HISTORIA DE CLIENTE DE AKAMAI

Proveedor de infraestructura de comunicaciones

Detención del avance del ransomware con Akamai

Prevención de posibles pérdidas por valor de 1 millón de USD

Prevención de posibles recursos de TI en la sombra

Visibilidad del tráfico este-oeste

El cliente

Este proveedor de infraestructura de comunicaciones de EE. UU. garantiza que las empresas y los particulares siempre estén conectados en el trepidante mundo actual. El proveedor se encarga de una amplia red de antenas de telefonía móvil y redes de fibra de las que los clientes dependen en su día a día.

Los desafíos

Limitaciones en la visibilidad y el control de los terminales

Con más de 6000 ordenadores portátiles distribuidos por toda la organización, el equipo de seguridad de TI cada vez estaba más preocupado por el riesgo que suponía la flota para el entorno de TI en general. Además, debían hacer frente a los problemas recurrentes de actividad de TI en la sombra que llevaban a cabo algunos usuarios expertos de la empresa.

Aunque el equipo de informática para usuario final ya había implementado algunas medidas de seguridad, estas eran limitadas. Ninguna de ellas podía controlar con precisión el acceso al sistema de los usuarios o limitar la comunicación punto a punto para detener la propagación del malware de manera eficaz; este último aspecto preocupaba especialmente a la organización.

Para abordar estas deficiencias, las partes involucradas querían mejorar la estrategia de seguridad de la empresa mediante la adopción de una solución que les permitiera implementar visibilidad y controles precisos de segmentación en los dispositivos de los empleados. Esto también les ofrecería la posibilidad de vigilar y evitar movimientos laterales no autorizados.

Selección de una solución

Los responsables de la seguridad habían estado considerando Akamai Guardicore Segmentation durante un tiempo y estaban interesados en utilizarla en diferentes casos de uso relacionados con la ciberseguridad. La organización optó por un enfoque por fases al ver un gran potencial en la visibilidad precisa y el proceso simplificado de creación de políticas.

Proveedor de infraestructura de comunicaciones

Ubicación
Estados Unidos

Sector
Infraestructura de comunicaciones

Solución
Guardicore Segmentation de Akamai

Resultados clave
- Prevención del ransomware
- Bloqueo de los recursos de TI en la sombra
- Visibilidad del tráfico este-oeste

Akamai

Dado que las políticas de segmentación definidas por software de Akamai no dependen de ninguna infraestructura subyacente, el proveedor tenía la posibilidad de abordar un número ilimitado de iniciativas de seguridad. Sin embargo, como la flota de ordenadores portátiles de empleados se había identificado como un punto de alto riesgo, el equipo dio prioridad a la implementación de agentes de Akamai en los terminales.

Guardicore Segmentation de Akamai

Una vez iniciado el proyecto, se implementó rápidamente el agente para Windows optimizado de Akamai en los ordenadores de la empresa. Esta medida permitió obtener visibilidad a nivel de proceso sobre el acceso de los usuarios y la actividad de los ordenadores portátiles.

De este modo, el equipo de seguridad de TI pudo crear y gestionar los controles de seguridad de los terminales de forma centralizada y basándose en datos precisos sobre el entorno. Poco después, se establecieron varias políticas, incluida una alerta sobre actividades específicas del protocolo de escritorio remoto (RDP) de Microsoft que también detecta los intentos fallidos de inicio de sesión.

Visibilidad precisa en acción

Poco después de la implementación, la política configurada para informar de cualquier actividad inusual relacionada con el RDP envió una oleada de alertas. Rápidamente se observó que un pirata informático estaba intentando realizar un ataque de fuerza bruta, ya que ocurrieron varios inicios de sesión fallidos uno tras otro.

El equipo de seguridad de TI siguió de cerca la situación y, dado que los atacantes seguían insistiendo, tomó la decisión de bloquear el RDP de todos los terminales con un agente de Akamai. Con tan solo unos clics, el equipo de TI creó y aplicó una nueva política de segmentación que inhabilitó el RDP y logró detener al atacante antes de que ningún terminal estuviera en peligro.

Detención del avance del ransomware

Durante el análisis post mortem, el equipo de seguridad pronto descubrió que todos los indicadores apuntaban a un importante y conocido agente de amenazas de ransomware.

Si la campaña hubiera tenido éxito, es probable que los atacantes hubieran intentado aplicar sus tácticas habituales, es decir, cifrar cualquier cosa que esté a su alcance para luego pedir un rescate. Teniendo en cuenta el tamaño de la organización del proveedor y las tendencias actuales, el rescate exigido por el atacante probablemente habría superado el millón de dólares. Además, si los activos esenciales para el negocio, como los sistemas de planificación de recursos empresariales (ERP), se hubieran visto afectados, el ataque habría provocado importantes interrupciones y tiempo de inactividad adicionales.

Sin embargo, gracias a la rápida actuación del equipo de seguridad y a Akamai, el intento de ataque no afectó a la organización de ningún modo.

Bloqueo de los recursos de TI en la sombra

Además de detener las amenazas externas, el equipo también pudo hacer frente a los desafíos internos a través de la plataforma. Antes de utilizar Akamai, la visibilidad limitada de los terminales permitía a algunos usuarios eludir los procesos oficiales y realizar actividades por su cuenta que no cumplían con las políticas oficiales de la organización. La nueva información y la capacidad de implementar controles de seguridad en los terminales permitieron al equipo de seguridad de TI frenar estas actividades de TI en la sombra. Esto incluía evitar que los miembros de la división de DevOps utilizaran nuevos recursos por su cuenta sin que estos pasaran por los canales oficiales para su autorización.

Ampliación de la protección con Akamai

Para el proveedor de infraestructura de comunicaciones, la protección de los terminales solo es el principio. También planea explorar nuevas funciones e implementar Akamai en su centro de datos, proteger su entorno de Citrix y aplicar controles de acceso de terceros para proveedores externos.

Gracias a la naturaleza flexible de la plataforma, el equipo tiene la seguridad de que puede ampliar la protección contra amenazas avanzadas en cualquier ubicación del entorno, sin que el futuro de la estrategia de fusiones y adquisiciones o de las iniciativas de transformación digital sea un impedimento.

Visite akamai.com/guardicore para obtener más información.

 | Asistencia | | Publicado el 23 de mayo