UNAH
UNIVERSIDAD NACIONAL
AUTÓNOMA DE HONDURAS

Facultad de Ingeniería

Departamento de Ingeniería en Sistemas

Auditoria Informática (IS-903)

Ing. Elmer Padilla

Auditoria de la seguridad lógica

Presentado por:

Génesis Raquel Izaguirre López 20151005232

Ciudad Universitaria, Tegucigalpa MDC, Francisco Morazán

Marzo, 2020.

Auditoria de controles lógicos de seguridad.

Introducción

Los sistemas informáticos también deben protegerse adecuadamente contra el acceso no autorizado y la destrucción o alteración accidental o intencional de los programas de software del sistema, los programas de aplicación y los datos. La protección contra estas amenazas se logra mediante la implementación de controles lógicos de seguridad.

Se recomienda que la seguridad lógica comience en el nivel más bajo, el sistema operativo, y avance con la seguridad de las funciones de escritorio y la usabilidad de las aplicaciones (también llamado "Endurecimiento" de un sistema).

Objetivos

- Mostrar los riesgos que se corren al no tener controles de seguridad lógicos.
- Enumerar lo que asegura cubre este tipo de auditoria.
- Proporcionar los pasos a seguir para hacer este tipo de auditorías.

¿Que son los controles lógicos?

Los controles de seguridad lógicos son aquellos que restringen las capacidades de acceso de los usuarios del sistema y evitan que usuarios no autorizados accedan al sistema. Pueden existir controles de seguridad lógicos dentro del sistema operativo, el sistema de administración de la base de datos, o bien programas de aplicación de los dos anteriores.

El número y los tipos de controles de seguridad lógicos disponibles varían con cada sistema operativo, sistema de administración de bases de datos, aplicación y en muchos tipos de dispositivos de telecomunicaciones. Algunos están diseñados con una amplia gama de opciones y parámetros de control de seguridad lógica que están disponibles para el administrador de seguridad del sistema. Estos incluyen ID de usuario, contraseñas con requisitos de longitud mínima y un número requerido de dígitos y caracteres, suspensión de ID de usuario después de intentos fallidos de inicio de sesión, restricciones de acceso a directorios y archivos, restricciones de hora del día y día de la semana, y restricciones específicas restricciones de uso de terminal. Otros sistemas operativos y aplicaciones están diseñados con muy pocas opciones de control. Para estos sistemas, los controles de seguridad lógicos a menudo parecen agregarse como una ocurrencia tardía, lo que resulta en configuraciones de control que son más débiles de lo que razonablemente deberían ser.

Riesgo

Si las unidades no garantizan que los sistemas estén en su lugar para establecer la seguridad lógica adecuada, la integridad del sistema, los datos y la disponibilidad de los sistemas pueden verse comprometidos. Tales compromisos podrían resultar en el robo de datos de propiedad: divulgación no autorizada (maliciosa, no maliciosa o accidental), modificación o destrucción de información; y / o errores y omisiones no maliciosos. Estas condiciones podrían tener un impacto adverso en la capacidad de la unidad para lograr sus objetivos y someter a la empresa a publicidad negativa en caso de que la información sensible se vea comprometida.

- Los usuarios tienen acceso a áreas distintas a las relacionadas con el desempeño de sus deberes, causando amenazas de acceso no autorizado, modificación o eliminación en los datos mantenidos.
- Acceso a recursos muy sensibles como el programa de software de seguridad que puede ser de naturaleza de misión crítica.
- Los empleados no tienen restricciones para realizar funciones incompatibles o funciones más allá de su responsabilidad.

Las herramientas de monitoreo y administraciones remotas presentan riesgos especiales para la seguridad de la información. Las herramientas remotas permiten a los operadores conectarse a través de una función remota y realizar actividades que normalmente realizarían en el sitio. Algunas instituciones financieras han aprobado tecnologías de acceso remoto como una solución central y común para todos los empleados que requieren acceso remoto.

Cobertura de este tipo de auditoria

El objetivo de los controles de acceso lógico es proteger las aplicaciones y los datos subyacentes, archivos de acceso no autorizado, modificación o eliminación.

Los objetivos de limitar el acceso son para asegurar que:

- Los usuarios solo tienen el acceso necesario para realizar sus tareas.
- El acceso a recursos muy sensibles como el programa de software de seguridad está limitado a muy pocas personas.
- Los empleados tienen restricciones para realizar funciones o funciones incompatibles más allá de su responsabilidad.

Procedimiento de auditoría

La importancia de los controles de acceso lógicos es el aumento donde los controles de acceso físico son menos efectivos. La existencia de una seguridad de acceso lógico adecuada es particularmente importante cuando una organización hace uso de redes de área amplia e instalaciones globales como Internet, generalmente dependen de las instalaciones de seguridad incorporadas disponibles bajo el sistema operativo o hardware en uso. Se pueden obtener

controles de acceso adicionales mediante el uso apropiado de programas de seguridad patentados. La forma más común de control de acceso lógico es identificadora de inicio de sesión (ids) seguidos de autenticación de contraseña. Para que las contraseñas sean efectivas debe haber políticas y procedimientos de contraseña apropiados, que son conocidas por todo el personal y respetadas.

Las organizaciones pueden personalizar la contraseña del sistema, por ejemplo, estableciendo longitudes mínimas de contraseña, forzando regular cambios de contraseña y rechazo automático de contraseñas puramente numéricas, de personas nombres o palabras que aparecen en el diccionario.

Las restricciones de menú pueden ser efectivas en el control de acceso a aplicaciones y utilidades del sistema. Los sistemas pueden ser capaces de controlar el acceso mediante la identificación de cada usuario individual a través de sus identificadores únicos de inicio de sesión y luego tener un perfil predefinido de menús autorizados para cada uno.

El auditor debe considerar cuán fácil sería para los usuarios "salir" del sistema de menús y obtener acceso no autorizado a sistema operativo u otras aplicaciones. El sistema a menudo plantea riesgos importantes ante personal administrativo con poderosos privilegios del sistema. Estos "superusuarios" pueden tener acceso a poderosas utilidades del sistema que pueden evitar los controles establecidos del sistema.

La administración debería haber introducido medidas para controlar las actividades de estos poderosos usuarios y, si posible, limite los privilegios del sistema del administrador individual a los requeridos por su función.

Los elementos críticos de un mecanismo de control de acceso deben incluir:

- Clasificación de los recursos de información según su criticidad y sensibilidad.
- Mantenimiento de una lista actual de usuarios autorizados y sus privilegios de acceso.
- Monitorear el acceso, investigar violaciones aparentes de seguridad y tomar acción correctiva apropiada.

Recursos, archivos e instalaciones que requieren protección:

- **Archivos de datos**: pueden consistir en archivos de transacciones o bases de datos.
- **Aplicaciones**: el acceso sin restricciones aumenta el riesgo de que las aplicaciones sean sujeto a enmiendas no autorizadas que conducen a fraude, pérdida de datos y corrupción.
- **Archivos de contraseñas**: si estos archivos no están protegidos adecuadamente y alguien puede leerlos habría poco para evitar que una persona no autorizada obtenga el inicio de sesión, identificación y contraseña de un usuario del sistema privilegiado. Cualquier usuario no autorizado quien obtuvo los permisos de acceso de un usuario del sistema privilegiado podría causar daños considerables. Incluso donde el identificador y la contraseña de un usuario ordinario se obtiene, el concepto por el cual los usuarios son responsables de sus acciones se pasan por alto.

- **Software y utilidades del sistema**: consisten en software como editores, compiladores, depuradores de programas. El acceso a estos debe restringirse ya que estas herramientas podrían utilizarse para realizar modificaciones en los archivos de datos y el software de aplicación.
- **Registros**: los archivos de registro se utilizan para registrar las acciones de los usuarios y, por lo tanto, proporcionan información de administradores de sistemas y gestión de organizaciones con una forma de responsabilidad. Si los archivos de registro no están protegidos adecuadamente, un hacker, estafador, podría eliminar o editar para ocultar sus acciones.

Bibliografía

- http://auditoriastics.blogspot.com/2016/05/unidad-7-auditoria-de-la-seguridad.html
- https://mario15494.wordpress.com/category/temas/auditoria-de-la-seguridad-logica/