Use case: Viesgo

Viesgo is an electric company that bases its business on the generation and distribution of electricity. With about 695,000 customers in northern Spain and an approximate production of 1,400 MW, of which a good part comes from clean and renewable sources, Viesgo is positioned as a fundamental agent in the energy transition of our country.

Context

Viesgo is committed to mobilize its IT to AWS Public Cloud and already has a relevant deployment running some of its relevant business processes.

Viesgo has autonomy in everything related to the management of its accounts and subscriptions, and in relation to security it delegates to Telefónica the protection of their perimeter.

Solution proposal

Commercial firewall technologies have been deployed to protect the client's AWS perimeter providing a policy for North/South and East/West traffic protection.

In this approach we have sought a deployment with micro-segmentation that secures each account and each environment ensuring that the flows are optimal - allowing only flows that enable specific traffic between elements - thus minimizing the possibility of the execution of lateral movements in case of attack.

In addition, VIESGO's environment has a "Security datalake" that receives inputs from the deployment including the information of the security elements, which allows to perform queries in search of anomalies in an ELB environment.

The security elements are also monitored by Telefónica's SOC so that policy violations or indications of such violations generate alarms that Telefónica's service manages, prioritizes or scales.

Outcomes

- Deployment of North/South policy.
- Deployment of East/West policy.
- Elimination of flows that functionally do not solve any problem and could therefore represent a risk.
- Identification of best practices and improvement points.

What have we learned?

Micro-segmentation is an approach that minimizes risk by allowing only viable flows in relation to the client's infrastructure.

The technique reduces risk as a consequence of eliminating connections that do not have to take place in the client's architecture by allowing more restrictive policies.

In addition, it allows the policy to be narrowed to active elements, even to each element of the deployments.