InnOvaciOnes de NegOciOs 4(2): 357 - 376, 2007

Soluciones administrativas y técnicas para proteger los recursos computacionales de personal interno-insiders (Administrative and technical solutions to protect

Pérez, M. T. & M. A. Palomo
UANL, San Nicolás de los Garza, N.L., 66450, México, mtperez@mail.ur.mx

Key words: Administrative solutions, computational security, culture of security, protection tools, technical solutions

Abstract. Nowadays the organizations know that the computational security in logical, physical, environment security of hardware, software, process of business, data bases, telecommunications, butt in other, are essential not solely for the continuity of the daily operations of the businesses, but also to obtain strategic advantages. If the organization does not worry to place policies of computational security, that does not have control computational security, that does not invest in protection tools, does not update itself in the new problems of internal attacks and that a culture in computational security does not foment, among other aspects, more likely this in a high risk of which some computational resource can be affected by internal personnel and in consequence part or all the Business can let operate. It is necessary to remember that the internal personnel of the areas of information technology or systems intentional business or not intentionally they can damage the computational resources since they have knowledge of the vulnerabilities that have the computational resources. I am made east summary with the purpose of which the people who read it have This paper has the aim to create a TI Resources Security Culture and to present some administrative and technical elements to protect the computational resources of from internal-insiders personnel.

Palabras claves: Cultura de seguridad, herramientas de protección, seguridad computacional, soluciones administrativas, soluciones técnicas

Resumen. Hoy en día las organizaciones aceptan que los controles en seguridad computacional – lógica, física y ambiental en hardware, software, procesos de negocio, bases de datos, telecomunicaciones, entre otros - son esenciales para darle continuidad a las operaciones diarias de los negocios, así como y también para obtener ventajas

Soluciones administrativas

estratégicas. Una organización que no se preocupa por aplicar políticas de seguridad computacional, establecer controles de seguridad, invertir en herramientas de protección, actualizarse en los nuevos problemas de ataques internos fomentar una cultura en seguridad computacional, etcétera, tiene mayor probabilidad de correr un alto riesgo, porque algún recurso computacional puede ser afectado por personal interno y en consecuencia una parte o todo el negocio puede dejar de operar, trayendo como consecuencia que la imagen de éste pueda ser dañada y que sus clientes pierdan la confianza. Hay que recordar que el personal interno de las áreas de tecnología de información o sistemas pueden dañar los recursos computacionales ya que ellos poseen conocimiento de las vulnerabilidades que poseen éstos últimos; también los usuarios de las diferentes áreas de forma intencional o no pueden también hacer daño. Por lo anterior, se proponen presentan en este artículo la implementación de una Cultura en Seguridad Computacional, así como soluciones administrativas y técnicas con la finalidad de disminuir los riesgos computacionales contra ataques internos.

Introducción

Las organizaciones invierten en seguridad computacional del 4% al 10% del total del gasto informático (Ernst & Young, 2001) (http//www.ey.com / "Encuesta de Seguridad Informática en Tecnologías 2001"). Este porcentaje, se destina por lo regular en la contratación de personal técnico altamente competente; éste a su vez compra e implementa "firewalls" – software para proteger redes -, software para la administración de cuentas de usuario, software antivirus, escaneo de correo electrónico, software para encriptar datos, seguridad inalámbrica, tarjetas inteligentes y en otras tecnologías avanzadas de seguridad. Pero las pérdidas siguen aumentando, causadas por por virus, caballos de troya, gusanos, caídas de telecomunicaciones, salidas de operación de la empresa por problemas de hardware, fallas en los sistemas aplicativos, los errores humanos, entre otros problemas siguen aumentando. Así lo señaló la encuesta de Ernst & Young de Octubre del 2003 (Ernst & Young, 2003) http//www.ey.com/global/Content.nsf/Mexico/Perspectivas_Seguridad_Informatica_1003_eyMexico.

Cabe señalar que hay dos tipos de individuos que pueden alterar los esquemas de seguridad en las organizaciones: personas externas y personas internas. Las primeras son los Hackers, (script kiddies, crackers, coders, old school hackers, entre otros); las segundas son conocidas en el mundo de la seguridad computacional como INSIDERS y se dedican especialmente a alterar los recursos computacionales desde el interior.

Hacker
Pirata cibernético

El término “hacker” ha cambiado en los últimos años, ahora se utiliza para referir a personas externas que pueden romper los esquemas de seguridad en los sistemas informáticos sin tener autoridad. Además pueden transmitir virus, robar información, dañar bases de datos, entre otros ataques, y esto lo hacen algunas veces como diversión.

Macleod (2007) comenta que los hackers se pueden clasificar en cuatro distintos grupos:

1. Script kiddies. Principalmente son personas jóvenes, quienes descargan scipts preescritos y son precompilados llamados ¨hacks¨, y se dedican a hacer vandalismo o destrucción de sistemas.
2. Crakers. Son criminales profesionales organizados en grupos, quienes hacen su forma de vida violando los sistemas computacionales y venden la información obtenida.
3. Coders. Son escritores de virus que se consideran parte de una comunidad poderosa.
4. Old school hackers. Tienden a verse así mismos como hackers en el sentido original de la palabra, a través de una broma inteligente “strip” obtienen el acceso a una parte de la tecnología computacional y llevan a cabo una tarea para la cual nunca fue diseñada o bien logran sobrepasar los límites de diseño.

Insider
Intruso

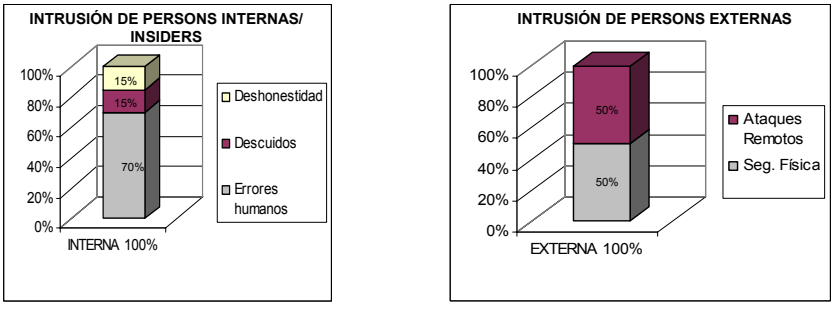
Se considera Intruso Interno o Insider a “Es cualquier persona que tiene un conocimiento detallado de las operaciones y procesos internos, o se le confían accesos privilegiados a recursos de la red o información sensible. El término “INSIDER” también es definido como personal que trabaja en la empresa cubriendo medio turno o turno completo”. (Steele & Wargo, 2007 p. 23).

Vista Research estima que el 70% de las violaciones de seguridad que involucran pérdidas de más de $100,000 dólares son perpetrados

internamente por empleados desleales o colaboradores resentidos , o también llamados INSIDERS. Asimismo, señala que un estudio elaborado por el Computer Security Institute y el FBI en conjunto reveló que las pérdidas promedio causadas por un ataque interno contra una compañía ascienden a 2.7 millones de dólares, mientras que un ataque externo causa pérdidas promediadas en $57,000 dólares. Por lo anterior, se puede pensar que las organizaciones se preocupan más por los ataques externos que los internos, pero los externos aquellos, a pesar del impacto que causan a la opinión pública, no resultan tan caros como se piensa. Con base en los antecedentes anteriores se analiza a los usuarios internos –INSIDERS / INTRUSOS y se proponen posibles soluciones administrativas y técnicas con la finalidad de disminuir los riesgos de ataques.

El estudio de Segu-Info (2007) señala que del 100% de la intrusión-amenaza, el 70% es generada por personal interno y el 30% por personal externo;, así mismo, el estudio revela que de ese 70% de intrusión interna el 70% se debe a errores humanos, 15% a descuidos y el otro 15% a personal deshonesto. Sin embargo, en el caso de la intrusión externa, el estudio la intrusión externa reveló que 50% se debió a problemas de seguridad física y el otro 50% fueron a causa de ataques remotos (Figura 1).

A continuación se muestra la gráfica.



Fuente: www.segu-info.com.ar 2007 - 17

Figura 1. Relación de la intrusión externa e interna.

Entonces, ¿por qué a las organizaciones les sale más caro los ataques internos? ¿Por qué frecuentemente el personal responsable de la seguridad computacional tiene que tratar con problemas causados por usuarios? Éstos abren correos electrónicos con virus que han sido replicados a través

de la red, malas conductas del personal, falta de pruebas al software antes de liberarse al ambiente productivo, olvidarse de respaldar archivos críticos, utilizar contraseñas débiles, pérdida de computadoras portátiles con datos confidenciales, no tener buenas técnicas de respaldos de datos, o ser engañados y convencidos a dar su contraseña a través de cualquier técnica de ingeniería social, entre otras situaciones.

Para minimizar el riesgo de que los INSIDERS puedan dañar, con intención o sin ella, los recursos computacionales en las organizaciones, se proponen dos tipos de soluciones: Soluciones Administrativas y Soluciones Técnicas. Éstas alternativas se deben soportar con una buena contratación de personal, educación, capacitación y cambio de cultura acerca de la concientización en seguridad computacional.

Soluciones administrativas

De acuerdo al Certifed Information Security Management, Information Systems Audit and Control Association (CISM REVIEW MANUAL, 2006). Las organizaciones deben definir, elaborar, implementar y darle seguimiento a las Políticas y Procedimientos relacionados a la Seguridad de Información. Las Políticas y Procedimientos son documentos oficiales y formales donde se dictan las reglas de seguridad computacional que la empresa quiere seguir y las obligaciones que tienen los usuarios al utilizar los recursos computacionales de la empresa donde estén trabajando. También los socios de negocios como son los proveedores, clientes, acreedores, prestadores de servicios, entre otros, se tendrán que alinear a las políticas de seguridad que esté manejando la empresa.

Hay tres consideraciones fundamentales que se deben de tomar en cuenta para implantar con éxito las Políticas y Procedimientos: En primer lugar, Primera, es necesario que éstos documentos sean aprobados por personal directivo del más alto nivel organizacional para asegurar su cumplimiento; , segundo a, que sean asignados recursos humanos para que monitoreen su cumplimiento y tercero a, es indispensable que se realicen revisiones periódicas con la finalidad de que siempre se tengan actualizadas y acordes con la situación real de la empresa y en el entorno tecnológico, tanto de hardware, software, telecomunicaciones, bases de datos, sistemas aplicativos, entre otros aspectos.

Políticas y procedimientos de seguridad computacional

Sean Steele & Chris Wargo (2007). Comentan que el desarrollar una adecuada política de seguridad es un proceso relativamente claro o preciso, pero es frecuentemente pasado por alto o no tomado seriamente. Tal vez porque es demasiado preciso las organizaciones tienden a no dedicar suficiente esfuerzo en el proceso.

Las políticas son documentos oficiales y formales de reglas para que los usuarios puedan tener acceso a todos los recursos computacionales. El plan para elaborarlas debe ser un proyecto que desarrolle los objetivos de seguridad computacional a largo, mediano y corto plazo de la organización, siguiendo el ciclo de vida completo desde la definición hasta la implementación, revisión y actualización.

La forma adecuada para diseñar la planeación de la seguridad en una organización debe partir siempre de la definición de Políticas que éstas definen: el **QUÉ** se quiere hacer en materia de seguridad computacional, para que a partir de ella se decida - mediante un adecuado plan de implementación - el **CÓMO** se alcanzarán en la práctica los objetivos fijados.

Las Políticas englobarán los objetivos, conductas, normas y métodos de actuación y distribución de responsabilidades y actuarán como documento de requisitos para la implementación de los mecanismos de seguridad computacional.

A partir de las Políticas seleccionadas se podrá definir el plan de implementación, que es muy dependiente de las decisiones tomadas en ella, en el que se contemplará: el estudio de soluciones, la selección de herramientas, la asignación de recursos y el estudio de viabilidad. Hay dos cuestiones fundamentales que deben tenerse en cuenta para implantar con éxito éstas: Es necesario que las políticas sean aprobadas para que esté respaldada por la autoridad necesaria que asegure su cumplimiento y la asignación de recursos y, es obligatorio, que se realicen revisiones periódicas que la mantengan siempre actualizada y acorde con la situación real del entorno.

Las políticas y el plan de implementación (y la implantación propiamente dicha) están íntimamente relacionados: las primeras definen el plan de implementación ya que ésta debe ser un fiel reflejo de los

procedimientos y normas establecidas en las políticas. El Plan debe estar revisado para adaptarse a las nuevas necesidades del entorno, los servicios que vayan apareciendo y las aportaciones que usuarios, administradores, etc. propongan en función de su experiencia. La revisión es esencial para evitar la obsolescencia de las políticas debido al propio crecimiento y evolución de la organización. Se deben fijar Los plazos de revisión deben estar fijados y permitir, además, revisiones extraordinarias en función de determinados eventos (por ejemplo, incidentes).

Definición de políticas y algunos títulos de declaraciones de políticas

Definición de políticas

El CISM Review Manual (2006). Especifica las políticas como "Declaraciones de alto nivel que establecen expectativas, dirección e intensiones de la alta dirección".

El término política es definido como una declaración de alto nivel sobre las creencias, metas y objetivos de la organización, y en general se establecen para el logro sobre el control de un área específica. Además, se recomienda que una política sea es breve (se recomienda) y sea es el conjunto de declaraciones de la Dirección. (CISM Review Manual, 2006; ISO/IEC 1779 y ISO/IEC 27001, 2005)

Las políticas pueden ser consideradas como la constitución general de la seguridad. A continuación se listan algunos títulos de declaraciones de políticas sobre seguridad computacional.

Títulos de declaraciones de políticas

1. Uso del Internet
2. Uso de correo electrónico
3. Control de accesos a todos los recursos computacionales - sistemas operativos, sistemas en aplicación, redes, correo electrónico, Internet, a sitios restringidos, entre otros.
4. Uso de discos extendibles – USB
5. Uso de tecnología móvil – notebook, computadoras personales, ipod´s, celulares inteligentes, entre otros.
6. Uso de VPN (Virtual Private Network - Redes privadas virtuales)

7. Orden y limpieza del escritorio
8. Control de acceso a terceros

Ejemplo de política

Para A todos los recursos computacionales , por ser como son áreas restringidas, el ingreso a los recursos de red, a laos aplicaciones tivos – Sistemas comerciales, de Recursos Humanos, Nóminas, Cheques, Mercado de Dinero - , a sistemas operativos, entre otros, todos los usuarios de la organización deberán tener una solicitud firmada por ellos, su jefe inmediato y el responsable de seguridad, para proceder a darles autorización o negación del acceso.

Definición de procedimiento, características y un ejemplo.

Definición de procedimiento

Son los pasos específicos de cómo la política deberá ser implementada. (Conference ISO/IEC 17799 y ISO/IEC27001). Es la secuencia de acciones concatenadas entre sí, que ordenadas en forma lógica permite cumplir un fin u objetivo predeterminado. (Directiva Nº002-77-INAP/DNR, Normas para la Formulación de los Manuales de Procedimientos) www.unmsm.edu.pe/ogp/ARCHIVOS/Glosario/indp.htm (1986)

Características

Los procedimientos señalan que éstos deben ser claros, sin ambigüedades e incluir todos los pasos necesarios para llevar a cabo tareas específicas, deben establecer resultados esperados y pre-requisitos para su ejecución. Los procedimientos deben de incluir también los pasos requeridos en caso de que ocurran situaciones inesperadas (CISM, 2006).

Ejemplo de procedimiento

Alta de Usuarios de nuevo ingreso a cualquier sistema en aplicación (Recursos Humanos, Finanzas, Producción, entre otros)

Alta

1. **Solicitante.** Es responsabilidad del solicitante llenar un formato (Se diseñará un formato para dar acceso tanto a privilegios del sistema operativo como de la aplicación) y se enviará al Gerente del Área.
2. **El gerente del área.** Evaluar si el acceso solicitado es adecuado al nivel y al riesgo de información que manejará el usuario que solicitó el alta a los recursos informáticos y firmará el formato correspondiente y lo enviará al área de RH Corporativa.
3. **Gerencia de R.H.** Evaluar si la persona que solicitó el acceso pertenece a la nómina de la empresa o si ya está contratado y firmará el formato y lo pasará a el área de normatividad.
4. **Normatividad/oficial de seguridad**. Evaluar los recursos computacionales que está solicitando el usuario y su jefe aprobando, y evaluará los roles y responsabilidades, si decide que es adecuado al nivel y riesgo, procederá a enviar el formato para que se den de alta los datos, si no lo comentará con el jefe que autorizó y se harán las modificaciones necesarias para que sea autorizado.
5. **STAFF de seguridad técnica y de aplicación.** Es responsabilidad del Staff TI dar de alta todos los datos que han sido solicitados a través del formato Solicitud de Cuenta de Usuario a nivel sistema operativo, a nivel sistema de aplicación.
6. **Para comunicar el user ID** y clave de acceso se enviará un mail al usuario que solicitó el permiso debido a que la clave de acceso es genérica y cuando el usuario firme por primera vez los sistemas de manera automática le pedirá que lo cambie para poderle permitir ingresar al sistema.

La empresa decidirá que procedimiento seguir con los formatos indicados y todo esto deberá quedar documentado. Algunos autores también mencionan los lineamientos y los estándares en el aspecto Administrativo. , pero para fines de este artículo no los incluimos.

Soluciones técnicas

Otra parte importante es tener al personal técnico competente para que seleccione, implemente y monitoree las herramientas de seguridad computacional, con base al riesgo que quiera tomar la empresa. ¿Que quiere

decir esto? Si la organización no invierte en herramientas de seguridad probablemente haya más riesgo en que sus recursos computacionales se puedan borrar, alterar, o perder, ya sea intencional o no intencionalmente por personal interno –INSIDER- para reducir el riesgo hay varias tecnologías de seguridad de información que se pueden implementar.

Cabe hacer mención, que la selección de herramientas de seguridad es con base a la arquitectura de hardware, software y telecomunicaciones, bases de datos, que se quiera proteger, así como lo que se quiera invertir en estas herramientas de protección y en personal para que las opere. Algunas tecnologías para reducir el riesgo de que los INSIDERS no puedan materializar sus amenazas son las siguientes:

Tecnologías de software de antivirus, antispyware, filtrado de paquetes o contenido y firewalls

Narasu Rebbapragada (2006), sugiere que las empresas deben al menos seleccionar e implementar en sus empresas solfware de antivirus, antispyaware, filtrado de paquetes o contenido y firewalls (contrafuego) ya que pueden proveer una convincente y sólida protección contra las amenazas. Este conjunto de software´s actualmente se puede encontrarse en un sólo paquete lla

Virus, software de antivirus y antispyware

Un virus informático es un programa o software que se auto ejecuta y se propaga insertando copias de sí mismo en otro programa o documento, otra de las características es que se puede adicionar a programas o archivos de forma que pueda propagarse, infectando las computadoras a medida que viaja de una computadora a otra, pueden dañar el hardware, software o archivos.

Los usuarios pueden compartir archivos o programas infectados, o cuando se envía información vía mail ésta puede contener virus. Otro código malicioso que puede dañar el hardware software o archivos y que es muy común son los gusanos. Es un código que se replica causando mas daño.

El software de antivirus fue diseñado originalmente para proteger las computadoras contra virus, pero ahora han mejorado y pueden cubrir problemas de gusanos y otro tipo de amenazas tales como el spyware,

(http://www.masadelante.com/faq-virus.htm , 2007). Spyware es un programa que acompaña a otro y se instala automáticamente en un computador (generalmente sin permiso de su propietario y sin que éste sea consciente de ello) para recoger información personal (datos de acceso a Internet, acciones realizadas mientras navega, páginas visitadas, programas instalados en el ordenador, entre otros). www/definición.org/spayware.(2007)

Filtrado de paquetes o contenido

La acción de filtrar paquetes es bloquear o permitir el paso a los paquetes de datos de forma selectiva, según van llegando a una interfaz de red. Las reglas de filtrado especifican los criterios con los que debe concordar un paquete y la acción a seguir, bien sea bloquearlo o permitir que pase, que se toma cuando se encuentra una concordancia. Estas reglas las deben fijar los usuarios de seguridad de información con los usuarios de seguridad técnica y deben ser colocados en el software. http://www.openbsd.org/faq/pf/es/filter.html. (2007)

Firewall – Contrafuegos

Un software de firewall o cortafuegos, es un elemento de software o hardware utilizado en una red para prevenir algunos tipos de comunicaciones prohibidos según las políticas de red que se hayan definido en función de las necesidades de la organización responsable de la red. La idea principal de un firewall es crear un punto de control de la entrada y salida de tráfico de una red. Un firewall correctamente configurado es un sistema adecuado para tener una protección a una instalación informática.

Ventajas de un firewall

- Protege de intrusiones: El acceso a los servidores en la red sólo se hace desde máquinas autorizadas.
- Protección de información privada: Permite definir distintos niveles de acceso a la información de manera que en una organización cada grupo de usuarios definido tendrá acceso sólo a los servicios y la información que le son estrictamente necesarios. http://www.descargar-antivirus-gratis.com/firewall.php (2007)

Tecnologías para monitorear datos

Sean Steele et al. (2007), señalan que debe de existir un software para monitorear los datos que son residentes y los que están en movimiento. Pocas organizaciones conocen donde residen sus datos o hacia donde van, en s Servidores, computadoras personales, almacenamiento de datos fuera de la empresa, datos entregados a socios de negocio, a vendedores, y datos enviados por correo electrónico; entonces las empresas modernas están inundadas de datos tanto residentes como en movimiento.

Por lo tanto cual se debe de tener un esquema de protección adecuada de almacenamiento de datos que residen en los discos duros de las computadoras, así como cuando estos datos viajan de un lugar a otro. En la descripción de puestos a los usuarios se deberán definir sus roles y responsabilidades, de quien debe almacenar datos, leerlos, eliminarlos, actualizarlos y trasmitirlos, así como también se debe de seleccionar las herramientas adecuadas para su monitoreo y control.

Tecnologías para controlar y monitorear la seguridad de usuario final

La tecnología móvil va en aumento. Los celulares inteligentes, las computadoras notebook y portátiles, los iPods, las Pda´s, - Personal Digital Assistants – Asistentes Digitales Personales- los discos extendibles, entre otros, se han perfeccionado y son utilizados por más usuarios internos/insiders, lo que conlleva tener un riesgo más alto de que la información pueda ser robada o destruida. Otras de las características de utilizar tecnología móvil es que son fáciles de trasladar y usar, pueden tener acceso vía remota, y más poder de procesamiento y capacidad de memoria. Pero también, tienen muchas desventajas tal como lo señala CISA Review Manual (2005). Por ejemplo, L la intercepción de información sensitiva, la pérdida o robo del recurso y de los datos contenidos en el mismo, la autentificación del usuario a la conectividad inalámbrica, la falta de encriptación de los datos, la interoperabilidad y el uso de subredes inalámbricas, entre otros, representando es un reto para a la selección y actualización en seguridad técnica por para el uso de tecnología móvil.

Otras tecnologías para proteger los recursos computacionales de los insiders

En esta categoría encontramos el Software para encriptar los discos duros de la tecnología móvil -notebook y computadoras portátiles, los iPods, la Pda´s (Personal Digital Assistants, Asistentes Digitales Personales) y tecnología de escritorio (computadoras fijas).

Es importante verificar periódicamente los parámetros de seguridad que fueron aprobados e instalados en los sistemas operativos (hardening the operating system) a través de una herramienta para el control y monitoreo, igualmente para la seguridad de las aplicaciones.

El acceso a la red es la más cara y ambiciosa y cara estrategia que usan las grandes organizaciones, en los sistemas de control de acceso a las redes o a los recursos de red, escaneando el tráfico de la misma para identificar quién está tratando de ingresar y que no está autorizado pasar por la red.

"Con los accesos remotos se puede manejar mejor la productividad, los servicios a los clientes y proveer mayor ventaja competitiva, no es sorprendente que más organizaciones están haciendo negocio vía Internet. Cuando los usuarios se contactan con accesos remotos, existen productos y servicios efectivos disponibles para minimizar las amenazas" (Swing and al., 2007). La tecnología de Redes Privadas Virtuales – Virtual Private Network (VPN). Puede tener los siguientes controles:

1. Restringe el acceso a selectivos archivos y aplicaciones
2. Administración de autorizaciones
3. Protege la red corporativa si una computadora personal fue infectada y trata de conectarse.

Los recursos para almacenamiento de datos, música, imágenes, entre otros USB flash-drive (también conocidos como memory sticks, memory keys, thumb drives, hand drives and jump drives) son un problema porque están donde quiera , se han vuelto muy populares por su bajo costo y de fácil uso, pero generan hay muchas complicaciones de seguridad. Los recursos consisten en un chip de memoria re-escribible, los insiders con motivos maliciosos pueden sacar datos sensibles o infectar con virus, gusanos o introducir otro tipo de daños.

Soluciones administrativas

Algunas recomendaciones para el uso y control de los flash-drive, se listan a continuación:

La primera recomendación para el control del almacenamiento portable, es controlar quien puede, y quien no, utilizar este recurso. Esto se consigue controlar a través de los permisos otorgados desde el sistema operativo; y la segunda recomendación, a los usuarios que se les haya permitido utilizar el flash-drive, es encriptar los datos, de esta forma si se pierden los flash-drive no podrán ser utilizados". (Zyskowski, 2006).

Se podrían listar algunas otras tecnologías pero éstas parecen ser las más utilizadas por las organizaciones; cabe aclarar también, que el personal de Seguridad Computacional, debe de tener en cuenta al menos las siguientes consideraciones, al seleccionar herramientas de seguridad computacional: el desempeño del software, características, diseño, precio y su fácil uso.

Área de recursos humanos y capacitación en cultura en seguridad computacional

Con las soluciones administrativas y técnicas podemos reducir el riesgo que los Insiders puedan materializar una amenaza, pero también existen otros factores importantes para que el riesgo disminuya aún más, se pueden tener todas las políticas, y procedimientos, Y las herramientas de seguridad computacional de acuerdo a la estrategia de la empresa, pero si el personal interno no se selecciona bien, se capacita y se concientiza sobre un nuevo cambio de Cultura en Seguridad Computacional, tal vez todos los esfuerzos sean en vano.

Área de recursos humanos

Por lo tanto, para que el Cambio de Cultura en Seguridad Computacional se dé en las organizaciones el área de Recursos Humanos y de Seguridad Computacional se tiene que coordinarse. Recursos Humanos debe participar en la contratación más idónea de personal, y el departamento de Seguridad Computacional capacitar para propiciar el cambio de cultura en aspectos de seguridad.

Swing et al. (2007), explica que en el pasado los departamentos de Recursos Humanos se concentraban principalmente en el reclutamiento y retención de empleados, se preocupaban por atraer al personal calificado más adecuado o con habilidades específicas y mantener su moral alta. Considerando en la actualidad los aspectos de seguridad computacional el rol de los departamentos de Recursos Humanos debe evolucionar y crecer. Reclutar y retener al personal sigue siendo deberá ser la meta principal, pero las organizaciones deben tomar en cuenta que el departamento de Recursos Humanos es la primera línea de defensa contra los ataques maliciosos de los Insiders.

Con base a lo anterior, podemos decir que las prácticas de contratación de personal son importantes porque aseguran que el más efectivo y eficiente personal se haya elegido y que la organización esté cumpliendo con los requerimientos de contratación legal.

T. L. Stanley (2007), comenta que al menos hay que verificar los siguientes requisitos cuando se realiza una contratación:

1. Historial de trabajo excelente
2. Buena trayectoria educacional
3. Confirmar retroalimentación de las referencias
4. Buen historial crediticio y comportamiento social positivo

CISA Review Manual (2005), agrega los dos requisitos siguientes:

5. Acuerdo de confidencialidad
6. Acuerdo de conflictos de intereses

Cabe hacer mención, para los empleados de nuevo ingreso y los que ya forman parte de la organización que se deberán elaborar programas de capacitación en Cultura en Seguridad Computacional, donde se den a conocer las políticas y procedimientos así como los aspectos más impactantes sobre seguridad computacional que estén sucediendo en nuestro entorno.

Capacitación en cultura en seguridad computacional

Primero vamos a definir que es cultura y después relacionarla a la Seguridad Computacional y finalmente se describirán comentarios donde se justifique la Capacitación en Cultura de Seguridad Computacional.

Definición de cultura

Partiendo del concepto que plantea Nakagawa (1990), la cultura es aquella parte de las interacciones y experiencias humanas que determinan como uno se siente, actúa y piensa. Es la cultura la que determina el sentido mismo de la visión que tiene el individuo de la realidad. Entonces retomando la definición, en las empresas se debe de proporcionar un ambiente de confort y seguridad para que con sus actitudes el personal contratado y socios de negocio se sientan, actúen y piensen de una manera positiva referente a la Seguridad Computacional.

Definición de seguridad de información

De acuerdo a varios autores, la Seguridad de Información es un concepto o una utopía y se reconoce a la Seguridad de Información como la integridad, disponibilidad, confidencialidad y no – repudiación de los activos. Por otro lado, la seguridad computacional se clasifica en las siguientes categorías de activos: Software, Comunicaciones, Datos, Hardware, Ambiental y Física, Personal y Organizacional y Administrativa. (Vadalis y Kazmi, 2007a,b),

- Integridad. La información debe ser exacta y completa. Para que esta condición llegue a cumplirse se requiere de la protección a accesos no autorizados, inesperados o modificaciones no intencionales. También la integridad asegura que los programas de computadora sean cambiados de una manera ordenada y autorizada.
- Confidencialidad. La información requiere protección de accesos no autorizados. Ésta se encarga de controlar quien obtiene y lee información de archivos, programas y datos dentro de un ambiente de cómputo. Los modelos de control de accesos de confiabilidad, se encargan de quién puede ingresar datos, y de quien puede leer datos y en que sistema de computadora.
- Disponibilidad. La información deberá estar disponible sobre una base de tiempo, ya sea si es necesitada para conocer los requerimientos de los negocios o para evitar pérdidas substanciales, con el fín de asegurar que los usuarios de sistemas tengan accesos no interrumpidos de

información, de recursos y de sistemas como: datos, programas y equipo de cómputo.

Con base a las definiciones anteriores el elemento humano interno-insiders y los Socios del Negocio son un factor clave en la concientización de la Cultura en Seguridad Computacional - Software, Comunicaciones, Datos, Hardware, Ambiental y Física, Personal y Organizacional y Administrativa- . Por lo tanto, los directores de alto nivel y los accionistas deberían reconocer que, en una organización, la primera línea de defensa en la seguridad computacional son todos sus empleados-insiders; son los mismos insiders, los que pueden alertar sobre las vulnerabilidades y fortalezas de seguridad. Entonces, para que no alteren los esquemas de seguridad computacional, se debe empezar por crear una conciencia Cultura de conciencientización, que inicie con el programa de inducción dirigido a los nuevos empleados contratados y a los que ya están.

John Swing, et al. (2007), explica que existen buenas políticas de Seguridad Computacional, donde y se establece claramente la conducta esperada de un empleado, al hacer uso de los recursos computacionales propiedad de la compañía, sin embargo, existen organizaciones con buenas políticas pero que no siempre son capaces de comunicarlas adecuadamente a todo su personal.

Las principales características de la capacitación sobre aspectos de seguridad computacional es que ésta debe ser mandatoria y repetitiva, es decir, todos los niveles jerárquicos deben tomar la capacitación. Ésta se puede programar cada trimestre o semestre y siempre debería estar apoyada por la alta dirección, dependiendo del riesgo de negocio. Por ejemplo, una empresa que se dedica a los aspectos financieros, como un banco o casa de bolsa, tiene más riesgo, que una empresa que únicamente se dedica a la comercialización de un producto, entonces se deberán programar los cursos de capacitación de acuerdo al riesgo.

Cultura en seguridad computacional

Para identificar como está el nivel de cultura en seguridad computacional de su organización, solo invite a alguien externo y pídale que intente violar todos los controles de seguridad computacional, por ejemplo, entrar a una área restringida, preguntar y acceder a la información con una

clave de acceso de otro usuario, tomar algún manual de desarrollo, pedir un dispositivo de respaldo y bajarlo en otra computadora, realizar una transacción, enviar información, utilizar el correo interno, preguntarle a cualquier persona datos confidenciales de algún proceso clave, utilizar una computadora personal, que pueda entrar a otros controles, entrar a otros accesos, y si algunos de estos controles fue violado entonces su empresa estará en serios problemas de seguridad computacional y, por lo tanto, refleja que su personal interno – insiders no está consciente de la importancia de la Cultura en Seguridad Computacional.

Por lo anterior, es de suma importancia que la Cultura en Seguridad Computacional abarque todas las áreas y niveles organizacionales, tanto internas como externas, ya que también deben deberían estar involucrados en esta Cultura los Socios de Negocios, como los clientes, prestadores de servicios (bancos, casas de bolsa- aseguradoras), los proveedores y el personal de soporte técnico (outsourcing), entre otros.

El cambio de cultura se logrará cuando todas las personas internas – insiders y socios del Negocio logren sensibilizarse de este cambio. El equipo de implementación debe diseñar una estrategia, que incluya a todos los niveles organizacionales en los cursos de concientización, de los directores de todos los niveles hasta los empleados internos y externos. En este proceso se deben agregar iniciativas creadoras, tales como: una campaña de la seguridad/privacidad, información regular acerca de la seguridad y privacidad en boletines internos, mensajes de seguridad en el intranet, carteles, concursos y foros de discusión, entre otras alternativas.

Para asegurar El CAMBIO EXITOSO de la NUEVA CULTURA seguridad/privacidad, el programa del cambio debe aplicarse sistemáticamente. La implementación debe incluir un mensaje fuerte y firme por parte de los accionistas y directores de primer nivel, ya que ellos tienen que ser un apoyo importante para que el cambio se dé más rápido.

Recomendaciones para el desarrollo de una cultura en seguridad computacional

- Para minimizar el riesgo de un ataque, por parte de las personas internas (insider), es indispensable que analicen, diseñen, se implementen y actualicen las Soluciones Administrativas, en este

caso como son las Políticas y Procedimientos, y que éstas se difundan mediante la capacitación y campañas de concientización.

- Las herramientas técnicas deberán ser adecuadamente seleccionadas, implementadas y monitoreadas, de acuerdo a las plataformas de hardware, telecomunicaciones, base de datos, sistemas operativos, sistemas en aplicación, entre otros. Las herramientas se podrán seleccionar con base a lo que la empresa quiera asumir como de riesgo e inversión.
- Si los empleados toman conciencia, ayudarán a reducir los gusanos, virus y spyware y es menos probable que se infecten los recursos computacionales.
- El seguimiento sobre el comportamiento de algunos usuarios, que tienen autoridades especiales, y que manejan información confidencial o que tienen los privilegios de modificar, borrar o cambiar información.
- Verificar los antecedentes laborales y su trayectoria profesional de para todos los puestos clave de la organización, así como para el área de de Sistemas se deberá tener mayor validación, debido a que ésta área está más familiarizada con las vulnerabilidades y sobre aspectos de seguridad computacional, y son las que pueden intencional o no intencional causar más daño.
- La capacitación continua a todos los niveles jerárquicos sobre aspectos de seguridad computacional es crucial.

Referencias

Borghello, C. F. 2001. Tesis Seguridad Informática, Su Implicancia e Implementación www.segu-info.com.ar.2007, p.17.

CISA Review Manual. 2005. The Information Systems Audit and Control Association, p. 75.

CISM REVIEW MANUAL. 2006. CERTIFIED INFORMATION SECURITY MANAGER, CISM, Information Systems Audit and Control Association p. 27.

Ernst & Young. 2001. "Encuesta de Seguridad Informática en tecnologías 2001" Ernst & Young México, http//www.ey.com. (2001)

Swing, J., J. Falcon & K. McGrane. 2007. IT Security: Preventing The March of Madness Business Communications Review; p. 30.

INAP, Directiva Nº002-77-INAP/DNR. 1986. Normas para la Formulación de los Manuales de Procedimientos) www.unmsm.edu.pe/ogp/ARCHIVOS/Glosario/indp.htm (1986).

ISO/IEC 1779 & ISO/IEC 27001. 2005. Information Security Management System Implantation –Student Manual. BSI Management Systems Inc.

Macleod, C. 2007.Top Hacker Secrets.; Management Services; 51, 2; p. 46.
Nakagawa, M. A. 1996. “A Closer Look at Culture”. p.22 y 23. Edit. Gránica S.A. p. 6. Citado por Girard, G. / Koch S.J., obra cit. p. 48 y 49.
Rebbapragada, N. 2006. All-in-One SECURITY, PC World; 24, 7; Computing, p. 100.
Stanley, T. L. 2007. Hire the right person SuperVision; 68,7 ; p.10.
Steele, S. & C. Wargo. 2007. An Introduction to Insider Threat Management, Information Systems Security, volume 16 Number 1-, 23- 29 -31.
Swing, J., J. Falcon & K. McGrane. 2007. p. 30. La tecnología de Redes Privadas Virtuales – Virtual Private Network (VPN).
Vadalis, S. & Z. Kazmi. 2007a. Information Systems Security, volume 16, number 1, January / february, p. 34.
Vidalis, S. & Z. Kazmi. 2007b. Security Through Deception, Information Systems Security, Jan/Feb: 16, number 1, p. 34-41.
Zyskowski, J. 2006. Thumb drives are too often the victims of convenience Federal Computer Week; Computing 20, 42; p. 41.

www.ey.com/global/ content.nsf/Mexico/ Perspectivas_Seguridad_Informatica_1003_ey Mexico. Ernst & Young México
www.masadelante.com/faq-virus.htm, 2007
definicion.org/spyware (2007)
www.openbsd.org/faq/pf/es/filter.html (1996-2007)
www.descargar-antivirus-gratis.com/firewall.php (1999-2007)