HISTORIA DE CLIENTE DE AKAMAI

Una universidad estatal selecciona Akamai para proteger la tecnología operativa crítica de sus edificios en 24 campus

Visibilidad completa de la red

Políticas de segmentación

Detección de amenazas y respuesta

El cliente

Importante universidad estatal

Esta importante universidad estatal responde a las necesidades de educación superior de más de 100 000 estudiantes, con más de 17 000 profesores y empleados en sus 24 campus.

El desafío

Centralización de la infraestructura de red de más de 600 edificios

Una importante universidad estatal quería incorporar sistemas de automatización de edificios de forma segura en una iniciativa estatal de campus inteligente. El equipo responsable de las instalaciones físicas y de los sistemas de tecnología operativa (OT) de la universidad estaba preocupado por la falta de segmentación que protegiera esos dispositivos y aplicaciones. También estaba preocupado por la red de TI de la universidad si se ponía fin a su actual aislamiento. En consecuencia, el equipo responsable emprendió una ambiciosa labor para centralizar sus sistemas de automatización de edificios y mejorar la seguridad.

El encargado del proyecto de la universidad explicó: "Hasta hace unos dos años, todos los campus trabajaban de manera prácticamente independiente. Nosotros nos ocupábamos de alojar el servidor de aplicaciones principal, pero los controladores de los distintos campus se alojaban en redes informáticas y no siempre estaban segmentados en VLAN separadas del resto del tráfico del campus".

Esto suponía que un ataque con éxito a los sistemas de control de un solo edificio podría propagarse fácilmente a la red de TI de un campus o viceversa.

Había, además, otro motivo económico para emprender el proyecto. "La universidad quería gestionar el consumo de energía y ver dónde podíamos reducir los costes", explicó el encargado del proyecto, "pero no conseguíamos recibir los datos de los campus porque todos los sistemas eran independientes".

"Esto nos obligaba a conectarlos, pero teníamos que hacerlo de forma segura. Con las conexiones procedentes de esos campus remotos en nuestro centro de datos, se podría crear una puerta trasera a nuestra red, lo que podría traducirse en posibles ataques".

Large State University

Sector
Educación

Solución
Guardicore Segmentation de Akamai

Resultados clave
- Prevención del movimiento lateral
- Acordonamiento de aplicaciones

Akamai

El ambicioso proyecto de incorporar todo en una infraestructura de red compartida abarcó a más de 600 edificios en 24 campus. El equipo de Automatización de las Instalaciones del departamento fue el elegido para llevar a cabo el proyecto.

Sin embargo, la gran complejidad de los sistemas de automatización de la universidad, así como el número de proveedores implicados, supusieron otro gran desafío.

"Nos tuvimos que ocupar de sistemas de ascensores, climatización, análisis de vibraciones, iluminación, distribución eléctrica y medición eléctrica. Aparte de todos nuestros servicios públicos principales, incluyendo la generación de vapor, la distribución eléctrica y el tratamiento de aguas residuales. Trabajamos con más de 260 contratistas de las distintas empresas que se ocupan de esos sistemas". Todos esos proveedores necesitaban acceso a la red, sin que esto supusiera riesgo alguno ni interferencias en los sistemas de control de los demás.

> Un sistema de gestión de firewall no puede competir con [Akamai].
>
> Responsable del proyecto universitario

Selección de una solución

Se busca: visibilidad del tráfico este-oeste y políticas centralizadas

Se utilizó Tempered Networks, proveedor de seguridad centrado en sistemas de control inteligentes y redes de Internet de las cosas, para establecer las conexiones norte-sur entre los campus remotos y el centro de datos principal de la universidad. Con ese desafío controlado, a la universidad aún le quedaba afrontar el problema de proteger frente a filtraciones a más de 300 servidores que se ejecutaban en el centro de datos.

"Estudiamos soluciones que supuestamente gestionaban el tráfico este-oeste, pero ninguna de ellas era tan fácil y sencilla como necesitábamos", recordó el encargado del proyecto de la universidad.

El equipo escuchó hablar por primera vez de Akamai cuando descubrió su herramienta gratuita de simulación de ataques y vulneraciones, Infection Monkey. Infection Monkey ayuda a los operadores de centros de datos a evaluar la resistencia de sus entornos a los ataques posteriores a la filtración y al movimiento lateral.

Una vez que el equipo descargó la herramienta y comenzó a utilizarla, se dio cuenta de que Akamai Guardicore Segmentation podía resolver los problemas que había detectado Infection Monkey.

Akamai Guardicore Segmentation es una de las pocas soluciones del mercado actual centrada principalmente en la microsegmentación. Facilita a los operadores la definición, creación e implementación de políticas de seguridad para controlar las comunicaciones entre aplicaciones individuales o agrupadas de forma lógica.

Ya en la primera presentación con la universidad, el equipo de Akamai demostró las capacidades de visualización únicas de la plataforma. Con Akamai Guardicore Segmentation, los operadores de centros de datos pueden ver todas las aplicaciones que se ejecutan en su entorno y asignar de forma gráfica las dependencias entre ellas.

"Funcionó al instante. Era exactamente lo que necesitábamos".

Akamai Guardicore Segmentation

Akamai frente a firewalls internos

"Con la gestión centralizada de firewalls, aún es necesario configurar las reglas de cada firewall individualmente. Con [Akamai], podemos crear un grupo de aplicaciones y decir: 'Queremos que estos sistemas solo se comuniquen entre sí'".

Los firewalls también plantean problemas de costes, recursos y gestión. "Gestionar todos esos firewalls sería sencillamente una pesadilla. Probablemente necesitaríamos media docena de personas solo para implementar el sistema y asegurarnos de que no se produjeran problemas y, posteriormente, al menos dos personas dedicadas exclusivamente a su gestión".

Además, los firewalls no ofrecen la flexibilidad necesaria para establecer y modificar políticas en el nivel de aplicación. "Con [Akamai], podemos dedicar un tiempo a analizar y entender lo que está sucediendo entre los sistemas y por qué necesitan comunicarse. Con los firewalls, es todo o nada. Un firewall simplemente bloquea todos los puertos, y basta".

Microsegmentación con gestión centralizada y sencilla

La velocidad y facilidad con que los miembros del equipo pueden crear e implementar reglas se mencionó como otra importante ventaja.

"El primer día que lo pusimos en marcha, lo instalamos en un par de sitios y, a continuación, intentamos crear una política para impedir que un proveedor pudiera ver a otro. Y así de simple, bloqueó al primer proveedor. Eso me demostró que este producto era lo que estábamos buscando", señaló el responsable del proyecto.

Para las herramientas y la metodología de microsegmentación de Akamai no se necesita un experto. "Tener algo tan sencillo que cualquier persona de nuestro equipo pueda usar fue algo definitivo para mí".

Más allá de la microsegmentación: detección y respuesta

Como ventaja añadida, la visibilidad obtenida con Akamai permitió sacar a la luz anomalías operativas en el centro de datos. "Identificamos un servicio de cola de impresión que se conectaba a una red que no era la nuestra", explicó el encargado del proyecto. "Cuando conseguimos rastrearlo, descubrimos que era la sesión de escritorio remoto de alguien que se había desconectado, pero que no la había cerrado, por lo que el servicio estaba continuamente intentando comunicarse con el servidor de impresión de su PC. Si ese PC se hubiera visto comprometido, podría haber constituido una vía de acceso al servidor de aplicaciones".

Ahora que el equipo utiliza activamente Akamai, la universidad ya está pensando en otras mejoras de seguridad y eficiencias que la solución hace posible.

"Un proyecto futuro está automatizando gran parte de la funcionalidad de la red si se produce un incidente. Por ejemplo, si detectamos una dirección MAC o un punto de acceso no autorizados en un edificio, podríamos utilizar [Akamai Guardicore Segmentation] para enviar un comando a la solución Tempered Networks para bloquear ese edificio y, a continuación, enviar una alerta a un operador para que lo corrija y que averigüe lo que haya ocurrido. Hasta ahora, no podíamos disfrutar de esa capacidad de detección".

La plataforma de Akamai permitió al equipo Automatización de las Instalaciones de la universidad conseguir el nivel de seguridad deseado de forma más rápida y sencilla que nunca. "Nunca habíamos tenido una herramienta tan proactiva como esta, capaz de supervisar constantemente todo", explicó el responsable del proyecto.

Como Akamai se encarga de supervisar el tráfico este-oeste del centro de datos, el equipo no necesita hacerlo. "Quiero que nuestro equipo pueda concentrarse en nuestro trabajo, que es ayudar a la universidad a ahorrar energía y dinero. No podemos centrarnos en eso si tenemos que preocuparnos por lo que está pasando en el centro de datos".

El equipo de la universidad se propuso encontrar una solución de microsegmentación sencilla. Con Akamai, encontraron eso y mucho más.

"Hace exactamente lo que promete".

Visite akamai.com/guardicore para obtener más información.

> Apenas lo instalamos, el equipo pudo acceder, implementarlo y establecer algunas reglas de protección que pronto se pusieron en práctica, y eso nos convenció.
>
> Responsable del proyecto universitario