Cómo hacer frente a los ciberataques protegiendo el Directorio Activo

ALSID

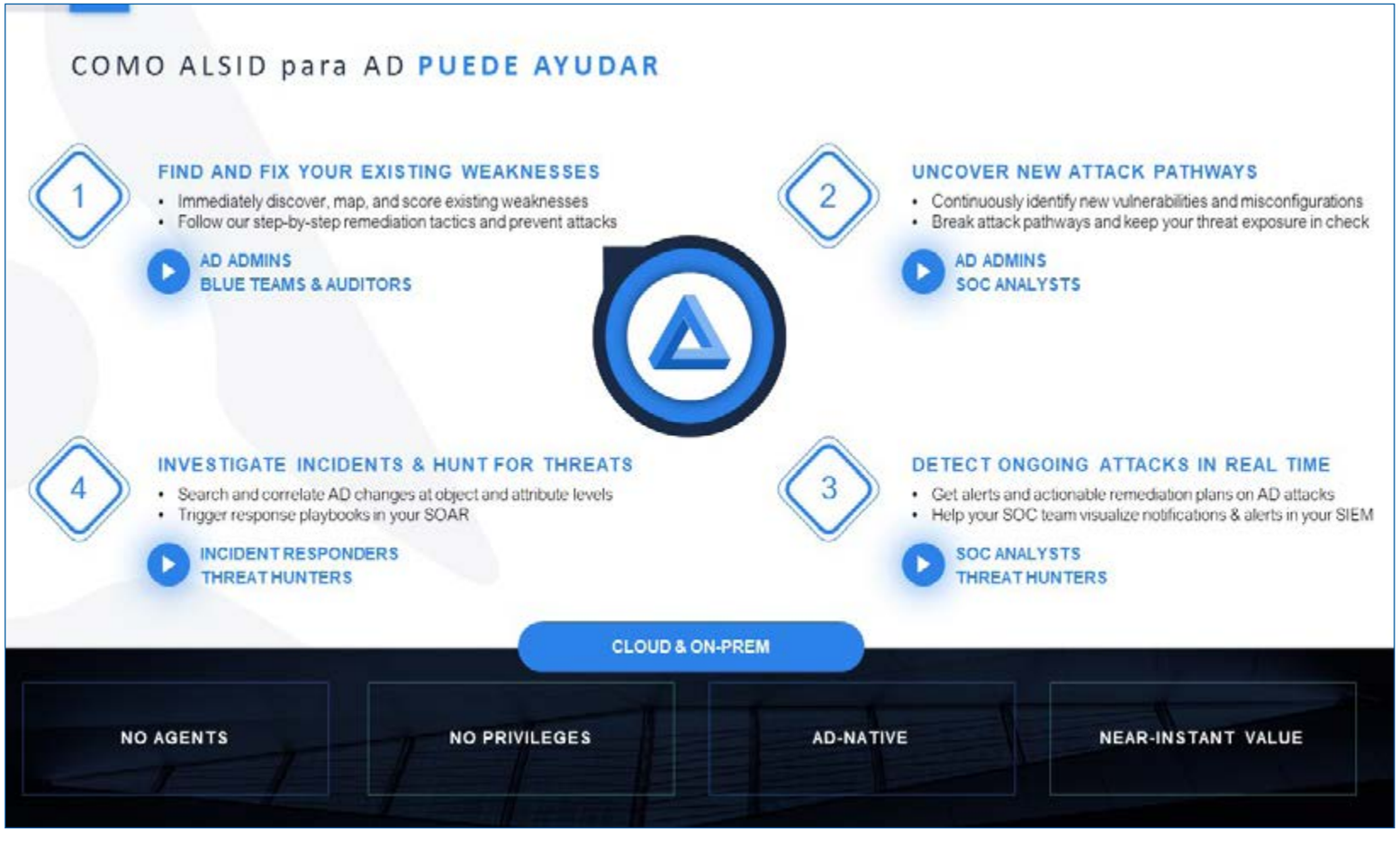
Junio 2020

Cómo hacer frente a los ciberataques protegiendo el Directorio Activo

En este webinar y de la mano de Jesús Barrajón, responsable de Alsid en la región de Iberia, no sólo se mencionan algunas de las tácticas y herramientas que utilizan los ciberdelincuentes para comprometer las empresas, sino de los pasos de un ciberataque contra el Directorio Activo y cuáles son las mejores prácticas para reducir los riesgos de que tu Directorio Activo se vea comprometido.

Los ataques de ransomware son solo uno de los muchos tipos de ataques que dependen de comprometer el Active Directory (AD), que a veces se olvida como un elemento de la seguridad de TI de una organización.

Tanto es así que un 24% de los responsables de IT no saben quién es el responsable de la seguridad del Directorio Activo dentro de su organización, y sólo un 21% aseguran haber seguido las



La propuesta de Alsid solo requiere una cuenta en modo lectura o una cuenta básica sin privilegios, por lo que no es nada intrusiva

mejores prácticas de seguridad al probar una restauración completa del Directorio Activo con éxito más de una vez. Y eso teniendo en cuenta que el 80% de los ataques utilizan el AD para ejecutar movimientos laterales y escalada de privilegios o que los kits de ataque contra el AD se pueden comprar por menos de un dólar en la Dark Web.

Asegura Jesús Barrajón que hace tiempo que el Directorio Activo se ha convertido en el principal objetivo de los ciberdelincuentes, ya que se trata de una estructura bastante antigua en la que se realmente no se ha puesto mucho foco en lo que a seguridad se refiere a pesar de que tiene información muy sensible y crítica de la empresa.

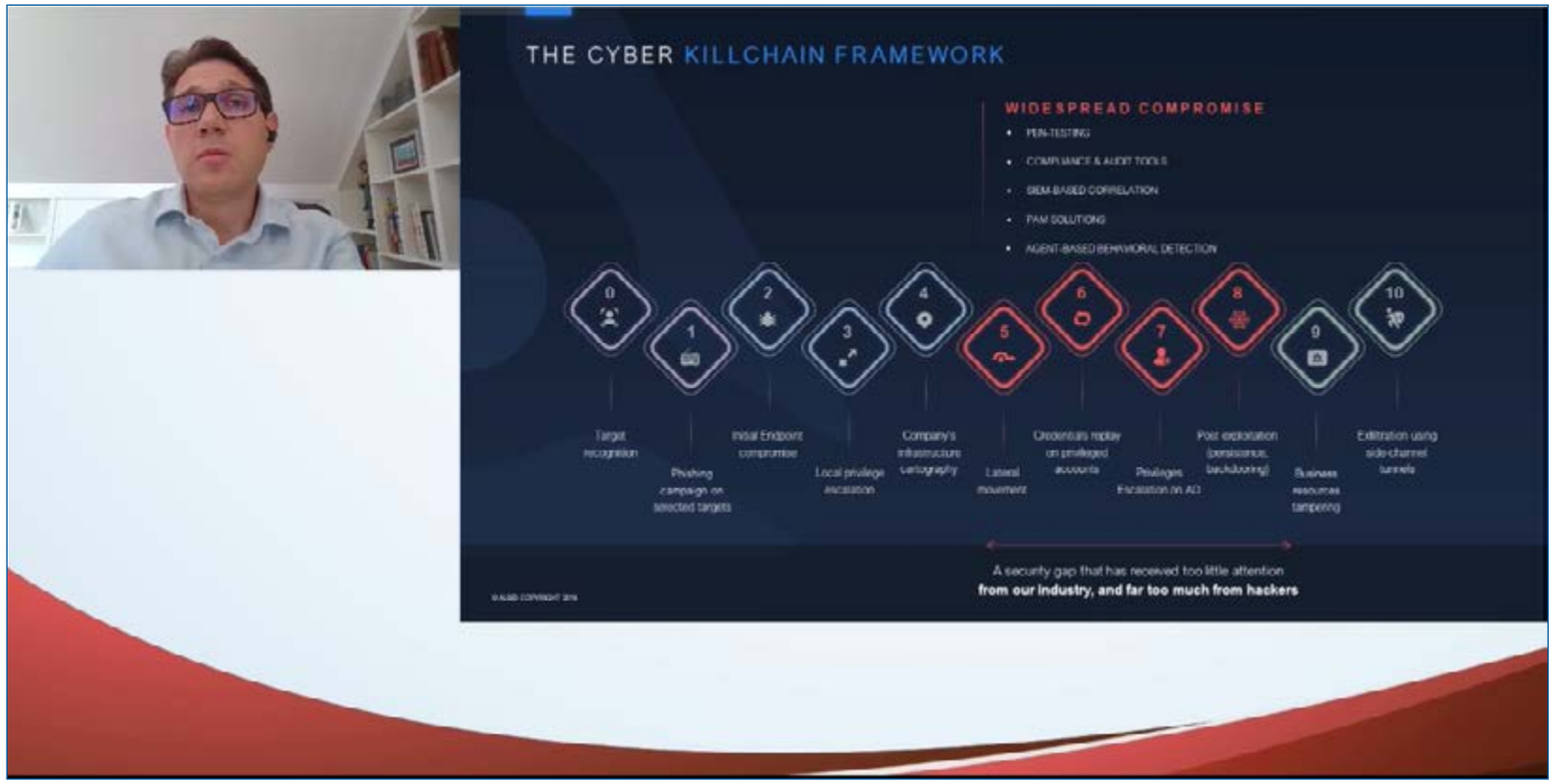
La situación actual es que el número de ataques se ha multiplicado, que la suplantación de identidad es cada vez más precisa, que el impacto económico de los ciberataques es cada vez mayor o que cada 14 segundos se produce un ataque de ransomware. En general, hay un aumento de infecciones masivas dirigidas a grandes organizaciones y los ciberdelincuentes están más activos que nunca.

CÓMO HACER FRENTE A LOS CIBERATAQUES PROTEGIENDO EL DIRECTORIO ACTIVO

CLICAR PARA VER EL VÍDEO

Que el Directorio Activo se haya convertido en la principal vía de ataque no es una casualidad, explica Jesús Barrajón, añadiendo que se trata de la "piedra angular de la infraestructura de TI y el acceso a todos los activos importantes dentro de una empresa".

El principal problema de seguridad es inherente al propio diseño del Directorio Activo. Se trata de una tecnología antigua, de casi 20 años, y al mismo tiempo es una estructura que está viva, que está continuamente en movimiento, con miles de cambios realizados todos los días en su base de datos, a lo que se suma el error humano. "Aunque comprometer el directorio activo no suena exótico, es algo fundamental para el éxito de la mayoría de los ataques", asegura Jesús Barrajón. Explica también el responsable de Alsid en España y Portugal que el compromiso del Directorio Activo es básico para hacer movimientos laterales y escalado de privilegios, "y aunque hay algunas táctica para protegerlo, no son del todo apropiadas", como los SIEM, que



pueden no detectar un ataque porque muchos no dejan logs, o que generan falsos positivos porque la enorme cantidad de logs que genera el Directorio Activo al estar en constante movimiento.

En cuanto a las herramientas basadas en monitorización, “están más orientadas a la detección, con lo cual para nosotros ya es tarde y además requieren el desplegar agentes y utilizar cuentas privilegiadas. Esto a nosotros no nos parece aceptable”.

Durante el webinar Jesús Barrajón explica cómo se producen diferentes métodos de ataque y el impacto que dejan en los clientes para demostrar cuán importante es poner una segunda barrera de protección para proteger el Directorio Activo. Con todo este conocimiento, la propuesta de Alsid es identificar los caminos de ataque y proporcionar recomendaciones paso a paso para bloquearlos antes de que sean utilizados, y todo ello de manera proactiva.

Dentro de nuestro plan de seguridad y de cara a mantener el Directorio Activo libre de caminos de ataque y que, de producirse, puedan ser detectados cuanto antes, se deben tener en cuenta los siguientes puntos: en primer lugar, se debe contar con una herramienta que en tiempo real sea capaz de detectar los nuevos caminos de un ataque al directorio activo; en segundo lugar, tendríamos que enviar esa información al SOC, asegurándonos de que no

DIRECTORIO ACTIVO, ¿ESTÁN SEGURAS LAS LLAVES DEL REINO?

Hoy, el Directorio Activo de Microsoft es tan común que aproximadamente el 90% de las compañías lo utilizan como método principal para proporcionar autenticación y autorización sin interrupciones. En consecuencia, se ha convertido en un objetivo principal para los ciberdelincuentes que buscan tener acceso a datos privilegiados de la empresa. Una vez dentro del Directorio Activo, pueden moverse a través de los sistemas y obtener acceso a una gran cantidad de datos críticos del negocio.

Enlaces de interés...

- Los tres ataques que un usuario con privilegios puede utilizar
- Seguridad del Directorio Activo. Q1 2020 Threat Intel Report [Alsid Intelligence]
- Asegurando el Directorio Activo: deteniendo ataques de forma proactiva
- Directorio Activo, ¿están seguras las llaves del reino?

enviamos falsos positivos; y, finalmente habría que establecer los procedimientos entre el equipo del SOC y el equipo que gestiona el Directorio Activo.

Asegura Jesús Barrajón que el objetivo de Alsid es ayudar a proteger el archivo "empezando desde la fase de anticipación, es decir, descubriendo y reforzando las rutas de ataque antes de que se encuentren y las utilicen los ciberdelincuentes". Entre las ventajas de la solución de esta compañía francesa es que no es nada intrusiva al no necesitar desplegar ni agentes ni cuentas privilegiadas; además, se puede desplegar tanto en el cloud como on-premise.

Alsid ayuda a los clientes en cuatro puntos fundamentales. En primer lugar, inmediatamente después de conectar la consola al cliente se van a identificar las rutas de ataque ocultas que pudiese tener ese directo reactivo y que podría utilizar un ciberdelincuente. En segundo lugar, se envían alertas en tiempo real cuando se descubran nuevas rutas de ataque. En tercer lugar, se va a pasar de la parte proactiva o preventiva a la parte más de detección monitorizando todos los eventos del archivo. Finalmente está la cuarta fase, más orientada al equipo respuesta o a los investigadores. En este último paso "van a poder ver un cambio radical en la eficiencia, en la efectividad, en la reducción de tiempos, ya que podrán ver los eventos a medida que estos ocurren", asegura Jesús Barrajón, añadiendo que "los datos que facilitaremos serán siempre precisos y no generarán falsos positivos, con lo cual este es un material muy valioso para los investigadores, sobre todo para reducir los tiempos de respuesta".

De esta forma se podrá reforzar de modo proactivo la seguridad, el directivo activo y caso de producirse un ataque, podremos ayudar en la fase de detección temprana y la respuesta.

Tras una demo del producto y explicar por qué la solución de Alsid no genera falsos positivos, destaca Jesús Barrajón que entre las ventajas de la propuesta es que "lo único que vamos a necesitar es una cuenta en modo lectura o una cuenta básica sin privilegios", y un tiempo de despliegue muy reducido; "en cuestión de una hora podríamos estar ya monitorizando y totalmente fuera de la red del cliente", asegura el responsable de Alsid para la región de Iberia.

Compartir en RRSS