ABC - Suplemento Empresa
domingo, 03 de noviembre de 2019

PROTEGER, ALERTAR Y RESPONDER

«La protección frente a los ciberataques debe formar parte de la estrategia de supervivencia y crecimiento de cualquier empresa con presencia online»

JOSÉ LUIS MARTÍNEZ CAMPUZANO
PORTAVOZ DE LA ASOCIACIÓN ESPAÑOLA DE BANCA

El coste anual de los ciberataques a escala mundial es enorme y todo apunta a que crecerá de forma exponencial en un futuro dominado por la digitalización de la economía y de la sociedad. El cibercrimen es cada vez más sofisticado y complejo. Por eso la respuesta para combatirlo también ha de evolucionar y combinar prevención, formación, concienciación y soluciones tecnológicas.

La ciberseguridad debe ser una prioridad para todos. El 70% de las empresas europeas no están preparadas para enfrentarse a las amenazas a través de internet, pese a que la gran mayoría ya ha tenido experiencias negativas relacionadas con estos delitos. Los riesgos cibernéticos pueden afectar a todas las áreas de negocio de una compañía y provocar graves daños, tanto económicos como reputacionales. En comparación, el coste de tomar medidas de prevención no resulta demasiado elevado. Es más, la protección frente a los ciberataques debe formar parte de la estrategia de supervivencia y crecimiento de cualquier empresa con presencia online.

La ciberseguridad es prioritaria para los bancos, que ponen todos los medios a su alcance para garantizar la seguridad de sus clientes y encarar los riesgos que seguro aparecerán en el futuro. A pesar de su probada experiencia en la protección de los datos personales y financieros de sus clientes, los bancos revisan continuamente su capacidad de protección, detección y respuesta ante los ciberataques. El esfuerzo por mejorar lo llevan en su ADN. Ponen la innovación financiera al servicio de este objetivo con herramientas como el big data o la inteligencia artificial, muy útiles para luchar contra las estafas que se propagan vía digital.

A medida que los bancos fortalecen sus barreras de protección, los ciberataques derivan hacia el eslabón más débil de la cadena, el cliente: «phishing», «vishing», «smishing»... términos que se refieren a robos de identidad y otros datos, engaños financieros e infecciones con virus a ordenadores y móviles. Los beneficios y enormes posibilidades que brinda la digitalización no debe llevarnos a bajar la guardia frente a sus riesgos. Las ciberestafas en la mayoría de los casos se aprovechan de la psicología y percepción de las personas. La mejor prevención en este caso se apoya en la formación y la sensibilización.

Riesgos
El 70% de las empresas de la UE no están listas para enfrentarse a las amenazas

Tendencias
Los ciberataques derivan hacia el eslabón más débil de la cadena, el cliente

La Asociación Española de Banca realiza periódicamente campañas de concienciación ciudadana junto a las fuerzas de seguridad para prevenir ataques de los cibercriminales. En julio nos unimos a la red «No More Ransom», una iniciativa de las fuerzas del orden y del sector privado que ofrece a las víctimas de robo de información online y extorsión una solución alternativa a la pérdida de sus valiosos archivos o tener que pagar el dinero exigido por los delincuentes. A finales del año pasado colaboramos en la campaña de Europol y la Federación Bancaria Europea contra el blanqueo de dinero a través de mulas (European Money Mule Action). Ciudadanos y empresas han de ser conscientes de los riesgos cibernéticos, porque les afectan. Y los delincuentes han de conocer la unidad de la comunidad pública y privada contra estos delitos.

Las autoridades conocen la velocidad de vértigo de la digitalización y la necesidad de que la regulación contribuya a limitar los riesgos a los que todos nos enfrentamos en la nueva era digital. Los bancos están sometidos a una regulación estricta y a una supervisión exigente que refuerza su ya robusta protección del cliente, pero no sucede igual con otros proveedores de servicios bancarios, grandes empresas tecnológicas exentas de este tipo de vigilancia y control. Los cambios regulatorios que han abierto la puerta a la competencia de estas compañías no deben dejar rendijas de seguridad que puedan aprovechar los cibercriminales por el bien del consumidor.