HISTORIA DE CLIENTE DE AKAMAI

Una empresa de resolución de filtraciones de datos utiliza las soluciones de Akamai como parte de sus servicios de recuperación y respuesta ante el ransomware

Visibilidad completa de la red

Segmentación en todas las infraestructuras de TI

Respuesta a las amenazas de ransomware

El cliente

Un fabricante de equipamiento internacional contactó con una empresa de servicios de resolución de filtraciones de datos con sede en Estados Unidos tras un grave incidente de seguridad.

El desafío

Ransomware de propagación rápida

Cuando un ataque de malware se propagó con éxito y afectó a las operaciones empresariales, el fabricante internacional comenzó a trabajar con la empresa de servicios de resolución de filtraciones de datos para restaurar y mejorar la seguridad de su entorno. El ataque, iniciado desde el portátil de un empleado, se había propagado rápidamente y afectado a la mayoría de los centros operativos, además de penetrar en los servidores de copia de seguridad de la organización.

Selección de una solución

Los métodos de contención iniciales, como la aplicación de reglas de restricción del acceso a Internet en los firewalls, no fueron capaces de contener la filtración de datos que empeoraba rápidamente. La complejidad del entorno y la realidad de las conexiones de red en una empresa distribuida convirtieron la implementación y aplicación de reglas de restricción con firewalls en un proceso lento e ineficaz.

Además, la visibilidad de las máquinas antiguas era un problema importante para los encargados de responder a incidentes, responsables de investigar y contener la filtración de datos. Ante la urgencia y la necesidad de acelerar la segmentación antes de que la propagación lateral afectara a todavía más activos, el proveedor de servicios de resolución de filtraciones de datos recomendó Akamai Guardicore Segmentation.

Breach Remediation Company

Sector
Tecnología de la información

Solución
Akamai Guardicore Segmentation

Resultados clave

- Mitigación de la propagación del ransomware mediante el movimiento lateral
- Visibilidad detallada de los flujos de red
- Protección de las máquinas antiguas y modernas
- Respuesta rápida a incidentes

Akamai

Ventajas de Akamai Guardicore Segmentation

Visibilidad instantánea

En un plazo de tres horas, la empresa de servicios de resolución de filtraciones de datos aprovisionó rápidamente agentes de Akamai en más de 3000 servidores de la empresa. Pocos minutos después de la implementación, comenzó a perfilarse una visibilidad precisa de los flujos de red y comunicaciones, lo que proporcionó al equipo de respuesta ante incidentes el contexto y los datos precisos que necesitaban para investigar la filtración y validar la contención.

Rápida implementación de políticas

Poco después de lograr esta visibilidad tan necesaria, los equipos tomaron medidas para segmentar los activos críticos del entorno más amplio. Se identificaron y protegieron rápidamente dos aplicaciones de producción cruciales, responsables de la única línea de fabricación en funcionamiento. Gracias a Akamai Guardicore Segmentation, se implementó inmediatamente una política para restringir las conexiones entre las subredes y partes del centro de datos infectadas y las aplicaciones, una tarea que hubiera llevado semanas con firewalls antiguos.

Una consulta simple también reveló que las máquinas antiguas conectadas a Internet, que por consiguiente eludían los firewalls antiguos, intentaban aplicar restricciones de contención. Tras descubrir una comunicación que incumplía los estándares, el equipo creó políticas que restringieron eficazmente el acceso a Internet a todos los servidores, incluidas las máquinas antiguas, en cuestión de minutos.

Prevención del movimiento lateral durante la recuperación

Durante la siguiente parte del proceso de recuperación, el equipo recreó los clústeres de aplicaciones del fabricante, incorporando agentes de Akamai. Configuraron una política inicial para bloquear todas las conexiones entrantes y utilizaron Akamai Guardicore Segmentation para identificar las dependencias. Después empezaron a autorizar las comunicaciones que fueran necesitando, siempre tras validar los requisitos y comprender el contexto. Este enfoque permitió al equipo recuperar y volver a poner online las aplicaciones afectadas por el ataque de ransomware sin riesgo de reinfección.

Protección futura

Akamai Guardicore Segmentation permitió a la empresa de servicios de resolución de filtraciones de datos ofrecer un valor añadido significativo a su cliente, el fabricante, a la vez que le ayudó a recuperarse del ataque de ransomware. Esto brindó a la empresa de servicios la oportunidad de aumentar sus ingresos, ampliar su cobertura y ayudar mejor a los clientes a alcanzar sus objetivos de TI y seguridad.

La segmentación del centro de datos interno que se inició durante la recuperación por fases redujo significativamente la superficie de ataque. A día de hoy, la estrategia de seguridad de la organización ha mejorado y el impacto de cualquier filtración futura se ha reducido considerablemente.

Visite akamai.com/guardicore para obtener más información.

> [Akamai] nos ayudó a frenar la propagación de un ataque y a restaurar las líneas de producción afectadas en un segmento de red "estéril" en tan solo cuatro horas y sin modificar ningún sistema de red subyacente. Todo ello mientras se llevaba a cabo la contención y la investigación de respuesta a incidentes (RI).
>
> Director de seguridad de la información de la empresa de resolución de filtraciones de datos