



Centro de Orientación de Seguridad

Microsoft

La seguridad es un proceso que se construye día a día

Quienes han estado en la industria de TI por algún tiempo, se han podido percatar de los cambios tan dramáticos que se han dado durante los últimos 10 años, especialmente en los campos relacionados con las soluciones de infraestructura y telecomunicaciones. En la década de los noventa, las inversiones en TI eran realizadas sin mayores objeciones o sin el soporte de análisis exhaustivos, simplemente las empresas debían estar a la vanguardia en su industria y eso era justificación suficiente para girar abultados cheques a los fabricantes de software y hardware, y a los proveedores de servicios. La cosa ha cambiado para bien. Hoy en día, no existe una inversión en TI que no sea sometida al más riguroso examen de Retorno Sobre la Inversión (ROI), o a un estudio de cómo optimizar el Costo Total de Propiedad (TCO) o inclusive a un análisis, aunque sea preliminar, de qué tan vulnerable será la compañía a amenazas en Internet con la adquisición de dicha solución.

Muchas personas ven la seguridad como algo nuevo, como una moda o una tendencia, y aunque si es algo nuevo, no puede catalogarse como una moda por varias razones. Anteriormente siempre se anteponía la funcionalidad a la seguridad, por ejemplo, cuando se establecieron los primeros protocolos que le dieron vida a Internet, nunca se construyeron pensando en la seguridad, eso vino después, dada la gran acogida que ésta tuvo y su indudable aplicación a los negocios. Así mismo sucedía con las soluciones y herramientas de TI, siempre se pensaba primero en la funcionalidad y luego en la seguridad. Sin embargo, la seguridad de la información difiere de las modas por que no es algo pasajero, no es algo que vaya a ser reemplazado por otra nueva moda; la seguridad es algo permanente y abarca cada vez nuevas esferas dentro de la industria de TI.

Constantemente los responsables de TI han querido sacarle el cuerpo a la seguridad por 3 grandes razones: primero que todo, nadie sabe realmente donde empieza y donde termina la seguridad dentro de TI, segundo, es una inversión que no va a generar un retorno inmediato, va a evitar ciertas pérdidas es verdad, pero no va a incrementar las ventas de la empresa y por último, y como resultado de las dos anteriores, no es una idea fácil de vender a la alta gerencia.



Cualquiera que sea la posición de la empresa ante la seguridad, es claro que la protección de sus activos de TI no puede entregarse enteramente a la funcionalidad de una serie de productos de seguridad (firewall, antivirus, sistemas de detección de intrusos, encriptación, etc.), la seguridad debe ser vista como una serie de procesos cuyo objetivo principal es el mejoramiento continuo de un Sistema de Gestión de Seguridad de la Información. A continuación me permitiré numerar 3 aspectos que deben ser reforzados antes de intentar implementar controles de seguridad y que ayudarán a sentar las bases para la construcción de una sólida estrategia de seguridad dentro de la organización.

El primer punto que debe ser tenido en cuenta cuando se pretende asegurar los activos de TI de la organización, es el compromiso de la alta gerencia hacia la seguridad. El enfoque que debemos tener es un enfoque de arriba hacia abajo (Top-Down Approach), en el cual siempre debemos tener tanto el respaldo, como el ejemplo de la alta gerencia. Si la alta gerencia entiende su rol y responsabilidad, también lo entenderán el resto de los empleados.

El siguiente punto en orden de importancia, es lograrle transmitir al todos los empleados que la seguridad no es responsabilidad de unos pocos, es responsabilidad de todos y como tal, todos los empleados están en la obligación, tanto proactivamente como reactivamente, de salvaguardar y proteger la información de la compañía. La forma más fácil de llegar a los empleados es a través de programas de concientización.

Por último, el tercer aspecto que debe ser considerado, es que tan bien definidos están los procedimientos y las políticas de seguridad dentro de la organización. Más allá de que también se encuentran configuradas las soluciones de seguridad, se deben establecer lineamientos claros de cómo espera la compañía que estas soluciones funcionen y bajo que criterios.

Como conclusión, la seguridad debe construirse como un proceso que tiende a mejorar continuamente y no como el resultado de una serie de soluciones de seguridad que posiblemente no son las adecuadas para la organización. Aunque muchos jefes de seguridad dentro de las organizaciones sigan pensando que la seguridad es una sensación, hoy en día existen los mecanismos para cuantificar el estado de la seguridad y definir los controles para alcanzar el riesgo aceptable.

En Microsoft tenemos recursos especialmente diseñados para que usted pueda gestionar de manera más efectiva la seguridad de la información de su organización.

Encuéntrelos en:

Microsoft Security Assessment Tool

<http://technet.microsoft.com/en-us/security/cc185712.aspx>

Microsoft Baseline Security Analyzer

<http://technet.microsoft.com/en-us/security/cc184924.aspx>