daibackup

Protocolo Hardening

daibackup
Security Backup And Recovery Service

Que es el Hardening

El hardening, en el contexto de la ciberseguridad, se refiere al proceso de asegurar y fortalecer un sistema informático o una red, reduciendo así las posibilidades de que sea explotado por amenazas y ataques cibernéticos. Consiste en aplicar medidas y configuraciones de seguridad adicionales para mitigar las vulnerabilidades y minimizar los riesgos de compromiso de la seguridad.

Es importante realizar el hardening en los sistemas y servidores debido a varias razones:

- Protección contra amenazas
- Cumplimiento normativo
- Mantenimiento de la reputación
- Mejora de la resistencia

Aquí te presentamos un protocolo de hardening para Linux y Windows que puedes implementar en tu empresa.

Protocolo de Hardening para Servidores Linux:

1. Actualización del sistema operativo:
    - Mantén siempre el sistema operativo actualizado con los últimos parches de seguridad y actualizaciones.
    - Configura la configuración de actualización automática para aplicar parches y actualizaciones de forma regular.
2. Configuración del firewall:
    - Configura y activa un firewall para bloquear el tráfico no autorizado.
    - Asegúrate de permitir solo los puertos y servicios necesarios para el funcionamiento del servidor.
    - Considera el uso de un firewall de aplicaciones web (WAF) para proteger aplicaciones web específicas.
3. Eliminación de software innecesario:
    - Elimina cualquier software o servicio innecesario que no se utilice en el servidor.
    - Deshabilita y elimina servicios y demonios no esenciales para minimizar las posibles vulnerabilidades.

4. Acceso seguro:
    - Desactiva el acceso root remoto y utiliza cuentas de usuario con privilegios limitados.
    - Utiliza claves SSH en lugar de contraseñas para autenticación remota.
    - Considera el uso de autenticación de dos factores para agregar una capa adicional de seguridad.
5. Seguridad de contraseñas:
    - Exige contraseñas fuertes y complejas para las cuentas de usuario.
    - Establece una política de cambio de contraseñas periódico.
    - Considera el uso de herramientas de gestión de contraseñas para almacenar contraseñas de forma segura.
6. Control de acceso:
    - Configura adecuadamente los permisos de archivos y directorios para restringir el acceso no autorizado.
    - Limita los privilegios de usuario a lo mínimo necesario para llevar a cabo sus funciones.
7. Auditoría y monitoreo:
    - Implementa registros de auditoría y habilita el monitoreo de eventos de seguridad.
    - Realiza análisis periódicos de los registros para detectar actividades sospechosas o intentos de intrusión.
8. Encriptación de datos:
    - Utiliza encriptación para proteger datos confidenciales en reposo y en tránsito.
    - Considera el uso de SSL/TLS para proteger las comunicaciones web.
9. Respaldos regulares:
    - Realiza copias de seguridad periódicas de los datos importantes y verifica su integridad.
    - Almacena las copias de seguridad en ubicaciones seguras y fuera del servidor.
10. Mantenimiento y revisión continua:
    - Realiza auditorías periódicas de seguridad para identificar posibles vulnerabilidades.
    - Mantén un seguimiento de las actualizaciones y los avisos de seguridad relevantes para el sistema operativo y el software utilizado.

Protocolo de Hardening para Servidores Windows:

1. Actualización del sistema operativo:
    - Mantén siempre el sistema operativo actualizado con los últimos parches de seguridad y actualizaciones.
    - Configura la configuración de actualización automática para aplicar parches y actualizaciones de forma regular.
2. Configuración del firewall:
    - Configura y activa el firewall de Windows para bloquear el tráfico no autorizado.
    - Asegúrate de permitir solo los puertos y servicios necesarios para el funcionamiento del servidor.

3. Eliminación de software innecesario:
    - Elimina cualquier software o servicio innecesario que no se utilice en el servidor.
    - Deshabilita y elimina servicios y características no esenciales para minimizar las posibles vulnerabilidades.
4. Acceso seguro:
    - Desactiva el acceso de cuentas de administrador remoto y utiliza cuentas de usuario con privilegios limitados.
    - Utiliza contraseñas complejas y cambia las contraseñas de forma regular.
5. Seguridad de contraseñas:
    - Exige contraseñas fuertes y complejas para las cuentas de usuario.
    - Establece una política de cambio de contraseñas periódico.
    - Considera el uso de herramientas de gestión de contraseñas para almacenar contraseñas de forma segura.
6. Control de acceso:
    - Configura adecuadamente los permisos de archivos y carpetas para restringir el acceso no autorizado.
    - Limita los privilegios de usuario a lo mínimo necesario para llevar a cabo sus funciones.
7. Auditoría y monitoreo:
    - Implementa registros de auditoría y habilita el monitoreo de eventos de seguridad.
    - Realiza análisis periódicos de los registros para detectar actividades sospechosas o intentos de intrusión.
8. Encriptación de datos:
    - Utiliza la encriptación BitLocker para proteger los datos en reposo en discos duros y dispositivos extraíbles.
9. Antivirus y antimalware:
    - Instala un software antivirus confiable y mantén las definiciones actualizadas.
    - Realiza escaneos periódicos del sistema en busca de malware y amenazas.
10. Mantenimiento y revisión continua:
    - Realiza auditorías periódicas de seguridad para identificar posibles vulnerabilidades.
    - Mantén un seguimiento de las actualizaciones y los avisos de seguridad relevantes para el sistema operativo y el software utilizado.

Es importante tener en cuenta que estos protocolos de hardening son solo pautas generales y que cada servidor y entorno puede tener requisitos específicos adicionales. Se recomienda consultar las mejores prácticas de seguridad específicas para los sistemas operativos y

software utilizados, así como contar con la ayuda de profesionales de seguridad cibernética calificados para realizar una evaluación exhaustiva de la seguridad.

DaiBackup puede ayudar a respaldar y mantener copias de seguridad actualizadas de tu sistema.