CONTENIDO

1. SEGURIDAD FÍSICA

La seguridad física es la parte más importante del mantenimiento de la seguridad de un sistema informático, y es a menudo pasada por alto por los administradores de sistemas descuidados que asumen que con echar de vez en cuando un vistazo rápido a los sistemas, es protección suficiente. Esto puede ser suficiente para algunos sistemas, pero en la mayoría de los casos, hay más factores que deben ser considerados antes de que un sistema puede darse por seguro físicamente.

- ¿Se encuentra el sistema en una superficie sólida y estable lo más cerca del suelo posible?
- ¿Está el sistema a salvo de la luz solar excesiva, viento, polvo, agua o temperaturas extremas de frío / calor?
- ¿Está el sistema situado en un sitio donde pueda tener un seguimiento, aislado y con poco tráfico humano?
- ¿Está la sala / edificio en el que se encuentra el sistema securizado con una cerradura o sistema de alarma para que sólo personal autorizado acceda? ¿Están las puertas cerradas con llave y las alarmas activadas fuera de horario de oficina?
- ¿Está el terminal del sistema bloqueado para evitar que alguien por casualidad pase por el sistema y lo use (aunque sólo sea por unos segundos)? ¿Están todos los usuarios desconectados del terminal?
- ¿Están los interruptores del terminal bloqueados o protegidos?
- ¿Existen dispositivos de entrada al sistema no asegurados / deshabilitados: unidades de disco bloqueadas / deshabilitadas? ¿Están los puertos paralelo / serie / infrarrojo / USB / SCSI asegurados o deshabilitados? ¿Existen discos duros conectados físicamente al sistema sin bloquear?

2. SEGURIDAD DE REDES

La seguridad de redes es la segunda parte más importante del mantenimiento de unos sistemas seguros. Si bien la seguridad física juega un papel importante, si opera en sus sistemas en un entorno de red / multiusuario, el sistema es mucho más susceptible a los ataques externos que un sistema autónomo. La seguridad de la red también es más difícil de evaluar, ya que requiere un conocimiento profundo de los diversos componentes y capas de su sistema y todos los servicios externos que interactúan con el sistema.

- Red Física: ¿está la red segura sin peligro de conexión no autorizada? ¿Tiene sólo el personal autorizado acceso a la red física a la que está conectado el sistema? ¿Conoce y confía en todos los diversos puntos donde se gestiona la conexión de red física / administrados por otra persona o entidad?
- ¿Están los otros sistemas de la misma red física y electrónicamente securizados? Si el sistema es razonablemente seguro, pero otro sistema de la red no lo es, la vulnerabilidad de su sistema se aumenta en gran medida.
- Tráfico de red aprobado:
    - ¿Conoce los nombres de los proveedores, la funcionalidad y la naturaleza del software en su sistema que participa en cualquier actividad de la red? ¿Ha comprobado que no existan parches de seguridad del software y recibe regularmente las actualizaciones de seguridad / vulnerabilidades del software que utiliza en la red?
    - ¿Ha probado a fondo cualquier servicio que funcione en la red para asegurarse de que por defecto no proporcionan a algún usuario no autorizado información de seguridad que se podría utilizar para atacar el sistema?
    - ¿Se limitan las capacidades de los usuarios para que la información sensible sobre el sistema no esté disponible en la red?
    - ¿Se permite la ejecución de la consola del sistema (o línea de comandos) sólo a usuarios autorizados?
    - ¿Es consciente de los agujeros de seguridad creados por cierto software que interactúa con otros?
    - ¿Mantiene suficientes registros (logs) de la actividad de red aprobada?
    - ¿Conoce todo el software que puede interactuar con la red, los números de puerto que utilizan, el tamaño y la ubicación de los ejecutables, etc?
    - ¿Se cambian las contraseñas de las cuentas de usuario de la red con regularidad?
    - ¿Se cifran los datos confidenciales que se transfieren a través de la red?
- Tráfico de red no aprobado:

- ¿Suele buscar intentos repetidos de conexión no autorizados para conectarse a su sistema a través de una red? ¿Mantiene registros suficientes de toda la actividad de red relacionada con su sistema?
- ¿Suele comprobar si los programas no autorizados que se ejecutan en su sistema que potencialmente podría permitir a un usuario conectarse a través de la red?
- ¿Monitoriza la actividad de red en busca de tráfico excesivo o inusual que llega a su sistema?

3. PROTOCOLOS / SERVICIOS

Una vez auditadas las capas físicas y de red de su sistema, la siguiente categoría en nuestro checklist de auditoría de seguridad informática es quizás una de los más complejas. Los ordenadores están hechos para calcular y, dependiendo del propósito de su sistema, se va a ejecutar diferente software y programas en cualquier momento. Es probable que en la mayoría de los casos, ya que todo el software fue desarrollado por diferentes personas con diferentes concepciones de la seguridad (y porque siempre hay gente que sabe más acerca de la seguridad), al menos uno de esos programas tiene algún tipo de problema de seguridad que podría ser explotado.

- Aunque en general es seguro asumir que el software que viene preinstalado en un nuevo sistema es razonablemente seguro, siempre se debe consultar con los desarrolladores de software sobre parches de seguridad, notas de versión y otra información relevante para su configuración particular.
- Para cualquier software que se instala en un nuevo sistema, asegúrese de que está plenamente seguro de las credenciales del desarrollador, todos los parches de seguridad, vulnerabilidades existentes y notas de la versión que existen. Debería hacer un hábito el consultar a los desarrolladores periódicamente para comprobar que no existan nuevos lanzamientos que puedan tener parches de seguridad. También es una buena idea suscribirse a los boletines de noticias de su software, o listas de correo generales, que puedan anunciar agujeros de seguridad.
- Una configuración errónea es probablemente la causa más común de que alguien explote un agujero de seguridad. La mayoría del software está desarrollado para ser razonablemente seguro, pero incluso el software más seguro puede ser utilizado para fines no deseados si está mal configurado. Siempre siga las instrucciones del proveedor para la instalación de software y siempre tome apuntes sobre cualquier problema que encuentre en el proceso de configuración. Si un programa requiere privilegios especiales para instalarse o ejecutar (por ejemplo, ejecutarse

como administrador en Windows), asegúrese de entender todas las implicaciones de tener que hacerlo y los posibles efectos secundarios creado en el proceso. Comprobar la configuración del software a fondo, tratar de romperla, trata de introducirse en ella (hackear), y ver si los demás pueden hacer lo mismo.

- Si un programa tiene acceso a datos sensibles, asegurarse de que sólo puede ser ejecutado por usuarios autorizados, y asegúrese de que los registros y la información que se almacena temporalmente, sea en un lugar seguro y decida rápido donde. Alguna gente puede hacer cosas asombrosas con la información que se encuentra en un archivo de registro del sistema.
- Si un programa se ejecuta como un *daemon* (demonio) (es decir, está en constante funcionamiento y responde a las peticiones de los usuarios a nivel local o en la red), asegúrese de que maneja correctamente desbordamientos de búfer, ataques de denegación de servicio y de sobrecarga general del sistema. Es generalmente una buena idea tener tan pocos servicios como sea posible ejecutándose como demonios, ya que permiten el acceso continuo y sin control por lo general a su sistema.
- Esté al tanto de todos los servicios que se supone que deben estar en ejecución en el sistema, la cantidad típica de los recursos (CPU por ejemplo, tiempo, memoria, espacio en disco) que ocupan. Compruebe si los demonios no identificables o software, o programas que no son habituales en su consumo de recursos. Recuerde que la mayoría de las violaciones de seguridad, ocurren con la configuración actual del sistema en lugar de instalar uno nuevo. A menos que tenga cuidado, un intruso puede manipular el sistema a su antojo y no notar nada fuera de lo común.
- Haga un recuento de los procesos para realizar un seguimiento de los patrones típicos de uso de software de los usuarios.

4. SEGURIDAD DE USUARIO

Las particularidades de la seguridad de los usuarios varía mucho dependiendo del sistema que se esté usando. En algunos casos, el sistema será una máquina aislada, realizando principalmente las funciones del servidor con muy pocos usuarios que realmente inicien sesión y usen directamente el sistema, por consiguiente los usuarios interactúan con las funciones del servidor. En otros casos, un sistema puede tener cientos de usuarios accediendo directamente al sistema de forma simultánea. Obviamente, el grado en el que la seguridad del usuario es una inquietud depende en gran medida de la tipología de sus usuarios, pero tenga en cuenta que un usuario que intente violar la seguridad, o que tenga malas prácticas de seguridad, puede afectar y posiblemente poner en peligro todo el sistema.

- Desarrolle un método estándar para la creación y mantenimiento de cuentas de usuario. Desarrollar políticas aceptables de uso claras y concisas y comunicarlo así a los usuarios. No crear cuentas de usuario para personas u organizaciones con quienes no ha interactuado de alguna forma, o que han sido conocidos por tener problemas de seguridad en otros sistemas.
- Debe fijar límites a la cantidad de recursos que un usuario puede consumir, desde el número de inicios de sesión a la cantidad de espacio en disco, asegúrese de que el usuario no puede causar un fallo de seguridad o acabar con el sistema por una estupidez (por ejemplo, una rutina en bucle, que crea una archivo de 10 MB cada vez).
- En algunos casos, es posible que desee limitar la forma en que un usuario puede conectarse a la red, si usted está proporcionando un inicio de sesión de terminal, asegúrese de que el propio terminal sea seguro y es mantenido. Si usted proporciona acceso directo a través de protocolos como telnet, considere ejecutar servicios como tcp_wrappers o identd para verificar que el usuario se conecta desde el sistema que dicen estar usando.
- Mantener registros detallados de la actividad del usuario, en concreto, la hora de conexión, la duración y el lugar desde donde ha entrado en el. En algunos casos es posible que desee registrar con más detalle con el recuento de procesos, historial de comandos de usuario y control de la actividad.
- Debe revisar periódicamente la actividad inusual del usuario, hay muchos programas disponibles que constantemente revisan los intentos fallidos por parte de los usuarios de obtener permisos de administrador, acceder a archivos que no deben, o realizar otras tareas no autorizadas.

5. SEGURIDAD DE DATOS

Los datos y el almacenamiento de archivos, en principio no parece presentarse como un riesgo de seguridad, ya que los usuarios tienen acceso a los archivos o no lo tienen. Resulta que hay muchas formas, y algunas complicadas, de acceder a los mismos datos en un sistema, y un buen administrador de sistemas debería ser consciente de todo esto.

- Conozca el esquema de propiedad de los archivos que el sistema implementa: ¿está basado en grupos, usuarios, roles o alguna combinación de estos? Conozca los diferentes niveles de protección que se pueden aplicar a los archivos y directorios y sea consciente de quien tiene acceso para realizar cambios en estas protecciones.
- Conozca la estructura general de los sistemas de archivo, cuánto se almacena dónde y quién accede normalmente a qué partes de ellos. Mantenga registros de actividad de disco (por ejemplo, cambios significativos en el espacio de disco utilizado) y de los problemas de disco.
- Asegúrese de que los usuarios sólo pueden tener acceso a las partes del sistema a las que deberían tenerlo; su esquema de protección debe incluir de forma clara y fácil una separación lógica y conceptual de los archivos de usuario y los datos de los archivos del sistema.
- Asegúrese de que los regímenes de propiedad de los archivos son compatibles para varios directorios (es decir, que el propietario de un directorio es titular de todos los archivos de ese directorio, etc)
- Asegúrese de que los usuarios no pueden tener acceso a más recursos de disco de lo previsto; a menudo la mejor solución para controlar esto es establecer quotas de disco.
- Si los sistemas de archivos están disponibles a través de cualquier red o protocolo de uso compartido, examine cuidadosamente la seguridad de estos protocolos (ver sección de «protocolos / servicios» más arriba). Siempre revise su configuración de estos servicios para asegurarse de que sólo los usuarios y equipos autorizados se les permite acceder a los datos compartidos; muchas configuraciones por defecto permiten el acceso no autorizado.
- Mantenga siempre copias de seguridad de los sistemas, el método más habitual es realizar copias de seguridad de archivos a una cinta y luego guardarla para proteger contra la pérdida de datos por incendio, inundación, etc. En el caso de los sistemas operativos, es una buena idea mantener una copia buena conocida de la configuración de su sistema operativo en un medio de sólo lectura, como un DVD-ROM o algún otro sistema.

- Si mantiene bases de datos, asegúrese de que la base de datos es accesible sólo por los usuarios autorizados, tanto en el lado del cliente (a través de una herramienta de consulta de datos como SQLnet) como en el lado del servidor (es decir, los archivos de bases de datos reales almacenados en el disco de su sistema). Al igual que con otros servicios, asegúrese de que las bases de datos tienen la seguridad adecuada.

6. CONTRASEÑAS

Las contraseñas son los componentes centrales en la mayoría de los esquemas de seguridad; las cuentas de usuario, los sitios web sensibles y los servicios del sistema están protegidos por ellas. Si conoce las contraseñas correctas, puede obtener privilegios de administrador en un sistema en el que ni siquiera sea un usuario o infiltrarse en un entorno en el que nunca ha trabajado antes.

Su debilidad como medida de seguridad está en su poder, una contraseña es todo lo que necesita para tener acceso completo a todo un sistema y las contraseñas PUEDEN descifrarse. Lo mejor que puede hacer es tratar de hacer que estas dos cosas sean muy poco probables.

- Requerir contraseñas únicas y complejas de todas las cuentas de usuario en el sistema, no es aceptable tener cuentas de «invitados» u otras cuentas que no requieren ningún tipo de autenticación. Si una cuenta no se ha usado para la conexión (es decir, que esa cuenta nunca será utilizada), quite su posibilidad de iniciar sesión por completo.
- Las contraseñas deben contener al menos 8 caracteres y una combinación de letras y números, mayúsculas y minúsculas. Las contraseñas no deben parecerse a cualquier palabra, nombre, idea o concepto que pueda aparecer en cualquier diccionario de cualquier parte del mundo. Un buen ejemplo: **jY2EHxq#y**
- Obligar la rotación (distinta a las anteriores) y caducidad de contraseñas. Los usuarios nunca deberían poder mantener una contraseña más de unos pocos meses, ya que alguien fácilmente podría (pero imperceptiblemente) romper por fuerza bruta una contraseña durante un largo período de tiempo. También debe asesorar a los usuarios contra el uso de la misma contraseña en otros sitios.
- El archivo de contraseñas o mecanismo que se use para almacenar las contraseñas debería estar encriptado y no debería estar disponible para el usuario medio. Si un usuario pudiera obtener el archivo de contraseñas, puede utilizarlo en otro sistema para intentar descifrar las contraseñas sin que te des cuenta.

- No escriba las contraseñas y no las guarde en otra cosa que no sea la memoria humana, a ser posible.
- Las contraseñas del sistema se deben cambiar al menos una vez al mes y no se deberían compartir con más gente de lo necesario.

7. ADMINISTRACIÓN DEL SISTEMA

Unas técnicas de administración de sistemas de calidad pueden marcar la diferencia en la seguridad. No hay un montón de cosas que haga falta hacer en la mayoría de los sistemas modernos, ya que hacen comprobaciones automáticas y mantienen al administrador del sistema informado de cualquier cambio sospechoso. Pero todavía hay algunos consejos generales a seguir:

- Periódicamente navegar a través de su sistema, mirar el contenido de los directorios del sistema, registros y otros archivos. Anote las ubicaciones y tamaños de archivos. Observe los patrones de uso de las máquinas y sus usuarios.
- Ejecute herramientas de cracking (como «CRACK» y «Satanás» en el entorno Unix) con regularidad para comprobar si hay vulnerabilidades en la configuración del sistema.
- Trate de romper la seguridad manualmente a través de diferentes medios.
- Sea consciente de las personas o grupos que puedan tener intenciones de penetrar en su sistema.
- Mantenga a sus usuarios informados de sus técnicas de seguridad y lo que se espera de ellos para mantener la seguridad.