Auditoría Active Directory
Lista de control

Mouhyi Eddine Lahlali

Esta lista de comprobación mejorada proporciona un marco detallado para auditar un entorno de Active Directory, centrándose en la seguridad, el cumplimiento y la
eficiencia operativa. La realización periódica de este tipo de auditorías puede reducir significativamente los riesgos de seguridad y ayudar a mantener una infraestructura AD sólida, segura y eficiente.

Configuración de seguridad avanzada

- Active la configuración avanzada de políticas de auditoría para garantizar una auditoría detallada de los eventos más importantes.
- Compruebe si existe algún SID nulo en los permisos de seguridad que pudiera permitir el acceso anónimo.
- Audite el uso de las cuentas de servicio para asegurarse de que están configuradas con el principio de mínimo privilegio y de que se han configurado los nombres principales de servicio (SPN) adecuados.
- Implemente LDAP Signing y LDAPS (LDAP sobre SSL) para protegerse de los ataques man- in-the-middle.

Gestión de acceso privilegiado

- Revise e implemente políticas de administración justa (JEA) para limitar el uso de comandos powershell según la función.
- Audite el uso de estaciones de trabajo con acceso privilegiado (PAW) para gestionar tareas sensibles con el fin de reducir las superficies de ataque.
- Garantizar la aplicación del modelo de niveles administrativos para separar las cuentas administrativas en función de su ámbito de administración.

Prácticas de seguridad de cuentas

- Aplique la configuración del Control de cuentas de usuario (UAC) para mitigar el impacto de un ataque de malware.
- Implantar la autenticación multifactor (MFA) para todas las cuentas administrativas y de usuarios sensibles.
- Revise y aplique políticas de bloqueo de cuentas para protegerse contra ataques de fuerza bruta.

Políticas de contraseñas detalladas

- Compruebe y aplique políticas de contraseñas detalladas (FGPP) para aplicar diferentes políticas de contraseñas dentro del mismo dominio, especialmente para cuentas de usuarios con privilegios elevados.

DNS y protección de redes

- Audite las zonas DNS y las configuraciones de seguridad y asegúrese de que las actualizaciones de DNS dinámico están protegidas.
- Revise y proteja las zonas DNS integradas en AD aplicando restricciones de listas de control de acceso (ACL).
- Asegúrese de que los controladores de dominio están correctamente aislados en la red para evitar accesos no autorizados.
- Sincronización horaria
- Compruebe que todos los controladores de dominio y servidores miembros están sincronizados con una fuente de hora fiable para evitar problemas de autenticación Kerberos.

Delegación de control

- Revise las delegaciones para garantizar que sólo se conceden los permisos necesarios y utilice funciones administrativas para la delegación siempre que sea posible.
- Audite los permisos delegados personalizados para detectar posibles excesos de privilegios y garantizar la segregación de funciones.

Gestión de objetos de directiva de grupo (GPO)

- Revisar y limpiar los GPO no utilizados y los GPO no vinculados.
- Audite la configuración de permisos de GPO para garantizar que sólo los usuarios autorizados puedan modificar los GPO de alto impacto.
- Implantar prácticas de control de versiones y gestión de cambios de GPO para realizar un seguimiento de los cambios y su impacto.

Protección de sistemas y objetos críticos

- Proteja los objetos críticos de AD con SDHolder administrativo y Security Descriptor Propagator para evitar cambios no autorizados.
- Active la función de papelera de reciclaje en AD para recuperar objetos eliminados.
- Audite y asegure la Política de Dominio Predeterminado y la Política de Controladores de Dominio Predeterminados revisando su configuración y asegurándose de que se aplican correctamente.
- Compruebe que se realizan copias de seguridad de AD con regularidad y pruebe los procedimientos de recuperación para asegurarse de que son eficaces.
- Revise el Plan de recuperación ante desastres (DRP) de Active Directory para asegurarse de está actualizado y es completo.

Registro, supervisión y auditoría

- Asegúrese de que la auditoría de AD está activada para eventos clave como la creación, eliminación y modificación de cuentas.
- Revise los registros de seguridad para detectar actividades sospechosas o infracciones de las políticas.
- Implemente una solución de registro centralizada para mejorar el análisis y la supervisión de los eventos relacionados con AD.

Copia de seguridad y recuperación

- Compruebe que se realizan copias de seguridad de AD con regularidad y pruebe los procedimientos de recuperación para asegurarse de que son eficaces.
- Revise el Plan de recuperación ante desastres (DRP) de Active Directory para asegurarse de está actualizado y es completo.

Replicación y topología de sitios

- Compruebe si hay errores o problemas en la replicación de AD utilizando herramientas como REPADMIN o AD Replication Status Tool.
- Revise la topología del sitio para asegurarse de que refleja la infraestructura de red actual y optimiza el tráfico de replicación.

Gestión de esquemas

- Audite los cambios en el esquema de AD para garantizar que están autorizados y documentados.
- Revise la versión del esquema y compárela con la versión actual de AD DS para comprobar la compatibilidad.