semperis

Informe Halftime *sobre seguridad de Active Directory*

2021

OPINIÓN DEL CEO DE SEMPERIS, MICKEY BRESMAN

Si queremos frenar los ciberataques debemos prestar especial atención a las prácticas fundamentales de seguridad de la identidad

Tras medio año de escalada de los ciberataques en todos los sectores empresariales y en todo el mundo, el CEO Mickey Bresman reflexiona sobre las tendencias de ciberseguridad que definirán a corto plazo la batalla contra los ataques maliciosos que amenazan los ingresos empresariales, la seguridad pública y la seguridad nacional.

¿Por qué las empresas siguen esforzándose por implantar las prácticas fundamentales de seguridad de Active Directory?

En primer lugar, Active Directory existe desde hace 20 años y al principio la seguridad no era necesariamente la prioridad de los equipos que configuraban AD. A esto hay que añadir que AD es en la actualidad mucho más complicado: cada entorno presenta numerosos niveles de permisos y complejidades.

AD sigue siendo el motor de la gestión de la identidad —el núcleo de la plataforma de identidad de la mayoría de las organizaciones—, pero todo lo que le rodea ha cambiado radicalmente. La protección básica de AD no era motivo de preocupación hace 15 años. Por eso, muchos de los errores que se cometieron entonces se han convertido en problemas que hay que abordar ahora. También destacaría la falta de conocimientos: hay profesionales que conocen muy bien AD, pero tienden a pensar más desde el punto de vista de las operaciones. Otros que conocen muy bien Red Team y la seguridad, pero no son expertos en AD. No es fácil encontrar esa combinación de conocimientos en una sola persona.

¿Qué pueden hacer las empresas en cuanto a formación o estructura organizativa para poner fin a la incomunicación entre los equipos de tecnologías de la información y de seguridad?

La identidad debe formar parte integral del marco más amplio de la ciberseguridad en la empresa. Los responsables de identidad deben dar prioridad a la ciberseguridad. Somos conscientes de que muchas organizaciones dependen de Active Directory para seguir con sus operaciones después de un ciberataque. Por tanto, ¿cómo se garantiza que, en el peor de los casos, se podrá restablecer esa funcionalidad lo más rápidamente posible? Hay empresas que empiezan a trasladar la responsabilidad de la identidad al área de seguridad. Incluso en las organizaciones en las que la identidad sigue encontrándose en el área operativa, los profesionales de tecnologías de la información conceden más importancia a la seguridad y se está dando mayor colaboración entre los equipos de seguridad y de tecnologías de la información, en particular en la gestión de la identidad y de Active Directory.

En mi opinión creo que es una tendencia positiva, cuando alguien está a cargo de cualquier aspecto del área de la identidad, debe centrarse en la seguridad.

¿Qué retos para la seguridad conlleva la gestión de un entorno de identidad híbrida?

Son muchos los retos que plantea la gestión de entornos de identidad híbrida, empezando por el hecho básico de que Active Directory y Azure Active Directory tienen poco en común, aparte del nombre. Azure AD es una pila diferente de protocolos, que requiere una gestión muy diferenciada, incluida la protección del sistema de identidad contra ciberataques. Por ejemplo, cuando realizo cambios en identidades en la nube, ¿afecta a mi posición general de seguridad en el centro de datos, en el entorno local? En un escenario híbrido, la superficie de ataque potencial se amplía para los adversarios. Es bastante común que los ataques comiencen localmente y pasen a la nube, o que vayan de la nube a local. Las organizaciones deben analizar ahora qué cambios se realizan en los sistemas de identidad en cada entorno y cómo la conectividad entre ambos puede crear un punto de entrada para los adversarios.

La gestión de la seguridad en un entorno híbrido también pone de relieve el modelo de responsabilidad compartida: la responsabilidad de Microsoft es asegurarse de que el servicio siga funcionando. Lo que usted haga con su entorno —incluida la seguridad— es responsabilidad suya.

¿Durante cuánto tiempo harán uso de un entorno híbrido la mayoría de las organizaciones?

La mayoría de nuestros clientes nunca abandonarán del todo sus centros de datos. En potencia, el modelo híbrido estará aquí para siempre. Las empresas examinarán qué conviene seguir ejecutando en el centro de datos y qué conviene utilizar como servicio prestado por Microsoft, AWS, Google u otro proveedor. Las empresas pueden ahora combinar la solución más adecuada para sus escenarios y requisitos. La nube no es la respuesta a todo.

Pero, con independencia de la combinación específica de sistemas y activos locales y en la nube, será necesario proteger el almacén de identidad. La identidad seguirá desempeñando un papel fundamental en el área de la protección que estamos desarrollando contra los adversarios. También es necesario asumir que, a medida que continúe el proceso de digitalización y adopción de la nube, mayor será la importancia de la protección de la identidad en la estrategia operativa y de seguridad.

UNLEASH PURPLE KNIGHT

Purple Knight permite a los equipos de sistemas informáticos y de seguridad detectar las brechas de seguridad de Active Directory

Con miles de descargas hasta la fecha, la herramienta gratuita de evaluación de la seguridad de AD ayuda a las organizaciones a identificar y abordar las brechas de seguridad que los adversarios suelen explotar en los ciberataques.

El lanzamiento de Purple Knight en marzo de 2021 cubría una necesidad que estaba desatendida, identificar y abordar las brechas de seguridad de Active Directory. Miles de profesionales de sistemas informáticos y de seguridad han descargado esta herramienta gratuita, creada por expertos en identidad de Semperis, que analiza más de 60 indicadores de exposición (IOE) y compromiso (IOC) en el entorno de Active Directory.

«No esperábamos este nivel de aceptación de Purple Knight en el mercado», comenta Mickey Bresman, CEO de Semperis. «Pero es una sorpresa muy agradable, ya que ahora las organizaciones pueden establecer una relación directa entre los ataques que observan en el mundo real y los puntos débiles de seguridad de Active Directory. Las organizaciones están empleando Purple Knight para asegurarse de que sus entornos de AD están preparados para este tipo de ataques.»

Bresman afirma que la respuesta que reciben de los clientes indica que Purple Knight detecta vulnerabilidades que incluso empresas de consultoría pasan por alto, una ventaja que atribuye al profundo conocimiento que el equipo de Semperis tiene de Active Directory —y de cómo lo utilizan las organizaciones.

«Hemos comprobado que muchas empresas no conocen muy bien las exposiciones de Active Directory que los adversarios pueden utilizar en su contra», explica Bresman. «Queríamos dar a los equipos de seguridad que no tienen conocimientos profundos sobre AD una forma de entender su posición de seguridad de AD —y luego solventar las brechas existentes para que los adversarios no las aprovechen.»

Purple Knight analiza el entorno de AD para identificar brechas de seguridad provocadas por actividad maliciosa o configuraciones erróneas que pueden haber estado al acecho en el sistema durante años. Ran Harel, Director de Productos de Seguridad de Semperis, afirma que muchas de las configuraciones erróneas que encuentra en los despliegues de Active Directory son resultado de la falta de comprensión del modelo general de seguridad o de la decisión de implementar correcciones rápidas que provocan vulnerabilidades de seguridad en el futuro.

«Esos son los escenarios que les gusta aprovechar a los atacantes, en particular las configuraciones erróneas con Kerberos y la directiva de grupo», dice Harel.

“Those are the scenarios that attackers love to take advantage of—especially faulty configurations with Kerberos and Group Policy,” said Harel.

Algunas de las vulnerabilidades más comunes descubiertas por Purple Knight son:

- Contraseñas que no se han cambiado con frecuencia, dejando a la empresa indefensa ante ataques por fuerza bruta
- Cuentas con privilegios elevados que no han sido revisados adecuadamente, por ejemplo, el grupo de administradores de claves empresariales
- Cuentas de Exchange con permisos de AD elevados que han proliferado con el tiempo
- Delegación de Kerberos configurada como «no restringida», escenario que facilita el abuso o la exposición involuntaria a usuarios inapropiados
- Configuración débil de la directiva de grupo, que crea vulnerabilidades de seguridad cuando los GPO se vinculan a Active Directory a nivel de dominio

"We wanted to give security teams that don't have deep AD expertise a way to understand their AD security posture—and then close any existing gaps so that adversaries won't use those against them."

Mickey Bresman, *Semperis* CEO

Purple Knight proporciona seguridad general de AD, así como puntuaciones individuales en las categorías de delegación de AD, seguridad de cuentas, seguridad de infraestructura de AD, seguridad de directiva de grupo y seguridad de Kerberos. En los informes iniciales de Purple Knight, las organizaciones obtenían puntuaciones medias del 61 %, una calificación de apenas aprobado. La seguridad de Kerberos fue la categoría con la puntuación más baja:

Puntuación media de las evaluaciones iniciales

PUNTUACIÓN GLOBAL	61%
Delegación de AD	**68%**
Seguridad de cuentas	**59%**
Seguridad de infraestructura de AD	**77%**
Seguridad de directiva de grupo	**58%**
Seguridad de Kerberos	**43%**

Los ciberdelincuentes creen que los permisos de administración de dominios poco rigurosos constituyen una oportunidad fácil de aprovechar, afirma Darren Mar-Elia, Vicepresidente de Productos de Semperis.

«A los ciberdelincuentes les gusta atacar por ahí porque les facilita la tarea», dice Mar-Elia. «Es el camino más corto a la cuenta del administrador de dominio. Y, una vez que la tienen, se acabó el juego.»

La protección continua contra vulnerabilidades de seguridad de AD requiere un buen mantenimiento de las cuentas, señala Ran Harel, Director de Productos de Seguridad de Semperis.

«Pero es muy difícil», añade. «Un usuario puede pertenecer a 20 grupos diferentes, que pueden tener subgrupos con derechos delegados. Es como si fueran espaguetis,hay que organizar los permisos de las cuentas con regularidad. Si no lo haces, la gestión de las cuentas empieza a perderse y el problema se agrava.»

Los resultados de los informes de Purple Knight ponen de manifiesto la ironía de que las grandes organizaciones, a menudo con más recursos, son especialmente susceptibles de quedarse rezagadas en la protección de sus sistemas críticos de identidad debido a su gran tamaño y a la complejidad de sus entornos, lo que les hace correr el riesgo de sufrir un ataque similar al de SolarWinds.

"Since Active Directory is a prime target for attackers attempting to steal credentials and deploy ransomware across the network, it's worth considering the repercussions of an Active Directory attack even if you're not directly responsible for its daily operation."

MICKEY BRESMAN
Semperis CEO

ACTIVE DIRECTORY IS THE ACHILLES' HEEL OF ENTERPRISE SECURITY

El CEO de Semperis llama a los responsables de seguridad a defender Active Directory

Podría parecer que Active Directory no es más que otro servicio que es preciso restaurar tras un ciberataque. Sin embargo, la realidad es que AD es una piedra angular. Si AD está en peligro, lo está todo su entorno.

Casi la mitad (47 %) de las organizaciones utiliza Active Directory como almacén de identidad principal. El 51 % lo utiliza con distinto grado de importancia junto a otros almacenes de identidades y solo un 1 % de las organizaciones no utiliza AD o lo está retirando.

Muchas organizaciones están adoptando un enfoque híbrido de la identidad y comienzan a centrarse en las interdependencias y complejidades de la nube que este origina —sin tener en cuenta el hecho de que todas las identidades en la nube continúan sincronizándose con Active Directory local. AD se utiliza como una fuente a partir de la cual sincronizar otros almacenes de identidades, de manera que cualquier problema que afecte a AD puede tener un efecto dominó, puesto que AD enlaza con otras aplicaciones de nube. Esta conexión potencialmente problemática entre activos basados en la nube y activos locales adquiere mayor relevancia ante la reacción improvisada de las organizaciones para dar servicio a trabajadores remotos con dispositivos móviles durante la pandemia.

En «Rethinking Active Directory Security» (Replanteamiento de la seguridad de Active Directory), publicado en Help Net Security, Mickey Bresman, CEO de Semperis, aborda la importancia de que las organizaciones dispongan de un plan de recuperación de Active Directory (AD) ante la eventualidad de un ciberataque. Este artículo le permitirá obtener más información sobre los pasos que deben seguir las empresas para reforzar sus defensas frente a los ciberataques relacionados con AD, entre los que figura asegurarse de que exista una monitorización específica de AD.

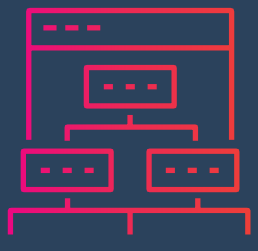
MORE RESOURCES

BLOGS

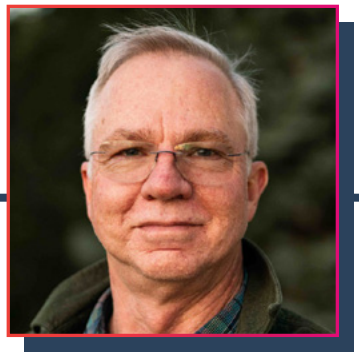
- Semperis Expert: SolarWinds Attack Highlights Need to Secure AD
- CISA's Ransomware Guidance Is Reminder to Include AD in Recovery Plan

WEBINAR

- What You Need to Know About Securing Active Directory



BUILDING A CYBER-RESILIENT ORGANIZATION



Los expertos en Active Directory tienen futuro en el ámbito de la seguridad

POR **GIL KIRKPATRICK,** *Chief Architect, Semperis*

En los últimos 20 años el mundo de los profesionales de Microsoft Active Directory (AD) ha cambiado considerablemente debido al crecimiento de las aplicaciones en la nube y a los cambios que se han producido en el panorama de las amenazas.

Al igual que en cualquier otro ámbito de las tecnologías de la información, la iniciativa y el deseo de incrementar los conocimientos para seguir el ritmo de la evolución de las tecnologías se encuentran entre los atributos más importantes que pueden mostrar los ingenieros y los arquitectos de AD.

Después de dos décadas centrándose en sistemas, usuarios y aplicaciones locales, la mayoría de los profesionales de AD son ahora responsables de la integración en la nube y de garantizar un acceso seguro a un entorno en el que ha desaparecido el perímetro de red tradicional. Los profesionales de AD deben llevar a cabo esta tarea mientras los ciberdelincuentes utilizan herramientas de ataque cada vez más sofisticadas para aprovechar los errores de configuración de AD y las vulnerabilidades de Windows, intentar obtener credenciales de los usuarios y mantener la persistencia en los sistemas locales.

Ante esta situación, los líderes tecnológicos están reconociendo la necesidad de facilitar la cooperación entre los equipos de seguridad e identidad a fin de garantizar el acceso seguro de los usuarios en la era de la computación en la nube y del aumento del teletrabajo.

En el futuro, los expertos en AD desempeñarán un papel más activo en los debates sobre seguridad. Aún no se ha llegado a ese punto, pero dado que AD sigue siendo una superficie de ataque recurrente para los ciberdelincuentes, los profesionales de AD pueden aprovechar este momento para aportar su experiencia a los esfuerzos de seguridad de la empresa. A medida que las organizaciones convierten la identidad en el aspecto central de su estrategia de seguridad y los administradores de AD se involucran más en las decisiones sobre seguridad, aquellos profesionales que puedan ampliar sus conocimientos y su capacidad tendrán un mayor valor para la empresa.

Los cambios en el panorama de las amenazas plantean nuevas oportunidades para los profesionales de Active Directory

En muchos aspectos, AD no se diseñó teniendo en cuenta los retos de seguridad actuales, y no se trata solo de vulnerabilidades como el problema que aprovecharon los ataques de Zerologon el año pasado. En la actualidad los atacantes también se benefician de los protocolos integrados en el sistema operativo Windows y el propio AD.

Además está el problema del ransomware. En los últimos años, se han observado ataques de ransomware que emplean técnicas de amenazas persistentes avanzadas (APT), como las que proporcionan herramientas como BloodHound y Mimikatz, para realizar reconocimiento y robo de credenciales. En un caso de 2020, un ataque de ransomware utilizó el recurso compartido SYSVOL en los controladores de dominio de AD para propagar malware por todo el entorno de destino.

Antes, la planificación de la recuperación de AD se centraba principalmente en eventos como desastres naturales, apagones o errores administrativos. En la actualidad, ante la posibilidad de que el ransomware interrumpa todas sus operaciones informáticas, las empresas deben prepararse para una situación mucho más probable: un ciberataque que las obligue a recuperar su AD desde cero.

Dar prioridad a la identidad

Los usuarios móviles y la computación en la nube han erosionado el perímetro tradicional de la red: el único punto de control entre usuarios, aplicaciones y activos de red es la identidad del usuario. La identidad digital afecta a todos los aspectos de la empresa moderna. Todos los usuarios necesitan acceder a sistemas y aplicaciones adecuados para realizar su trabajo. Sin embargo, controlar el acceso de forma segura es mucho más que una cuestión de productividad. El exceso de permisos, las contraseñas débiles y otros muchos problemas potenciales ocasionan filtraciones de datos, infecciones por malware, daños financieros sustanciales —y noches en vela entre los responsables informáticos y de la empresa.

A medida que crece el ecosistema de aplicaciones en la nube que utilizan los trabajadores, la gestión de las necesarias integraciones con AD se convierte en un reto, y no solo para el equipo de identidad. La ampliación de las directivas de seguridad y acceso del AD local a la nube también constituye un problema de seguridad. Para los expertos en AD acostumbrados a su modelo de permisos para el entorno local, puede resultar chocante el cambio de mentalidad que implica la integración de AD local con Azure Active Directory (AAD). (Para un debate más profundo sobre las implicaciones de gestionar tanto AD local como AAD en un entorno híbrido, consulte «Top Risks to Watch for in Shifting to Hybrid Identity Management»

(Principales riesgos que conlleva la adopción de gestión de identidad híbrida), de Doug Davis, Director de Producto Senior de Semperis).

Aumentar los conocimientos sobre identidad y seguridad

Para los profesionales de Active Directory y otros servicios de identidad que quieran contribuir a la estrategia de seguridad de la empresa, la clave es mantenerse al día, uno de los aspectos más difíciles (y gratificantes) de una carrera en tecnologías de la información. No hay más que pensar en todas las tecnologías que un profesional informático ha utilizado a lo largo de su vida y que ya no son relevantes. ¿Cuántas tecnologías han llegado al final de su vida útil y ya no reciben soporte? La educación es la clave para adaptarse a las realidades cambiantes de la seguridad y las operaciones informáticas.

Un aspecto positivo es que se pueden encontrar abundantes recursos para profesionales informáticos en Internet. Por ejemplo, Channel 9, ofrece excelentes vídeos de formación sobre productos Microsoft. Microsoft también ofrece guías de preparación para los exámenes de certificación en sus productos. Algunas certificaciones de seguridad que los profesionales de la identidad pueden consultar son «Security, Compliance, and Identity Fundamentals" y «Security Fundamentals.». Estas y otras certificaciones, además de ser buenos puntos de prueba para el currículum, brindan a los profesionales de la identidad una base sólida sobre los conceptos de seguridad que deberán aportar a las conversaciones con los líderes tecnológicos.

De todos modos, no hay nada mejor que la experiencia. Tener experiencia práctica en un entorno de laboratorio —no solo con AD local, sino también con entornos híbridos que utilizan Azure, AWS y Google Cloud Platform— es la única manera de adquirir verdadera capacidad para gestionarlo de manera eficaz y segura.

No deje nunca de formarse en los ámbitos de la identidad y la seguridad

Como en todas las trayectorias profesionales de las tecnologías de la información, el cambio es la única constante. El dominio de cualquier aspecto de este sector, desde la seguridad hasta el desarrollo de aplicaciones, requiere un compromiso para mantenerse al tanto de las distintas tecnologías y tendencias. Con el aumento de los riesgos de seguridad relacionados con la identidad y la creciente adopción de la nube, los profesionales de AD deben comprender el papel que desempeña la gestión de la identidad en la estrategia de seguridad de la organización, y esforzarse por liderar el debate sobre este aspecto.

Tres pasos para reforzar Active Directory a la luz de los recientes ataques

POR **BRIAN DESMOND,** *Principal, Ravenswood Technology Group*

En un reciente webinar que presenté junto a Semperis (responsables de la herramienta de evaluación de seguridad Purple Knight), nos centramos en un denominador común en los últimos ataques de alto perfil: Active Directory. En la sesión «Cómo aprovechan Active Directory los atacantes: Lecciones que pueden extraerse de las infracciones de alto perfil», analicé en compañía de Sean Deuby y Ran Harel de Semperis cuatro ataques recientes que aparecieron en las noticias: SolarWinds, los ataques de día cero de Hafnium Exchange, el ataque de Colonial Pipeline y el ataque al servicio de salud de Irlanda. Aunque cada caso fue diferente en términos tácticos y lo llevaron a cabo diferentes ciberdelincuentes, todos ellos tuvieron consecuencias devastadoras. En nuestro análisis cubrimos tres de las medidas preventivas más importantes que las organizaciones pueden adoptar para protegerse de los ciberataques.

1 Proteja el correo electrónico de amenazas avanzadas

Uno de los puntos de entrada más comunes para los atacantes es el correo electrónico. Las campañas de phishing avanzado resultan muy convincentes para los usuarios finales, y sirven a los atacantes para obtener credenciales válidas y/o introducir malware en los puntos de conexión. Es de vital importancia que las organizaciones adopten una metodología en varios frentes para protegerse de estas amenazas. La formación en materia de seguridad y los simulacros de phishing son importantes para educar y medir el riesgo. Por mucha formación que se imparta, los atacantes seguirán teniendo éxito. Para evitarlo, la estrategia defensiva debe incluir una solución avanzada de protección contra amenazas por correo electrónico que vaya más allá de las herramientas antispam y antivirus. En la situación actual conviene disponer de un servicio que haga uso de algoritmos de aprendizaje automático y otros métodos avanzados para detectar y bloquear mensajes de phishing y archivos adjuntos sospechosos.

«Habría que haber vivido muy aislado el último año para no haberse enterado de las importantes noticias sobre ciberseguridad que se producían cada semana. Pasamos mucho tiempo hablando de las nuevas formas de ataque, pero en realidad los responsables de las amenazas no están en esto en busca de novedades. Lo que quieren es entrar y para ellos Active Directory es una superautopista.»

— SEAN DEUBY, *Director de Servicios de Semperis*

2 Evite el movimiento lateral

Cuando un atacante compromete un ordenador cliente o un servidor miembro, intentará desplazarse lateralmente a través de la red y escalar sus privilegios. Si impedimos el movimiento lateral dificultaremos enormemente la actividad del atacante. Se pueden establecer algunos controles técnicamente sencillos —aunque a veces operativamente difíciles— para bloquear el movimiento lateral. En primer lugar, la contraseña del administrador local debe ser diferente en cada punto de conexión. Microsoft ofrece una solución gratuita llamada Local Administrator Password Solution (LAPS) para ello. En segundo lugar, no se deben anidar cuentas de dominio en el grupo de administradores locales para facilitar el soporte informático. El personal informático debe utilizar LAPS para recuperar credenciales administrativas de puntos de conexión específicos.

3 Acceso seguro a credenciales con privilegioscredentials

Una defensa fundamental consiste en evitar que los adversarios obtengan acceso privilegiado, en particular el de Administrador de dominio. Si un adversario puede escalar sus privilegios, podrá conseguir un control mayor o incluso un control completo de toda la red. Es extremadamente importante implementar controles efectivos que aíslen y protejan las credenciales de los privilegios. Dos de los conjuntos de controles más comunes que implementamos en Ravenswood Technology Group son los conceptos de controles de seguridad por niveles y de estaciones de trabajo de acceso privilegiado (PAW). Los controles de seguridad por niveles evitan que se expongan las credenciales de alto privilegio en activos de mayor riesgo, como los ordenadores cliente, donde podrían sustraerse. Las PAW aíslan las tareas que un administrador realiza desde su estación de trabajo de uso diario a una estación de trabajo altamente segura, protegiendo las credenciales y la sesión del administrador de vectores de amenaza como el correo electrónico, el acceso a Internet y algunos tipos de malware.

¿Está su AD preparado para el panorama actual de amenazas?

En este webinar solo analizamos cuatro de las innumerables infracciones que aparecen a diario en las noticias. Es imprescindible reforzar el entorno informático de su organización y Active Directory debe ser un componente central de la estrategia de refuerzo de prácticamente cualquier empresa. Si desea realizar una evaluación gratuita de los controles de seguridad de Active Directory, utilice Purple Knight. Ravenswood y Semperis son probablemente las dos organizaciones (aparte de la propia Microsoft) con más experiencia combinada en seguridad de AD. Disfrutamos de una alianza extremadamente sólida que ayuda a organizaciones de todo el mundo a elevar el nivel de seguridad de la identidad híbrida.

Si desea más recomendaciones para proteger su organización, consulte el seminario web bajo demanda. Y, por supuesto, puede descargar Purple Knight de forma gratuita para identificar y abordar las brechas de seguridad de AD y ganar confianza en la seguridad de su entorno de AD, por muy complejo, enrevesado o descuidado que resulte.

ROI práctico de la recuperación rápida de Active Directory

POR **SEAN DEUBY,** *Director of Services, Semperis*

Aunque todos los gestores o administradores de tecnologías de la información saben que un sólido plan de recuperación de Active Directory es un componente esencial de cualquier estrategia de continuidad del negocio, resulta muy complicado calcular el rendimiento práctico de la inversión (ROI) de un plan de recuperación de AD optimizado. Hay demasiadas variables en juego para obtener un cálculo exacto y justificable. Empecemos por aclarar algo: no voy a ofrecer ningún tipo de calculadora interactiva del ROI.

Lo que me gustaría más bien es analizar formas prácticas de obtener rendimiento de la inversión que garantice una recuperación adecuada de AD, lo que le permitirá hacer sus propios cálculos y llegar a sus propias conclusiones. Perder un controlador de dominio es un problema en sí mismo, pero veamos otro escenario cada vez más común con consecuencias catastróficas: un ataque de ransomware que elimina todos los controladores de dominio de todos los sitios de la empresa. En esta situación, la recuperación de AD puede ser un reto obligado y a la desesperada.

El último año hemos analizado decenas de ataques de ransomware en los que los ciberdelincuentes modificaron AD de una u otra forma —mucho más allá de los cambios básicos en cuentas de usuario o contraseñas— para acceder a los sistemas informáticos y moverse lateralmente para propagar el malware. Los arquitectos del ransomware cuentan ahora con ingenieros que diseccionan AD y sus actualizaciones de seguridad en busca de oportunidades para elevar los permisos y distribuir rápidamente el malware por toda la organización. Los análisis forenses realizados tras los ataques de ransomware que afectan a AD han revelado que los responsables de las amenazas se centran principalmente en los cambios en cuentas de grupo, cuentas de usuario, objetos de la directiva de grupo, SYSVOL y controladores de dominio.

Teniendo en cuenta estas tácticas de los ciberdelincuentes, analicemos los siguientes factores que afectan al cálculo del ROI de recuperación de AD:

Coste de las pérdidas operativas

Es probable que una parte importante de sus operaciones dependa de que AD esté en funcionamiento para autenticar a los usuarios como base para dar acceso a aplicaciones, sistemas y datos. Por cada hora que AD no está operativo, ¿cuántos ingresos o qué productividad perdería su empresa? ¿Cuántas horas, días o semanas harían falta para que la empresa llegara a un punto de no retorno y no pudiera recuperarse económicamente? ¿Recuerda el ataque de ransomware a la ciudad de Baltimore? La recuperación de sus operaciones tardó meses y tuvo un coste de más de 18 millones de dólares.

Ausencia de un plan de continuidad del negocio que incluya AD

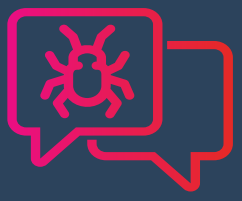
Si su organización es lo suficientemente madura, contará con un plan de continuidad del negocio (BC) y recuperación de desastres (DR) que define la actividad necesaria para restaurar las operaciones de negocio después de una interrupción. La mayoría de los planes tienen en cuenta la pérdida de infraestructura o la pérdida de una ubicación después de un desastre natural. Pero pocas empresas tienen un plan específico para restaurar el negocio después de un ciberataque, especialmente cuando es tan impredecible como los ataques de ransomware. La forma de recuperar AD en un escenario como este depende de los cambios que los ciberdelincuentes hayan realizado en AD. Es posible que piense recuperar una versión anterior de AD, pero ¿cómo establece hasta dónde debe retroceder para encontrar una versión segura? ¿Qué sistemas, servicios y aplicaciones dependientes de AD se verán afectados o no funcionarán lo más mínimo debido a una recuperación a gran escala a un estado anterior de AD? ¿Está seguro de que puede localizar una copia de seguridad reciente y libre de malware para restaurar? Sin un plan o la posibilidad de entender lo que ha cambiado en AD antes de la recuperación, su organización dedicará un tiempo incalculable en solucionar todos los problemas que ha causado la recuperación.

La recuperación podría no ser la respuesta

Si todos los cambios realizados por los delincuentes durante un ataque se reducen a añadir una cuenta al grupo de administradores de dominio, por ejemplo, quizá la respuesta correcta no sea recuperar AD tal como se encontraba unos días atrás o el mes anterior. Un método menos costoso podría consistir en monitorizar los cambios en AD y desautorizar los cambios en cuentas «protegidas» (como el grupo administradores de dominio) o revertir automáticamente un cambio a una configuración autorizada.

Las consideraciones anteriores se resumen en tres riesgos: riesgo de una recuperación lenta, riesgo de una recuperación que genere más trabajo de reparación y riesgo de una recuperación que pueda considerarse excesiva para el tipo de cambios que se han realizado en AD.

CASOS PRÁCTICOS:



Semperis proporciona recuperación de desastres «cyber-first» de gran calidad para Active Directory. Algunos de los resultados que nuestros clientes han comentado después de desplegar Semperis Active Directory Forest Recovery:

- La aerolínea israelí El Al desplegó Semperis ADFR y redujo el tiempo de recuperación completa del bosque de AD de 24 a 2 horas.

- Un minorista global con 2,2 millones de usuarios y 500 DC adoptó Semperis ADFR en sustitución de una solución existente y redujo el tiempo de recuperación de un bosque de AD de 6 días a 6 horas.
- Una empresa dedicada a la atención sanitaria con un DIT de 65 GB redujo el tiempo de recuperación del bosque de AD de 1,5 días con la solución existente a menos de 4 horas con Semperis ADFR.

Un método diferente para calcular el ROI de la recuperación de AD

En lugar de analizar el ROI de la recuperación de AD con algún tipo de calculadora que haya encontrado en Internet, la mejor opción es analizar varias situaciones reales y evaluar cómo le iría a su sistema actual de recuperación de AD respondiendo a las siguientes preguntas basadas en los factores señalados anteriormente:

- ¿Qué partes críticas de la operación dependen de AD para su funcionamiento? ¿Cuál es el coste estimado de un periodo de inactividad?

- ¿Cuánto tiempo se tarda en recuperar AD en función de los cambios sufridos en un ataque?

- ¿Tiene visibilidad de los cambios maliciosos que se han realizado en AD y, si no es así, hasta dónde tendrá que investigar y cuánto tiempo tardará?

- ¿Influirá la recuperación en otras partes de las operaciones que tendrá que solucionar y, si es así, cuánto tiempo tardará? (Recuerde que algunas contraseñas de cuentas de usuarios y de ordenadores no coincidirán, lo que impedirá la posibilidad de iniciar sesión en el dominio. Además, es posible que en las versiones anteriores falten cuentas, suscripciones a grupos, registros DNS, etc.).

- ¿Tiene la certeza de que la recuperación le dejará en un estado de seguridad conocido? Tenga en cuenta la diferencia entre reanudar operaciones comerciales y recuperar operaciones comerciales: si no tiene una copia de seguridad limpia y libre de malware para la recuperación, corre el riesgo de volver a introducir las mismas vulnerabilidades que permitieron el ataque original.

En resumen, el ROI de la recuperación de AD tiene mucho más que ver con su capacidad para recuperar un estado productivo y seguro conocido después del ataque que con una calculadora de ROI online que no tiene en cuenta las innumerables variables implicadas en un ataque de ransomware. Examine algunos escenarios y analice específicamente cuáles son sus capacidades de recuperación en la actualidad para averiguar qué costes puede eliminar si dispone de una solución de recuperación de AD adecuada, diseñada para proteger, prevenir y recuperarse de los cambios maliciosos en AD.

Cómo defenderse de ataques a Active Directory que no dejan huella

POR **GUIDO GRILLENMEIER,** *Chief Technologist,Semperis*

Los ciberdelincuentes están utilizando nuevas tácticas y técnicas para acceder a Active Directory, lo que hace que sus ataques resulten cada vez más peligrosos y sea más necesario detectarlos.

Uno de los aspectos más importantes de cualquier estrategia de ciberseguridad es la detección. Para poder responder con celeridad es fundamental tener la capacidad de detectar a los atacantes que entran en la red, se mueven dentro de ella o, lo que es peor, la administran. Y dada la media de días que permanece un atacante sin ser detectado en una red, 146 días según Microsoft, parece obvio que se les da muy bien trabajar sigilosamente.

Cuando se trata de detectar acciones potencialmente maliciosas en Active Directory (AD), la mayoría de las organizaciones confían en la consolidación del registro de eventos del controlador de dominio y en soluciones SIEM para detectar inicios de sesión y cambios anormales. Todo esto funciona siempre que la técnica de ataque deje rastro en el registro.

Se ha comprobado que ciertos tipos de ataques no dejan ninguna huella apreciable o, al menos, ninguna evidencia de actividad maliciosa. Algunos ejemplos:

Ataque de DCShadow

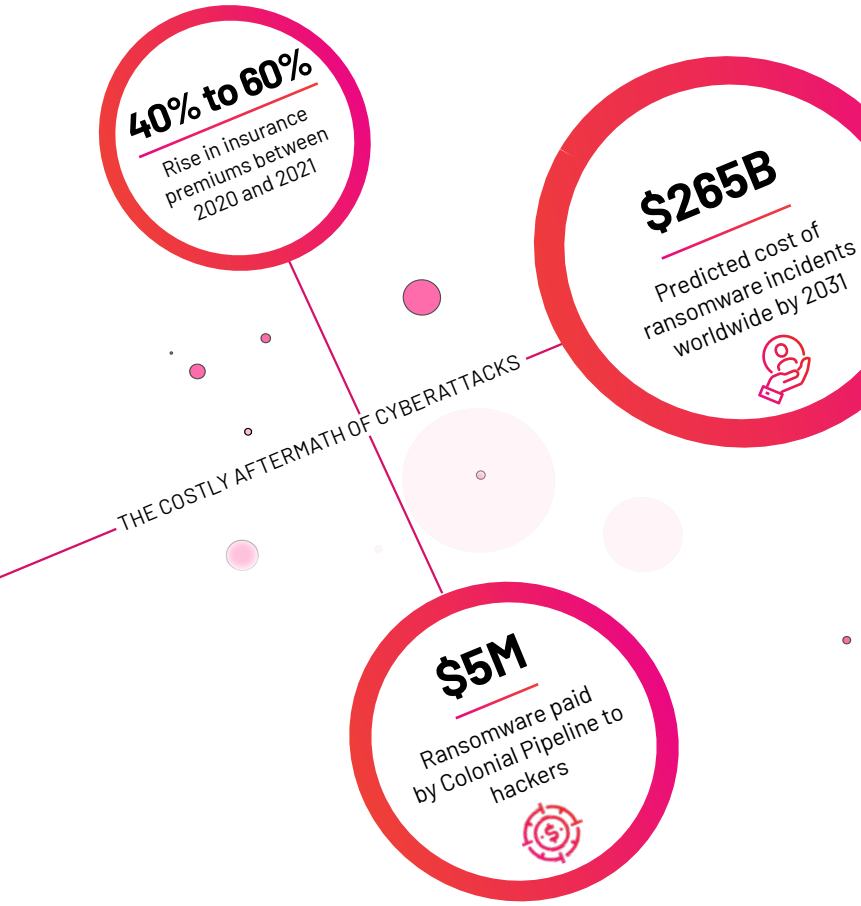
Este ataque utiliza la funcionalidad DCShadow de la herramienta de hackers Mimikatz. En primer lugar registra un controlador de dominio (DC) no autorizado modificando la partición de configuración de AD. A continuación, el atacante realiza cambios falsos de carácter malicioso (por ejemplo, cambios en la pertenencia a grupos de administradores de dominio o incluso cambios menos obvios como añadir el SID del grupo de administradores de dominio al atributo sidHistory de un usuario normal en riesgo). Esta técnica de ataque evita el registro tradicional basado en SIEM, pues el DC no autorizado no informa de los cambios. Los cambios se inyectan directamente en el flujo de replicación de los controladores de dominio de producción.

Cambios en la directiva de grupo

Un ataque documentado relacionado con el ransomware Ryuk dio lugar a cambios en un objeto de directiva de grupo que propagó la instalación de Ryuk a puntos de conexión remotos de la organización afectada. De forma predeterminada, los registros de eventos no incluyen detalles sobre lo que se ha cambiado en una directiva de grupo. Por tanto, si un atacante realiza un cambio malicioso (como en el caso de Ryuk), lo único que se ve es que una cuenta con acceso a la directiva de grupo ha realizado un cambio, lo que probablemente no desencadenará ninguna alarma.

Ataque de Zerologon

Tras la publicación de un código de vulnerabilidad de prueba de concepto, un atacante con acceso a la red de un controlador de dominio pudo enviar mensajes Netlogon especiales que consistían en cadenas de ceros,



forzando la sustitución de la contraseña del ordenador del controlador de dominio por una cadena vacía. De este modo, sin inicio de sesión —es decir, con inicio de sesión cero— el atacante es ahora dueño del controlador de dominio, puede realizar cambios en AD y puede seguir utilizando esta vía para atacar otros sistemas de la infraestructura. Es poco probable que sus herramientas de monitorización vigilen cambios imprevistos de contraseñas en los DC.

No es casualidad que estos ataques no dejen rastro. Están diseñados para eso. Los delincuentes dedican muchísimo tiempo a inspeccionar el funcionamiento exacto de sus entornos objetivo y a buscar formas de eludir, ofuscar y sortear cualquier forma de detección, incluido el registro.

Dada la existencia de este tipo de ataques, la pregunta es qué se puede hacer al respecto, tanto de forma proactiva como reactiva.

Protección frente a cambios maliciosos en Active Directory

Hay tres maneras de proteger su organización frente a cambios maliciosos en AD:

- **Vigile la presencia de cambios maliciosos en AD:** esta tarea va más allá de SIEM e implica una solución de terceros diseñada para ver todos los cambios realizados en AD —independientemente de quién los haga, en qué DC, con qué solución, etc.—, en una situación ideal leyendo y entendiendo el tráfico de replicación de los propios DC. Esta monitorización debe incluir también los cambios en la directiva de grupo. En muchos casos, las soluciones diseñadas para monitorizar los cambios en AD pueden definir objetos protegidos específicos cuyos cambios deben monitorizarse, por ejemplo, cambios en la pertenencia en los administradores de dominio. De este modo, cada vez que se modifiquen estos objetos protegidos se activarán las alarmas. La solución debe cubrir tanto los cambios en las directivas de grupo como la visibilidad de la replicación.

- **Busque el rastro de DCShadow:** Mimikatz deja algunos artefactos a su paso y hay señales que indican que se ha utilizado DCShadow en la red. La comprobación periódica de la seguridad de AD debería incluir la búsqueda de estas señales en AD. Tenga en cuenta que si encuentra algún rastro de Mimikatz DCShadow en su entorno deberá actuar rápidamente, pues está siendo víctima de un ataque. En ese momento, le convendrá tener también una solución que le muestre qué cambios se han realizado en el nivel de replicación para analizarlos y, si es posible, revertirlos.

- **Tenga capacidad para recuperar AD:** Su organización debe tener la capacidad proactiva de recuperar partes o la totalidad de AD si determina que se ha producido una vulnerabilidad.

  En algunos casos puede recurrir a copias de seguridad y a una estrategia de DR para recuperar AD en situaciones de ciberataque. Si necesita recuperar todo el servicio de AD, potencialmente como la próxima víctima de un ataque de malware, tenga en cuenta que una buena copia de seguridad del controlador de dominio no equivale a una recuperación rápida y fluida del servicio de AD. Le conviene practicar periódicamente todo el proceso de recuperación, siguiendo la completa «Guía de recuperación del bosque de Microsoft AD». Pero es igualmente válido recurrir a soluciones que reviertan los cambios hasta el nivel de atributos o incluso revertir automáticamente los cambios cuando se detecten para proteger los objetos.

En la actualidad los ciberdelincuentes suelen adoptar la táctica de atacar Active Directory y modificarlo para que se adapte a sus intereses, hasta el punto de que quizá haya dejado ser práctico el antiguo modelo de monitorizar cambios en los eventos de auditoría de AD. Las organizaciones que se toman en serio la seguridad y la integridad de su AD deben buscar otras formas de conseguir visibilidad de cada cambio en AD y tener capacidad para revertirlo o recuperarlo cuando sea necesario.

WEBINAR

HOW ATTACKERS EXPLOIT ACTIVE DIRECTORY: LESSONS LEARNED FROM HIGH-PROFILE BREACHES

MORE RESOURCES

WEBINAR

- Would Your Organization Fail the Active Directory Security Assessment?

BLOGS

- Timeline of a Hafnium Attack
- Active Directory Security: Abusing Display Specifiers

¿Conoce las vulnerabilidades de seguridad de su Active Directory?

POR **SEAN DEUBY,** *Director of Services, Semperis*

La seguridad de Microsoft Active Directory (AD) implica lidiar con diversos riesgos, que van desde los errores de gestión hasta las vulnerabilidades sin parches. A menudo se dice que los ciberdelincuentes se centran en AD para elevar privilegios y conseguir persistencia en la organización. Cuando se investiga una filtración de datos típica suele descubrirse que probablemente se han utilizado credenciales robadas, a veces para la entrada inicial, a veces para acceder a sistemas críticos, pero siempre en detrimento de la organización atacada.

El refuerzo de AD comienza por el conocimiento de las vulnerabilidades y los errores comunes de configuración y gestión que allanan el camino a las amenazas. Para proteger AD, los administradores deben saber cómo se realizan los ataques a su entorno. Sin embargo, ¿cuántos podrían aprobar un examen sorpresa sobre el tipo de agujeros de seguridad por los que penetran los ciberdelincuentes en sus ataques?

Fallo de autenticación

Por curioso que parezca, algunos de los errores de configuración más frecuentes y dañinos que afectan a Active Directory están relacionados con el proceso de autenticación. Supongamos un escenario en el que una organización desea permitir una aplicación de terceros o propia que no está integrada con AD, pero quiere que los usuarios activos puedan consultar AD. La ruta más fácil es simplemente habilitar el acceso anónimo a Active Directory. Si bien esta acción puede mejorar la productividad de administradores muy ocupados, también permite que usuarios no autenticados consulten AD. Si se habilita esa posibilidad sin controles de mitigación, el perfil de riesgo de la organización aumentará sustancialmente.

La vulnerabilidad Zerologon que se produjo en 2020 fue aprovechada rápidamente por los atacantes porque les permitía cambiar o eliminar la contraseña de una cuenta de servicio en un controlador de dominio. Los resultados de una vulnerabilidad pueden ser catastróficos. Contraseñas débiles, contraseñas que no caducan, ausencia de contraseñas... todo ello son señales de advertencia de la falta de seguridad del entorno de AD de una organización.

Las directivas de contraseñas seguras deberían estar a la orden del día en toda infraestructura de Active Directory. Cualquier cuenta con el indicador PASSWD_NOTREQD debería acarrear automáticamente una vigilancia especial y contar con razones de peso para esta configuración. Además, las contraseñas deberían cambiarse periódicamente, en particular las de las cuentas de servicio. Mantener la misma contraseña durante mucho tiempo aumenta la probabilidad de que un ataque por fuerza bruta tenga éxito, pues los atacantes tendrán más oportunidades para intentarlo.

Problemas de autenticación que conviene tener en cuenta:

- Ordenadores y objetos de cuentas de servicio administradas de grupo (gMSA) con contraseñas establecidas hace más de 90 días
- Contraseñas reversibles que se encuentran en objetos de directiva de grupo (GPO)
- Acceso anónimo a Active Directory
- Vulnerabilidad Zerologon (CVE-2020-1472) si no se aplica el parche.

Conceder permisos excesivos

Dado que la mayoría de los entornos de AD han estado en producción durante años, sus superficies de ataque han aumentado. Muchas de las vulnerabilidades acumuladas de un bosque pueden deberse a que alguien necesita que se realice una tarea, normalmente con prisa, y la ruta con menos privilegios para conseguirlo es demasiado larga, no tiene fácil acceso o simplemente no se conoce. Por ello, se conceden privilegios excesivos al usuario, grupo o permiso solo para garantizar que se atiende la petición y se cierra la incidencia. Naturalmente, ese derecho no se elimina, por lo que la superficie de ataque no deja de crecer.

En realidad, no es raro que los entornos de AD tengan un número innecesariamente alto de administradores de dominio, lo que puede ser aún más preocupante si esas cuentas quedan huérfanas y están esperando simplemente a que alguien se aproveche de ellas en un ataque. Las cuentas de servicio con permisos excesivos también plantean un alto riesgo, pues sus contraseñas suelen estar configuradas para no caducar y muchas de ellas serán débiles (lo que las convierte en un buen objetivo para kerberoasting). A medida que crece el número de usuarios con privilegios administrativos, también aumenta la superficie de ataque que debe protegerse. La pertenencia a estos grupos debe controlarse atentamente.

Naturalmente, se producen errores. Por ejemplo, a medida que crece un entorno de AD y aumenta su complejidad, alguien puede pasar por alto los permisos heredados y conceder inadvertidamente demasiados privilegios a una cuenta. Pero si los atacantes toman la iniciativa ni siquiera una gestión adecuada de la delegación de privilegios es suficiente.

Un ejemplo puede ser el impacto de un ataque a AdminSDHolder. Recordemos que el contenedor AdminSDHolder almacena el descriptor de seguridad que se aplica a grupos privilegiados. De forma predeterminada, el proceso de SDPROP (propagador de descriptores de seguridad) compara cada 60 minutos los permisos de los objetos protegidos y revierte cualquier discrepancia de acuerdo con la configuración definida en AdminSDHolder.

En un ataque a AdminSDHolder, los ciberdelincuentes aprovechan SDPROP para mantener la persistencia sustituyendo los permisos de un objeto por las modificaciones no autorizadas del atacante. Si se identifican los cambios en los permisos y se deshacen, pero no se detectan los cambios no autorizados en AdminSDHolder, se restablecerán los cambios del atacante.

Auditar los permisos y monitorizar la actividad sospechosa es la mejor defensa contra el abuso de privilegios.

Problemas de permisos que conviene tener en cuenta:

- Objetos con privilegios que tienen propietarios sin privilegios
- Cambios en permisos en el objeto AdminSDHolder
- Usuarios sin privilegios con derechos de sincronización de DC en el dominio
- Cambios en el esquema del descriptor de seguridad predeterminado en los 90 últimos días

SECURING AZURE ACTIVE DIRECTORY

Los principales riesgos de seguridad que hay que tener en cuenta al adoptar la gestión híbrida de identidad

POR **DOUG DAVIS,** *Senior Product Manager, Semperis*

Es fácil comprender por qué las empresas están gravitando hacia un modelo de gestión de identidad híbrido que promete lo mejor de ambos mundos: la nube y local. En un entorno centrado en Active Directory, el cambio a la nube implica la integración con Azure Active Directory.

Después de todo, Azure Active Directory (AAD) se ha diseñado con la vista puesta en las aplicaciones SaaS, proporcionando un único inicio de sesión y control de acceso. Conforme aumenta la adopción de la nube, la capacidad de gestionar el acceso local y de la nube se está transformando en una necesidad para las empresas. El uso de AAD junto a Active Directory (AD) ayuda a hacer realidad la gestión híbrida de identidad.

Sin embargo, como siempre ocurre en el ámbito de las tecnologías de la información, se aplica el principio «ver si hay agua antes de lanzarse a la piscina».

Cambio radical con el cambio a la nube

Trasladar partes de las operaciones informáticas a la nube requiere ajustes. Lo mismo ocurre con la autenticación de usuarios. Desde un punto de vista conceptual, las organizaciones deben tener en cuenta tres aspectos fundamentales.

1. Un nuevo modelo de autenticación

Después de 20 años gestionando la identidad de cierta manera, la incorporación de AAD obligará a realizar ajustes esenciales. La ampliación de la autenticación a la nube, en lugar de utilizar exclusivamente AD local, requiere una mentalidad y una metodología diferentes. En AAD no hay unidades organizativas, bosques ni objetos de directiva de grupo. Los conceptos sobre protección de identidad en AD (y sus implicaciones) no son válidos en AAD.

Muchos administradores empiezan creyendo que la protección de AAD es similar a la de AD, y no es así. Es posible que ya esté utilizando AAD sin darse cuenta. Si su organización utiliza servicios de Microsoft en la nube, como Office 365, ya está utilizando AAD en segundo plano. AAD también se emplea en buena medida para conectarse a otras aplicaciones SaaS ajenas a Microsoft, como Salesforce. Todos estos factores introducen nuevas consideraciones y opciones. Por ejemplo, ¿deberían mantenerse AD y AAD separados o fusionarlos mediante Azure AD Connect? Es necesario comprender muchos conceptos nuevos para poder tomar estas decisiones y mantener la seguridad de los sistemas de información.

2. La extensión del perímetro

Cuando una organización adopta la nube, el concepto de perímetro de las redes tradicionales deja de existir. Para los administradores que han pasado las dos últimas décadas gestionando AD a nivel local, este cambio supone un enorme ajuste. En un entorno de identidad híbrida, las organizaciones deben estar preparadas para protegerse de un sinfín de posibles puntos de entrada.

3. Cambios radicales en el modelo de permisos

La adopción de AAD también supone un cambio drástico del modelo de permisos que las organizaciones deben proteger. A nivel local es relativamente fácil controlar quién tiene acceso físico a los controladores de dominio, y los puntos de entrada de gestión global están bien definidos y documentados. En un entorno de AD híbrido, las identidades también se almacenan en la nube, donde se encuentran expuestas a cualquiera que tenga acceso a Internet. De pronto, los administradores se enfrentan a un modelo intrínsecamente abierto para las conexiones de acceso inicial. Si a esto añadimos el mayor número de servicios, roles y permisos necesarios, el impacto en el panorama de riesgos es significativo.

Microsoft ha tratado activamente de elaborar materiales de formación para preparar a las empresas para los cambios provocados por la adopción de AAD. Sin embargo, muchas organizaciones de tecnologías de la información siguen sin apreciar plenamente las implicaciones de la gestión de identidad híbrida. Dado que cada vez más empresas adoptan un sistema híbrido, los atacantes han ampliado su forma de actuar.

En septiembre de 2020, los investigadores de Mandiant (FireEye) observaron que se había producido un incremento de los incidentes relacionados con Microsoft 365 y Azure Active Directory, en su mayoría vinculados a correos electrónicos de phishing que intentaban atraer a las víctimas para que introdujeran sus credenciales de Office 365 en un sitio de phishing. Los investigadores de Mandiant también observaron que los atacantes utilizaban un módulo de PowerShell llamado AADInternals, que les permite pasar del entorno local a AAD, crear puertas traseras, robar contraseñas y realizar otras acciones maliciosas. Estas amenazas seguirán aumentando con el crecimiento exponencial del interés por Azure y Office 365.

Permisos, permisos, permisos permissions

Con mucho, de los tres temas mencionados anteriormente, el mayor riesgo para la seguridad procede de los cambios en el modelo de permisos. Hay un gran número de servicios que están disponibles cuando las organizaciones pasan a un entorno de identidad híbrida. En lugar de un conjunto bien definido de grupos administrativos en Active Directory, en Azure AD hay roles que para muchos resultan desconocidos. Aquí se encuentra esta lista de roles. Cada rol tiene una larga lista de permisos asignados. Es difícil entender los permisos asignados a cada rol solo por su descripción, pero muchos tienen un alto nivel de acceso que no es evidente.

Además, la vinculación de cualquier servicio SaaS con AAD, que es probablemente la razón por la que se ha puesto en juego AAD, añade modelos de permisos que se deben gestionar. Microsoft Teams, por ejemplo, utiliza la integración de SharePoint en el back-end. Si la configuración es incorrecta y se añade un invitado a Teams, se puede dar la situación de que este nuevo usuario tenga acceso a los archivos almacenados en SharePoint para Teams. Es posible que los administradores no sean conscientes de que estos archivos están ahora disponibles para usuarios invitados que se han incorporado al canal para una charla rápida. Además, la posibilidad de añadir aplicaciones en Teams amplía en la práctica el modelo de permisos a estas herramientas de terceros. Es solo un ejemplo de la matriz de problemas complejos que plantea cada servicio gestionado a través de AAD.

De hecho, es fundamental hacer un seguimiento de los permisos de las aplicaciones de terceros y este es un aspecto que no se gestiona suficientemente en la mayoría de las implementaciones de AAD. Estas solicitudes de permiso activarán una ventana emergente que aparece una sola vez e indica los permisos que necesita la aplicación. Estas listas pueden ser largas y conviene revisarlas cuidadosamente antes de aceptarlas, pero esto rara vez se hace.

Las organizaciones también podrían encontrarse con estos dos nuevos escenarios relacionados con los permisos que se deben entender en un contexto de seguridad:

- **Herramientas de terceros que extraen datos de Azure AD y los almacenan en su propia base de datos.** Por ejemplo, una aplicación registrada en Azure AD que permite que un sistema de CRM lea perfiles de usuarios o que tiene otros permisos de lectura en la práctica puede recuperar y almacenar datos para sí misma. Una vez que los datos se extraen de Azure AD, se encuentran en una base de datos externa, dejando que la organización dependa del marco de seguridad de la herramienta de terceros.

- **Herramientas de terceros con acceso de escritura que pueden realizar cambios en su herramienta.** En este caso, la autenticación requerida para realizar cambios en el inquilino se traslada de Azure AD a cualquier control que tenga la herramienta de terceros. Un usuario podría iniciar sesión en la herramienta sin autenticación multifactor porque no admite el inicio de sesión único (SSO), operando en su lugar con la aplicación que actúa como proxy de permisos que realiza la acción en su nombre sin algunas de las verificaciones que suelen ser obligatorias.

Las organizaciones de tecnología de la información deberían plantearse seriamente la posibilidad de restringir quién puede aprobar las aplicaciones o, al menos, contar con una norma clara sobre los permisos que deberían considerarse imprescindibles. La adopción de una metodología de identidad híbrida requiere un modelo de permisos mucho más amplio. Para ello, las organizaciones deben establecer una sólida regulación sobre las aplicaciones que se activarán y los derechos de acceso que tendrán.

Comprender el riesgo de la gestión de identidad híbrida

Tanto si la autenticación se gestiona en la nube como si se hace a nivel local o de ambas formas, resulta imprescindible dar prioridad a la seguridad. Aunque gestionar la identidad en un entorno híbrido puede parecer tan sencillo como vincular un dispositivo Windows con AAD, conviene tener en cuenta los cambios que conlleva en el panorama de riesgos. Puede abrir la puerta a problemas que en el futuro podrían causar verdaderas preocupaciones. El conocimiento siempre es una primera línea de defensa, pero resulta desalentador comprobar la cantidad de documentación que se requiere para entender plenamente la seguridad en AAD. Las herramientas nativas o de terceros que automatizan esa comprensión y reducen la complejidad de la seguridad ayudarán a reducir el riesgo de seguridad durante y después del despliegue del entorno híbrido.

NUEVAS PERSPECTIVAS DE PROTECCIÓN DE SISTEMAS DE IDENTIDAD HÍBRIDA

De los expertos en seguridad de identidad presentes en #HIPEurope2021

«Cuando un atacante consigue acceso a AD, es urgente actuar. Tenemos que asegurarnos de que el atacante no pueda llegar a todos los bosques de Active Directory. Es necesario analizar la brecha, ver el potencial impacto e implementar una red de seguridad. Se trata de recuperar AD en cuestión de horas, no de días.»

Ben Cauwel
Responsable de Seguridad de Accenture

«Uno de los grandes problemas de la seguridad en la nube es que algunos no entienden todavía el modelo de responsabilidad compartida.»

Jan de Clercq
Arquitecto de Seguridad Senior de HPE

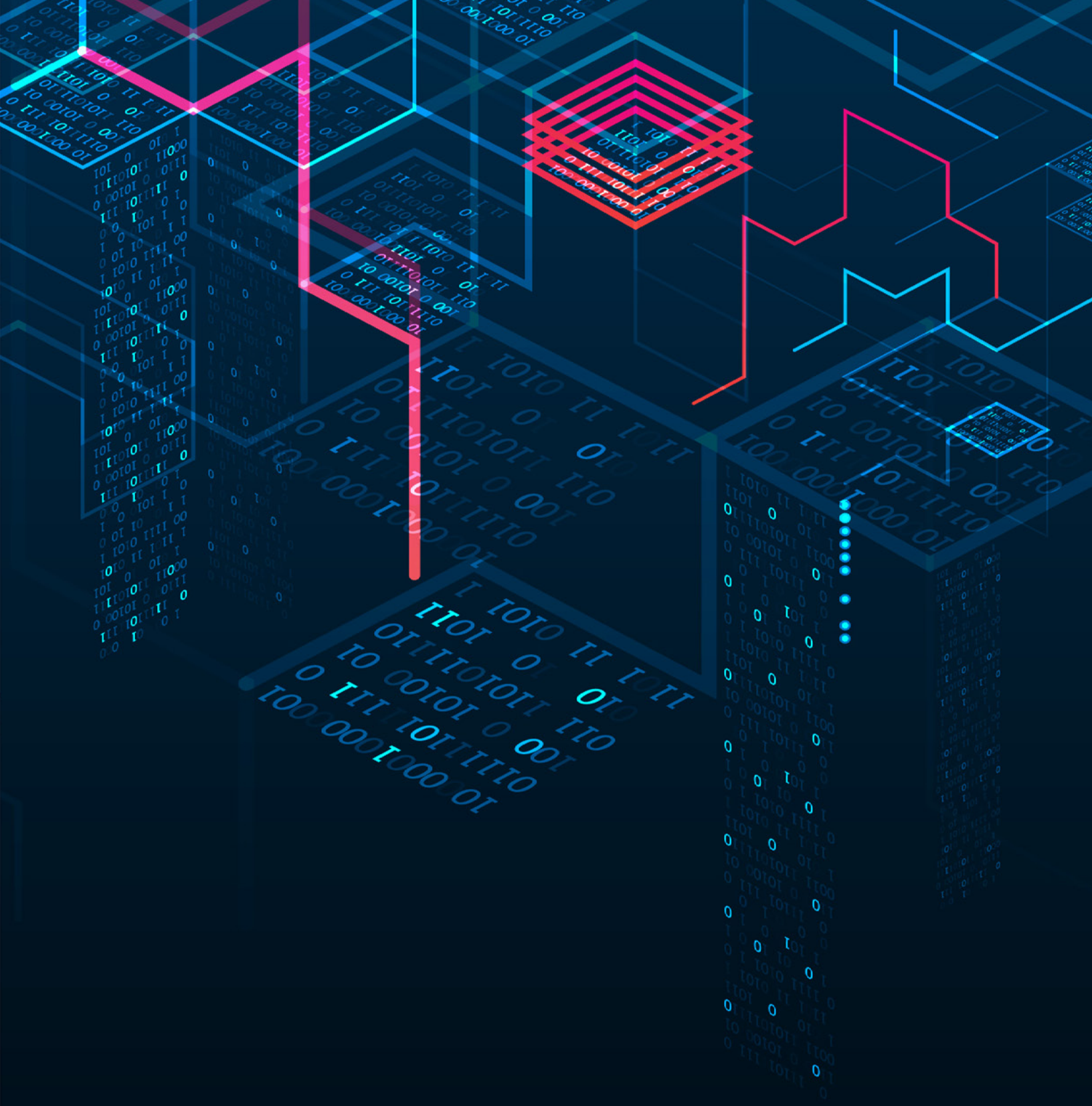
Join us for HIP Global 2021

DECEMBER 1-2

REGISTER →

Pamela Dingle
Directora de Estándares
de Identidad de Microsoft

«Quienes no hayan implementado MFA deben establecer el orden de sus prioridades. Los atacantes están encontrando medios para entrar en la infraestructura local y se aprovechan de que algunos de ustedes tienen la idea equivocada de que los usuarios, simplemente por haber accedido a los sistemas locales, ya son de confianza. Sufrir una infracción es complicado, caro y dañino. Implementar MFA no es difícil, pero la alternativa es enormemente problemática.»



semperis

semperis.com