IDENTIFICACIÓN Y AUTENTICACIÓN

AUTOR: JAVIER CHINCHILLA MORALES

NOVIEMBRE: 2020

San Marcos

Introducción

Es la primera línea de defensa para la mayoría de los sistemas computarizados, permitiendo prevenir el ingreso de personas no autorizadas. Es la base para la mayor parte de los controles de acceso y para el seguimiento de las actividades de los usuarios.

Tabla de contenido

Identificación y autenticación

Definiciones

Identificación: es el momento en que el usuario se da a conocer en el sistema;
Autenticación: es la verificación que realiza el sistema sobre esta identificación.

Implementación de sistemas de identificación y autenticación

El gran crecimiento de las redes, interconexiones y telecomunicaciones en general, incluido el uso de Internet de forma corriente, ha demostrado que la seguridad física no lo es todo. Es un punto que debe complementarse necesariamente con la implementación de controles para la seguridad lógica de los sistemas y computadoras.

Es esa tendencia de interconexión de redes con otras redes, o de una simple PC a Internet la que nos da la pauta de que aún si usamos tarjetas electrónicas para acceder a nuestra oficina, hay otras puertas traseras mucho menos evidentes que debemos controlar porque nuestros sistemas están virtualmente a la espera de que alguien intente utilizarlos.

Al igual que se consideró para la seguridad física, y basada en ella, existen cuatro tipos de técnicas que permiten realizar la autenticación de la identidad del usuario, las cuales pueden ser utilizadas individualmente o combinadas:

- Algo que solamente el individuo conoce: por ejemplo una clave secreta de acceso o password, una clave criptográfica, un número de identificación personal o PIN, etc.
- Algo que la persona posee: por ejemplo una tarjeta magnética.
- Algo que el individuo es y que lo identifica unívocamente: por ejemplo las huellas digitales o la voz.
- Algo que el individuo es capaz de hacer: por ejemplo los patrones de escritura.

Para cada una de estas técnicas vale lo mencionado en el caso de la seguridad física en cuanto a sus ventajas y desventajas. Se destaca que, en los dos primeros casos enunciados, es frecuente que las claves sean olvidadas o que las tarjetas o dispositivos se pierdan, mientras que, por otro lado, los controles de autenticación biométricos serían los más apropiados y fáciles de administrar, resultando ser también, los más costosos por lo dificultosos de su implementación eficiente.

Desde el punto de vista de la eficiencia, es conveniente que los usuarios sean identificados y autenticados solamente una vez, pudiendo acceder a partir de allí, a todas las aplicaciones y datos a los que su perfil les permita, tanto en sistemas locales como en sistemas a los que deba acceder en forma remota. Esto se denomina "single login" o sincronización de passwords.

Una de las posibles técnicas para implementar esta única identificación de usuarios sería la utilización de un servidor de autenticaciones sobre el cual los usuarios se identifican, y que se encarga luego de autenticar al usuario sobre los restantes equipos a los que éste pueda acceder. Este servidor de autenticaciones no debe ser necesariamente un equipo independiente y puede tener sus funciones distribuidas tanto geográfica como lógicamente, de acuerdo con los requerimientos de carga de tareas.

La Seguridad Informática se basa, en gran medida, en la efectiva administración de los permisos de acceso a los recursos informáticos, basados en la identificación, autenticación y autorización de accesos.

Esta administración abarca:

- Proceso de solicitud, establecimiento, manejo, seguimiento y cierre de las cuentas de usuarios. Es necesario considerar que la solicitud de habilitación de un permiso de acceso para un usuario determinado, debe provenir de su superior y, de acuerdo con sus requerimientos específicos de acceso, debe generarse el perfil en el sistema de seguridad, en el sistema operativo o en la aplicación según corresponda.
- Además, la identificación de los usuarios debe definirse de acuerdo con una norma homogénea para toda la organización.
- Revisiones periódicas sobre la administración de las cuentas y los permisos de acceso establecidos. Las mismas deben encararse desde el punto de vista del sistema operativo, y aplicación por aplicación, pudiendo ser llevadas a cabo por personal de auditoría o por la gerencia propietaria del sistema; siempre sobre la base de que cada usuario disponga del mínimo permiso que requiera de acuerdo con sus funciones.
- Las revisiones deben orientarse a verificar la adecuación de los permisos de acceso de cada individuo de acuerdo con sus necesidades operativas, la actividad de las cuentas de usuarios o la autorización de cada habilitación de acceso. Para esto, deben analizarse las cuentas en busca de períodos de inactividad o cualquier otro aspecto anormal que permita una redefinición de la necesidad de acceso.
- Detección de actividades no autorizadas. Además de realizar auditorias o efectuar el seguimiento de los registros de transacciones (pistas), existen otras medidas que ayudan a detectar la ocurrencia de actividades no autorizadas. Algunas de ellas se basan en evitar la dependencia hacia personas determinadas, estableciendo la obligatoriedad de tomar vacaciones o efectuando rotaciones periódicas a las funciones asignadas a cada una.
- Nuevas consideraciones relacionadas con cambios en la asignación de funciones del empleado. Para implementar la rotación de funciones, o en caso de reasignar funciones por ausencias temporales de algunos empleados, es necesario considerar la importancia de mantener actualizados los permisos de acceso.
- Procedimientos a tener en cuenta en caso de desvinculaciones de personal con la organización, llevadas a cabo en forma amistosa o no. Los despidos del personal de sistemas presentan altos riesgos ya que en general se trata de empleados con capacidad para modificar aplicaciones o la configuración del sistema, dejando "bombas lógicas" o destruyendo sistemas o recursos informáticos. No obstante, el personal de otras áreas usuarias de los sistemas también puede causar daños, por ejemplo, introduciendo información errónea a las aplicaciones intencionalmente.
  Para evitar estas situaciones, es recomendable anular los permisos de acceso a las personas que se desvincularán de la organización, lo antes posible. En caso de despido, el permiso de acceso debería anularse previamente a la notificación de la persona sobre la situación.

Los programas para el control de acceso a los recursos del sistema de información permiten manejar el identificador y autenticación de los usuarios, el contro de acceso de cada recurso disponible y el mantenimiento de información de eventos sobre el sistema para la posterior investigación y detección de fraudes. Estos programas pueden brindar un ajustado control de seguridad, especialmente en áreas tales como:

- Definición de usuarios, Recordemos que los derechos de usuarios comunes no deberían ser los mismos que los de gerentes, programadores, secretarias, etc. De ahí la necesidad de clasificar los usuarios por tipos.
- Definición de derechos de usuarios luego de que el acceso ha sido otorgado, Una vez que un usuario ha tenido acceso al sistema, tendrá disponibles ciertas funciones, y otras no, dependiendo de la definición que hayamos hecho. Por ejemplo, un usuario de tipo A puede leer los archivos de información de clientes, pero no podrá actualizarlos. Un usuario de tipo B podrá hacer esas actualizaciones.
- Establecimientos de logs o información de eventos, típicamente, un log es un archivo que describe todos los eventos ocurridos. Si tuviésemos que expresar lo que dice un log de forma coloquial, podríamos decir algo así: “El día 3 de mayo a las 9:45 am, el usuario Anibal Fernandez pidió Autorización de acceso a las planillas de clientes. El acceso fué concedido. El usuario modificó el teléfono del cliente Nro. 567 y cerró el sistema a la hora 10:15 am”. Esta información es guardada, por supuesto, de forma codificada, para luego poder hacer investigaciones en caso de ser necesario.

En el momento de implementar un sistema de seguridad, entonces, se crea la clasificación de usuarios, se crean las cuentas de usuarios con las claves de acceso y esta información se mantiene en una base de datos generalmente encriptada. Por supuesto, una vez más cabe aclarar que todo esto se desprende de ciertos programas y políticas de seguridad, dentro de un marco preestablecido.
Este tipo de sistemas incluye o debería incluir el control sobre accesos remotos a través de otras redes, o bien a través de Internet.
Vale decir, debe detectar todo tipo de intento de acceso a un recurso para realizar el control pertinente.
Los hacker’s son los especialistas en encontrar los baches de seguridad en puertas traseras a los sistemas, por controles que son violados y a través de accesos remotos. (Para aprender sobre los 7 métodos de autentificación más utilizados dirijase al siguiente link)

Conclusiones y recomendaciones

En todo sistema informático es de vital importancia proteger cada uno de sus componentes, como son: hardware, software, datos, memoria y usuarios. Cualquiera de estos es vulnerable a ataques. Para mejorar la seguridad de un sistema de información se puede hacer uso de los servicios de seguridad cuya meta es evitar los ataques a sus componentes, evitando así la interrupción, intercepción, modificación y generación de contenido diferente al que el usuario original pretende enviar. Si se cumplen estos servicios de seguridad se considera que los datos están protegidos. Los servicios son: confidencialidad, integridad, disponibilidad, no repudio, control de acceso, autenticación.

Referencias bibliográficas

- Carpentier, J. (2016). *La seguridad informática* en la PYME. Editorial ENI.
- Cañon, L. (2015). *Ataques Informáticos Ethical Hacking y conciencia de seguridad informática en niños. (Trabajo de Fin de Grado).* Universidad Piloto, Colombia.

San Marcos

www.usanmarcos.ac.cr

San José, Costa Rica