DRAFT

IT Consultores Diciembre, 2009

Políticas de seguridad TI: El factor humano

Muchas empresas han transformado rápidamente la forma en que prestan servicios a sus clientes mediante usos ingeniosos de las más avanzadas tecnologías de la información. Pero las ventajas de las TI para el negocio no dejan de tener un alto coste, como es la necesidad de proteger los sistemas de virus dañinos, brechas de datos accidentales o incluso ataques deliberados. Y, en las empresas de hoy, más globales y abiertas a socios y clientes, de las que, además, entran y salen continuamente portátiles u otros dispositivos móviles con información sensible, no hay forma de protección que no pase por el convencido compromiso de los empleados con la seguridad corporativa.

Las brechas pueden a menudo empezar de una manera muy personal. Por ejemplo, con un grupo de amigos tomando algo en una cafetería donde algún empleado vaya con su PC corporativo y decida utilizarlo para navegar o para enviar algún correo electrónico personal. La mayoría de nosotros estamos ya familiarizados con las soluciones tecnológicas que pretenden resolver estos problemas, como cortafuegos, contraseñas y certificados digitales.

Pero el componente tecnológico es sólo una parte de la solución, las políticas que soportan estos mecanismos resultan igualmente importante, y cuando de políticas se trata, resulta imprescindible el compromiso de los usuarios. De hecho, se está convirtiendo en algo vital para cualquier negocio global no sólo implementar una excelente política de seguridad, sino también priorizarla y comunicarla a los empleados de forma eficiente y significativa para ellos.

Una herramienta de protección vital

Según un sondeo llevado a cabo por Computing Technology Industry Association (CTIA) en Estados Unidos, casi el 40% de las firmas entrevistadas por la asociación habían reportado alguna brecha de seguridad TI importante durante los últimos seis meses. ¿Cuántas de ellas se podrían haber prevenido considerando el factor humano en el entorno de trabajo? Muchas tuvieron sus raíces en la pérdida accidental de un laptop, un Backberry o cualquier otro dispositivo móvil, en empleados utilizando redes no adecuadamente securizadas para trabajar desde sus casas, y en trabajadores que descargaron software "inapropiado" sobre la red de la compañía.

Una política de seguridad efectiva es, en pocas palabras, una herramienta de protección vital para cualquier tipo de empresa. Pero la paradoja reside en que, pese a su importancia, las políticas de seguridad a menudo no son seriamente consideradas por los gestores empresariales hasta que la organización ha sufrido algún incidente de seguridad importante. Cuando lo cierto es que la política más efectiva no es aquella que se desarrolla durante un momento de crisis, sino la que se construye, actualiza y comunica de manera continuada después de una revisión sistemática de las necesidades de seguridad corporativas.

¿Cuál es la forma de desarrollar las mejores políticas de seguridad? Las grandes compañías y aquellas que tienen más en juego han dedicado recursos significativos a estudiar este asunto. Por ejemplo, la firma de transporte rápido aéreo de paquetería FedEx, que invierte más de 1.000 millones de dólares anuales en TI, concede una importancia fundamental al desarrollo de una estrategia de seguridad TI sólida y consistente, que no sólo abarque y se geste en la sala de servidores, sino en la que también se impliquen sus ejecutivos de alto nivel.

FedEx entrega más de 3,3 millones de paquetes cada día laborable, así como la información asociada a cada uno de ellos a empleados y clientes que la soliciten. Para la compañía, "la información sobre el paquete es tan importante como el paquete mismo", en palabras de su cofundador Frederick W.Smith. Dado el a
lto nivel de penetración de las TI en esta organización, no es pues extraño que la seguridad de la información se haya convertido en una cuestión de máxima prioridad para FedEx.

El camino hacia una buena política

En una corporación global, la política de seguridad es más efectiva si está alineada con las estrategias de negocio corporativas tanto a nivel de sedes como de oficinas regionales, según Linda Brigance, CIO de la división de Asia-Pacífico de FedEx. De otro modo, pueden surgir problemas relacionados con la variación de los niveles de tolerancia al riesgo entre unidades de negocio y con las diferencias culturales entre las partes de negocio y legales de la operación.

Además, las políticas de seguridad también habrán de ser efectivas en costes y comunicadas constantemente. Cada persona dentro de la empresa, como se ha dicho ya, tendrá que ser responsable de la seguridad TI, no sólo el departamento de tecnologías de la información.

A continuación se incluye un listado que Brigance recomienda seguir para el correcto diseño, despliegue y comunicación de políticas de seguridad TI:

Paso 1: Conformidad legal

El primer paso imprescindible será analizar las áreas en las que la compañía pueda estar sujeta a obligaciones legales que la exijan la aplicación de políticas específicas. Cumplir las leyes relevantes al respecto será una garantía de que se tienen los controles adecuados en

funcionamiento antes de que la organización se vea sometida a auditorías o a tenga que luchar contra cualquier nueva amenaza a su seguridad.

Paso 2: Priorizar la información
Estudie la información utilizada en la toma de decisiones críticas relacionadas con la organización y sus clientes. Priorice la información que resulte más sensible o crítica para el negocio. Áreas obvias en este sentido incluirán la información financiera, los datos sobre clientes o la información corporativa en general, así como aquella que debe permanecer especialmente securizada, como es la relacionada con las tarjetas de crédito utilizadas para la facturación. También habrá de darse prioridad a los sistemas y datos sensibles utilizados por los propios clientes y proveedores.

Paso 3: Identificar los eslabones más débiles
Identifique los puntos más débiles de su organización. No olvide que las políticas que parecen más simples a menudo pueden tener consecuencias significativas. Un ejemplo podría ser la frecuencia establecida para los cambios de contraseñas. Contratar "hackers benignos" para que pongan a prueba sus recursos puede resultar muy útil cuando el propósito es identificar y valorar los puntos más vulnerables de la seguridad TI corporativa. Algunos de estos profesionales están capacitados para descubrir vulnerabilidades en cualquier área, incluidas el uso de nombres convencionales para datos sensibles o contraseñas débiles susceptibles de ser descubiertas con facilidad, por poner sólo un par de ejemplos.

Paso 4: Designe encargados de imposición de políticas
Elija a algunas personas encargadas de fomentar e imponer el cumplimiento de las políticas. Conviene que el grupo incluya profesionales externos al departamento TI, de las áreas legales, de recursos humanos, y de auditoría, además, por supuesto, de grupos de usuarios finales. Necesitará el apoyo de los ejecutivos senior para conseguirlo, y ellos, a su vez, tendrán que ser "educados" sobre la importancia de la seguridad de la información para el negocio y sobre los riesgos de no contar con una política fuerte y respetada por todos.

En el caso de FedEx, esta función es realizada por el grupo Enterprise Security Council, dirigido desde la sede corporativa de la organización en Estados Unidos. Además, en él participan representantes regionales de todo el mundo. El grupo realiza una evaluación y ampliación continua de las políticas de seguridad para asegurar que la información permanece siempre adecuadamente custodiada.

Paso 5: Defina un proceso claro y sencillo
Finalmente, decídase por un proceso de desarrollo claro y sencillo. Uno de los mayores errores cometidos por las empresas en este tipo de proyectos es intentar hacerlo todo de una vez, sin un período de gracia para la transición, y sin definir claramente los recursos que estarán dispuestas a dedicar. Plazos y expectativas irrazonables sólo provocarán la resistencia general al cambio.

La revisión y actualización de las políticas deberán convertirse en parte esencial de este proceso de desarrollo, dado que no pasa un día sin que surjan nuevas amenazas, sin que ello suponga que pueden olvidarse las más antiguas. Es esencial contar con políticas que circulen y sean claramente comprendidas a cada nivel y en todas y cada una de las divisiones corporativas. Sólo así las buenas prácticas en seguridad se convertirán en hábitos y su importancia dejará de ser cuestionada. Lograr que la gente comprenda y haga suyas unas buenas políticas de seguridad representa el mejor instrumento para conseguir una buena seguridad corporativa.

Este documento forma parte de nuestros programas de entrenamiento a manera de ayudarle a establecer un sistema de seguridad y control basado tanto en el soporte tecnológico, como en la <culturización> del recurso humano el cual es pieza clave o fundamental para el éxito de un programa de Seguridad en su Departamento de Tecnología de la información. Hace poco una nota en un medio de Internet decía: ... ""Hay una mentalidad global que tiene que ver con creer que los casos de brechas de seguridad y robo de información sólo suceden en la televisión", afirmó en entrevista el director de Investigación de la estadounidense, Bryan Sartin."" cnnexpansion.com Dic/16/2008. No vea este tópico como un costo, No lo vea como algo ajeno o lejano a sus bienes confidenciales que maneja en su sistema informático; Hoy el cibercriminal ya no es un tipo solitario aislado en algún cuarto en alguna parte del mundo, no Señor; Es crimen organizado cuyo blanco o target ES cualquier sistema conectado, esté donde esté geográficamente hablando.

Un término ahora usado comunmente en el ambiente de seguridad en tecnologías de la Información es: "Out in the wild"; es decir: "Afuera en la Jungla" para referirse al espacio global en el cual se mueve Su Información. Precisamente porque ahora es nuestra obligación extender nuestros esquemas de seguridad ya no a nuestro mundo real cada día mas inestable socialmente hablando sino a la comunidad mundial que es Internet, en la cual el delincuente puede ser cualquier tipo en cualquier parte del planeta tocando a su puerta .

Mil gracias por su visita!!

La Seguridad no es solo un proceso tecnológico.... es un proceso organizacional!

2da Calle, 2da etapa No. 37, Jardines del Valle, 504- 544-0334 504-9840-1996
www.econsultores.biz ** email: helpdesk@econsultores.biz**