Historias de clientes de Akamai

Prevención de amenazas internas en un distrito escolar estadounidense

Un gran distrito escolar de Texas implementó la microsegmentación de Akamai para proteger el tráfico de este a oeste

Aplicaciones seguras

Ataques internos mitigados

Visibilidad del tráfico

Un líder en excelencia educativa

En 2022, la Agencia de Educación de Texas otorgó una calificación de "A" a un gran distrito escolar público con más de 75 000 estudiantes. Líder en excelencia educativa, este distrito ofrece experiencias de aprendizaje sin igual, diseñadas para preparar e inspirar a cada estudiante a vivir una vida plena y honorable. Con ese fin, el departamento de Operaciones Tecnológicas del distrito se centra en crear y mantener la mejor infraestructura posible para adaptarse de forma segura a las generaciones actuales y futuras de contenido y herramientas digitales en beneficio de todos los interesados. Cuando el nuevo responsable de ciberseguridad del departamento detectó una debilidad en el enfoque de seguridad del distrito, Akamai Guardicore Segmentation ayudó a cerrar la brecha.

Necesidad de acabar con las amenazas internas

Tradicionalmente, el distrito escolar de Texas se apoyaba en firewalls y geovallas para mantener su entorno de TI a salvo de las amenazas externas. Sin embargo, carecía de una manera de evitar las amenazas internas; en concreto, aquellas que presentan los usuarios con intenciones maliciosas. "Si hubieran podido acceder a un sistema, habría sido fácil para ellos acceder a todos los demás", explicó el encargado de ingeniería de sistemas del distrito.

Texas School District

Ubicación

Texas, Estados Unidos

Sector

Sector público

Solución

Akamai Guardicore Segmentation

Akamai

Al carecer de visibilidad de las comunicaciones legítimas entre los sistemas internos, el distrito escolar no podía detener el tráfico de este a oeste ilegítimo y malicioso. Una vez que se reconoció la amenaza que planteaba esta situación, el departamento de Operaciones Tecnológicas, compuesto por ingeniería de redes y de sistemas, y ciberseguridad, comprendió la necesidad de recurrir a una solución completa para mitigar el riesgo. "Seríamos negligentes si no pusiéramos en marcha una solución para garantizar la seguridad total de la información asociada con nuestros estudiantes y todo el personal", señaló el encargado.

Implementación gradual y sencilla de la microsegmentación

Tras evaluar las opciones disponibles, el distrito escolar eligió Akamai Guardicore Segmentation. En palabras del encargado, "Era una de las mejores soluciones del mercado".

El departamento de Operaciones Tecnológicas auditó su entorno para identificar las aplicaciones y los sistemas que debían protegerse usando Akamai Guardicore Segmentation. "Empezamos con las aplicaciones de primer nivel, pero nuestra intención era protegerlas todas con la solución", prosiguió el encargado.

Con la guía de Akamai, el distrito pudo aislar fácil y rápidamente las aplicaciones prioritarias —como Active Directory y SQL Server— con políticas de segmentación precisas para eliminar los flujos de datos no deseados entre sistemas. El proceso de auditoría y despliegue favoreció la colaboración entre los distintos departamentos. "Todos colaboramos a la hora de decidir cómo etiquetaríamos los dispositivos, acordonaríamos los activos y demás. De este modo, Akamai Guardicore Segmentation nos proporcionó una base común para trabajar codo con codo".

Una vez acordonados los recursos, el distrito escolar recibe notificaciones sobre los posibles problemas. "Ningún tipo de tráfico puede pasar a menos que esté autorizado", explicó el encargado de ingeniería de sistemas del distrito escolar. Así pues, el distrito tenía la tranquilidad de que la solución de Akamai protegía inmediatamente esas aplicaciones.

"Una vez que nos hacíamos una idea del tráfico hacia y desde una aplicación, podíamos pasar al modo de bloqueo si era necesario. Akamai Guardicore Segmentation proporciona una vía directa para implementar gradualmente la protección en todo nuestro entorno", afirmó el encargado.

> Akamai Guardicore Segmentation nos ofrece una visibilidad inigualable de nuestro entorno, que nos permite garantizar la protección de nuestras infraestructuras críticas frente a cualquier tráfico de este a oeste no autorizado.
>
> — Encargado de ingeniería de sistemas, distrito escolar de Texas

> "Nos encanta utilizar Akamai Guardicore Segmentation. Es fácil de configurar y gestionar, y es una solución de valor incalculable para cualquier distrito escolar que desee protegerse de las amenazas internas".
>
> — Encargado de ingeniería de sistemas, distrito escolar de Texas

Mejora de la visibilidad en todo el entorno

Aunque algunas aplicaciones no pueden acordonarse, el distrito escolar se benefició igualmente de la nueva visibilidad de las comunicaciones entre esas aplicaciones y otras, como Active Directory. Todos los grupos del departamento de Operaciones Tecnológicas pueden ver los flujos de datos de entrada y salida de cualquier aplicación que esté acordonada, lo que básicamente permite obtener visibilidad de lo que ocurre con todos los sistemas del entorno. "Akamai Guardicore Segmentation facilita una vista actualizada de cómo funcionan las cosas y ofrece una manera sencilla de identificar el tráfico no deseado. Además, podemos configurar fácilmente la solución para permitir o bloquear el tráfico según sea necesario", declaró el encargado.

Esta visibilidad permite a los equipos de ingeniería de redes y de sistemas, así como de ciberseguridad, trabajar juntos según sea necesario para afrontar los problemas a medida que surgen. "Cuando recibimos aviso de tráfico sospechoso, la solución de Akamai proporciona el contexto que necesitamos para encontrar una solución que evite cualquier elemento indeseado y garantice al mismo tiempo que nuestro entorno funcione según lo previsto", explicó el encargado.

Prevención del acceso remoto no autorizado

Según el encargado de ingeniería de sistemas del distrito escolar, Akamai Guardicore Segmentation ayuda continuamente a neutralizar los ciberataques: "Nuestros sistemas son blanco de direcciones IP maliciosas de forma habitual. La solución de Akamai proporciona una vista de la actividad inusual, como la de los puertos en un servidor web, lo que nos permite bloquear el acceso y los posibles ataques".

Además, Akamai Guardicore Segmentation funciona a la perfección con otras herramientas de seguridad, con lo que mejora aún más la estrategia de seguridad del distrito. Por ejemplo, el distrito escolar utiliza una solución de gestión de acceso privilegiado (PAM) para proporcionar a los proveedores externos el acceso necesario a sistemas específicos. En lugar de permitir el acceso con el protocolo de escritorio remoto (RDP) a esos servidores, el distrito exige que su departamento de ingeniería use la solución PAM para gestionar los servidores de forma remota. Y Akamai Guardicore Segmentation impide el acceso a través de RDP.

Como explicó el encargado de ingeniería de sistemas del distrito escolar, esta medida de seguridad combinada impide que los usuarios accedan a los servidores de forma remota como anteriormente era posible: "Al utilizar la solución de Akamai para bloquear el acceso a través de RDP, podemos garantizar que nadie se conecte de forma remota a nuestro entorno de servidor".

Implementación de aplicaciones con más confianza

Hasta la fecha, el distrito escolar ha implementado Akamai Guardicore Segmentation en 375 de sus 500 servidores y tiene previsto proteger todas las aplicaciones posibles con la solución de microsegmentación. "Estamos implementando nuevas aplicaciones constantemente, a veces hasta una por semana, y desde el principio las protegemos con la solución de Akamai. Esto nos da más confianza, ya que Akamai Guardicore Segmentation nos permite visualizar cómo funcionan y se comunican nuestras aplicaciones", concluyó el encargado de ingeniería de sistemas del distrito.

| Publicado en noviembre de 2024