Caso de uso: Viesgo

Viesgo es una compañía eléctrica que basa su negocio en la generación y en la distribución de electricidad. Con cerca de 695.000 clientes en el norte de España y una producción aproximada de 1.400 MW, de los cuales buena parte procede de fuentes limpias y renovables, Viesgo se posiciona como un agente fundamental en la transición energética de nuestro país

Contexto

Viesgo apuesta por movilizar su TI a Cloud Pública AWS y cuenta ya con un despliegue relevante que ejecuta algunos de sus procesos de negocio relevantes.

Viesgo cuenta con autonomía en todo lo relativo a la gestión de sus cuentas y suscripciones y en relación a seguridad delega en Telefónica la protección del perímetro.

Solución propuesta

Se han desplegado tecnologías de firewall comercial que protegen el perímetro AWS del cliente proporcionando una política para la protección Norte/Sur y Este/Oeste.

En esta aproximación se ha buscado un despliegue con microsegmentación que asegura cada cuenta y cada entorno asegurando que los flujos son óptimos – no permitiendo sino flujos que habilitan tráfico especifico entre elementos – minimizando así la posibilidad de en caso de ataque, la ejecución de movimientos laterales.

Además, el entorno de Viesgo cuenta con un "Security datalake" que recibe inputs de la instalación incluida la información de los elementos de seguridad y que permite en un entorno ELB realizar consultas en busca de anomalías.

Los elementos de seguridad además se monitorizan desde el SOC de Telefónica con lo que las violaciones de política o los indicios en relación con dichas violaciones generan alarmas que el servicio de Telefónica gestiona, prioriza o escala.

Resultados

- Despliegues de políticas norte/sur.
- Despliegues de políticas este/oeste.
- Eliminación de flujos que funcionalmente no resuelven un problema de la instalación y que por tanto podrían representar un riesgo.
- Identificación de buenas prácticas y puntos de mejora.
- Evaluación del estado de la seguridad de la suscripción.
- Identificación de buenas prácticas y puntos de mejora.

¿Qué hemos aprendido?

La microsegmentación es una aproximación que minimiza el riesgo como consecuencia de permitir únicamente flujos viables en relación a la infraestructura del cliente.

La técnica reduce el riesgo como consecuencia de la eliminación de conexiones que no han de tener lugar en la arquitectura del cliente permitiendo políticas más restrictivas.

Además, permite bajar la política a los elementos activos incluso a cada elemento de la instalación.