Seguridad Digital

Un nuevo plan director a tres años

La seguridad de la información es una de las grandes prioridades de Bankinter. Para atender a ese compromiso, en 2021 se acometieron los proyectos acordados dentro del Plan Director de Seguridad. El objetivo es garantizar un alto nivel de confidencialidad, integridad y disponibilidad a clientes, empleados, accionistas y proveedores. Además, durante el ejercicio Bankinter decidió que el área de Seguridad de la Información pase a llamarse Seguridad Digital y elaboró un nuevo Plan Director, que marca la estrategia y los objetivos en seguridad de la información de la entidad para los próximos tres años.

El modelo para la lucha contra los ciberdelincuentes está basado en tres líneas de defensa: la primera está formada por la tecnología, el negocio, las operaciones, etc.; la segunda la integran los órganos de control de riesgo y de cumplimiento normativo; y la tercera línea la defiende Auditoría Interna.

Desde el punto de vista de la organización, en la primera línea se implantó en 2018 un nuevo modelo dentro de la Dirección de Seguridad de la Información con tres gerencias: riesgos tecnológicos, ciberseguridad y monitorización de la seguridad y prevención del fraude electrónico. En 2021 se creó una nueva gerencia para potenciar la continuidad y respuesta ante incidentes.

Sobre esa nueva estructura reforzada, Bankinter ha emprendido un conjunto de proyectos con un nivel de madurez superior y cuyo principal foco ha estado en los vectores de mayor amenaza. Es importante destacar que no sólo es necesario proteger los activos de la entidad; también hay que velar por la seguridad dentro de la cadena de suministros para garantizar un correcto funcionamiento de los procesos de negocio.

Concienciación

La actividad del área se completa con el desarrollo de planes de concienciación de los usuarios, que son el eslabón más débil de la cadena de seguridad. La entidad lleva a cabo programas de formación online para los empleados a través de la Intranet y se realizan simulaciones para obtener información confidencial (contraseñas, datos de identificación, etc.) a través de correos electrónicos, mensajes de texto (smishing) llamadas telefónicas (vishing), etc. El objetivo es conocer su reacción en situaciones que pueden ser aprovechadas por los ciberdelincuentes. La labor de concienciación se extiende también al personal externo.

La creciente importancia de la seguridad de la información se pone de relieve con la rápida expansión del cibercrimen, cuyas actividades han evolucionado y se han hecho mucho más peligrosas. Inicialmente se trataba de prácticas individuales de aficionados, cuya motivación no era fundamentalmente económica. Ahora, el cibercrimen ha creado grandes y sofisticadas estructuras empresariales que son capaces de atacar sectores económicos enteros.

El robo a empresas de datos confidenciales masivos, los ataques de acceso de servicio y el phishing (suplantación de una empresa o entidad pública para conseguir información confidencial de la víctima), los accesos a Swift o el malware con cifrado (*ransomware*) son las principales estrategias de los ciberdelincuentes.

Las instituciones financieras están especialmente expuestas a este tipo de manipulaciones y fraudes como consecuencia de su contacto permanente con el público y por las propias características de su negocio, parte del cual descansa sobre el sistema de pagos.