Cinco tips para el diseño de políticas

Yolanda Robles: http://bsecure.com.mx/autores.php?id_autor=52

Fuente: http://bsecure.com.mx/articulo-64-6622-380.html

Jorge, diseñador gráfico, trabaja para una de las empresas editoriales más grandes del país. Al momento de ingresar a la organización, le hicieron firmar una serie de documentos en los que le explicaban los mecanismos de seguridad internos. Durante todo el tiempo que ha laborado ahí, oficiales verifican su equipo de cómputo al acceder y salir de las instalaciones. Seis meses después de haber dejado de prestar sus servicios en dicha institución, Jorge ya no puede ingresar a las oficinas… sin embargo, aún conserva los permisos para acceder al sistema en Internet desde el cual el equipo de redacción puede subir y actualizar notas, agregar o modificar imágenes, y mucho más. Si Jorge tuviera intenciones maliciosas, la editorial en cuestión hace mucho tiempo que se habría visto en serios problemas.

Éste es uno de los casos que ejemplifican cómo la mejor de las estrategias de seguridad de la información puede ser vulnerable por una pequeña omisión en los procesos, por no seguir una simple política o por la falta de las mismas. A final de cuentas, como se explica en el sitio del Instituto Nacional de Estándares y Tecnologías de Estados Unidos (NIST, por sus siglas en inglés), “el administrador de seguridad es responsable de habilitar las políticas y debe tener la capacidad para controlar y mantener, de manera centralizada, los permisos de acceso”.

Es claro que en dicha editorial no existe un lineamiento que lleve al departamento de Recursos Humanos a notificar al responsable de los accesos sobre la baja de empleados para que sean eliminados sus permisos. O, si existe tal procedimiento, no se está llevando a cabo.

En una editorial tan grande, la rotación de empleados es muy fuerte. Por ende, el número de oportunidades que se están dejando a la buena voluntad de los ex empleados, es enorme. ¿Puede su empresa darse el lujo de correr con un riesgo similar? En la mayoría de los casos, la respuesta será no.

Más allá de la protección tecnológica, es necesario normar los procesos y procedimientos de la organización para minimizar lo más posible las vulnerabilidades. De nada sirve el mejor equipo de hardware, robustecido con las aplicaciones de seguridad más recientes, si con el tiempo no se actualizan o si, de entrada, no se modifica la contraseña de fábrica de los equipos.

En este sentido, las políticas de seguridad informática surgen como una herramienta organizacional para concientizar a los colaboradores de la organización sobre la importancia y sensibilidad de la información y servicios críticos que permiten a la empresa crecer y mantenerse competitiva.

Proponer o identificar una política de seguridad requiere un alto compromiso con la organización, agudeza técnica para establecer fallas y debilidades, y constancia para renovar y actualizar dicha política en función del dinámico ambiente que rodea las organizaciones modernas.

Pero, ¿cómo diseñar políticas que sean lo suficientemente claras, prácticas y flexibles para minimizar en la mayor medida posible los riesgos operativos?

Tip #1: Entendimiento

Lo primero que hay que hacer es entender que una política de seguridad informática es una forma de comunicarse con los usuarios, ya que las mismas establecen un canal formal de actuación del personal, en relación con los recursos y servicios informáticos de la organización.

Diversas fuentes de seguridad informática explican que no se puede considerar una política como una descripción técnica de mecanismos, ni una expresión legal que involucre sanciones a conductas de los empleados, "es más bien una descripción de lo que deseamos proteger y él por qué de ello, pues cada política de seguridad es una invitación a cada uno de sus miembros a reconocer la información como uno de sus principales activos así como un motor de intercambio y desarrollo en el ámbito de sus negocios", expone el sitio Monografías.com.

Un adecuado diseño de políticas debe considerar elementos como el alcance de las políticas (instalaciones, sistemas y personal sobre los que aplican); objetivos de la política y descripción clara de los elementos involucrados en su definición; responsabilidades por cada uno de los servicios y recursos informáticos aplicado a todos los niveles de la organización; requerimientos mínimos para configuración de la seguridad de los sistemas que abarca el alcance de la política; definición de violaciones y sanciones por no cumplir con las políticas, y responsabilidades de los usuarios con respecto a la información a la que tiene acceso.

Para asegurar su entendimiento, las políticas deben redactarse en un lenguaje sencillo y claro, libre de tecnicismos y términos ambiguos que impidan la comprensión de las mismas.

Tip #2: Estructura

Una vez que se ha entendido qué son las políticas y cuál es su objetivo, es momento de esbozar los lineamientos que normarán el comportamiento de los empleados así como los procedimientos de una organización.

Es importante que al momento de formular las políticas de seguridad informática, se consideren los siguientes aspectos:

- Efectuar un análisis de riesgos informáticos, para valorar los activos y así adecuar las políticas a la realidad de la empresa.

- Reunirse con los departamentos dueños de los recursos, ya que ellos poseen la experiencia y son la principal fuente para establecer el alcance y definir las violaciones a las políticas.
- Comunicar a todo el personal involucrado sobre el desarrollo de las políticas, incluyendo los beneficios y riesgos relacionados con los recursos y bienes, y sus elementos de seguridad.
- Identificar quién tiene la autoridad para tomar decisiones en cada departamento, pues son ellos los interesados en salvaguardar los activos críticos de su área.
- Monitorear periódicamente los procedimientos y operaciones de la empresa, de forma tal que las políticas puedan actualizarse oportunamente, de ser necesario.
- Detallar explícita y concretamente el alcance de las políticas con el propósito de evitar situaciones de tensión al momento de establecer los mecanismos de seguridad que respondan a las políticas trazadas.

Tip #3: Apego a estándares

De acuerdo con el NIST, el desarrollo de las políticas se deriva de la legislación existente, la ética, las regulaciones o las prácticas comúnmente aceptadas. Para garantizar la viabilidad y la correcta aplicación de las políticas, es necesario apegarse a lo que se ha determinado por estándares internacionales, como el ISO 17799.

Una política se suele dividir en puntos más concretos a veces llamados normativas. Y en este sentido, en términos de seguridad de la información, el ISO 17799 agrupa las siguientes líneas de actuación:

Seguridad organizacional (aspectos relativos a la gestión de la seguridad dentro de la organización):

- Clasificación y control de activos
- Seguridad del personal
- Seguridad física y del entorno
- Gestión de comunicaciones y operaciones
- Controles de acceso
- Desarrollo y mantenimiento de sistemas
- Gestión de continuidad de negocio
- Requisitos legales

Evidentemente, una política ha de cumplir con la normativa vigente en el país donde se aplica; si una organización se extiende a lo largo de diferentes países, su política tiene que ser coherente con la normativa del más restrictivo de ellos. En este apartado de la política se establecen las relaciones con cada ley: derechos de propiedad intelectual, tratamiento de datos de carácter personal, exportación de cifrado... junto a todos los

aspectos relacionados con registros de eventos en los recursos (logs) y su mantenimiento.

Tip #4: Validación por parte de la alta gerencia

La política de seguridad es un documento de alto nivel que denota el compromiso de la gerencia con la seguridad de la información. Contiene la definición de la seguridad de la información bajo el punto de vista de cierta entidad.

En caso de que hasta este momento la alta dirección no se haya involucrado más allá del encargo inicial de establecer las políticas, es momento de hacer que tomen parte. La retroalimentación y aprobación de estos lineamientos por parte de los directivos permitirán la correcta implementación de las políticas así como una adecuada y oportuna aplicación de las sanciones, en caso de requerirse así.

Si bien muchas iniciativas de seguridad son impulsadas por la misma gente de sistemas, regulaciones como las que se han emitido en Estados Unidos (como The Government Information Security Reform Act), establecen como obligatorio que las compañías tengan procedimientos para detección, reporteo y respuesta de incidentes de seguridad informática.

Tip#5: Implementación y ajustes

Si ya se han estructurado lineamientos con apego a estándares, con base en los requerimientos del negocio y con la aprobación de la alta dirección, es momento de dar a conocer las políticas e implementarlas en los procesos y procedimientos de la organización.
Es importante una buena estrategia de difusión de las políticas para garantizar que los empleados las entienden y las ponen por obra, estando conscientes de que una omisión en las políticas puede acarrearles una sanción o hasta el despido.

Por último, pero no menos importante, es el hecho de que las políticas de seguridad deben seguir un proceso de actualización periódica sujeto a los cambios organizacionales relevantes, como son: el aumento de personal, cambios en la infraestructura de cómputo, alta rotación de personal, desarrollo de nuevos servicios, regionalización de la empresa, cambio o diversificación del área de negocios, etcétera.

Siempre que una política ya no se ajuste al entorno, es hora de revisarla y modificarla. Una vez realizado el ajuste, es necesario difundirlo entre los empleados para asegurarse de que no existan huecos de seguridad por ignorancia o negligencia.