boletín técnico®

imef ejecutivos de finanzas

NUM. 40 / 2004

COMITÉ TÉCNICO NACIONAL
DE TECNOLOGÍA DE INFORMACIÓN

Seguridad en TI

ISC. José Gabriel Vilchis P.

Los avances en las tecnologías de la información, han permitido a las organizaciones realizar nuevas formas de envío y recepción de información entre sus clientes, empleados, proveedores e instituciones, lo que conlleva a pensar de manera seria en el concepto de seguridad en los sistemas, mismo que engloba la integridad de los recursos, la disponibilidad y la confidencialidad.

El concepto de seguridad contempla la protección de la información contra el acceso o modificación NO autorizados, la protección del sistema restringiendo los servicios a usuarios ilegítimos y las medidas preventivas necesarias para detectar, documentar y contrarrestar tales amenazas.

No obstante, hoy en día no basta con crear un perímetro de seguridad protegiendo el acceso por entes externos a la organización, ya que según diferentes estudios y encuestas indican que la mayoría de los sucesos, los riesgos son internos, incidentes causados por individuos pertenecientes o empleados en las organizaciones afectadas.

Para una protección adecuada, es necesario contemplar los siguientes niveles de seguridad:

- Autenticación
- Autorización
- Privacidad
- Confidencialidad
- Integridad
- No Repudio
- Disponibilidad

El primer paso es elaborar una estrategia de seguridad para determinar las medidas a implementar con el objetivo de experimentar una reducción en el riesgo. Estas medidas deben ser ubicadas con precisión y mantenidas con la adopción de una estrategia pro activa de gestión cíclica de riesgo que incluya el monitoreo, y respuesta activa de redes y sistemas ante posibles incidentes de seguridad.

La estrategia de seguridad se determina a partir de un análisis técnico donde se identifican los objetivos y posibles amenazas, midiendo a su vez las soluciones que sean más adecuadas a la organización.

Una amplitud de herramientas y servicios hoy en día se ofrecen para diversos usos en los sistemas y las tecnologías utilizadas por las organizaciones, quienes deberán cumplir con la tarea de garantizar cada nivel de seguridad dentro de la estrategia establecida, debemos considerar en nuestra organización asegurar que dichas estrategias cubran las necesidades más relevantes en seguridad, entre las más relevantes podemos enunciar los siguientes:

- Proyectos de Autenticación, asegurar los accesos remotos a los recursos corporativos.
- Implantación de Cortafuegos, segmentar las redes en diferentes dominios de seguridad.
- Seguridad en Aplicaciones WEB, utilización de cortafuegos con plenitud de asegurar las vulnerabilidades en el código de aplicaciones y de servidores Web, bloqueando así ataques a través del código de las aplicaciones.
- Proyectos de Autorización, Implementar sistemas de autorización que gestionen de forma centralizada los privilegios de acceso a los sistemas de información.
- Proyecto de Aseguramiento de Red Pública, establecer túneles cifrados para interconectar de forma segura los centros y delegaciones de una organización.
- Proyectos de Control de Contenidos, monitoreo y control de contenidos en aplicaciones de correo electrónico y acceso inapropiado a páginas Web.
- Compartir de Documentos en forma segura, repositorio gestionado que asegura la integridad y autenticidad de la información, soportado con normas y políticas establecidas en ocasiones con soporte legal al no repudio.
- Análisis de Vulnerabilidades, simulaciones de ataque con herramientas para determinar las vulnerabilidades en la red y el sistema operativo.
- Gestión de Ancho de Banda, implantación de soluciones que gestionen el tráfico para predecir rendimiento y efi-

ciencia para las aplicaciones que se ejecutan.

- Sistemas de Detección de Intrusos, sondas en la red para el reconocimiento de intrusos y ataques en tiempo real, así como detener las actividades no autorizadas.

- Balanceo de Cargas, soluciones de hardware para alta disponibilidad y balanceo de conexiones.

- Implementación de sistemas de gestión de certificados, diseño y mantenimiento en la utilización de la firma electrónica, implementar proyectos de PKI (Public Key Infraestructura) con ventajas para su uso y cifrado seguro e inmediato.

Hoy en día tras la evolución en las tecnologías de información y en puerta el uso de proyectos como la facturación electrónica, nos llevan a dedicar recursos y tiempo a gestionar nuestras medidas de seguridad en nuestros sistemas y verificar las tecnologías empleadas en nuestros procesos, por lo que es tan relevante considerarlo como parte de la protección misma de la organización.

ISC. José Gabriel Vilchis P.
Sub Director Corporativo de Sistemas y Comunicaciones.

ESTIMADO SOCIO

Cualquier comentario, observación o sugerencia a este Boletín, favor de hacerlo llegar directamente al autor.

ISC. José Gabriel Vilchis P.
Sub Director Corporativo de Sistemas y Comunicaciones.

e-mail: gvilchis@grupo-iamsa.com.mx