Administración de la amenaza interna con la seguridad de Active Directory

La anatomía de una amenaza interna y cómo proteger a Active Directory

por Alvaro Vitta, consultor de seguridad de primer nivel, Quest Software

Introducción

"¿Quiere decir que fue un trabajo interno?"

Desde la primera historia sobre un crimen y las personas que quisieron resolverlo, se ha llegado a ese momento en que alguien descubre un elemento de prueba que indica que un infiltrado estuvo involucrado. Asombrados, los personajes intercambian miradas con recelo mientras uno de ellos dice: "¿Quiere decir que fue un trabajo interno?"

Lamentablemente, las miradas y las preguntas como esas se están convirtiendo en una característica habitual de las investigaciones de casi todas las filtraciones de datos. Al descubrir que alguien ha accedido a los datos en la red de manera ilegítima, los administradores del área de TI creen en un principio (eso esperan, en realidad) que la amenaza provino del exterior. Pero como lo demuestran las recientes filtraciones de datos que acaparan las primeras planas, un desliz en la seguridad interna, ya sea accidental o malicioso, a menudo posibilita el ataque a pesar de una fuerte seguridad externa.

En este documento, el foco está puesto en Microsoft Active Directory (AD) como primer blanco de los atacantes debido a la importancia de AD en la autenticación y autorización de todos los usuarios. Los lectores verán cómo se desarrolla una típica amenaza interna y cómo se elimina con las mejores prácticas de seguridad de Active Directory a fin de minimizar el riesgo de la amenaza interna a la disponibilidad, confidencialidad e integridad de AD.

Las amenazas internas y su impacto en la empresa

Muchas empresas creen que las amenazas internas, en las cuales los empleados, antiguos empleados, contratistas o usuarios válidos obtienen acceso no autorizado a una red de la empresa y los recursos conectados a ella pueden causar tantos daños como los ataques iniciados de manera externa.[1] La atención se centra en los empleados actuales o antiguos, pero los proveedores de servicio y los socios empresariales desempeñan un papel creciente en perpetrar y facilitar los delitos cibernéticos.

El costo financiero de una filtración de datos como consecuencia de un ataque interno, incluidos el tiempo y el dinero para restaurar la seguridad de los sistemas, es

[1] *"Delitos cibernéticos en EE. UU.: Riesgos crecientes, preparación reducida – Conclusiones clave de la Encuesta del estado de los delitos cibernéticos en EE. UU. en 2014", PwC, mayo de 2014, http://www.pwc.com/en_US/us/increasing-it-effectiveness/publications/assets/pwc-2014-us-state-of-cybercrime.pdf*

Alrededor de 95 millones, o la quinta parte, de las cuentas de AD son atacadas cada día.

considerable. Aproximadamente la quinta parte de las empresas cree que el costo podría exceder la cifra de USD 5 millones, pero más de la mitad de las empresas francamente admiten que no tienen idea qué tan alta o baja puede ser la estimación de las pérdidas potenciales debido a un ataque interno.[2]

Los escenarios y las historias humanas que giran en torno a los ataques internos reflejan todos estos delitos:

- Espionaje económico transfronterizo.
- Conspiraciones bien planificadas para robar secretos comerciales.
- Antiguos empleados insatisfechos con amplios privilegios de acceso a la red.
- Empleados descontentos que usan credenciales que un supervisor compartió de manera confiada.
- Nombre de usuario y contraseña de un representante de una empresa proveedora que se robaron durante un ataque de suplantación de identidad.
- Usuarios autorizados que encontraron y copiaron datos de tarjetas de crédito, y luego los vendieron en el mercado negro.

El costo más amplio de una filtración de datos cometida por infiltrados incluye la pérdida de información confidencial, los daños a la reputación y las interrupciones de los sistemas críticos.[3]

Amenazas internas y Active Directory

Más del 90 % de las grandes empresas del mundo usan AD, lo que da un total de 500 millones de usuarios de cuentas activos.

Alrededor de 95 millones, o la quinta parte, de esas cuentas son atacadas cada día.[4]

Las empresas usan AD para brindar autenticación y autorización a los empleados, los contratistas, los socios y los clientes. A través de AD también le otorgan acceso a recursos de redes basadas en Windows, como recursos compartidos y archivos, bases de datos, servidores de correo electrónico, algunas aplicaciones en las instalaciones y aplicaciones basadas en la nube. Sin AD, pierden Exchange, colaboraciones, comunicaciones en tiempo real, SharePoint, bases de datos de SQL Server, servidores web y otros recursos sin los cuales pocas empresas pueden trabajar.

El fortalecimiento de la seguridad externa no garantiza la seguridad de AD porque las amenazas más grandes a la seguridad de AD son las internas, y más de la mitad del mal uso interno involucra el abuso de privilegios.[5] Esto se extiende al uso incorrecto accidental o malicioso de grupos sensibles, cuentas elevadas y permisos de AD que pueden debilitar los protocolos de seguridad y dar lugar a accesos no autorizados a datos confidenciales basados en Windows.

El acceso no autorizado a AD es como tener una tarjeta de acceso robada: una vez que los atacantes están dentro del edificio, pueden tomar el ascensor, recorrer las oficinas, abrir los escritorios y revisar los cajones. Con tantas cuentas que se atacan de manera incesante desde adentro y afuera, la amenaza interna a AD es clara y está presente.

¿Es difícil asegurar a Active Directory?

AD fue creado para ser seguro, pero como en la analogía de la tarjeta de acceso, la seguridad se quiebra cuando el acceso elevado se encuentra en las manos incorrectas.

Tenga en cuenta tres áreas principales con las que los administradores del área de TI tienen que lidiar:

Falta de automatización

- Los controles de acceso se deben evaluar y remediar de manera continua, pero no hay un proceso automatizado para realizar esto en AD.
- La implementación y prueba continua de los procesos completos de recuperación ante desastres deberían proteger contra

[2] *"Amenazas internas y la necesidad de una respuesta rápida y dirigida", SANS Institute, abril de 2015, https://www.sans.org/reading-room/whitepapers/analyst/insider-threats-fast-directed-response-35892*

[3] *"Administración de las amenazas internas", PwC, febrero de 2015, http://www.pwc.com/en_US/us/increasing-it-effectiveness/publications/assets/managing-insider-threats.pdf*

[4] *John Fontana, "El zar de Active Directory reúne a la industria para una seguridad e identidad mejores", ZDNet, 9 de junio de 2015, http://www.zdnet.com/article/active-directory-czar-rallies-industry-for-better-security-identity/.*

[5] *"Informe de investigaciones de filtración de datos 2015", Verizon, abril de 2015, https://msisac.cisecurity.org/resources/reports/documents/rp_data-breach-investigation-report-2015_en_xg.pdf*

el tiempo de inactividad prolongado y la pérdida de datos en AD, pero AD no brinda de forma nativa una manera automatizada de probar e implementar un escenario completo de recuperación ante desastres de AD en todas las controladoras de dominio (DC).

- Cuando se detectan acciones o accesos no autorizados a AD, no hay manera de prevenirlos ni de remediarlos de manera automática, y tampoco de autolimpiar las credenciales obsoletas.
- Sin controles de cambios automatizados e integrados en AD, las empresas están sujetas a accesos no autorizados y accidentales, e interrupciones costosas.

Factores humanos, empresariales y comerciales

- Cuando se transfieren empleados entre unidades empresariales, la mayoría de las empresas aplican procesos deficientes para desvincularlos. Los administradores dejan a los usuarios con una autoridad elevada, acumulada a través de los requerimientos del trabajo previo, que no necesitarán más.
- No se puede evitar que los administradores de AD accedan a recursos sensibles de Windows.
- La fidelidad de los datos y los estándares de nomenclatura de la empresa en AD son difíciles de aplicar, lo que dificulta la categorización del acceso, la revisión de los derechos y la auditoría de los activos.
- Por confianza y conveniencia de la empresa, es común que cada uno de los empleados, los contratistas y los socios empresariales conozcan y compartan las credenciales privilegiadas de AD de los otros.

Limitaciones de AD

- La falta de un contexto de seguridad retrasa la detección de las filtraciones de datos.
- AD no permite que las empresas apliquen de manera completa una verdadera cuenta de usuario con menos privilegios (LUA), lo que da como resultado usuarios con privilegios más altos y más acceso que el que necesitan para llevar a cabo su trabajo. Por ejemplo, si un administrador quisiera delegar la habilidad en AD para que el empleado del servicio al usuario JSmith mueva los objetos de usuario desde la unidad organizativa (OU) de planificación hasta la OU de ingeniería, el administrador tendría que otorgarle a JSmith el derecho de eliminar cualquier objeto de usuario desde la OU de planificación y escribir en ella. Eso abarca muchos más permisos que los que JSmith necesita (y que el administrador realmente quisiera otorgar) para ejecutar estas actividades e incrementar de manera considerable la exposición de la empresa a los riesgos.

Las herramientas tradicionales para la información de la seguridad y la administración de eventos (SIEM) están sujetas a limitaciones en la auditoría de registros nativos. Por ejemplo, el registro de auditoría nativo indica que se modificó un objeto de política grupal (GPO), pero no registra qué configuración se cambió o sus valores antes y después del cambio.

Por lo tanto, la seguridad de AD es un equilibrio constante entre el otorgamiento a los usuarios de los derechos que necesitan para realizar su trabajo y mantenerlos, incluso los administradores de dominio, fuera de los grupos de seguridad que pueden acceder a bases de datos confidenciales, carpetas y archivos que contienen recursos humanos, información sobre tarjetas de crédito o registros médicos.

Anatomía de un ataque interno a Active Directory

Considere esta historia ficticia que describe cómo una amenaza interna causada por controles débiles de seguridad puede afectar a AD.

Al aproximarse el fin del soporte para Windows Server 2003, un minorista de productos médicos llamado Acme emplea a JSmith mediante un contrato de cuatro semanas para que ayude a actualizar su entorno a Windows Server 2012. PBrown, el administrador de AD en Acme, agrega a JSmith al grupo de administradores del dominio.

El día viernes de la segunda semana de JSmith, Acme rescinde el contrato, pero nadie le dice a PBrown que elimine a JSmith del grupo de administradores. El lunes siguiente, PBrown se entera de que JSmith ya no trabaja para Acme y elimina al contratista del grupo de administradores.

En los siguientes pasos se describen lo que ocurre durante el fin de semana.

> La seguridad de AD es un equilibrio constante entre el otorgamiento a los usuarios de los derechos que necesitan para realizar su trabajo, y mantenerlos fuera de los grupos de seguridad que pueden acceder a recursos confidenciales.

Para que la creación de la cuenta nueva no llame la atención, sigue las convenciones de nomenclatura de Acme para cuentas de servicio de respaldo.

1. Creación de una cuenta falsa

Descontento porque Acme rescindió el contrato de manera prematura, JSmith busca maneras, incluso ilícitas, para compensar los ingresos que pensaba recibir. A través de un amigo, se entera del sitio de un mercado negro donde puede hacer dinero fácil al vender los datos de las tarjetas de crédito.

JSmith inicia sesión en la red de Acme desde su casa mediante el uso de sus credenciales de administrador y crea una cuenta nueva de administrador para él mismo. Para que la creación de la cuenta nueva no llame la atención, la llama corpsvcbk1, siguiendo las convenciones de nomenclatura de Acme para cuentas de servicio de respaldo. Cuenta con poder usar corpsvcbk1 en caso de que Acme elimine o restablezca la contraseña de su cuenta de administrador original.

2. Obtención de privilegios de administrador del dominio

JSmith nota que hay un grupo llamado CorpOperations, que es miembro del grupo de administradores del dominio. Crea una cuenta nueva en el grupo y la llama corpsvcbk1. Luego cubre su rastro al agregarla al grupo anidado CorpOperations, que le da privilegios indirectos de administrador del dominio sin disparar alertas (el sistema de monitoreo genérico de Acme está configurado para monitorear solo los cambios directos al grupo de administradores del dominio).

3. Acceso a los servidores de archivos

JSmith localiza los servidores de SQL y los servidores de archivos donde Acme almacena los datos de las tarjetas de crédito y la información de identificación personal (PII).

Modifica el GPO que evita que los administradores inicien sesión en ciertas bases de datos y servidores de archivos, luego inicia sesión de manera local en SQL1 y FSRV1. Agrega su cuenta corpsvcbk1 al grupo de administradores locales en SQL1 y le asigna el rol de administrador del sistema en SQL Server.

Al echar un vistazo, encuentra la base de datos no cifrada de tarjetas de crédito y exporta todos los registros a través de la conexión remota hasta su equipo portátil.

En FSRV1 localiza los archivos que contienen la PII. De nuevo, cubre su rastro, agrega su cuenta de administrador a un grupo anidado llamado FinanceOps, un miembro del grupo integrado de administradores en FSRV1. En la carpeta Cuentas por cobrar encuentra el archivo Customer_PII.xlsx. Para acceder al archivo, agrega su cuenta de administrador al grupo Cuentas por cobrar; eso evita que su cuenta se muestre en la lista de control de acceso, pero sin embargo, le da plenos derechos al archivo. Abre el archivo, se asegura de que es el deseado y lo copia a una unidad de red asignada a su equipo portátil.

4. Configuración del espionaje

Después, JSmith modifica una clave de registro que disminuye el LmCompatibilityLevel y la seguridad de las sesiones lo suficiente como para que él instale software malicioso (malware) que espíe como las credenciales de acceso SQL1 y FSRV1 se pasan las credenciales entre sí. Eso le permitirá descifrar credenciales adicionales en el futuro a medida que los administradores realicen la autenticación, de modo que, incluso si Acme elimina su cuenta falsa corpsvcbk1, puede continuar robando más datos de tarjetas de crédito.

5. Limpieza

JSmith elimina su cuenta corpsvcbk1 de los grupos de administradores, limpia los registros (para borrar la evidencia de su ataque) y decide mantener el malware en la red para futuras hazañas.

Los controles de seguridad y las políticas de seguridad de Acme no son suficientes para evitar el ataque interno contra Active Directory. Las tácticas de JSmith garantizan que le llevará mucho tiempo a Acme detectar la filtración de datos; para ese momento es probable que JSmith haya recuperado el ingreso perdido y Acme esté en medio de una recuperación de la filtración de datos.

Mejores prácticas de seguridad para Active Directory

No hay un enfoque contundente para la seguridad de Active Directory, pero las empresas pueden protegerse de las amenazas internas a AD al seguir varias pautas:

1. Establezca expiraciones de cuentas y grupos para el acceso temporal a grupos confidenciales.

a. En vez de la membresía permanente a grupos confidenciales, use membresías de grupos temporales con fechas y horarios de comienzo y fin automáticos.

b. Establezca fechas de expiración de cuentas cuando se creen cuentas para el personal temporal, como contratistas, pasantes y visitantes.

2. Evite la creación no autorizada de cuentas al definir una lista blanca de credenciales autorizadas que tienen permiso para realizar esta tarea. Si alguien que no está en la lista aprobada crea una cuenta de usuario, el evento genera un correo electrónico de alerta. También puede generar la corrección que deshabilita la cuenta del creador o la cuenta creada.

3. Monitoree en tiempo real no solo los cambios directos (es decir, se puede realizar el seguimiento en registros de seguridad nativos) a grupos empresariales privilegiados en AD, sino también las adiciones de miembros anidados (es decir, la membresía indirecta a grupos de AD elevados), que los servidores de Windows no registran.

4. Monitoree los siguientes grupos empresariales para buscar cambios de membresía directos y anidados:

   Administradores, Operadores de impresión, Operadores de configuración de red, Administradores DHCP, Operadores de respaldo, Desarrolladores de confianza de bosques entrantes, Operadores de cuentas, Editores de certificados, Propietarios del creador de política grupal, Administradores de dominio, Controladoras de dominio, Administradores de la empresa, Operadores de servidores, Servidores RAS e IAS, Administradores de esquema.

5. Monitoree los cambios en tiempo real a la configuración de GPO en AD. No se pueden rastrear los valores anteriores y posteriores de estas configuraciones en registros nativos, lo que puede representar una amenaza de puerta trasera a AD.

6. Independientemente de los permisos de usuario, evite los cambios no autorizados a configuraciones de GPO y grupos empresariales importantes al usar una lista blanca de usuarios autorizados. Con una lista blanca, incluso si los atacantes obtienen derechos de administrador por parte de credenciales comprometidas, se negarán los cambios a las membresías en grupos privilegiados, como Administradores de dominio y Administradores empresariales. La lista blanca también se aplica para hacer cambios a configuraciones de GPO confidenciales, como deshabilitar o negar el inicio de sesión a servidores importantes y debilitar la autenticación de NTLM.

7. Monitoree en tiempo real cualquier actividad sospechosa, como inicios de sesión a servidores confidenciales luego del horario habitual de trabajo y cambios a claves de registro confidenciales, como LmCompatibilityLevel. La última es una táctica de puerta trasera para disminuir los valores que se utilizan en el protocolo de autenticación NTLM.

8. Realice auditorías de los cambios de permisos y las actividades realizadas en bases de datos y servidores de archivos (incluidos archivos, recursos compartidos y carpetas) que contienen datos confidenciales.

9. Revise de manera continua los derechos de acceso de usuarios y los privilegios para servidores y grupos confidenciales. Revise los permisos de las bases de datos de SQL Server y los permisos NTFS en AD y servidores de archivos SQL.

10. Aplique la separación de tareas para evitar, por ejemplo, que los contratistas se conviertan en miembros de grupos de administradores del dominio. Aplique un modelo de acceso con menos privilegios para AD y Windows.

11. Implemente un proceso automatizado para desaprovisionar usuarios en el que se incluya la deshabilitación o eliminación de cuentas, la eliminación de cuentas de todos los grupos y las listas de distribución, la eliminación de acceso VPN remoto y la notificación de manera automática a los departamentos de Administración de Instalaciones, Seguridad y Recursos Humanos.

La seguridad de AD como parte de una estrategia integral de GRC

La seguridad de Active Directory también desempeña un papel importante en la gestión, la administración de riesgos y el cumplimiento (GRC).

La seguridad de AD se extiende a la habilidad de la empresa para demostrar que tiene los controles adecuados para AD y todo el entorno de Windows, incluidos SharePoint, Exchange y SQL Server. Demostrar el cumplimiento significa poder informar de manera eficaz detalles al nivel de AD, como la información sobre usuarios privilegiados en la actualidad y en el pasado; cuentas de antiguos empleados y contratistas; y la configuración, la actualización y el estado de los parches de los servidores. Una estricta seguridad de AD es parte esencial de GRC y de la preparación cuidadosa para una auditoría.

Conclusión

La amenaza interna a AD es real, generalizada y costosa. El predominio de AD en empresas de todo el mundo lo convierte en un blanco atractivo para los adversarios, que pueden explotar las limitaciones técnicas y los factores humanos, a fin de realizar filtraciones de datos desde el interior de las empresas.

Monitorear los registros de eventos de AD es un comienzo, pero muchas amenazas internas se aprovechan de los eventos de AD que no se registran. Además, la lista de elementos que hay que buscar en un ataque sospechoso es larga, y no hay una manera automática de protegerse contra todos.

Ya sean accidentales o maliciosas, las amenazas internas son perniciosas por naturaleza. Las empresas continuarán equilibrando la necesidad de permitir que sus administradores de sistemas realicen tareas con alguna autonomía, contra la necesidad de otorgar solo los privilegios requeridos para esas tareas. Mientras tanto, las mejores prácticas de seguridad de Active Directory son una parte importante de la estrategia integral de GRC.

Acerca del autor

Alvaro Vitta es un consultor de seguridad de primer nivel especializado en la seguridad para Quest Software. Ha evaluado, diseñado, probado e implementado soluciones de seguridad para grandes empresas, tanto del sector público como del privado, desde el año 2000 en las áreas de IAM, seguridad de Active Directory y gestión, riesgo y cumplimiento (GRC). 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.
A/A: Departamento LEGAL
4 Polaris Way
Aliso Viejo, CA 92656

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