**Principio de mínimo privilegio**

Los controles de seguridad desempeñan un rol fundamental para mantener la privacidad y seguridad de los datos confidenciales. Uno de los controles más comunes es el principio del mínimo privilegio, también conocido como PoLP o privilegio mínimo. Este principio de seguridad se basa en otorgar a los usuarios únicamente el nivel mínimo de acceso y autorización necesarios para llevar adelante una tarea o función específica.

El privilegio mínimo representa un control de seguridad clave que respalda la tríada de confidencialidad, integridad y disponibilidad (CID) de la información. En esta lectura, explorarás cómo el principio de mínimo privilegio ayuda a reducir el riesgo, cómo se implementa habitualmente y por qué es esencial someterlo a auditorías periódicas.

**Reducir el acceso disminuye el riesgo**

Toda empresa debe estar preparada para enfrentar el riesgo de robo, uso indebido o abuso de datos. La aplicación del principio de mínimo privilegio puede reducir significativamente el riesgo de incidentes costosos, como las filtraciones de datos, mediante las siguientes medidas:

* Limitando el acceso a la información confidencial.
* Reduciendo las posibilidades de modificación, alteración o pérdida accidental de datos.
* Facilitando la supervisión y la administración del sistema.

El principio de mínimo privilegio reduce considerablemente la probabilidad de un ataque exitoso al conectar recursos específicos a determinados usuarios y establecer límites a sus acciones. Es un control de seguridad importante que debe aplicarse a todos los activos. Para implementar efectivamente el mínimo privilegio es fundamental empezar por definir de manera clara quiénes son los usuarios o entidades involucradas.

**Determinar el acceso y la autorización**

Para implementar el principio de mínimo privilegio, es necesario determinar el acceso y la autorización previamente. Para lograrlo, hay dos preguntas clave que deben responderse:

* ¿Quién es el usuario en cuestión?
* ¿Cuánto acceso requiere a un recurso específico?

Identificar un usuario suele ser un proceso sencillo. Usuario puede ser una persona (cliente, personal, proveedor) o un dispositivo o software conectado a la red empresarial. En general, cada usuario debería tener su propia cuenta, y estas cuentas, por lo general, se almacenan y gestionan dentro del servicio de directorio de la organización.

Estos son los tipos más comunes de cuentas de usuario:

* **Cuentas de invitado:** se proporcionan a usuarios externos que necesitan acceder a una red interna, como clientes, colaboradores externos o socios comerciales.
* **Cuentas de usuario:** se asignan al personal en función de sus responsabilidades laborales.
* **Cuentas de servicio:** se otorgan a aplicaciones o software que necesitan interactuar con otros programas en la red.
* **Cuentas privilegiadas:** tienen permisos elevados o acceso administrativo.

Es una buena práctica determinar un nivel de acceso inicial para cada tipo de cuenta antes de implementar el principio de mínimo privilegio. Sin embargo, el nivel de acceso apropiado puede cambiar de un momento a otro. Por ejemplo, una persona que trabaja en servicio de atención al cliente solo debería tener acceso a tu información mientras te está brindando asistencia. No obstante, cuando esta persona comience a atender a otro cliente y ya no te esté asistiendo activamente, tus datos deberían volver a quedar inaccesibles. El mínimo privilegio solo puede reducir el riesgo si las cuentas de usuario son monitoreadas de forma rutinaria y consistente.

**Consejo profesional:** Las contraseñas desempeñan un papel importante al implementar el principio del mínimo privilegio. Incluso si las cuentas de usuario están asignadas adecuadamente, una contraseña insegura puede comprometer los sistemas.

**Auditoría de los privilegios de cuentas**

Establecer las cuentas de usuario adecuadas y asignarles los derechos de acceso o privilegios apropiados es un paso inicial muy valioso. Sin embargo, realizar auditorías periódicas de estas cuentas es una parte esencial para mantener seguros los sistemas de tu empresa.

Existen tres enfoques comunes para auditar las cuentas de usuario:

* Auditorías de uso
* Auditorías de privilegios
* Auditorías de cambios de cuenta

Como profesional de seguridad, es posible que participes en cualquiera de estos procesos.

**Auditorías de uso**

Cuando se realiza una auditoría de uso, el equipo de seguridad revisa a qué recursos está accediendo cada cuenta y de qué forma los usuarios interactúan con estos recursos. Estas auditorías son útiles para determinar si los usuarios están cumpliendo con las políticas de seguridad de la organización. Además, permiten identificar si un usuario tiene permisos que podrían ser revocados debido a que ya no están siendo utilizados.

**Auditorías de privilegios**

Con el paso del tiempo, es común que los usuarios acumulen más privilegios de acceso de los que realmente necesitan, un fenómeno conocido como arrastre de privilegios. Esto puede suceder si un empleado recibe un ascenso o cambia de equipo, lo que conlleva cambios en sus responsabilidades laborales. Las auditorías de privilegios tienen como objetivo evaluar si el rol de un usuario se encuentra en consonancia con los recursos a los que actualmente tiene acceso.

**Auditorías de cambios de cuentas**

Los servicios de directorio de cuentas mantienen inventarios y registros asociados a cada usuario. Los cambios en una cuenta generalmente se guardan y pueden utilizarse para auditar el directorio en busca de actividades sospechosas, como múltiples intentos de cambiar la contraseña de una cuenta. Realizar auditorías de cambios de cuenta ayuda a asegurar que todas las modificaciones en las cuentas sean realizadas por usuarios autorizados.

**Nota:** La mayoría de los servicios de directorio se pueden configurar para alertar a quienes administran el sistema sobre actividades sospechosas.

**Conclusiones clave**

El principio de mínimo privilegio es un control de seguridad que puede reducir el riesgo de acceso no autorizado a información y recursos confidenciales. Configurar y ajustar las cuentas de usuario con los niveles adecuados de acceso y autorización es un paso importante para implementar el mínimo privilegio. La auditoría de las cuentas de usuario y la revocación de derechos de acceso innecesarios son prácticas fundamentales que contribuyen a mantener la confidencialidad, integridad y disponibilidad de la información de manera efectiva.