tarea;
4. Los aplicativos desarrollados "in-house" suelen ser más propensos a vulnerabilidades que aquellos desarrollados por firmas de software comercial. Aunque las de estos últimos son más publicitadas; y
5. Las empresas que permiten el uso de dispositivos personales entre sus empleados, están más propensas a ataques.

Nuestros expertos recomiendan es que se realice una prueba de penetración cada 6 meses, pero sin dejar de lado los puntos anteriores.

Toda organización que maneje información confidencial debe tener la responsabilidad de asegurar que la configuración de su red y sus defensas sean seguras. Además, ninguna compañía quiere ser una distribuidora de malware.

Si alguien te ofrece una respuesta simple o un "curita" sin realmente ver las necesidades que tu organización necesita, deséales suerte, la van a necesitar.

Llámanos y nosotros te ayudaremos.

www.mexis.net

t.+52(55)50004499