



El COACAB organiza con SGS una sesión sobre ciberseguridad

El sector logístico, y especialmente los agentes de aduanas y representantes aduaneros por el papel que juegan en las operaciones de comercio internacional, están intensamente expuestos y son más vulnerables a los ataques cibernéticos.

En el marco de las sesiones informativas sobre temas de actualidad que organiza el Colegio Oficial de Agentes de Aduanas y Representantes Aduaneros de Barcelona, el martes 19 de febrero tuvo lugar en la sede del COACAB una sesión dedicada a la ciberseguridad.



Luis Romero, Fabio Murillo y Susanna Caminals, de SGS junto a David Soler, Director del COACAB

Para analizar esta complicada cuestión intervinieron los expertos de la firma SGS Cyberlab: Juan Luis Romero Pozo, Team Leader Penetration Testing; Fabio Murillo Alonso, Customer Experience CyberLab Madrid, acompañados de Susanna Caminals, Governments & Institutions (GIS) TransitNet Project Manager, Spain.

Estos profesionales abordaron la importancia que tiene hoy en día el hecho de gestionar adecuadamente la seguridad en una empresa, sea ésta de la dimensión que sea, dado que cualquier compañía se gestiona a través de diferentes dispositivos conectados a Internet y con múltiples usuarios. Por tanto, la ciberseguridad es un reto que incluso las pequeñas y



Colegio Oficial de Agentes de Aduanas y Representantes Aduaneros de Barcelona

medianas empresas deben afrontar ya que una mala gestión de la seguridad puede ocasionar serios impactos económicos, afectar a la reputación y, por consiguiente, hacer perder la confianza de los clientes.

El sector logístico, y especialmente los agentes de aduanas y representantes aduaneros por el papel que juegan en las operaciones de comercio internacional, están intensamente expuestos y son más vulnerables a los ataques cibernéticos. Se trata de un colectivo que utiliza dispositivos conectados, diversas aplicaciones informáticas y se comunica constantemente con múltiples clientes, proveedores y administraciones.

Es evidente que cualquier ataque cibernético que se produzca en algún eslabón de la cadena logística, como por ejemplo los que han venido sufriendo algunas navieras, puede tener repercusiones en la actividad diaria de cualquier empresa. El ataque a un tercero puede generar que nuestra información más sensible, como cuentas bancarias y documentos privados, quede expuesta. Otras consecuencias perjudiciales de un ciberataque pueden ser la inhabilitación de los sistemas, la suplantación de la personalidad o la falsificación y eliminación de datos.

Los técnicos de SGS Cyberlab, que presentaron las soluciones que la compañía ofrece ante los desafíos de seguridad, también se refirieron a las regulaciones que existen, y que son de obligado cumplimiento, como el nuevo Reglamento General de Protección de Datos (RGPD) vigente desde el mes de mayo del pasado año. Este reglamento establece que las organizaciones son responsables de la gestión de los datos que manejan y, por tanto, deben asegurar que utilizan los medios técnicos y formativos adecuados para esa gestión.

Los expertos de SGS Cyberlab, compañía especializada en el análisis de riesgos y vulnerabilidades tecnológicas, finalizaron destacando que es necesario que cualquier empresa despliegue una correcta estrategia de ciberseguridad para evitar o minimizar el impacto de un ataque en los sistemas de la organización.