

## LA SEGURIDAD Y LOS CONTROLES LÓGICOS

El gran crecimiento de las redes, interconexiones y telecomunicaciones en general, incluido el uso de Internet de forma casi 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.

Ya hablamos en ediciones anteriores sobre los riesgos que enfrentamos por dejar esas puertas físicas o lógicas sin un control adecuado. Pero recordemos que el objetivo final de toda seguridad informática es integridad de datos y programas, lo que incluye la disponibilidad, confidencialidad y confiabilidad de la información. También hablamos de cuáles son los controles físicos, su clasificación y uso. Hablemos entonces de los controles lógicos.

Los controles lógicos son aquellos basados en un software o parte de él, que nos permitirán:

- Identificar los usuarios de ciertos datos y/o recursos: hacer una clasificación de tipos de usuarios y sus objetivos de acceso a los sistemas.
- Restringir el acceso a datos y recursos de los sistemas: establecer los permisos por tipo de usuario. Por ejemplo, establecer que un usuario común de un sistema no tendrá acceso a los datos financieros de la organización.
- Producir pistas para posteriores auditorias: todos los movimientos hechos por los usuarios deben ser registrados y guardados a modo de historia de lo que ha ocurrido. Generalmente archivos llamados "logs", son los que mantienen este tipo de información.

Los controles:

### (1) Identificación y autenticación de usuarios

Identificación es el proceso de distinguir una persona de otra; y autenticación es validar por algún medio que esa persona es quien dice ser. Pensemos en un policía pidiendo a alguien que se identifique. Bien, si una persona dice "me llamo Juan Carlos Piró", se está identificando. Pero el oficial seguramente querrá hacer una autenticación, para asegurarse de que esta persona no miente, y le pedirá su documento personal, que será en ese caso el control usado. En las calles de Buenos Aires la policía ya está contando con dispositivos de autenticación a través de huellas dactilares, para incrementar el nivel de control y de esa forma también, buscar en una base de datos el historial de la persona. En Estados Unidos, estos controles están en la base de todo sistema de seguridad, en aeropuertos, para identificación de terroristas, en municipios para controlar que la gente sin permisos de manejo traten de adquirir una licencia de conducir en otras ciudades, etc. En todos los niveles, este es un control con demanda nunca tan creciente como en este momento.

Encontrar una forma satisfactoria de control de identificación y autenticación no es muy fácil. Algunas técnicas son muy fáciles de violar, otras son muy costosas y otras son consideradas muy intrusas. Los modelos más generalmente usados se basan en una de estas técnicas:

- O Lo que el usuario sabe: comúnmente, las claves de acceso que pueden utilizarse para sistemas generales (acceso a la PC) u específicos (acceso a una Base de Datos). Es el más ampliamente usado. Para otorgarle la característica de ser un buen control, a veces se añaden ciertas especificaciones: la clave debe cambiarse de forma periódica y nunca debe ser mostrada en una pantalla. Algunos sistemas muestran asteriscos al momento del ingreso de una clave (\*\*\*\*\*) y otros simplemente no muestran nada, para ni siquiera dar la

evidencia de cuántos dígitos tiene esa clave.

Otras características que hacen a las claves un buen control, es:

- el forzar un tamaño en dígitos mínimo
- obligar mezclas de números y letras (no sólo números o sólo letras)
- prohibir el uso de datos personales, como nombre apellido o fecha de cumpleaños como clave
- obligar un tiempo mínimo de uso de clave para no volver a la anterior luego de haberla cambiado
- prohibir el uso de claves ya usadas anteriormente

O Lo que el usuario tiene: como ya expuesto en el anterior artículo, ejemplos de este tipo de control son las tarjetas magnéticas y las tarjetas electrónicas. Pero también los carnés de conducir, y las tarjetas de identificación son controles de autenticación.

La típica tarjeta de identificación de un empleado posee una foto. A pesar de que ese tipo de tarjetas no son legibles por la computadora, cualquier persona puede hacer una comparación entre la foto y el rostro de alguien. El requerimiento de poseer la tarjeta en todo momento, limita la posibilidad de que alguien pueda usar la tarjeta de otro empleado. Esas tarjetas podrían también ciertas características legibles para las computadoras, que sirvan a modo de permiso de acceso o "login". Como las fotos pueden ser falsificadas fácilmente, en algunos casos se les aplica algún sello de seguridad o código que no sea reproducible corrientemente.

En el esfuerzo de disminuir el personal de guardia en los edificios, algunas organizaciones utilizan cámaras que lees las tarjetas. El empleado inserta la tarjeta en una ranura que permite verla en primer plano con un monitor. Luego, este mismo empleado mira hacia una cámara y las dos imágenes son transmitidas a un guardia que hará la comparación para dar o no los permisos de acceso.

O Algo específico del usuario: como ejemplos podemos nombrar las características faciales, huellas dactilares, voz, etc. Estos controles son los más automatizados dentro de esta clasificación. Los controles biométricos ya fueron descriptos en detalle anteriormente. Hay una gran variedad de controles de este tipo, generalmente basados en las siguientes características del usuario:

- Huellas dactilares
- Patrones de la retina
- Geometría de la mano
- Dinámica de la firma
- Patrones de la voz

La necesidad de evitar operaciones fraudulentas crece exponencialmente. Si los perpetradores de estos delitos sienten que pueden ser identificados, muchos no correrán el riesgo. Aquellos que sientan que permanecerán anónimos usualmente continúan con los actos ilegales.

## (2) Programas de control de acceso

Programas diseñados para administrar los permisos de acceso a los recursos del sistema de información. Permite manejar el identificación y autenticación de usuarios, el control 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 fue 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 *hackers* 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.

### (3) Otras consideraciones

Así una computadora se encuentre aislada, no contactada a ningún tipo de red, el control sobre el acceso a la misma es muy importante. Los discos rígidos pueden contener información crítica, imposible de reemplazar. Inclusive piense en una computadora portátil, olvidada en la mesa de un bar. ¿Está la información debidamente resguardada aunque esa computadora caiga en otras manos?

Hay muchos dispositivos que bloquean el acceso a la computadora, alarmas de detección de movimiento y otros. Estos mecanismos pueden ser necesarios cuando realmente la información a resguardar es crítica.

El análisis y diseño de un sistema de seguridad apropiado siempre implica evaluar el costo del control sobre los beneficios de mantener los recursos resguardados. Por supuesto, no todos los controles son aplicables en todas las circunstancias y a veces puede ser difícil decidir el control apropiado, en función de los riesgos que se corren, por los costos económicos.

Aunque no lo pensemos, estamos viviendo en un ambiente repleto de controles. Ahora que conocemos un poco más, piense en todos los controles existentes desde que sale de su casa, hasta que hace una transacción en un cajero automático por ejemplo. Llaves de la casa, alarmas de la casa, idem con el automóvil, el equipo de música del automóvil -algunos con claves de seguridad-, tarjetas magnéticas, claves de acceso...

Hasta la próxima.