

Active Directory, protegiendo el corazón de la empresa

¿Quién no ha oído hablar del Directorio Activo? Existe desde Windows 2000 y es una pieza fundamental para autorizar usuarios, accesos y aplicaciones en toda una organización, lo que le convierte en un objetivo prioritario para los atacantes. Si un ciberdelincuente es capaz de acceder al Directorio Activo podrá acceder a todas las cuentas de usuario, bases de datos, aplicaciones y todo tipo de información. Por lo tanto, un compromiso del Active Directory, particularmente cuando tarda en detectarse, es, sencillamente, un desastre.

La identidad se ha convertido en algo problemático de proteger. Recuerda Nuno Antunes Ferreira, director para España y Portugal de Semperis, que la razón por la cual la identidad llama la atención de los ciberdelincuentes es “porque vivimos en un mundo sin muros físicos ni lógicos, sin muros que nos defiendan”. El trabajo híbrido, que muchas organizaciones han mantenido después de la pandemia, o el fenómeno de los nómadas digitales, es una constante, dice también el directivo, añadiendo que los usuarios esperan poder trabajar y ser productivos en cualquier momento y en cualquier lugar, “de ahí la necesidad de saber quién es quién, dónde está, lo que puede hacer y desde qué dispositivo y red está trabajando”. Y por eso es importante proteger los sistemas de identidad de las empresas, Active Directory y Azure Active Directory, “porque si controlas al Directorio Activo de una organización, controlas la organización”.

Semperis es una compañía fundada en 2014 con el objetivo de ayudar a las empresas a proteger su directorio activo, detectando vulnerabilidades, interceptando ciberataques y recuperándose rápidamente del ransomware y otras



Uno de los sectores más críticos de las infraestructuras y de los clientes es el directorio activo



“LA INTERRUPCIÓN DEL DIRECTORIO ACTIVO NO ES UNA OPCIÓN” (ANADAT)



CLICAR PARA VER EL VÍDEO

emergencias de integridad de datos. Y lo hace a través de dos herramientas: Directory Service Protector (DSP) y Active Directory Forest Recovery, sobre los que nos habla David Carbonero, Cloud Architect Specialist de Anadat, partner de referencia de Semperis en España con más de 20 años en el mercado y cuyo objetivo es “ayudar a los clientes con la operación de sus entornos más críticos”.

Lo primero que destaca David Carbonero es que uno de los sectores más críticos de las infraestructuras y de los clientes es el directorio activo. Las aplicaciones empresariales locales y en la nube se basan en Active Directory y Azure Active Directory, lo que las convierte en una pieza fundamental de su infraestructura de TI. Su flujo constante, gran cantidad de configuraciones y un panorama de amenazas cada vez más



“LAS EMPRESAS DEBEN REALIZAR URGENTEMENTE UNA EVALUACIÓN DE LOS ENTORNOS DE AD” (SEMPERIS)



CLICAR PARA VER EL VÍDEO

La tecnología patentada de Semperis desacopla Active Directory del sistema operativo subyacente para evitar la reinfección de malware

a los administradores a abordar primero los problemas más importantes. La herramienta detecta cambios maliciosos que se haya podido producir durante un ciberataque y los notifica a los administradores. Opcionalmente, puede revertir las modificaciones automáticamente tan pronto como se detecten, lo que permite a las empresas responder a las infracciones con mayor rapidez.

“La recuperación del directorio activo es siempre, siempre la primera operación que hay que realizar o nada funcionará”, explica Nuno Antunes. Aquí

sofisticadas hace que proteger el Directorio Activo no sea fácil. “Entendemos que la interrupción del servicio de validación de identidades no es una opción”, asegura el ejecutivo explicando que Semperis Directory Services Protector (DSP) es “un radar”, una herramienta “que me va a permitir monitorizar y ver los eventos que se pueden producir en el directorio activo cuando esté sufriendo un ataque. La solución supervisa continuamente

AD y Azure AD en busca de indicadores de exposición y proporciona una vista única de las actividades, tanto en las instalaciones como en la nube.

Semperis Directory Services Protector puede escanear una implementación de Active Directory o Azure AD en busca de vulnerabilidades y configuraciones erróneas, priorizando los fallos de seguridad en función de su gravedad para ayudar



Los secretos de Semperis Active Directory Forest Recovery (ADFR)

Respondidas por David Carbonero, Cloud Architect Specialist de Anadat, las siguientes preguntas desvelan las características más destacadas de Semperis ADFR

- **¿Es necesario dar de alta el servidor ADFR en el Dominio?** No, no hace falta. El Servidor ADFR es una máquina que debe estar siempre configurada en un grupo aparte.
- **¿Se puede gestionar con el servidor ADFR más de un bosque?** Sí. Si tienes distintos bosques necesitas varias licencias, una para cada bosque, y con el producto puedes crear un plan de backup diferente para cada bosque o dominio que tengas
- **¿Se puede restaurar el Directorio Activo en los mismo Controladores de dominio o necesito es necesario desplegar nuevos servidores?** La herramienta nos permite restaurar el Directorio Activo sobre los mismos DCs, pero en el caso de que los DCs estén infectados, la herramienta me permite restaurar el AD sobre máquinas nuevas recién instaladas. Una de las grandes ventajas del producto es que desacopla el sistema operativo del directorio activo, por lo que al hacer el backup del AD, solamente se copian los objetos, y mediante esos objetos es capaz de restaurar el AD sobre las máquinas recién instaladas.
- **¿Para el ADFR se necesita algún servidor de BBDD?** No. Semperis ADFR integra un SQL Server Express, que es una versión gratuita de Microsoft, y no necesitamos licenciar ningún servidor.
- **¿Cómo conecta el servidor ADFR con los Controladores de Dominio?** Mediante unos agentes. Por eso es muy importante instalar el servidor ADFR en una red independiente que solamente tenga conexión con los controles de dominio mediante estos agentes. De esta manera los backups van a estar siempre protegidos y seguros ante un ataque de tipo ransomware y me va a garantizar el poder levantar las máquinas.

es donde entra Semperis Active Directory Forest Recovery, que promete ayudar a las empresas a restaurar rápidamente las implementaciones de AD y Azure AD después de un ciberataque. El producto puede reducir el tiempo de inactividad hasta en un 90%. Cuando un ataque de ransomware o de limpieza (wiper attack) elimina los controladores

de dominio, la recuperación de su bosque puede prolongarse durante días o incluso semanas, con el riesgo de que el malware vuelva a impactar durante el proceso. Pero con Active Directory Forest Recovery (ADFR) de Semperis, puede recuperar el directorio activo con unos pocos clics de ratón y menos de una hora.

Active Directory Forest Recovery (ADFR) permite restaurar la copia de seguridad más reciente, incluso si los controladores de dominio estaban infectados cuando se realizaron las copias de seguridad. La tecnología patentada de Semperis desacopla Active Directory del sistema operativo subyacente para evitar la reinfección de malware.

Los secretos de Semperis Directory Services Protector (DSP)

David Carbonero, Cloud Architect Specialist de Anadat, responde a algunas preguntas clave sobre Semperis DSP

- **¿Con DSP puedo crear reglas automatizadas para deshacer un cambio en el AD?** DSP Me permite crear reglas automatizadas para responder a ciertos ataques basadas en cambios de atributos u objetos. Es decir, si un atacante, por ejemplo, se quiere añadir como administrador de dominio al grupo domain admin y quitar a los administradores actuales, el DSP puede deshacer esa operación de forma automática.
- **¿Con DSP puedo comprobar el nivel de seguridad de mi AD?** La herramienta de DSP incorpora un módulo que valida tu infraestructura de AD, chequea el directorio activo y proporciona visibilidad e información sobre cómo solventar esas vulnerabilidades que tienes en el directorio activo
- **¿Se pueden enviar los eventos encontrados a un SIEM?** Semperis DSP genera muchísimos eventos y tienes dos formas de recopilarlos. Bien mirando el log del propio servidor o bien enviando todos los datos a un SIEM
- **¿Puedo enterarme si una regla creada ha detectado algo en el sistema?** Sí. La herramienta tiene un panel de monitorización que muestra por pantalla cualquier cambio que se produzcan en el AD. Como decíamos antes, podemos crear reglas automatizadas, pero también tenemos la posibilidad de deshacer un cambio de forma manual.
- **¿DSP necesita de un SQL Server?** Sí. Si Son tantos eventos los que se generan que necesitamos un SQL Server Express para almacenar todos los cambios que se realicen en la configuración de la propia herramienta, y además un SQL server aparte para almacenar todos los datos que se cambien en el Directorio Activo.
- **¿Necesito desplegar agentes en los DCs?** Efectivamente, necesitamos desplegar unos agentes en los DCs (controladores de dominio)
- **¿DSP conecta con Azure?** Con DSP existe la posibilidad de monitorizar en la misma herramienta nuestro DA y el Azure AD. Si el cliente tiene configurado que el AD esté replicado su director activo con Azure, tengo tiene un módulo, mediante una máquina virtual, que puedo conectar a la parte de Azure y así poder ver y observar los cambios que se puedan producir en Azure.

"La interrupción del servicio de validación de identidades no es una opción"

David Carbonero,
Cloud Architect Specialist, Anadat



No es necesario realizar restauraciones de prueba y error en busca de copias de seguridad limpias. No es necesario reconstruir AD desde cero.

Las joyas de la corona


Los sistemas de identidad son las joyas de la corona de cualquier organización. Así lo asegura Nuno Antunes, añadiendo que la recuperación del directorio activo tras un ciberataque "es siempre la primera operación que hay que realizar, o nada funcionará. Explica que no ayuda el hecho de

que el AD tenga 22 años y se creara sin tener en cuenta la seguridad y que gracias a la tecnología de Semperis se pueden ir un paso más allá del backup tradicional al lograr recuperaciones automatizadas, muy rápidas y con garantías de que no hay malware.

La experiencia de muchos años en el mercado lleva a Nuno Antunes a pedir a las empresas una evaluación "urgente" de los entornos de AD; "en términos prácticos, esto significa actualizar y corregir muchas vulnerabilidades identificadas en

Enlaces de interés...

- [2021 Semperis Active Directory Security Halftime Report](#)
- [Purple Knight Proves Essential in Securing AD for Southern Utah University](#)
- [Anadat Insights](#)

los últimos años", para lo que la empresa ofrece Purple Knight una opción gratuita que ayuda a las organizaciones "a priorizar su remediación urgente de identidades tanto para AD como para Azure AD". La versión comercial de esta herramienta es DSP, que incorpora enormes capacidades en lo que respecta a la supervisión proactiva y continua de los directorios de las organizaciones, no sólo en lo que respecta a los vectores de ataque comunes, sino también a los cambios reales que se producen casi en tiempo real". 



"Las empresas deben realizar urgentemente una evaluación de los entornos de AD"

Nuno Antunes,
Director España y Portugal, Semperis

Compartir en RRSS

