La banca intensifica su inversión en seguridad ante la carrera digital

La debilidad del negocio, el cierre de oficinas y los avances tecnológicos han convertido la **banca online** en el futuro del sector financiero. Pero el camino no está exento de peligros. "Es vital, y todo un desafío de gestión, proteger el valor de la marca, de nuestros activos, de nuestra propiedad intelectual y de la información de nuestros clientes ante las innumerables amenazas existentes en un mundo virtual", agrega **Fernando Rodríguez Baquero**, director general de recursos técnicos de Banco Popular, quien asume que la exposición al negocio digital requiere "inversiones de forma sostenida" para protegerse de los riesgos inherentes al mismo. Inmersa en la carrera por liderar la digitalización del negocio, la banca española está haciendo grandes esfuerzos en este sentido.

Aunque no resulta barato. Desde el sector ilustran cómo en líneas generales solo **el 3% de los gastos de cada proyecto** se destina a seguridad, si bien en el caso de iniciativas puramente digitales, dependiendo del tipo de desarrollo, ese porcentaje se eleva a horquillas de entre el 20% y hasta el 40% de la inversión, coinciden en señalar desde entidades como Bankia o Sabadell. La operativa de banca online, exponen, debe ser segura o no ser, por lo que la seguridad forma parte del ADN de todo nuevo proyecto.

"La inversión es elevada porque requiere una actualización y vigilancia continua más allá del momento en que se estrena el servicio", agrega **Xavier Serrano**, director e IT_control de Banco Sabadell, que detalla que hoy día las soluciones digitales nunca son válidas durante años porque los ciberdelincuentes siempre estudian cómo franquear las nuevas barreras y es necesario innovar continuamente para contrarrestarles.

Identidad robada

"Los principales avances que se están produciendo en el ámbito de la seguridad están relacionados con la protección del que entendemos que puede ser el eslabón más débil o menos protegido, que es el cliente que consume los servicios del banco de forma digital", explican desde Bankia. La suplantación de la identidad de un cliente a través del uso de virus informáticos, o mediante correos electrónicos o llamadas telefónicas en las que el defraudador se hace pasar por la entidad son el principal reto del sector financiero, centrado en evitar que un tercero opere con la cuenta de un cliente o altere sus sistemas de alerta.

Engaño al banco

La banca también sufre ataques directos. Desde Experian revelan que uno de los principales frenos a la concesión de crédito online, uno de los grandes mercados en los que aspira a expandirse el sector, radica en las barreras necesarias para impedir que el banco sea estafado mediante la suplantación de la identidad del cliente o la acumulación de peticiones de crédito a través de perfiles falsos.

Desvío de nóminas

Un fraude creciente es la infiltración en los sistemas informáticos de determinadas empresas para monitorizar el pago de las nóminas y modificar las cuentas corrientes objeto del pago que se facilita a sus bancos para así propiciar transferencias masivas a cuentas de terceros.

Bloqueo de webs

Los ataques para derribar o paralizar las webs de las entidades financieras son otro de las grandes amenazas que afronta el sector, si bien los expertos advierten que con cada nuevo servicio ofertado se generan nuevas estafas.
La profesionalización de estos atacantes, que han dejado de ser hackers aficionados en busca de retos y se han convertido en organizaciones criminales, junto con la ausencia de legislación o persecución policial global multiplican la amenaza, dice.

"Los bancos quieren dirigir a sus clientes al canal online pero eso atrae a hackers, defraudadores y otros ciberdelincuentes que ven mayores oportunidades para ellos", subraya Alexandros Triantafyllou, director para la Península Ibérica de la unidad de fraude e identidad de la firma Experian, especializada en el control de riesgos crediticios y la prevención de estafas digitales.

"Los niveles de fraude online en la industria española no son tan altos como en otros países, pero están creciendo", advierte.

A nivel global, cuatro de cada diez ataques informáticos que implicaron el robo de datos personales o la suplantación de una identidad se concentraron el año pasado en el sector financiero y en el de medios de pago, según la información recopilada por la Anti-Phishing Working Group (APWG), una coalición internacional en respuesta al crimen cibernético que engloba 1.800 instituciones entre representantes de la industria, los gobiernos y las fuerzas del orden.

En España, "en los últimos años se han multiplicado los casos de malware informático (software malintencionado) y ordenadores infectados y prácticas de phishing (suplantación de identidad)_en red, lo que requiere mayor protección para las transacciones digitales de banca", denuncian desde la Asociación Española de Empresas Contra el Fraude (**AEECF**).

Ataques simulados y control de los dispositivos

En su apuesta por **mejorar la ciberseguridad**, el grupo financiero que preside Ana Patricia Botín ha puesto en marcha el Santander Cyber Security Program un programa de control, prevención y respuesta a las amenazas digitales implantada en toda la entidad. Además, el grupo ha incluido a sus firmas subsidiarias en los ciberataques simulados que llevan a cabo terceros para testar la capacidad de detección y reacción de la entidad, y a los que también suelen someterse el resto de firmas del sector.

"Los métodos tradicionales de identificación, claves de acceso, mensajes SMS de confirmación, e incluso certificados digitales ya no son suficientes", aduce Xavier Serrano, responsable de seguridad tecnológica en Banco Sabadell, revelando que hoy día es necesario implementar controles adicionales que miden los patrones de conducta, modus operandi, o cálculos de riesgo operacional de los clientes, como parte de la prueba de verificación de las operaciones.

Desde la firma de servicios financieros Experian, por ejemplo, han desarrollado sistemas de análisis de los dispositivos desde los que se conecta el cliente para verificar a través de que medio está operando o desde qué país se ha conectado y añadir así garantías adicionales a la comprobación tradicional de su identidad.

En su opinión, no obstante, **"educar al cliente"**, es clave para evitar que sea objeto de engaños. Uno de los grandes retos del sector en este campo, coinciden todos los expertos consultados, es encontrar el delicado equilibrio entre dar seguridad y una experiencia de usuario agradable para que el fraude evitado no vea empañado por la pérdida de clientes.

Fuente: http://cincodias.com/cincodias/2016/03/04/mercados/1457116764_618428.html