Riesgos Cibernéticos en el Sector Fintech

¿Por qué el sector Fintech?

La transformación digital está a la vanguardia de los bancos y las organizaciones de servicios financieros, provocando una expansión exponencial del sector Fintech. Los bancos digitales, las organizaciones de financiación alternas, proveedores de software de pagos, remesas y otras empresas bancarias están añadiendo productos y servicios al ecosistema financiero, a un ritmo rápido.

Las Fintech permiten transferir dinero, gestionar inversiones y acceder a recursos financieros en línea. La digitalización, almacenamiento de los datos de los clientes e información financiera, así como el carácter sensible de los propios datos, hacen que el sector sea especialmente propenso a los ataques cibernéticos. De acuerdo con un informe los riesgos más comunes son el phishing y el malware, donde el 48% de las empresas dentro del sector Fintech han sido blanco de ataques por ransomware, sin embargo, las amenazas son más amplias, ya que se potencializan las vulnerabilidades del sector.

¿Estamos realmente en peligro?

El sector Fintech se ha vuelto vulnerable por las siguientes razones:

Ritmo de la transformación digital

El ritmo tan acelerado de la transformación digital en el sector financiero significa que, al seguir el ritmo del propio negocio, a menudo se descuida la seguridad cibernética. En un sector que se beneficia enormemente del uso de la Inteligencia Artificial, resulta sorprendente que la seguridad cibernética no esté suficientemente adoptada, ya que no se invierte demasiado en esta área. Las organizaciones están poco preparadas para proteger sus datos; aunque es probable que este riesgo se mitigue con el tiempo, uso de análisis avanzados y automatización en la seguridad, lo cual sigue siendo un reto.

Información en la nube

La nube ha aumentado drásticamente la eficiencia de los procesos bancarios, permitiendo flexibilidad, así como una rápida innovación. La nube (consiste esencialmente en que las empresas alquilan “digitalmente” recursos de sistemas informáticos) es una estrategia rentable que implica la subcontratación de servicios auxiliares (por ejemplo, procesadores de pagos en tiempo real, soluciones de autenticación de identidad) a proveedores de software bancario. Aunque predominantemente en el espacio del negocio al consumidor (B2C), las predicciones son que los bancos digitales continuarán la tendencia de pasar rápidamente de negocio a negocio (B2B) o negocio a negocio finalizando con el cliente (B2B2C), lo que refleja una mayor inversión en financiación de tecnología financiera B2B. La mayor dependencia de proveedores externos implica un aumento equivalente en las plataformas informáticas y una mayor amenaza para la seguridad de la red.

Seguridad en aplicaciones

El uso de servicios en la nube para optimizar los pagos y transacciones, como monederos digitales, herramientas destinadas a la elaboración de presupuestos y otras aplicaciones móviles. Un estudio sobre la seguridad en las aplicaciones muestra que, de las 100 empresas de nueva creación más destacadas y mejor financiadas, todas y cada una de las aplicaciones móviles analizadas contenían al menos una vulnerabilidad de seguridad de riesgo medio, mientras que el 97% de las aplicaciones mostraban al menos dos vulnerabilidades de riesgo medio o alto.

Implicaciones para la privacidad

La banca abierta va en aumento y tiene el potencial de mejorar la vida de los clientes bancarios de todo el mundo, sobre todo en aquellas zonas donde amplios sectores de la población no tienen acceso a la banca personal tradicional. El intercambio de datos entre bancos, proveedores de servicios financieros y externos ayudan en el proceso de diseño de productos financieros para mejorar la experiencia del cliente. Productos digitales como la calificación crediticia, rastreadores de ahorro y aplicaciones que ayudan a administrar/elaborar presupuestos, responden a los hábitos bancarios de los usuarios, creando una experiencia más digerible y sencilla al usuario. Este intercambio de datos conlleva mayores responsabilidades en relación con el uso ético y legal de los datos y la necesidad de una estrecha vigilancia de la seguridad de la información. Si no se gestionan bien las implicaciones para la privacidad existe la posibilidad de que se produzcan costosas violaciones de datos que afecten a los usuarios y a los reguladores de la privacidad. Es fundamental gestionar las responsabilidades ante clientes, empleados, otras empresas y organismos reguladores, así como mitigar los costos que pueda asumir la misma compañía.

Error humano

El error humano es un elemento que prevalece en el sector bancario. Ninguna cantidad invertida en seguridad cibernética protegerá contra errores u omisiones dentro de la organización. Estadísticas reflejan que el 60% de las notificaciones de violación de datos personales a la Oficina del Comisionado de Información en 2019 fueron el resultado de un error humano.

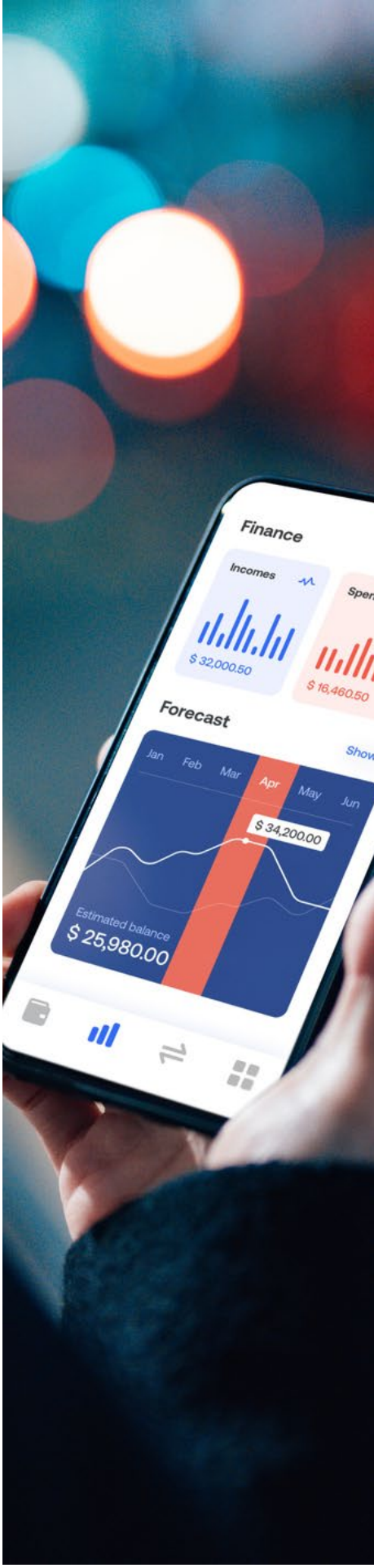
Software obsoleto

El uso de un software obsoleto, así como programas con código público, genera vulnerabilidades importantes para las organizaciones Fintech. Como los programas con código público están disponibles para su libre uso y se puede utilizar para compartir y modificar libremente la información, esto facilita a los delincuentes cibernéticos a conocer las vulnerabilidades del software con más facilidad, a comparación de un software con código privado.

Seguro de Cyber

La confianza y reputación son de suma importancia en el sector Fintech, y seguirán siéndolo a medida que el sector se vuelva más complejo, cambiante, innovador y receptivo. Las organizaciones deben demostrar fiabilidad a la hora de contar con una seguridad cibernética sólida, especialmente cuando se trata del uso de datos donde el riesgo de robo, manipulación o destrucción de datos, son una gran amenaza del sector.

La transferencia de riesgos mediante un seguro de Cyber ayudará a contar con un programa cibernético saludable. Es importante mencionar que muchas pólizas tradicionales no responderán a una violación cibernética. Una cobertura afirmativa bajo una póliza de Cyber independiente será vital.



Una póliza de protección de datos (Cyber) está diseñada para responder a los siguientes eventos, que no necesariamente serían cubiertos por pólizas más tradicionales:

a. Violación de datos de un ataque cibernético.
b. Pérdida financiera e impactos reputacionales tanto a la compañía como a los altos directivos por la falla de un sistema informático debido a un ataque malicioso.
c. Defensa regulatoria, multas y sanciones civiles como resultado de una violación de la seguridad (asegurable por ley).
d. Costos de respuesta a la violación.
e. Solicitud de rescate (ransom) tras un ataque a los sistemas informáticos.

Cobertura de Responsabilidad Civil Profesional Tecnológica

Para las empresas Fintech, también será crucial tener en cuenta el seguro de Errores y Omisiones Tecnológicos. Diseñado para cubrir las pérdidas financieras a los clientes del asegurado debido a un error u omisión en la prestación de servicios profesionales tecnológicos, es una subcategoría del seguro de responsabilidad civil profesional, aplicado específicamente a las empresas tecnológicas.

Si una empresa genera ingresos a partir del suministro de servicios o productos tecnológicos, este seguro puede ser vital, el cual complementa a una póliza independiente de protección de datos.

Estrategia integral

Implementar una estrategia integral de seguridad cibernética para el sector Fintech es fundamental para salvaguardar las actividades, reputación e ingresos de la compañía. Un ataque cibernético puede tener ramificaciones de gran alcance. Comprender estos riesgos y mitigarlos de manera proactiva es clave.

Nuestro equipo de expertos en riesgos cibernéticos trabajará con usted para crear una solución personalizada que proteja y asegure su trabajo exactamente donde lo necesite y garantice que los riesgos cibernéticos se integren en su proceso de gestión de riesgos. Mantener la confianza es vital.

Para mayor información:

Ricardo Millán
Head ProFin México
ricardo.millan@lockton.com

Moisés García
ProFin México
moises.garciab@lockton.com