BankWorks PHOENIX®

Cómo las empresas pueden reforzar su Seguridad Cibernética en un Mundo de Amenazas en Aumento

En un contexto donde los ataques de ransomware han aumentado un 20% en tan solo un año, las organizaciones enfrentan una creciente presión para mantener la seguridad cibernética mientras reducen costos. Presentamos siete estrategias clave para que los Directores de Seguridad de la Información (CISO) equilibren estas demandas de manera efectiva:

1. **Optimizar las soluciones existentes:** Muchas organizaciones tienen capacidades cibernéticas no utilizadas. Activar estas funciones y comprender completamente las herramientas optimiza los recursos financieros de la organización, también fortalece su postura cibernética existente, lo que contribuye a un entorno de seguridad más robusto y confiable.
2. **Revisar Estrategias de Subcontratación:** Evaluar si ciertas tareas de seguridad cibernética serían más eficientes si se gestionaran internamente o mediante un Proveedor de Servicios Gestionados (MSP). Además, la concienciación y formación continuas de los empleados son cruciales.
3. **Consolidar Herramientas de Ciberseguridad:** Reducir la complejidad y los costos mediante la consolidación de soluciones. La gestión de múltiples productos de seguridad con varias consolas crea puntos ciegos; simplificar esto aumenta la eficacia.
4. **Aumentar Medidas de Resiliencia:** Invertir en capacidades de copia de seguridad y otras medidas de recuperación de desastres cibernéticos para reducir gastos en caso de violación. Las pruebas regulares de planes de respuesta a incidentes son esenciales.
5. **Automatizar y Afinar Herramientas:** Identificar procesos manuales que puedan automatizarse. La IA y la automatización pueden reducir significativamente los costos asociados con las violaciones de datos.

6. **Implementar el Modelo Zero Trust:** Zero Trust es un modelo de seguridad basado en el principio de "nunca confiar, siempre verificar". Este enfoque reduce el riesgo de violaciones cibernéticas hasta en un 50% al evitar la explotación de permisos excesivos y falta de segmentación de red.
7. **Priorizar la Prevención:** Muchas herramientas de seguridad "detectan" en lugar de "prevenir" los problemas. Enfocarse en prevenir en lugar de detectar problemas es más rentable a largo plazo. Cuantificar el retorno de inversión de la prevención puede justificar el gasto inicial.

A pesar de las limitaciones presupuestarias, las organizaciones pueden mantener una sólida ciberseguridad al adoptar enfoques innovadores y alineados con las últimas tecnologías. Al consolidar, automatizar y optimizar, junto con la formación continua y la implementación de estrategias de prevención, las empresas pueden enfrentar las amenazas cibernéticas de manera más efectiva y eficiente.

Fuente: World Economic Forum

7 retos clave del Sector Financiero en Latinoamérica para el 2024

Finnovating, la plataforma global de matching B2B basada en IA, ha identificado los 7 retos principales que enfrentará el sector financiero en Latinoamérica durante el año 2024. Estos desafíos surgieron de un análisis detallado de más de 22 millones de interacciones realizadas en su comunidad durante el último año, y se espera que tengan un impacto significativo en la industria financiera de la región.

1. **La Disrupción Tecnológica:** La introducción de nuevas tecnologías como la inteligencia artificial, GenAI, el blockchain y la computación en la nube está transformando la forma en que las instituciones financieras ofrecen sus productos y servicios.
2. **La Transformación Digital:** El sector financiero latinoamericano se encuentra en medio de una transformación digital, donde la adopción de tecnologías innovadoras será fundamental para su competitividad futura.
3. **Sostenibilidad e Inclusión Financiera:** La falta de información sobre los riesgos y oportunidades relacionados con la sostenibilidad dificulta la toma de decisiones informadas en este ámbito. La inclusión financiera también es un desafío clave que debe abordarse de manera efectiva.
4. **La Regulación:** La industria financiera está fuertemente regulada para proteger a los consumidores y garantizar la estabilidad financiera. Las instituciones financieras deben prepararse para adaptarse a los cambios normativos.
5. **Ciberseguridad e Identidad Digital:** La ciberseguridad sigue siendo una amenaza creciente para el sector financiero. Las instituciones financieras deberán invertir significativamente en medidas de ciberseguridad para proteger sus sistemas y datos, además de abordar retos relacionados con la biometría, la identificación digital y las nuevas generaciones de KYC y KYB con IA.
6. **Riesgos de Crédito y de Mercado:** A pesar del fuerte crecimiento económico, existen riesgos estructurales en Latinoamérica debido a la volatilidad económica, inflación y la incertidumbre política, lo que aumenta la probabilidad de incumplimiento de los prestatarios y afecta la volatilidad de las divisas.
7. **Cooperación con las Fintech:** Las empresas tecnológicas financieras están desafiando las normas establecidas en el sector financiero. Más del 70% de estas fintech son B2B, lo que representa una importante palanca de digitalización e innovación para las instituciones financieras.

Fuente: Tekios Noticias

BankWorks Phoenix la única Solución Financiera totalmente integrada que responde de principio a fin al modelo de negocio de las instituciones financieras innovadoras que van hacia su transformación digital