Azure Active Directory y Seguridad de Office 365

No permita que su Active Directory en las instalaciones sea su talón de Aquiles.

Escrito por Alvaro Vitta

INTRODUCCIÓN

Setenta por ciento de las empresas de Fortune 500 compraron Office 365 en un período reciente de 12 meses. Microsoft dice que Office 365 es el producto comercial de mayor crecimiento de todos los tiempos.

Eso no es ninguna novedad.

Sin embargo, Active Directory (AD) en las instalaciones aún juega un papel importante al ser la fuente autorizada para las solicitudes de autenticación y autorización de Office 365. Los administradores de sistema de la gran mayoría de las empresas utilizan la sincronización Azure AD unidireccional en este entorno de directorio híbrido: sincronizan sus usuarios AD autorizados en las instalaciones, grupos, atributos y contraseñas hasta la nube para su autenticación y autorización para Azure AD y Office 365.

Eso significa que si el Active Directory en las instalaciones no es seguro, Azure AD y Office 365 no serán seguros.

En este documento se describe una metodología de seguridad para gobernar un entorno de Azure Active Directory híbrido en las instalaciones. Los administradores de sistema encontrarán explicaciones detalladas y listas de verificación para mejorar su posición de seguridad y evitar que su AD en las instalaciones se vuelva el talón de Aquiles de la seguridad de Azure AD y Office 365.

LA SITUACIÓN DEL DIRECTORIO HÍBRIDO: EN LAS INSTALACIONES ACTIVE DIRECTORY Y AZURE ACTIVE DIRECTORY

Toda empresa que ejecuta Microsoft Office 365 tiene Azure AD, que es necesario a fin de almacenar las identidades de usuario y otras propiedades de los arrendatarios para las aplicaciones de productividad de Office, Exchange Online, SharePoint Online, Lync Online y toda aplicación personalizada en la nube.

Al mismo tiempo, más del 90 % de las empresas han ejecutado y aún ejecutan AD en las instalaciones como el mayor almacenamiento para la autenticación de los empleados, la administración de la identidad y las políticas de control de acceso detrás de los productos en las instalaciones como

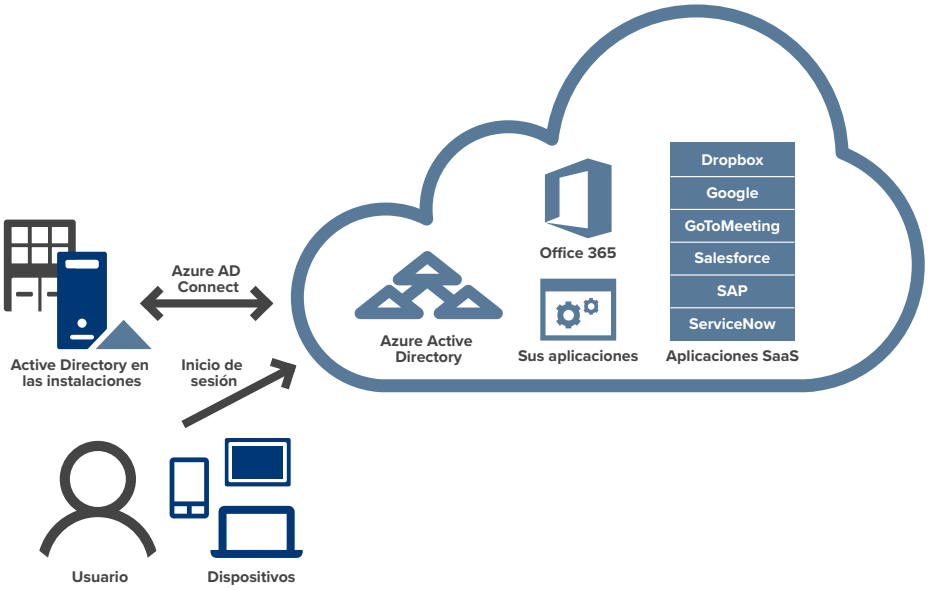

Figura 1: Diagrama de flujo de trabajo de sincronización de Azure AD Connect

> El acceso a las aplicaciones de Office 365 y sus datos correspondientes está controlado por las cuentas de usuario y sus membresías de grupo en el AD en las instalaciones.

Office, Exchange, SharePoint, Lync y cientos de aplicaciones de línea de empresa personalizadas.

Para abordar la situación del directorio híbrido, Microsoft ha proporcionado la herramienta de administración Azure AD Connect para que los administradores de sistema puedan sincronizar contraseñas, identidades, usuarios, grupos y sus atributos correspondientes (que posiblemente incluyen hashes de contraseña) desde el AD en las instalaciones con Azure AD sin la necesidad de crear nuevos elementos (consultar Figure 1).

Actualmente, Azure AD Connect es el punto único de compra de Microsoft para esta conexión. Reemplaza las herramientas de administración de Active Directory, DirSync y Azure AD Sync, y permite actualizar o migrar las implementaciones existentes de esas herramientas de manera rápida y fácil.

EL ENTORNO DE DIRECTORIO HÍBRIDO ES TAN SEGURO COMO SU ENLACE MÁS DÉBIL.

Cuando el Active Directory en las instalaciones es la fuente autorizada, los administradores pueden controlar y administrar las cuentas de usuario a través del complemento Usuarios y computadoras de Active Directory. Crean y eliminan cuentas de usuario, contactos y grupos; modifican las membresías de grupo y desactivan cuentas en el AD en las instalaciones. Los cambios se replican en un plazo de tres horas cuando utilizan Azure AD Connect 1.0 o en 30 minutos si usan la versión 1.1.

Mientras tanto, las funciones de seguridad en la nube de Microsoft, como la seguridad profunda en capas, proporciona un enfoque integral en capas en los niveles lógico, físico y de datos. Lamentablemente, el AD en las instalaciones no incluye los mismos tipos de controles.

Por eso, a pesar de la seguridad profunda en capas integrada en Office 365, prevalecen los controles de acceso de Active Directory en las instalaciones. Eso significa que el acceso a las aplicaciones de Office 365 y sus datos correspondientes está controlado por las cuentas de usuario y sus membresías de grupo en el AD en las instalaciones. Como resultado, los controles compensatorios (o la falta de controles) que gobiernan el AD en las instalaciones determinarán si el acceso a Azure AD y a Office 365 es seguro o no.

La falta de controles de seguridad compensatorios dentro del entorno del AD en las instalaciones es una receta para las infracciones de datos y las amenazas internas en un entorno de directorio híbrido con la sincronización unidireccional del AD en las instalaciones para asegurar Azure AD.

ANATOMÍA DE UNA INFRACCIÓN DE DATOS EN UN ENTORNO DE DIRECTORIO HÍBRIDO

Un informe de Ponemon Institute titulado "Abuso del usuario con privilegios y la amenaza interna" destaca tres riesgos principales por factor humano en el abuso de acceso de los usuarios con privilegios:

- El 73 % de los que respondieron dijo que los usuarios con privilegios creen que tienen el poder de acceder a toda la información que pueden ver ("Puedo hacerlo, por lo tanto, tal vez lo haga").
- El 65 % dijo que los usuarios con privilegios acceden a datos confidenciales por curiosidad ("Tengo curiosidad, por lo tanto, tal vez lo haga").
- El 54 % dijo que la empresa designa derechos de acceso privilegiado que van más allá del puesto o responsabilidad del individuo ("Nada me detiene, por lo tanto, tal vez lo haga").

Tenga en cuenta este escenario, en el que esos factores de riesgo crean una posición de seguridad debilitada, una infracción de datos y un uso de información privilegiada en un entorno de directorio híbrido.

Sam es un contratista del área de TI y administrador de dominios que trabaja en una empresa financiera de tamaño mediano. La empresa utiliza grupos de AD en las instalaciones para otorgar acceso a las aplicaciones en las instalaciones y usa una sincronización unidireccional de grupos y membresías para su arrendatario de Azure AD a fin de obtener el acceso a Office 365.

1. Mary, la nueva colega de Sam, olvida la contraseña de la cuenta de servicio utilizada para ejecutar una aplicación financiera en varios servidores de Windows. Le pide a Sam que delegue sus derechos para restablecer las contraseñas.
2. Sam utiliza el asistente de delegación del complemento incorporado Usuarios y computadoras de Active Directory para delegar el acceso a Mary a fin de que restablezca las contraseñas en la unidad organizativa (UO) que contiene la cuenta de servicio. Sam no tuvo en cuenta que la UO también contiene otras cuentas de servicio y cuentas administrativas (miembros de los grupos de administradores de dominios). Tampoco tuvo en cuenta que le está otorgando a Mary un acceso mayor del que necesita para llevar a cabo la tarea.
3. Mary restablece la contraseña en la cuenta de servicio de la aplicación financiera.
4. Mary descubre que también puede restablecer las contraseñas de otras cuentas de administración elevadas. Restablece la contraseña de una cuenta de administración privilegiada.
5. Inicia sesión con la cuenta de administración y otorga permisos a su cuenta secundaria para poder hacer cambios en la membresía de grupo en cualquier grupo del AD.
6. Utiliza sus derechos delegados para agregar su cuenta secundaria al grupo de operaciones financieras dentro del AD en las instalaciones de la empresa.
7. Al igual que muchos otros grupos, la membresía del grupo de operaciones financieras en el AD en las instalaciones está sincronizado con Azure Active Directory para otorgar acceso a las aplicaciones de Office 365 de la empresa. En este caso, la membresía del grupo proporciona acceso a datos financieros Sarbanes-Oxley (SOX) en los documentos de SharePoint Online de Office 365.
8. Mary tiene curiosidad. Descubre que tiene acceso a información financiera confidencial en el SharePoint Online de Office 365 de la empresa.
9. Abre las carpetas, encuentra un archivo llamado AcquisitionsPending.docx, lo abre y hace tres capturas de pantalla. Este archivo contiene información sobre la adquisición propuesta de un competidor comercial público.
10. Mary utiliza su conocimiento interno para comprar 10.000 acciones de la empresa objeto de la adquisición. Tres meses después, se realiza la adquisición. Mary vende sus acciones y obtiene una ganancia del 30 %.
11. A continuación se realiza una investigación de SEC, que involucra a los equipos de finanzas, cumplimiento y legal durante meses. Mary es procesada por uso de información privilegiada, pero el daño a la reputación de la empresa perdura.

Este es un ejemplo de cómo una falta de controles de seguridad compensatorios sobre la fuente autorizada para las políticas de acceso (aquí, en Active Directory en las instalaciones) puede afectar las aplicaciones y los datos a los que acceden los usuarios en Office 365.

> Mary tiene curiosidad y descubre que puede acceder a información financiera confidencial en el SharePoint Online de Office 365 de la empresa.

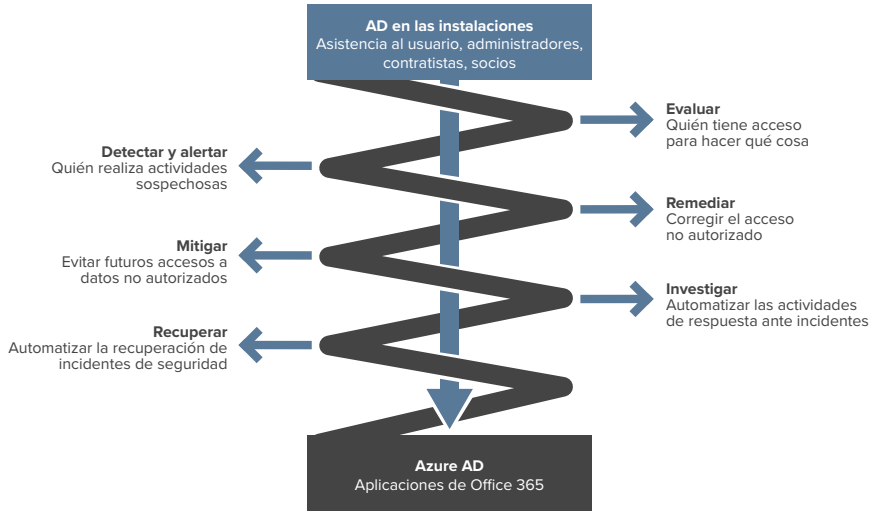

Figura 2: Metodología de seguridad para directorio híbrido

La seguridad del directorio híbrido comienza al evaluar continuamente los privilegios y el acceso, y al establecer la línea de base de la configuración de seguridad.

UN ENFOQUE PARA FORTALECER EL ENLACE DEBILITADO EN EL ENTORNO DE DIRECTORIO HÍBRIDO

Quest recomienda un enfoque para la seguridad en el entorno de directorio híbrido que proteja el acceso a AD en las instalaciones y, en consecuencia, mejore la seguridad de Azure AD y Office 365. El resultado es una posición de seguridad de directorio híbrido aún más global.

Según se muestra en la Figura 2, el enfoque cubre seis áreas de consulta.

Evaluar

¿Dónde comienza la seguridad del directorio híbrido? Comienza al evaluar continuamente los privilegios y el acceso, y al establecer la línea de base de la configuración de seguridad. Esto incluye informar periódicamente qué usuarios tienen acceso para realizar qué tareas, ya sea directamente a través de sus cuentas o indirectamente a través de una membresía de grupo.

Las evaluaciones deben incluir detalles sobre todos los usuarios con los tipos de acceso más confidenciales:

- Permisos para restablecer contraseñas de usuarios y restaurar el AD.
- Permisos para restablecer contraseñas de usuarios sobre cualquier objeto.
- Grupos con privilegios elevados, como los administradores de complementos, administradores de dominios, administradores de esquemas y administradores empresariales.
- Grupos comerciales confidenciales, como el personal de finanzas, ejecutivo y de D+I.
- Datos confidenciales, como la información de identificación personal, datos e información de la Industria de Tarjetas de Pago (PCI) requeridos para cumplir con SOX e HIPAA.
- Grupos anidados que indirectamente son parte de un grupo con privilegios elevados o un grupo comercial confidencial.
- Permisos sobre el objeto AdminSDHolder
- Cuentas inactivas (último inicio de sesión de más de 90 días, cuentas vencidas, último restablecimiento de contraseña que excede la política de contraseñas)
- Permisos para iniciar sesión en controladores de dominios
- Permisos para instalar software en controladores de dominios

Detectar y alertar

¿Qué sucede en el caso de que haya cambios de seguridad que se desvían de las líneas de base de la evaluación? El sistema debe detectarlos tan pronto ocurran y alertar automáticamente a los administradores.

Los cambios de mayor interés incluyen las actividades sospechosas más comunes:

- Contraseñas de usuario cambiadas por no propietarios
- Cambios de membresía directos e indirectos (grupo anidado) en grupos con privilegios elevados
- Cambios en los permisos de seguridad en el objeto AdminSDHolder

- Cambios en la configuración confidencial del Objeto de política grupal (GPO), como “Negar inicio de sesión de manera local,” el nivel del Administrador de LAN NT (NTLM) y las políticas de AppLocker
- Eliminaciones masivas de cuentas
- Designación de permisos confidenciales de AD, como delegación de restablecimiento de contraseña del usuario en UO confidenciales
- Múltiples intentos fallidos de inicio de sesión seguidos por un inicio exitoso en los controladores de dominios
- Inicios de sesión en controladores de dominios durante horas no laborales
- Eliminaciones o modificaciones masivas de objetos y atributos de AD
- Adición de un usuario al grupo de administradores, seguido de un inicio de sesión exitoso y la eliminación del grupo

Remediar

¿Cómo remedian continuamente los administradores el acceso no autorizado y los cambios de seguridad para respetar las líneas de base de la evaluación? Para tener un entorno de reparación automática que no requiera la intervención de seres humanos, deben automatizar la corrección de todas las maneras posibles:

- Revertir los cambios en los grupos no autorizados sobre la base de las listas blancas de usuarios autorizados para hacer cambios de membresía. Los cambios realizados por usuarios que no estén en la lista se revertirán automáticamente.
- Revertir los cambios o eliminaciones masivas de objetos de AD como membresías de grupo, usuarios y atributos en AD en las instalaciones automáticamente.
- Automatizar el flujo de trabajo para detectar cuándo están inactivas las cuentas de usuario (por ejemplo, sin inicio de sesión en los últimos 120 días).
- Trasladar cuentas inactivas a un contenedor de usuarios deshabilitados y eliminarlas automáticamente si no se utilizan en tres días.
- Para las cuentas creadas por usuarios que no se encuentran en la lista blanca, deshabilitar la cuenta iniciadora y la cuenta creada.

Mitigar

¿Qué hace que el acceso no autorizado siga ocurriendo después de la corrección? El principio de menor privilegio es un modelo de acceso que restringe aún más el permiso generalmente disponible para las tareas de AD y permisos de GPO, mitigando así la recurrencia del riesgo.

Las técnicas de mitigación se enfocan en los controles automatizados en los puntos de explotación más evidentes:

- Externalizar los permisos de AD y controlarlos en un modelo proxy. El modelo restringe no solo quién puede hacer qué en AD, sino también qué objetos dados pueden ver los usuarios. Por ejemplo, delegar derechos en AD para un usuario con el fin de trasladar cuentas de una UO a otra UO también significaría delegar derechos adicionales para eliminar cualquier objeto de usuario de la UO de origen y escribirlo en la UO de destino. Similar al escenario de la empresa financiera de más arriba, esos derechos adicionales son innecesarios y excesivos para la operación de traslado. Un modelo basado en proxy con un acceso menos privilegiado permitiría realizar solo el traslado, sin los derechos innecesarios para eliminar y escribir.
- A continuación, se debe poner en marcha un modelo de permisos de lista blanca en tiempo real en los objetos de AD y GPO. La lista blanca garantiza que solo las cuentas de servicio en un modelo de proxy con acceso menos privilegiado pueden hacer cambios en los grupos de administradores y GPO de controladoras de dominio. Esto garantizará que no se abuse ni exploten los permisos con privilegios nativos (como los miembros del grupo de administradores de dominios).
- Utilice membresías de grupo temporales combinadas con flujos de trabajo de aprobación para mitigar el riesgo que surge de las membresías permanentes en grupos confidenciales y privilegiados. Esto también disminuye el período de oportunidad para un acceso no autorizado.
- Emplee el almacenamiento de contraseñas para proteger las cuentas de servicio poderosas que controlan el modelo de proxy con acceso menos privilegiado. El producto para almacenamiento de contraseñas debería manejar automáticamente las cuentas con privilegios y también las cuentas de usuarios comerciales confidenciales.

Investigar

¿Cómo identifica y contiene la empresa los incidentes de seguridad? Realiza investigaciones rápidas del ciclo de vida del acceso de los usuarios y grupos en un AD en las instalaciones.

La corrección automatizada de cambios de seguridad no autorizados ayuda a los administradores a respetar las líneas de base de la evaluación sin intervención humana.

Las investigaciones eficaces cuentan con una auditoría forense de 360 grados para correlacionar los eventos, las actividades de acceso y la configuración de seguridad en múltiples repositorios indexados.

Las investigaciones eficaces cuentan con una auditoría forense de 360 grados y una búsqueda de texto completo para correlacionar los eventos, las actividades de acceso y la configuración de seguridad en múltiples repositorios indexados. Las búsquedas deben revelar los caminos más probables hacia cualquier infracción de datos potencial:

- Toda actividad en AD, GPO, archivos y computadoras por parte de un usuario dado en un período dado.
- Toda actividad en UO, grupos, archivos, computadoras, usuarios y atributos que contengan una palabra dada como "finanzas" o "salario".
- Configuración de seguridad y cambios para un usuario dado, incluido el estado de una cuenta de usuario en AD, departamento, última hora de inicio de sesión, expiración de la cuenta, archivos accesibles, membresías de grupo, cambios a este objeto y actividades iniciadas por el usuario.
- La información de membresía de cualquier grupo dado, incluidos los cambios recientes a la membresía.

Lo que es más importante, las investigaciones dependen de la información contextual relacionada con un incidente. Si, por ejemplo, una búsqueda de "NTLM" revela un cambio en un GPO, el próximo paso es encontrar el nombre del GPO, la configuración que contiene "NTLM", los valores anteriores y posteriores para la configuración, el lugar en que se originaron los cambios y la controladora de dominio sobre el que se realizó el cambio.

Recuperar

¿Cómo se ajusta la empresa al continuo estado de infracción de datos potencial y amenaza interna? Supone que ocurrirá una infracción y se prepara para recuperar los cambios no autorizados en AD en las instalaciones, Azure AD y Office 365.

Todo plan de contingencia debe cubrir los aspectos básicos, con el nivel de automatización que resulte más práctico:

- El respaldo diario de la información de la base de datos de AD, incluidos los atributos, seguridad y configuración de GPO, membresías de grupos de dominios cruzados y todos los atributos del usuario, incluidas las contraseñas.
- Control estricto y auditorías de la delegación de derechos para respaldar y restaurar los objetos de Active Directory.
- Cifrado de los respaldos de AD en disco (cifrado en reposo) para evitar la exposición de la base de datos NTDS.dit.
- Respaldo diario y recuperación automatizada de los metadatos del bosque de esquema de Active Directory; debido a que el respaldo de AD no protege esto, requiere un producto de terceros para garantizar una recuperación rápida y automatizada de los bosques de AD completos o del dominio.
- Establecimiento de un objetivo de tiempo de recuperación (RTO) para una completa recuperación de Active Directory.
- Documentación y evaluación de planes de recuperación ante desastres (DR) parcial y completa al menos una vez por año.
- Capacitación cruzada para el personal del área de TI sobre la activación y ejecución del plan de DR de AD.

CONCLUSIÓN

En las empresas que sincronizan Active Directory en las instalaciones con Azure Active Directory, automatizar los controles compensatorios para Active Directory en las instalaciones es la mejor manera de reducir el riesgo de infracción de datos y de ataque interno.

El enfoque integral detallado en este documento fortalece la posición de seguridad de la empresa en un entorno de directorio híbrido. Promueve una mejor administración del acceso a AD en las instalaciones y a todas las aplicaciones, recursos y datos que dependen de AD. El enfoque también evita que AD en las instalaciones se vuelva el talón de Aquiles de la seguridad de Azure AD y Office 365.

ACERCA DEL AUTOR

Alvaro Vitta es un consultor de soluciones principal que se especializa en la seguridad para Quest. Alvaro ha evaluado, diseñado, probado e implementado soluciones de seguridad para grandes empresas, para plataformas en las instalaciones y basadas en la nube, tanto del sector público como del privado, durante más de 15 años en las áreas de administración de identidad y acceso, Active Directory y gobierno, riesgo y cumplimiento en empresas globales. Alvaro posee certificaciones industriales, entre las que se incluyen CISSP, CISSO, MCSE e ITIL.

Si tiene alguna pregunta sobre el posible uso de este material, comuníquese con:

Quest Software Inc.
Attn: LEGAL Dept
4 Polaris Way
Aliso Viejo, CA 92656

Visite nuestro sitio web (www.quest.com) para obtener información sobre nuestras oficinas regionales e internacionales.