

Microsoft® *Análisis de Riesgos de Infraestructura Informática* Risk Assessments



¿Quieres conocer el nivel de riesgo que hay en tu red?

El termino de seguridad informática, es hoy en día la suma de múltiples defensas, sin embargo aun siguen existiendo problemas, aunque es cierto que no hay sistema (s) 100% seguro, también es cierto que un gran porcentaje de intrusiones se deben a malas configuraciones en estos sistemas.

¿Le gustaría saber que tanto esta su red propensa a un ataque?, mediante Risk Assessments usted puede obtener información fehaciente de que tan vulnerable es su red, este estudio esta basado en esquemas de seguridad desarrollados por Microsoft, y lo mejor de todo es que no tiene costo en absoluto.

Defensas Profundas

Tal vez usted tenga un esquema de seguridad bastante robusto, pero ¿ha analizado que metodología es la correcta no solo desde el punto de vista de los fabricantes de appliances o programas de seguridad?. Los estudios de nivel de riesgos informáticos pretender dar un panorama general del estado de su red y ayudarle a desarrollar un esquema de seguridad que comprenda varios niveles, observe el siguiente esquema:



Defensas Perimetrales: Filtrado de Paquetes, Inspección completa, Detección de Intrusos

Defensa a nivel de Red: Listas de Control con VLANs, Firewalls internos, Auditorias, Detección de Intrusos

Defensa de Equipos: Endurecimiento de Servidores, Detección de Intrusos a nivel de equipo, Filtrado de IPSec, Auditorias

Defensa de Aplicaciones: Validación, Verificación de HTML / Origen de Cookies, Asegurar el IIS

Recursos e Información: Bases de Datos, Aplicaciones y Servicios en Red, Archivos Compartidos

Seguridad de Servidores

Dentro de Risk Assessments usted podrá recibir recomendaciones que se ajusten precisamente a su esquema de red, estas recomendaciones dependerán de lo observado durante el análisis, una muestra de ello es la seguridad dentro de los servidores:

- A) Restricción de ejecutables: mediante herramientas tales como Appsec.exe o AppSense Application Manager usted puede crear políticas restrictivas que limiten la instalación de ejecutables en un servidor.
- B) Políticas de restricción de Software las cuales le permitirán definir que programas pueden ser utilizados de manera segura, así como prevenir que usuarios puedan descargar programas que pudieran significar un peligro para su servidor.
- C) Asegurando Terminal Services, si usted hace uso de estos servicios, debería considerar lo siguiente:
 - * Configurar la encriptación a High
 - * Deshabilitar el control remoto
 - * Deshabilitar funciones de mapeo

Estas son solo una pequeña muestra de lo que significa realizar un estudio de riesgos informáticos dentro de su red, además de dar estas recomendaciones, se le dará soporte en la manera de cómo puede hacerlo de una manera simplificada.

Los puntos que son revisados a detalle son:

- Administración de Parches
- Seguridad de Servidores
- Seguridad del IIS
- Seguridad de sistema de correo Exchange
- Endurecimiento de Servidores de Bases de Datos
- Endurecimiento de la Red
- Respuesta ante Incidentes

Solo con el conocimiento de los puntos débiles, se podrá desarrollar un plan que pueda reducir a un nivel mínimo el nivel de riesgos en su red.

Si desea recibir mas información al respecto y saber si usted puede ser candidato para un estudio de riesgos gratuito, por favor contáctenos a la dirección soporte@realnetsa.com.mx



Para más información acerca de este servicio por favor póngase en contacto con nosotros.

RealNet, S.A. de C.V.
"Administración y Seguridad de Redes"
Guaymas 11bis Col. Roma C.P. 06700
México, D.F.
info@realnetsa.com.mx
Tel: (01 55) 5219 8656
Fax: (01 55) 5208 8201

www.realnet.com.mx