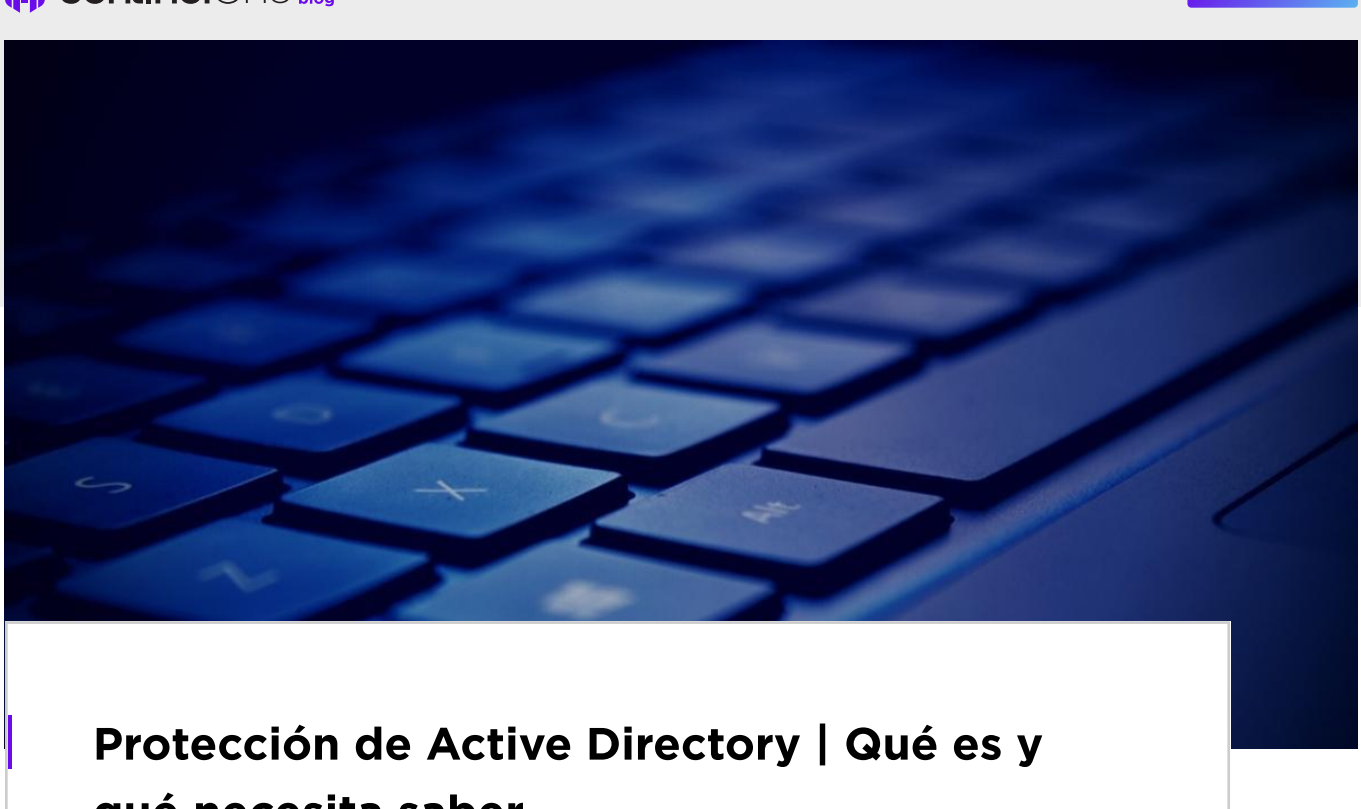

Protección de Active Directory | Qué es y qué necesita saber

enero 18, 2022
by SentinelOne

Los ciberdelincuentes actuales han sido capaces de aprovechar las vulnerabilidades de Active Directory (AD). A ojos del agresor, se trata de una llave maestra capaz de desbloquear el resto de la red. AD proporciona los servicios de directorio que permiten a los administradores gestionar permisos y controlar el acceso a recursos de la red. Esto lo convierte en esencial para las operaciones diarias de una empresa, pero también un objetivo enormemente atractivo. Active Directory se encarga de administrar permisos y la autenticación, y eso obliga a facilitar a todos los usuarios un fácil acceso. Desafortunadamente, esto lo hace particularmente difícil de proteger. Sin embargo, una protección adecuada cierra lagunas de seguridad ignoradas para aumentar el nivel protección de la empresa.

Active Directory y las en las operaciones de red

El papel de AD en las operaciones de red es tan amplio que la mayoría de los clientes (comprensiblemente) carecen del conocimiento necesario para encargarse de su seguridad. No se trata solamente de aplicar parches a las vulnerabilidades conocidas o corregir los errores de configuración. Cualquier ajuste expuesto o parámetro mal ajustado puede permitir a un ciberdelincuente infiltrarse en el sistema. La protección de AD implica ver de las exposiciones, detectar ataques en tiempo real, administrar las directivas de seguridad, y requiere datos sobre las desviaciones de cumplimiento cuando los usuarios no respectan esas directivas de manera sistemática. Hay situaciones más dinámicas en las que se producen grandes cambios (por ejemplo, las fusiones y adquisiciones) que complican exponencialmente la administración.

El valor de Active Directory para los ciberdelincuentes

Para la mayoría de las empresas, AD es el repositorio central de todas las cuentas y sistemas dentro de la red, y es responsable de toda la autenticación y autorización a la red. Se trata de un objetivo muy lucrativo para los ciberdelincuentes, ya que si consiguen comprometer AD pueden conseguir acceso a todos los recursos de red y a los derechos y privilegios necesarios para realizar cambios que compliquen su localización y expulsión del entorno.

Desafortunadamente, muchas herramientas gratuitas y de código abierto, como Bloodhound y Mimikatz, facilitan los ataques contra AD. Los ciberdelincuentes utilizan estas herramientas para identificar cuentas capaces de concederles derechos administrativos y llevar a cabo sus ataques de forma que puedan elevar sus privilegios y ocultar sus movimientos. AD puede ser el Talón de Aquiles de una empresa cuando se trata de preparación frente a ataques de ransomware. Prácticamente todos los ataques importantes de ransomware incluyen una fase en la que se aprovechan de AD para obtener información, privilegios o ambos. Si no se protege adecuadamente, AD puede convertirse rápidamente en el mejor aliado de un ciberdelincuente.

Adopción de las medidas necesarias para proteger Active Directory

Hay algunas buenas prácticas que deben adoptar las empresas, como reforzar AD, reducir al mínimo las cuentas con privilegios, utilizar servidores de saltos, y respetar guías de implementación técnica seguras. Pero estas medidas no son suficientes para garantizar la protección de AD. Las empresas competentes deberían implementar soluciones de seguridad de la identidad que proporcionaran visibilidad de las credenciales comprometidas que pudieran abrir vías de ataques, y permitir el acceso a AD. También es absolutamente vital disponer de visibilidad de las exposiciones y vulnerabilidades de AD.

Nuevas herramientas para proteger Active Directory

Últimamente han parecido nuevas herramientas capaces de ayudar a las empresas a proteger AD. Las soluciones de detección y respuesta ante amenazas para la identidad (ITDR) se consideran en la actualidad un elemento esencial de la defensa de AD, ya que pueden contribuir a proteger frente a ciberdelincuentes que atacan la infraestructura de AD desde dentro de la red. Para disfrutar de una detección de amenazas más rápida y completa, además de mejores tiempos de investigación y respuesta, las empresas necesitan detectar a los ciberdelincuentes que buscan las credenciales, los derechos en la nube, y Active Directory, y las soluciones ITDR pueden ayudar. Peter Firstbrook, vicepresidente de Gartner Research, afirmó recientemente, la «detección y respuesta ante amenazas para la identidad es una función crítica de cualquier solución que se autodenomine XDR», dando todavía más credibilidad al valor de ITDR.

Protección de Active Directory: una prioridad

Incluso Microsoft calcula que 95 millones de cuentas de AD reciben ataques al día, y ese número casi con total seguridad no ha dejado de aumentar. Los ciberdelincuentes reconocen que la naturaleza única de AD le otorga un enorme valor y lo hace muy difícil de proteger, y aprovechar sus vulnerabilidades se ha convertido en una prioridad para ellos. Finalmente, los defensores no pueden garantizar sus servicios de directorio si no entienden los riesgos o disponen de información clara cuando esos activos están siendo atacados. Una solución ITDR proporciona visibilidad permanente de las exposiciones, errores de configuración y credenciales de las que desean apoderarse los ciberdelincuentes durante un ataque basado en la identidad. Los ciberdelincuentes no van a dejar de atacar AD en un futuro cercano, pero las empresas actuales disponen en la actualidad de herramientas y recursos que pueden detectar y neutralizar a los atacantes que buscan explotar credenciales y Active Directory.

¿Te gusta este artículo? Síguenos en LinkedIn, Twitter, YouTube or Facebook para ver el contenido que publicamos.

Lee acerca de Ciberseguridad

- 10 maneras de proteger su Active Directory