Sobrevivir a los problemas comunes de seguridad de Office 365

¿ES SU AD LOCAL EL ESLABÓN MÁS DÉBIL?

Una guía para profesionales de la tecnología informática

PARA PROTEGER UN ACTIVE DIRECTORY DE UN ENTORNO LOCAL EN UN ENTORNO HÍBRIDO.

Quest

INTRODUCCIÓN

Office 365 cuenta con más de **60 MILLONES DE USUARIOS MENSUALES ACTIVOS** y la adopción de la plataforma está aumentando por razones sólidas. Permite a las organizaciones reducir la infraestructura y los costes relacionados con la concesión de licencias y el mantenimiento, al tiempo que incrementa la eficiencia del almacenamiento. Asimismo, Office 365 permite que los empleados trabajen desde cualquier lugar y en cualquier dispositivo, a la vez que aumenta la capacidad de adaptabilidad y la continuidad del negocio.

Sin embargo, pasar de un Active Directory (AD) de un entorno local a un directorio basado en la nube, como Azure AD de Office 365, todavía hace reflexionar a algunos responsables de la toma de decisiones por una razón común: la seguridad. Como sabemos, las brechas de seguridad pueden afectar de forma negativa a la rentabilidad de una empresa (y dañar su reputación).

En 2016, una investigación del Ponemon Institute detectó que el coste medio de una infracción de datos ascendía a 4 millones de dólares por incidencia.

Introducción (continuación)

¿Hacia dónde deberían dirigirse las preocupaciones en torno a la seguridad? Microsoft promete un acuerdo de nivel de servicio con un respaldo financiero del 99,9 % para Office 365; sin embargo, el control de cambios, el control de acceso y la seguridad general de los datos sigue siendo responsabilidad de los clientes, y el incremento del uso de AD en entornos híbridos agudiza esta preocupación. Considere lo siguiente: el 75 % de los clientes de Office 365 con más de 500 usuarios sincronizarán su AD local con Azure AD, de forma que crearán un entorno de AD híbrido.

Esta situación puede conducir a brechas peligrosas e ineficiencias que pueden tener consecuencias ruinosas. Cualquier punto débil en la forma en que se configure el AD local se traspasará a Azure AD. Las organizaciones se enfrentan a todas las limitaciones de seguridad de AD y Azure AD nativos, lo que duplica la superficie que necesitan para gestionar y prevenir las posibles divulgaciones de datos no autorizadas y las amenazas internas.

Introducción (continuación)

Proteger los datos

Proteger los datos que almacena en un entorno híbrido significa tomar las medidas necesarias para proteger el AD local, desde el proceso previo a la migración hasta el proceso posterior. En este libro electrónico se identificarán los pasos para preparar el AD local para sincronizarse con Azure AD y proteger los datos durante la migración; además, incluye las prácticas recomendadas para mantener un entorno híbrido más seguro.

PREMIGRACIÓN: ORGANIZAR LA MUDANZA

Muchas organizaciones trabajan bajo la suposición de que las infracciones y otras formas de pérdida de datos son costes inherentes a la actividad empresarial y aplican estrategias para minimizar el riesgo. Antes de la migración, los datos almacenados en el AD local deberían evaluarse de forma exhaustiva y consolidarse para eliminar los elementos obsoletos o no esenciales. Los tres objetivos durante este proceso deberían ser:

- **Reducir el objetivo**: mantenga solo lo que los usuarios necesitan y elimine los datos que ya no sean necesarios por razones empresariales o de cumplimiento normativo; los datos obsoletos no sirven para otro propósito que el de aumentar el riesgo de exposición y el incumplimiento normativo.
- **Analizar las cuentas de usuarios**: elimine los ID duplicados y las cuentas inactivas, establezca correspondencias entre los nombres de los usuarios y los nombres de dominio planificados para su uso en Office 365, y corrija las deficiencias de accesos temporales que se hayan podido otorgar a los usuarios para probar las funciones de Office 365.
- **Reforzar los protocolos de acceso**: identifique las contraseñas débiles y exija que los usuarios finales las refuercen, actualice los permisos administrativos para controlar el personal actual y mantenga los accesos a los datos de los usuarios actualizados.

Consejo para profesionales informáticos

La herramienta IDFix de Microsoft le ayudará a eliminar las cuentas duplicadas identificando y corrigiendo los errores de los objetos del Active Directory local antes de sincronizar usuarios, contactos y grupos en el entorno de Microsoft Office 365.

MIGRACIÓN: NO PERDER DE VISTA LOS DATOS

Una vez que se ha gestionado el exceso de datos y las cuentas duplicadas, se han resuelto los problemas de acceso y se han cumplido los protocolos de seguridad, ya está listo para migrar a Office 365. Aunque la parte más difícil del trabajo ya está hecha, mantener la atención durante todo el proceso de migración asegurará que los datos no se vean comprometidos. Los administradores de tecnología informática deberían disponer de tiempo para auditar y generar informes y alertas de los cambios durante la migración para garantizar la seguridad de los datos. Los tres elementos que se deben vigilar son:

- El **acceso**: las empresas a menudo acuden a consultores externos para que las asesoren sobre la migración, lo que podría significar acceso temporal concedido a personal externo a la organización.
- Los **procesos de conservación en previsión de contenciosos**: es probable que haya datos en tránsito retenidos con fines legales, como archivos PST de Outlook o mensajes de correo electrónico archivados; es fundamental que se registre una cadena de custodia clara para minimizar cualquier riesgo legal o de cumplimiento normativo.
- Los **problemas**: si surgen anomalías relacionadas con los datos durante la transferencia, como datos a los que acceden usuarios no autorizados, reaccione inmediatamente para solucionar el problema. "Más vale prevenir que curar" es la regla que siempre se debe seguir cuando se trata de datos esenciales.

Consejo para profesionales informáticos

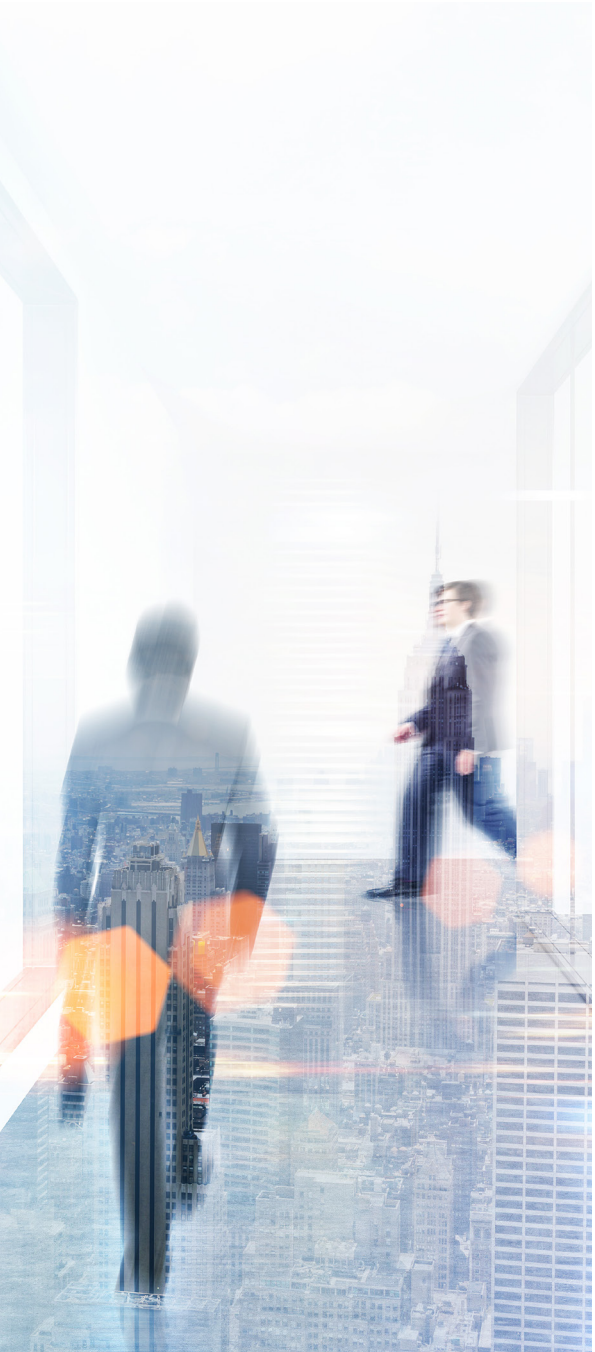
La migración a Office 365 ofrece la oportunidad de revisar los proveedores de soluciones actuales. Cada proveedor debería proporcionar opciones para tratar datos confidenciales durante el proceso de migración para garantizar la integridad de los datos a lo largo de su ciclo de vida. Si ese no es el caso, puede que no estén velando por sus intereses.

Posmigración: Mantener el avance de la seguridad

La migración a un entorno de AD híbrido ofrece una oportunidad única, aunque ardua, de reducir el riesgo asociado con el exceso de datos, permisos o accesos obsoletos, y cuentas de usuario duplicadas en el AD local. Ahora que todo está en orden, tenga en cuenta las cuatro prácticas recomendadas del proceso posterior a la migración que se incluyen a continuación y que crean una metodología de ciclo de vida para mantener el entorno organizado que ha creado:

1. Evaluar continuamente
2. Detectar y alertar
3. Corregir deficiencias y mitigar
4. Investigar y recuperar

POSMIGRACIÓN: EVALUAR CONTINUAMENTE



1 Evaluar continuamente

La auditoría del entorno híbrido es fundamental para comprender quién tiene acceso a permisos, grupos privilegiados, grupos empresariales confidenciales, objetos de directiva de grupo (GPO) y datos en todo momento. Una evaluación minuciosa del AD local y Azure AD debería permitirle identificar fácilmente los puntos siguientes:

- La superficie de ataque, los puntos más vulnerables y el perfil de riesgo
- Las personas que tienen acceso a los datos confidenciales
- La manera en que accedieron
- Quién tiene los permisos con más privilegios de acceso en AD, los servidores y las bases de datos de SQL
- Los sistemas que son vulnerables a las amenazas de seguridad

Consejo para profesionales informáticos

Al igual que una cámara de seguridad que siempre está funcionando "por si acaso", es importante revisar de manera continua quién tiene acceso a los datos y por qué, para garantizar que los datos confidenciales solo están disponibles para aquellas personas que tienen que verlos. Esto se aplica tanto a las preocupaciones de seguridad como de cumplimiento normativo.

POSMIGRACIÓN: DETECTAR Y ALERTAR

2 Detectar y alertar

La identificación en tiempo real de actividades sospechosas en el entorno de AD híbrido es clave para minimizar el impacto de un ataque interno o de una infracción de datos. Las medidas de seguridad proactivas deberían permitirle correlacionar datos informáticos dispares procedentes de numerosos sistemas y dispositivos para detectar rápidamente los siguientes elementos:

- Derechos y actividades irregulares por parte de usuarios
- Cualquier actividad sospechosa de una cuenta con privilegios
- Cambios que podrían indicar una amenaza interna significativa
- Indicación rápida de una intrusión
- Si un ataque por fuerza bruta está en progreso

También es una buena idea pensar en soluciones que mejoren las herramientas de auditoría nativas. Las herramientas de auditoría nativas de AD, Azure AD y Office 365 carecen del control y la visibilidad necesarios para cumplir con la conformidad normativa. Existen muchos problemas funcionales, entre los que se incluyen los siguientes:

- La dificultad para configurar una auditoría.
- La necesidad de configurar un buzón de correo/objeto cada vez.
- La incapacidad de supervisar las políticas de auditoría si cambian o las deshabilitan otros administradores.
- La incapacidad de configurar de forma automática nuevos buzones u objetos con la política de auditoría deseada.
- La ausencia de alertas en tiempo real, con solo una cantidad limitada de acciones de alerta.
- Un tiempo de retención limitado de los datos auditados antes de que se pierdan de forma permanente.
- La dificultad de interpretar eventos.

POSMIGRACIÓN: CORREGIR DEFICIENCIAS Y MITIGAR

3 Corregir deficiencias y mitigar

Si se produce una infracción, o se comete un error de acceso, es necesario saber dónde se encuentran los problemas que se desvían del comportamiento normal y corregirlos inmediatamente. Tener un proceso de elaboración de informes que le permita detallar todo lo que sucede a lo largo del ciclo de vida le preparará para actuar con rapidez cuando sea necesario.

La aplicación automatizada de la directiva de seguridad en el entorno de AD híbrido reduce el riesgo de error humano y mitiga la posibilidad de que puedan volver a producirse. El proceso debería garantizar que:

- los controles de acceso permitan la entrada a los usuarios de la lista blanca y se la impidan a los de la lista negra;
- los usuarios tengan el nivel más bajo de derechos de usuario posible para hacer su trabajo;
- los recursos confidenciales se encuentren protegidos;
- sea posible una corrección rápida y manual de los cambios no autorizados.

Consejo para profesionales informáticos

Los errores comunes de los empleados pueden poner la confidencialidad de los datos en peligro. Ofrezca una formación integral para usuarios de empresas que cubra las prácticas recomendadas para compartir datos dentro y fuera de la organización. Esta formación debería revisarse anualmente para garantizar que estas prácticas se encuentren actualizadas en lo que al cambio tecnológico se refiere.

POSMIGRACIÓN: INVESTIGAR Y RECUPERAR

4 Investigar y recuperar

Si se produce un incidente de seguridad, debe recuperarse rápidamente para minimizar el tiempo de inactividad y la pérdida de productividad. Este proceso debería permitirle analizar información básica de seguridad para que pueda comprender cómo ocurrió el incidente y por qué. Este proceso debería ayudarle a:

- evitar que un incidente se repita,
- crear un sistema para probar el plan de continuidad del negocio sin salirse de la línea,
- determinar cuánto tiempo se tardará en recuperarse de forma manual de un incidente de seguridad de AD,
- diseñar el mejor método para conseguir que el AD vuelva a funcionar.

¿CÓMO PUEDE AYUDAR QUEST SOFTWARE?

Las soluciones de Quest pueden ayudar a simplificar el proceso de migración, la seguridad y la gestión de Office 365, Azure AD y el entorno híbrido de AD con una red de expertos y socios de todo el mundo. Con su destacada trayectoria de entregas de proyectos de migración y consolidación, así como con su catálogo completo de soluciones, Quest puede ayudarle a:

- modernizar el AD para asegurar la idoneidad para la nube,
- reducir el tiempo de migración y de implementación,
- protegerse contra infracciones de seguridad,
- mitigar los riesgos de cumplimiento normativo,
- automatizar la realización de backup y la recuperación,
- optimizar los costes de licencia para maximizar el ROI.

Con casi dos décadas de experiencia en migración de plataformas de Microsoft, Quest permite a las organizaciones incorporar Office 365 y Azure AD sin el lastre de los riesgos, el miedo, la incertidumbre o los costes desorbitados. Obtenga más información acerca de cómo Quest puede **preparar su entorno híbrido para el éxito**.

Quest

Join the Innovation.