Ciberamenazas internas en el sector bancario.

Auriga analiza los distintos tipos de riesgos procedentes del personal en el sector y apuesta por un modelo Zero Trust como pilar de la seguridad bancaria.

Madrid, 16 de marzo de 2026
El sector bancario lleva años reforzando sus defensas frente a un entorno digital cada vez más hostil. Ataques externos, campañas masivas de phishing y ransomware o sofisticadas intrusiones forman parte del día a día de los departamentos de ciberseguridad. Sin embargo, existe un tipo de amenaza que, por su naturaleza, resulta aún más compleja de gestionar: la que surge dentro de la propia organización.

Auriga, proveedor de software líder para el sector de la banca y de pagos y experta en el sector, alerta de que las amenazas internas no son nuevas, pero sí más visibles y potencialmente más dañinas debido a un entorno hiperconectado y altamente digitalizado como el actual.

> *"El factor humano ha sido siempre uno de los principales vectores de riesgo en cualquier organización. En el ámbito financiero, donde confluyen datos sensibles, sistemas críticos y operaciones de alto valor económico, el impacto puede ser especialmente severo. No existe una fórmula mágica para erradicar por completo estos riesgos. Lo que sí existe es la capacidad de identificarlos, entenderlos y reducir su impacto mediante procesos, tecnología y cultura corporativa"*
>
> *Néstor Santolaya, cybersecurity product expert de Auriga.*

Una amenaza histórica con nuevas formas

Centrándose en los riesgos, posibles brechas de seguridad y, en general, amenazas que provienen o se originan dentro de la propia organización, Auriga las clasifica en dos grandes bloques: aquellas en las que existe intencionalidad por parte del empleado y aquellas en las que no.
En ambos casos, el daño potencial es elevado, aunque las motivaciones y circunstancias difieren sustancialmente:

- **Cuando existe intencionalidad:**
  Desde el empleado que actúa de forma autónoma en beneficio propio hasta quien es incentivado económicamente por terceros, pasando por quien actúa por despecho tras una salida conflictiva de la empresa. En estos casos, el riesgo puede estar en un mero **ánimo de lucro individual**, como el conocido caso de Rodney Reed Caverly, empleado del departamento de TI de un banco estadounidense, que desplegó malware en un centenar de cajeros automáticos para extraer efectivo durante meses sin ser detectado.
  También pueden producirse situaciones de **coacción** por parte de **grupos criminales**, en las que el empleado facilita el acceso fraudulento a terceros. Esta presión no siempre implica una compensación económica: puede incluir amenazas, doxing o intimidación contra el propio trabajador o su entorno familiar, lo que en algunos casos deja al empleado con escaso margen para negarse a colaborar.

También existen casos donde el móvil no es económico, sino emocional, como en situaciones de un **despido** o malas praxis laborales que el empleado considera injustas.

- **Sin intención, pero con consecuencias:** No todas las amenazas internas responden a una voluntad maliciosa. De hecho, muchas se producen por negligencia, desconocimiento o manipulación externa. Aquí, el **uso de software no autorizado**, el **envío accidental de información** confidencial por canales no seguros o la **publicación en redes** sociales de imágenes que revelan datos sensibles son prácticas más habituales de lo que se piensa. Herramientas de acceso remoto o aplicaciones de mensajería no aprobadas pueden abrir puertas inesperadas a los sistemas corporativos. Estos casos pueden partir de algo tan sencillo como la ingeniería social practicada sobre empleados (reciben un email con apariencia legítima en el que hay un link que da acceso) o incluso llegar a la suplantación de un directivo con un audio generado con inteligencia artificial –este fue el caso del banco belga Crelan en el que los atacantes suplantaron al CEO para ordenar transferencias fraudulentas–.

Protegerse incluso de lo desconocido

La evolución tecnológica, y especialmente el auge de la inteligencia artificial generativa, han multiplicado la sofisticación de los ataques. Los deepfakes, suplantaciones hiperrealistas y campañas automatizadas hacen cada vez más difícil distinguir lo legítimo de lo fraudulento.

Ante este escenario, Auriga subraya la necesidad de adoptar un enfoque estructural basado en el principio de **Zero Trust**: no confiar por defecto en ningún usuario, dispositivo o conexión, incluso si se encuentran dentro de la red corporativa.
Este modelo implica limitar privilegios, reforzar la autenticación multifactor, establecer mecanismos de doble validación en operaciones críticas y garantizar que únicamente el software, los comandos y las operaciones explícitamente autorizadas puedan ejecutarse en los sistemas críticos.

De este modo, se reduce la superficie de ataque no solo frente a malware tradicional, sino también ante técnicas Living-off-the-Land (LotL) que intentan aprovechar herramientas legítimas del propio sistema. La revisión periódica de accesos, la correcta definición de canales oficiales y la aplicación de políticas de mínimo privilegio se convierten en pilares fundamentales.

> *"La seguridad ya no puede basarse únicamente en perímetros. Debe estar integrada en cada proceso, cada usuario y cada transacción. Protegerse de las amenazas externas es imprescindible, pero protegerse también de los riesgos internos es, hoy más que nunca, una prioridad estratégica para la banca"*
>
> *concluye Santolaya.*

Acerca de Auriga

Auriga es un proveedor líder de software y soluciones tecnológicas para la banca y el sector de pagos, y especialista en soluciones omnicanal innovadoras para la banca y otras instituciones financieras. Sus soluciones, desplegadas en más del 74 % de los cajeros automáticos de Italia, se basan en una moderna arquitectura tecnológica, y mejoran el time-to-market para nuevos servicios mientras al mismo tiempo que reducen los costes y protegen los dispositivos críticos de ciberataques, logrando una ventaja competitiva a largo plazo. Auriga es una compañía global, con presencia en Italia, Reino Unido, España, Bélgica, Polonia y México, y está expandiéndose en Europa occidental y oriental, Latinoamérica y Asia-Pacífico.

Más información sobre Auriga:
https://www.aurigaspa.com/es/

Para más información:

Jesús Martínez - jesus.martinez@alephcom.es
Esther Gago - esther.gago@alephcom.es
Aleph Comunicación - Tel.: 91 386 69 99

Contacto Auriga:

Antonella Comes
Chief Marketing Officer
antonella.comes@aurigaspa.com