HISTORIA DE CLIENTE DE AKAMAI

Una gran empresa de servicios financieros protege el acceso remoto con Akamai tras un ataque de ransomware

Visibilidad completa de la red

Rápida implementación de políticas

Protección de los trabajadores remotos

El cliente

Una gran empresa de servicios financieros con sede en Brasil.

El desafío

Ampliación del acceso remoto

Al igual que en muchas otras organizaciones, la pandemia de COVID-19 provocó un aumento de las necesidades de acceso remoto en este proveedor de servicios financieros, y gran parte del personal de TI del banco pasó a trabajar desde casa con dispositivos gestionados por la empresa. Cuando los usuarios empezaron a acceder a los datos y las aplicaciones que necesitaban para sus funciones, principalmente fuera de la red corporativa segura, la superficie de ataque de la organización creció rápidamente.

Víctimas de un incidente de ransomware

Poco después de pasar a un modelo de teletrabajo, un ataque de ransomware efectuado con éxito afectó a una base de datos crítica de Oracle Cloud en el banco, que posteriormente descubrirían que se originó en un entorno de infraestructura de escritorio virtual (VDI). El departamento de seguridad y el de TI sabían que necesitaban tomar medidas rápidas para limitar la pérdida de datos financieros confidenciales. Además, comprendieron que, si no podían determinar y proteger el vector de ataque original, existía un riesgo real de que el ransomware se propagara lateralmente tanto a los servidores de copia de seguridad como al entorno de producción de la organización. Si esto ocurriera, el banco se tendría que enfrentar a importantes pérdidas financieras y de datos.

Selección de una solución

Guardicore Segmentation de Akamai ya se utilizaba ampliamente en otras áreas del banco. Antes del ataque de ransomware, la plataforma era responsable de gestionar y aplicar las políticas de segmentación de más de 23 000 servidores con cargas de trabajo que abarcaban infraestructuras locales, virtuales, bare metal y VDI, así como entornos de contenedores Azure y OpenShift.

Large Financial Services Company

Sector
Servicios financieros

Solución
Guardicore Segmentation de Akamai

Resultados clave

- Mitigación de la propagación del ransomware mediante el movimiento lateral
- Visibilidad detallada de los flujos de red
- Protección del acceso remoto mediante la segmentación de los entornos de VDI
- Respuesta rápida a incidentes

Akamai

Como solución de segmentación basada en software, el banco la había utilizado anteriormente en diversas iniciativas de seguridad y cumplimiento, incluida la gestión del acceso de los administradores a las soluciones de salto y la segmentación de aplicaciones Swift. Conociendo el historial de la plataforma de proporcionar una visibilidad excelente y una implementación rápida de políticas, el equipo de respuesta se puso en marcha rápidamente para aprovechar las funciones de Guardicore Segmentation de Akamai y solucionar la vulneración.

Beneficios de Guardicore Segmentation de Akamai

Visibilidad en el nivel de proceso

A través la plataforma, el equipo de respuesta a incidentes del banco pudo investigar los flujos de comunicación históricos. Así, rastrearon el incidente de ransomware hasta dar con el origen del ataque: una conexión de la VDI remota del administrador de la base de datos que se comunica con una base de datos de Oracle Cloud.

Rápida implementación de políticas

Después de identificar el vector de ataque, el equipo aceleró la segmentación de la VDI, convirtiéndola en una prioridad máxima. El proceso de planificación de políticas comenzó un sábado y utilizó las funciones de visibilidad de Guardicore Segmentation para determinar las posibles necesidades en cuestión de políticas. El martes siguiente, el banco ya tenía políticas aplicables para las más de 3000 conexiones VDI a Oracle Cloud.

Recuperación ante el ransomware

El equipo implementó agentes de Akamai en la aplicación de copia de seguridad y configuró el acordonamiento de las aplicaciones, definiendo, hasta el nivel de proceso, lo que podía comunicarse con el activo. A continuación, se implementó en la zona de vulneración, lo que bloqueó la propagación del ransomware mediante reglas de denegación globales.

Para reducir el riesgo adicional derivado del acceso de los teletrabajadores, también se establecieron políticas para las dos soluciones de VDI que utilizan los empleados del centro de llamadas, lo que prevenía aún más el desplazamiento lateral no autorizado entre los terminales del banco.

Lograr la aplicación de políticas de segmentación en solo tres días permitió a la empresa de servicios financieros reducir drásticamente el impacto del incidente de ransomware y mejorar en gran medida la seguridad del acceso remoto de cara al futuro.

> La visibilidad proporcionada por [Guardicore Segmentation de Akamai] era como un haz de luz brillante en la oscuridad.
>
> Director de seguridad de infraestructura de una gran empresa de servicios financieros

Visite akamai.com/guardicore para obtener más información.