TÍTULO: Política de Acceso Lógico a Servidores y Archivos Electrónicos

Código: SI 03 001 Versión: 0 Vigencia: xx/11/2011

1- OBJETIVO

El propósito de esta política es establecer las pautas de acceso a los servidores de la compañía y el esquema de permisos de acceso a los archivos.

2- ALCANCE

Esta política aplica a todos los empleados de EPSA y es aplicable a todos los servidores de la compañía y su contenido.

3- DESCRIPCIÓN

a) Verificación del control de acceso lógico

El acceso lógico a los servidores deberá contemplar las siguientes pautas:

- Desactivar la opción de escribir/modificar los permisos de acceso para todos los archivos ejecutables y binarios.
- Restringir el acceso a archivos source del sistema operativo, archivos de configuración, y sus directorios; sólo disponible para los administradores autorizados.
- No deben haber archivos world-writable a menos que sean específicamente requeridos por algún programa de aplicación.
- Los archivos de sistema deben ser read-only para imposibilitar cambios desautorizados.
- Como meta, se debería imposibilitar a los usuarios instalar, eliminar, o editar scripts sin una revisión administrativa.
- Asegurarse de que se configure el sistema operativo de modo que los nuevos archivos y directorios creados hereden el control de acceso apropiado, y que esta política de seguridad se propague en la jerarquía de subdirectorios.
- Los administradores deben desactivar la habilidad de los subdirectorios de saltear las directivas de seguridad de niveles mayores, a menos que el salteo sea requerido. Muchas de las políticas de seguridad pueden ser salteadas en una base de directorio. La conveniencia de poder crear excepciones en la política global se compensa con la amenaza de la aparición de un agujero en la seguridad a través de un usuario malintencionado controlando un subdirectorio distante.

b) Instalar y configurar las capacidades de encripción de archivos

Algunos sistemas operativos proveen encripción de archivos opcional; también existen paquetes third-party de encripción. Estos pueden resultar útiles si el control de acceso del sistema operativo resulta insuficiente para mantener la confidencialidad del contenido de los archivos. Para el caso en que las relaciones entre las categorías de archivos y las categorías de usuario sean muy complejas, se puede recomendar el uso de estos programas.
La encripción agrega complejidad, por eso se debe comparar la relación necesidad de uso vs. costo de uso.
La seguridad proporcionada por controles de acceso fuertes, es reforzada con el uso de encripción.

- Encripción de datos - Recomendación

Recomendamos utilizar GNUPG para la encripción de la información almacenada en el server. GnuPG es un reemplazo gratis y completo del PGP. Puede ser utilizado sin restricciones, y se atiene a los estándares de RFC2440 (OpenPGP).

La instalación de paquetes y documentación se encuentra en:
http://www.gnupg.org/(en)/download/index.html

c) Mecanismos de logueo del sistema y red

Los Log files suelen ser el único indicio de comportamiento sospechoso. Una falla en la activación del mecanismo de reconocimiento de esta información, puede debilitar o eliminar la habilidad de detectar intentos de intrusión y de determinar cuando la intrusión tuvo éxito o no. Problemas similares pueden resultar del hecho de no tener una base de procedimientos y herramientas para procesar y analizar estos log files.

Se necesitan los logs para:

- Alertar de que algo sospechoso (que requerirá futura investigación) ha ocurrido.
- Determinar el grado de actividad de una intrusión.
- Ayudar a recuperar los sistemas.
- Proveer información requerida para procedimientos legales.

d) Tipos de categorías de Log

Usuarios

- Información de Login/Logout: ubicación y momento de intentos y logueos fallidos en cuentas privilegiadas.
- Cambios en el status de autenticación, como la activación de privilegios.

Procesos

- Usuario efectivo y real ejecutando el proceso.
- Procesar el tiempo de start-up, argumentos.
- Procesar status de salida, hora, duración, recursos consumidos.

Sistemas

- Acciones que requieren privilegios especiales.
- Status/ errores reportados por subsistemas de hardware y software.
- Cambios en el status del sistema, incluyendo paradas y reinicios.

Redes

- Pedidos de inicio de servicio.
- El nombre del usuario/host requiriendo el servicio.
- Tráfico de mensajes de red (packets).
- Nuevas conexiones.
- Duración de la conexión.
- Flujo de la conexión.

Sistema de archivos

- Cambios en Access Control Lists y protección de archivos.
- Accesos de los archivos (abrir, crear, ejecutar, eliminar).

Aplicaciones

- Las aplicaciones -y servicios- especifican información (por ejemplo, mail logs, FTP logs, Web server logs, modem logs, firewall logs, SNMP logs).

e) Proteger logs para asegurarse que son confiables

- Los log files debe ser resguardados del acceso y modificación de usuarios no autorizados.
- La información en los logs debe ser almacenada en un archivo en un host separado, dedicado a este propósito.
- Almacenar la información de logs en un dispositivo "write-once/read-many" (ej. CD-ROM o tape) o en un dispositivo "write-only" (ej.: impresora), para eliminar la posibilidad de la modificación de la información.
- Encriptar los log files, especialmente aquellos archivos que serán enviados por una red.

f) Mecanismo de logging - Recomendación

Recomendamos usar una de estas herramientas para chequear la consistencia del log y su posible forzado:

- chklastlog
  ftp://ftp.cerias.purdue.edu/pub/tools/unix/logutils/chklastlog/

- chkwtmp
  ftp://ftp.cerias.purdue.edu/pub/tools/unix/logutils/chkwtmp/

- loginlog
  ftp://ftp.cerias.purdue.edu/pub/tools/unix/logutils/loginlog/

- trimlog
  ftp://ftp.cerias.purdue.edu/pub/tools/unix/logutils/trimlog/

4- RESPONSABILIDAD DE APLICACION

Todo el personal.

5- DISPOSICION

En el caso de una violación de la política, podrán tomarse medidas disciplinarias que pueden llegar hasta la terminación con causa de la relación laboral y contractual, sin perjuicio de las consideraciones legales que correspondan.

6- HISTORICO DE CAMBIOS

Confeccionó:Juan Martín Ferraro	Revisó: Cristian Conde	Aprobó: H. Arébalo
Firma	Firma	Firma
COMITÉ DE SI	GERENTE DE SISTEMAS	GERENCIA GENERAL