Wayne O Evans Consulting, Inc.

400 Security Training and Consulting

Implementando Políticas de Seguridad

La seguridad y , en especial, las políticas de Seguridad están ahora tomando un mayor peso específico en la empresa y han dejado de ser consideradas un reto sólo para el Dpto. de Tecnologías de la Información. Los sistemasAS400 siempre han estado considerados un sistema muy seguro , pero esto ahora no es bastante– los responsables de TI tienen que probar que disponen de una política definida, y que la configuración de sus sistemas AS400 está conforme a ella.

Más del 60% de las instalaciones con AS/400 no disponen de una política de seguridad, siendo ésta la cuestión que más veces aparece durante una auditoría de seguridad. A menudo las organizaciones disponen de una política de seguridad porque así lo exigen algunas entidades reguladoras . La política de seguridad se crea entonces para encajar con esos requisitos y sólo sirve para almacenar el polvo encima de ella. No existen datos actualizados para medir la efectividad de la política de seguridad pero sospecho que menos del 10% de las organizaciones con AS/400 disponen de una política de seguridad que sea un documento utilizado como parte de las decisiones diarias acerca de la seguridad. Este artículo describe el proceso que puede hacer de tu documento de política de seguridad una herramienta útil en vez de ese documento que atrae el polvo.

Gestión de la Política de Seguridad Informática

Para asegurar que los sistemas informáticos son usados de forma efectiva y productiva, los propietarios, operadores y usuarios de estos sistemas deben conocer de forma clara los estándares aceptados para el uso de las computadoras.Una política de Seguridad Informática proporciona esta pauta en la gestión para los usuarios , los implementadores del sistema y responsables de seguridad.

Por qué es esencial una Política de Seguridad para las Computadoras

A menudo la dirección asigna a un individuo la tarea de responsable de seguridad del AS400 sin ninguna otra directriz que "mantenga el sistema seguro". La Dirección nunca le pediría a un programador : " Escriba un programa " sin más detalles , pues los resultados serían impredecibles.Los programadores reciben detalladas especificaciones del input y output esperado cuando se crea una nueva aplicación.De forma similar el responsable de seguridad necesita conocer los requisitos de su trabajo. Una política de seguridad para las computadoras le proporciona al responsable de seguridad los requisitos para ese trabajo.

Un segundo beneficio de la política de seguridad es que elimina la necesidad del responsable de seguridad de tener que justificar el porqué se han implementado controles específicos. Con demasiada frecuencia sus usuarios retan las decisiones del responsable de seguridad. Si el responsable de seguridad puede referirse a una determinada política de seguridad informática y decir " Yo simplemente estoy implementando lo que la Dirección ha solicitado , si no estais de acuerdo, pedir entonces que la política de seguridad de cambie ", se ahorra tiempo de discusiones sobre los méritos de determinados controles del AS400. La política de seguridad para las computadoras ahorra tiempo y esfuerzos para justificar la puesta en funcionamiento de decisiones sobre la seguridad.

5677 West Circle Z Street
Tucson, AZ 85713-4416
E-mail: WOEvans@aol.com

Phone (520)-578-7785
Fax (520)-578-7786

Si no existe una política de seguridad escrita, los responsables de seguridad configurarán los parámetros de seguridad según sus propias sensaciones acerca de la seguridad. Como sea, la racionalidad que se encuentre en estas configuraciones a menudo no queda documentada. Un nuevo responsable de seguridad que apele a esas "decisiones racionales" está perdido . Una política de seguridad documenta el motivo para las decisiones de seguridad asegurando así una implementación más consistente de la seguridad en casos de cambios en el responsable de seguridad.

Las acciones que se aceptan de los usuarios de Pcs necesitan ser documentadas y explicadas a los usuarios. Cuando no existe una política escrita , los individuos con frecuencia interpretan lo que es aceptable de diferentes maneras. La política de seguridad informática necesitada estar bien detallada. Una política de seguridad como " Las computadoras no pueden ser usadas para uso personal " necesita ser explicada. Lo que es uso personal podría ser interpretado de formas diferentes.Una política de seguridad provee directrices en temas tan específicos como la postura de la Dirección respecto a :

- Descargar y contemplar pornografía.
- Envío y recepción de chistes (correspondencia no esencialmente del negocio)
- Mirar cotizaciones de precios de acciones
- Envío y recepción de e-mails personales
- Uso de las computadoras para hacer compras online durante las pausas del trabajo.

Una política de seguridad informática da a los usuarios un conocimiento claro de las actividades que les están permitidas. Si un trabajador debe ser despedido por acciones inapropiadas, una política de seguridad que ha sido comunicada a los usuarios de las computadoras también ahorrará tiempo en disputas legales.

Pasos esenciales en la Gestión de la Política de Seguridad

Este artículo detalla los pasos para desarrollar una Política de Seguridad Informática que se usará para las decisiones diarias de seguridad.

PASO 1: Obtener el apoyo de la Dirección

La Dirección tiene la responsabilidad última en la política de seguridad.La Dirección tiene la responsabilidad de definir la política de seguridad aunque debe delegar la mayoría del trabajo y debería ser la propietaria del documento de política de seguridad.

Antes de empezar en el proyecto de la política de seguridad, hay que conseguir el apoyo de la Dirección para la financiación, adecuación y aplicación de la política de seguridad informática. La Dirección necesitará por su parte, comprender el tiempo y los costes que requerirán la creación y mantenimiento de la política de seguridad. Yo recomiendo facilitar a la Dirección una copia de este artículo como el paso necesario para informarles.

PASO 2: Iniciar la investigación y buscar un modelo de Política de Seguridad a copiar.

Existe un dicho sobre que un buen programa nunca se escribe . Los buenos programas copian a otros buenos programas. La habilidad de un programador no está en su efectividad escribiendo código sino en cómo incorpora satisfactoriamente las mejores rutinas de otros programas para construir una aplicación útil. Lo mismo ocurre con un documento de política de seguridad.Unos buenos documentos de política de seguridad no se escriben sino que se copian de otros documentos de política de seguridad.
En tu búsqueda para crear un documento útil para la política de seguridad , uno de los primeros lugares para empezar es en Internet. Simplemente introduciendo las palabras de búsqueda "Security Policy" (" Política de Seguridad") obtendrás suficiente información para varios días de lectura. Existen también web sites que te asesoraran en la creación de un documento de política de seguridad. Uno de gran utilidad es *http://www.baselinesoft.com/ que describe el libro* "**Information Security Policies Made Easy"** por Charles Cresson Wood. Este libro tiene "las mejores prácticas" tomadas de los documentos de seguridad de varias compañías. El website ofrece un kit que incluye una copia del libro, CD ROM y una licencia amplia por organización para reproducir estos materiales y puede pedirse por $795. Navegando por Internet encontrarás otros vendedores de plantillas de documentos de política de seguridad. Yo recomiendo utilizar un mismo modelo estilo "las mejores prácticas" para escribir el propio documento de seguridad.

PASO 3: Escribir la Política de Seguridad

Un documento modelo de las prácticas de seguridad es la mayor ayuda pues provee del vocabulario y de las áreas de interés más importantes de tu política de seguridad. Al menos deberás personalizar el documento para que se adecúe a los requisitos de seguridad de tu instalación. Los requisitos de seguridad de la informática y computadoras propiedad y uso de una organización diferirán de los requisitos de otra organización. Es por eso importante que cada organización formule su propia política de Seguridad.

Al empezar a escribir la política de seguridad hay que considerar cómo organizar la información para que los lectores puedan centrarse en las diferentes partes de la Política de Seguridad. Una de las formas de organización que encuentro útil es distinguir tres categorías de información . Les he dado nombres a cada una de estas categorías .

> Políticas de Seguridad Corporativa. son las declaraciones fundamentales sobre la filosofía del negocio las cuales forman las bases para las políticas específicas de máquinas y humanos. Son a menudo 10 mandamientos o verdades universales . Las declaraciones de la política a este alto nivel serían del estilo:
>
> - Respeto a los individuos
> - Servicio los clientes
> - Proteger los activos de la empresa
> - Honestidad e Integridad en las acciones.

Estas políticas de negocio fundamentales necesitan ser detalladas en declaraciones más específicas de política de seguridad. El modelo de documentación al estilo " las mejoras prácticas" es muy útil en el detalle de esta información.

Estándares de Seguridad Informática son una expresión de las políticas corporativas de seguridad para unas plataformas informáticas específicas. En el AS/400 estas deben ser declaraciones como :

- El valor de sistema QSECURITY debe ser 40
- La longitud mínima del password QPWDMINLEN debe ser 6
- El acceso a la línea de comandos debe estar prevenido contra usuarios finales.
- El perfil de usuario para la clase de usuario USER debe ser LMTCPB**(**YES)
- Los ficheros inactivos deben ser desabilitados después de 31 días.

Con frecuencia , las organizaciones completan los estándares de seguridad informática y consideran que eso ya es una política de seguridad.
Esto es sólo parte de las consideraciones de seguridad.

Guías para el usuario de computadoras. les dan a los usuarios instrucciones sobre cómo realizar las actividades del negocio de una forma segura. En la sección de guía a los usuarios se recomiendan prácticas como

- No de su password a otros.
- No instale programas personales en su computadora.
- Programas antivirus para el PC deben estar instalados y ejecutarse en todas las computadoras personales.

PASO 4: Aprobación de la Política de Seguridad

Después de que esté escrita la política de seguridad informática, la revisión de la Dirección provocará probablemente algunos cambios para afinar la política con las necesidades de la organización. Las políticas generales de alto nivel son fáciles de acordar pero en su detalles es normal que aparezcan diferencias de opinión. Recursos Humanos, Sistemas de Información, Asesoría legal y los Representantes de los Trabajadores deberían participar en la revisión del documento de seguridad. Muchos de los comentarios individuales de las áreas pueden incorporarse pero una reunión para la revisión final debería celebrarse para ayudar a resolver cualquier postura respecto las cuestiones de esa política. Una vez resueltas estas cuestiones, el documento final de seguridad debería ser enviado a todas las áreas que deban aprobarlo.

PASO 5: Comunicación de la Política de Seguridad

Hay un último e importante paso después de que se haya aprobado la política de seguridad. Esta política de seguridad debe comunicarse al usuario y a los implementadores de sistemas informáticos. Por desgracia, demasiadas organizaciones fallan en este último paso tan

importante.Una política de seguridad sólo es útil si esta política guía y ayuda a los usuarios en sus tareas diarias. Muchos proyectos para concienciar de la seguridad informática distribuyen la política de seguridad a través del website corporativo o en copia de papel. Hay que reconocer que las personas están ocupadas y no tienen tiempo para leer documentos de política de seguridad con múltiples páginas. Los proyectos de más éxito crean un boletín mensual sobre la preocupación de la seguridad con una página que se centra en una tema en concreto.

Software para la Política de Seguridad

El proceso de crear la documentación y administrar la política de seguridad informática puede ser una tarea muy intensa.. El software "Policy Center " de la compañía Pentasafe puede automatizar y simplificar muchos de los pasos de la política. La eliminación de tareas repetitivas le permite al administrador disponer del tiempo para centrarse en la creación de la política y la comunicación a la comunidad de usuarios. El "Policy Center" es un software que corre en un PC con Windows 98/2000/NT/ME). El centro de administración donde se archiva la información de los usuarios debe de disponer de Windows NT o 2000 para el archivo de la base de datos de la política de seguridad.
El software " Policy Center" te ayuda en todas las fases de la definición y gestión de la Política de Seguridad Informática.
"Policy center" tienes los siguientes servicios.

- Creación y Modificación de la Política: Documentos y declaraciones pueden crearse o copiarse de la documentación existente. La "**Policy Library" o Biblioteca de Políticas** está incluida como parte de Policy Center e incluye Information Security Policies Made Easy V.7 creado por Charles Cresson Wood, experto en seguridad líder en el sector. Ejemplos de documentos de seguridad pueden ser usados como punto de partida para tu propia política de seguridad. Definiciones ya existentes pueden copiarse y modificarse para cumplir con los requisitos de tu organización.
- Aprobación de la Política: El software "Policy center" gestiona el documento de seguridad en todas sus fases : borrador, revisión, aprobación, publicación y archivo. Mientras la política de seguridad se está gestando, será marcada con status *Borrador* (Draft) .Después que la política está completa , puede ser movida al status *Revisión (*Review) y enviada a los supervisores adecuados. Actualizaciones pueden incorporarse al documento y el documento final enviarse a los que deben aprobarlo. Las aprobaciones de las revisiones son monitorizadas y así cuando se han recibido todas , el documento de seguridad es movido al status *Aprobado* Approved. El estado del documento cambia a *Publicado* (Published) después que la política de seguridad es colocada en el web site corporativo y se envía una nota de aviso a los usuarios del sistema. Finalmente se moverá al status de *Archivo* (Archive) a efectos de su backup.
- Comunicación de la Política y Educación de los Usuarios.: El "Policy center" no sólo notifica a los usuarios de los documentos publicados sobre seguridad. El administrador de la política puede crear cuestionarios y publicarlos para la comunidad de usuarios. El cuestionario es útil para asegurar que los usuarios además de haber leído la política de seguridad también la entienden. Los resultados

del cuestionario pueden utilizarse para detectar a aquellos usuarios en los que hay que centrar esfuerzos para que comprendan la política.

- Informe de incidencias de violación: El "policy center" incluye un módulo opcional que puede utilizarse para informar y monitorizar de incidentes en la seguridad. Los usuarios disponen de un formulario donde reportar actividades sospechosas. Ese informe es enviado al administrador de la política. Dicho administrador puede decidir si el incidente necesita o no de un seguimiento. El software "Policy Center" puede usarse para enviar incidentes determinados a los responsables si estas incidencias necesitan un seguimiento.

La biblioteca de políticas del software "Policy Center" contiene " las mejores prácticas" generales de Charles Cresson Wood. Es un producto excelente pero PentaSafe planea mejorar el software Policy Center en próximas versiones al extender el soporte a una más estrecha integración de la política de seguridad con configuraciones conocidas del AS/400 . Políticas de seguridad específicas para la plataforma AS/400 se preve que harán el soporte más aplicable para el responsable de seguridad del AS/400.

Conclusión

Disponer de una política de seguridad es importante pero hacer de la política de seguridad una parte del entorno de trabajo diario es esencial. La comunicación con los usuarios del sistema es la clave para hacer que esa política sea efectiva. El software para la gestión de políticas automatiza la tarea de comunicación a los usuarios de los cambios de la política de seguridad . La posibilidad de cuestionarios puede usarse para hacer una rápido test y asegurar que los usuarios han entendido además de leído esa política.