Publicado en Madrid el 04/11/2024

Scalian Spain: "En el sector financiero, la pregunta es cuándo va a llegar el ciberataque"

El control de la autorización y la microsegmentación de la infraestructura, claves para afrontar el problema de fuga de información y ransomware, entre otros, según un portavoz de la consultora especializada en IA

Para Roberto Romero, director de la unidad de negocio de ciberseguridad de la consultora Scalian Spain, la pregunta que compete a los directivos responsables en el sector financiero no es si van a ser atacados, sino cuándo. Por eso, añade, el punto de partida debe ser "muy pesimista, y las instituciones financieras deben pensar que los malos son muy buenos haciendo su trabajo y que hay que ser mejores que ellos para superarlos".

Desde la filial española de Scalian Group, tienen la mirada puesta en una fecha: el 17 de enero de 2025, cuando las autoridades competentes de los distintos países de la Unión Europea comiencen a supervisar la aplicación de la directiva comunitaria en materia de ciberseguridad, DORA.

Esta norma busca la operatividad en el área digital de las organizaciones financieras y convive con otras regulaciones como la directiva SRI2, PCI, NIS o la más antigua y para las empresas cotizadas norteamericanas, SOX.

Un entorno hiperregulado, con una vocación cada vez más exhaustiva y para perímetros concretos de las compañías, en el que, sin embargo, no se logra poner fin a los hackeos, la suplantación de identidad de empleados y gestores, y que afecta a los clientes, que sienten que su dinero no está seguro en estas entidades.

Esta percepción social viene respaldada por datos. Son los que ofrece el estudio de GrantThornton y que explican que el 80% de los ciberataques en la banca están dirigidos a los empleados. Además, citan también a los proveedores como vía de acceso a la información interna de la empresa.

Esta situación, más allá del perjuicio para los afectados, supone, explica Roberto Romero un aumento de costes exponencial para las empresas, además de un "choque de trenes" entre la seguridad y la operatividad. Tanto los costes como los tiempos para implementar sistemas avanzados adecuados al marco legal son muy altos.

El punto de partida para atajar aquí el cibercrimen es la "política de confianza cero", que supone que todos son sospechosos dentro de la organización y que solo se van a recibir permisos para acceder a determinados datos y/o ejecutar distintas tareas. Esto significa acceder únicamente a lo que se esté autorizado y en el momento en el que se deba, olvidándose de esos privilegios que serán retirados después, en caso de cambio en el desempeño de las funciones.

Junto a una buena segregación funcional y gestión de accesos, desde Scalian apuestan por un control centralizado y homogéneo de la autorización mediante modelos ABAC (Attributed Based Access Control), esta combinación va a permitir trabajar en entornos grandes y complejos de una forma ajustada a cumplimiento, pero a la vez ágil y versátil.

Se trata, en definitiva, de afrontar los retos que surgen de las nuevas regulaciones en materia de ciberseguridad y de hacerlo con los mejores resultados, la mayor operatividad posible y "sin tirar la casa por la ventana".

Datos de contacto:
Carmen de Blas
Miss Zoe comunicación
639 00 72 10

Nota de prensa publicada en: Madrid

Categorías: Finanzas Inteligencia Artificial y Robótica Software Ciberseguridad Innovación Tecnológica Consultoría