Haciendo simple IT Soluciones de Seguridad

Penetration Test

IT STAFFING SOLUTIONS

Las 2 preguntas claves para saber si conviene contratar una empresa staff de seguridad informática:

1. ¿Es estratégica para mi empresa, la función/skill que estoy evaluando? (Fuente: Banco: Autenticación de usuario para un Sistema de HomeBanking)
2. ¿Esta función /skill es el "core competency" de mi empresa?¿Lo hacemos bien, tenemos gente capacitada, recursos, etc? (Fuente: Gartner Group)

VENTAJAS

Menor Costo
Reducción de problemas de staffing
Mejores habilidades
Objetividad e independencia
Conocimientos de nuevos problemas
Performance del servicio
Infraestructura especializada

DESVENTAJAS

Confianza
Dependencia
Parte de infraestructuras compartidas
El día después de terminar el contrato

¿QUÉ ES UN PENETRATION TESTING?

Es intento localizado y limitado en el tiempo, para obtener acceso y tomar control de la información, utilizando técnicas de un atacante. Se asemeja a los eventos reales de una intrusión, utilizando las últimas técnicas y herramientas con los siguientes objetivos:

-Prueba que una vulnerabilidad específica es explotable

-Proporciona resultados tangibles para el gerenciamiento de las acciones a tomar (los patches, procedimientos y controles de seguridad son verificables.)

-Permite entender como un ataque real puede impactar en los negocios de la organización y sus activos clave.

Se realiza en dos espectros o posibilidades:

OUTDOOR: Las vulnerabilidades son probadas desde el exterior (a través del firewall Perimetral y/o IDS) hacia los dispositivos con presencia en Internet. Simulando el ataque de un hacker fuera de la organización.

INDOOR: El estado de los servidores es testeado desde el interior de la organización, tal cual lo podría hacer un empleado o persona conectada a la red local. Para realizar este trabajo personal de Openware se conectará con un equipo propio a la red del cliente.

OBJETIVOS DEL PENETRATION TEST

Lograr un nivel apropiado de la seguridad perimetral interna/externa, teniendo como objetivo la defensa de los activos de la empresa. (Imagen, BD´s, información, disponibilidad, etc.)

Tomar métricas de la operatoria y situación actual de la seguridad de la plataforma tecnológica. Demostrar en forma explícita el alcance de las falencias de seguridad a través de servicios de ataques programados.

Proveer de un documento que detalle los puntos a reparar y la forma de concretar las correcciones necesarias.

Lograr una optimización del área de IT/Desarrollo, con miras a tener una visión "security-centric" de los negocios, poniendo foco en la confiabilidad, disponibilidad y escalabilidad de las estructuras. (Extendiendo el concepto a socios y clientes)

Planificar, en caso de necesidad, la inserción de servicios de outsourcing en forma gradual y medida.

CYOS technology
www.cyosgt.com

Cel 56.30.02.73
oscargarcia@cyosgt.com

Cel 56.30.55.14
clarafernandez@cyosgt.com

¿Por qué seguridad informática?

CONTRATACIÓN DE SEGURIDAD INFORMATICA PARA SU EMPRESA

Existen muchos mitos acerca de la seguridad, ¿Cuáles se ha oído usted decir?

MITOS DE LA SEGURIDAD

- NO EXISTE 100% DE SEGURIDAD
- LOS HACKERS SON EXPERTOS EN INFORMÁTICA Y REDES
- MI EMPRESA NO TIENE INFORMACIÓN CONFIDENCIAL O DE IMPORTANCIA
- HASTA AHORA...NUNCA NOS PASO NADA
-LA GENTE DE SISTEMAS SE OCUPA DE LA SEGURIDAD DE LA INFORMACIÓN Y ME DICEN QUE ESTA TODO OK.
-YA COMPRAMOS UN FIREWALL

Si Ud. NO permite que un desconocido ingrese a su empresa por la puerta, por qué permitiría que lo haga por Internet. 95% de los encuestados por Computer Security Institute/FBI 2002 reportan problemas de seguridad. 75% citan la conexión a Internet como un punto frecuente de ataques, 186 empresas (35%) reportan la valuación de sus pérdidas financieras en $377.8M, por robo de información, sabotaje de datos, etc. Las tres primeras tecnologías de protección más utilizadas son el control de acceso/passwords (100%), software anti-virus (97%) y firewalls (86%) Fuente:

Cree que está seguro. Pregúntese: ¿Cuánto cuesta no tener sistemas por un día? ¿Cuánto cuesta un fraude a mis Bases de Datos? ¿Cuánto vale perder la imagen ante el mercado?

SEGURIDAD

La seguridad no es un producto, como un firewal, es un proceso continuo. El problema de la Seguridad está en su gerenciamiento y no en las tecnologías disponibles El costo de la defensa depende de la valuación de los activos a defender.

CYOS SEGURIDAD

CYOS le ofrece una decisión basada en “papeles complementarios y responsabilidades compartidas”. De esta forma la empresa y CYOS tienen definidos sus roles, permitiendo a la empresa rescatar el valor real del outsourcing, pero al mismo tiempo conservar el control de IT, reduciendo costos, CYOS se convierte en proveedor de información detallada de management, monitoreo y de recomendaciones técnicas. La empresa se transforma en un consumidor de este flujo de información y conserva el control de su propia infraestructura y aplicaciones

INFORMACIÓN

La información debe considerarse como un recurso intangible con el que cuentan las Empresas y por lo tanto tiene valor para éstas, al igual que el resto de los activos, debe estar debidamente protegida. Si no la protegemos es probable que exista: Pérdida de reputación, Interrupción no planeada de negocios, servicios, producción. Pérdidas financieras y de tiempo. Robo de información sensible

RESPONSABILIDAD

La seguridad, no es responsabilidad exclusiva del área de IT, ya que están faltante de tiempo, recursos y personal calificado en seguridad. Están enfocadas en dar funcionalidades y respuestas a los usuarios finales, rompiendo la distancia y la objetividad necesaria a la hora de fijar normas y políticas de seguridad.

CYOS technology
www.cyosgt.com

HEMOS TRABAJADO EN IMPLEMENTAR SOLUCIONES DE SEGURIDAD

Permítanos hacerlo para usted