PRAXIS

Revolución de la Ciberseguridad en la Banca Digital

Abraham Ivan Garcia Rivera
Gerencia Karpay

More connected than ever

En la era digital en la que vivimos, la banca ha experimentado una transformación radical gracias al avance tecnológico. La aparición de la banca digital ha revolucionado la forma en que las personas gestionan sus finanzas, brindando una conveniencia sin precedentes al permitir el acceso a servicios bancarios desde cualquier lugar y en cualquier momento a través de dispositivos conectados a internet. Desde la transferencia de fondos hasta el pago de facturas y la inversión en línea, la banca digital ha democratizado el acceso a los servicios financieros, eliminando las barreras geográficas y temporales que antes limitaban la participación en el sistema bancario tradicional.

La revolución digital en la banca trae nuevos riesgos. A medida que aumentan las transacciones en línea, tanto las instituciones como los usuarios enfrentan crecientes amenazas cibernéticas. Los ciberdelincuentes usan herramientas cada vez más avanzadas para explotar vulnerabilidades y poder acceder de manera ilegal a información financiera.

Amenazas Cibernéticas en la Banca Digital

La banca digital enfrenta diversas amenazas cibernéticas, como:

- **Phishing:** buscan engañar a los usuarios para robar información confidencial
- **Malware y Ransomware:** bloquean el acceso a datos a cambio de un rescate.
- **Hacking:** Explotan vulnerabilidades en la infraestructura de TI para robar datos o interrumpir servicios
- **Fraudes financieros:** Implican falsificación de transacciones o suplantación de identidad.

En este sentido, el informe Tendencias de fraude bancario digital en América Latina 2024 de BioCatch destaca el crecimiento de los fraudes con dispositivos robados desde, al menos, 2018. De hecho, los casos denunciados de fraude bancario digital crecieron un 32 por ciento en el primer semestre de 2024 respecto al mismo período del año anterior.

El troyano bancario Grandoreiro, activo desde hace siete años, ha atacado a más de 1.500 instituciones financieras, de las cuales más del 20 por ciento están en América Latina.

En julio de 2024, Asia Pacific bank sufrió un ataque de denegación de servicio (DDoS), interrumpiendo su plataforma de banca en línea y otros servicios esenciales. Este incidente evidenció la vulnerabilidad de las instituciones financieras frente a la saturación deliberada de sus sistemas

Vulnerabilidades y Desafíos de Seguridad

Incremento de ataques dirigidos a dispositivos IoT: Explotación de vulnerabilidades en dispositivos conectados, como cámaras IP y routers.

Evolución del ransomware: Ataques con encriptaciones avanzadas y estrategias de doble extorsión, afectando sectores críticos como la salud y las finanzas.

Insurgentes Sur No. 64, Torre B, Oficina 501, 502 y 503, Col Juárez, Alcaldía Cuauhtémoc, CDMX, C.P. 06600

praxisglobe.com
55 5080-0048

Ataques a dispositivos móviles: Incremento del malware móvil, phishing por SMS y explotación de vulnerabilidades en Android e iOS.

Amenazas Persistentes Avanzadas (APT): Ataques encubiertos y prolongados que utilizan vulnerabilidades de día cero y técnicas de ingeniería social para infiltrarse en redes y sistemas.

Mayor brecha de talento en ciberseguridad: Brecha de talento en la industria de la ciberseguridad, lo que dificulta la protección efectiva de sistemas y datos ante las crecientes amenazas cibernéticas.

Estrategias de Mitigación y Defensa

Para protegerse contra las amenazas cibernéticas, las instituciones financieras implementan una serie de estrategias de mitigación y defensa, destacando como principal enfoque la ciberseguridad proactiva. Según un informe de M-Trends el 17% de los ciberataques afectaron a organizaciones de servicios financieros.

Entre las estrategias más comunes, el uso de firewalls y sistemas de detección y prevención de intrusiones (IDS/IPS) ha demostrado reducir en un 40% los intentos exitosos de intrusión en redes financieras, de acuerdo con datos de IBM publicados en su informe anual de seguridad cibernética de 2024. La encriptación de datos sensibles garantiza la confidencialidad de la información crítica, y es una medida adoptada por el 98% de las principales instituciones bancarias del mundo, según un estudio de Ponemon Institute publicado en el primer semestre de 2024.

A medida que las amenazas cibernéticas evolucionan, las instituciones financieras deben adoptar nuevas estrategias innovadoras como:

1. Inteligencia Artificial y Machine Learning (IA/ML)
2. Arquitectura de confianza cero (ZTA)
3. Autenticación Biométrica Avanzada
4. Blockchain para la Seguridad de las Transacciones
5. Protección contra Ransomware mediante Segmentación y Copias de Seguridad
6. Ciberinteligencia y Threat Hunting (Caza de Amenazas)

A medida que las instituciones financieras han adoptado estrategias avanzadas como la inteligencia artificial (IA), la arquitectura de confianza cero (ZTA) y la autenticación biométrica, se han logrado mejoras significativas en la ciberseguridad frente a los métodos tradicionales.

Por ejemplo, la IA y el aprendizaje automático permiten detectar anomalías en tiempo real y prevenir amenazas como malware o phishing con alta precisión, **se prevé que en 2024 el gasto en seguridad informática será de 183.900 millones, un 13,4% más que en 2023. Para el próximo año crecerá casi dos puntos porcentuales más, un 15,1%, hasta los 211.552 millones de dólares.** Según la firma de análisis, la migración a entornos cloud será clave en este aumento en la inversión, así como la adopción de IA.

Insurgentes Sur No. 64, Torre B, Oficina 501, 502 y 503, Col Juárez, Alcaldía Cuauhtémoc, CDMX, C.P. 06600
praxisglobe.com
55 5080-0048

Educación y Concientización

La educación y la concientización son fundamentales para una estrategia de ciberseguridad efectiva, especialmente en el ámbito financiero. Las instituciones realizan programas de capacitación dirigidos tanto a empleados como a clientes, enfocándose en enseñar a identificar amenazas como los correos electrónicos de phishing, crear contraseñas seguras y proteger dispositivos de malware. Esto ayuda a establecer una cultura de seguridad que involucra a todos los niveles de la organización y a los usuarios finales.

Dado que las amenazas cibernéticas son cada vez más sofisticadas, las instituciones financieras deben adoptar un enfoque proactivo que combine tecnología avanzada, prácticas de seguridad sólidas y la concientización constante de los usuarios. Colaborar con otros actores del sector y compartir información sobre mejores prácticas también es esencial para mitigar los riesgos y mantener la seguridad en la banca digital.

La **especialidad de Karpay en PRAXIS** desarrolla sistemas de misión crítica para instituciones bancarias, complementadas con servicios de consultoría informática orientados a la **ciberseguridad en la banca digital**.

Nuestra misión es asegurar que la protección frente a **amenazas cibernéticas emergentes**, mediante escaneos estáticos y dinámicos que permiten detectar vulnerabilidades en tiempo real, incrementando la **confianza de nuestros clientes en la estabilidad y protección de sus operaciones financieras**.

Además, nuestro compromiso con la **adaptación a nuevas amenazas** nos permite colaborar estrechamente con reguladores y otros actores del ecosistema bancario para mantener un entorno financiero robusto y confiable.

ANA LAURA RODRIGUEZ GOMEZ
Gerente de KARPAY

55 5080 0048

ekarpay@praxisglobe.com

ANA LAURA RODRIGUEZ GOMEZ

Referencias

https://www.acelerapyme.gob.es/novedades/pildora/la-importancia-de-la-ciberseguridad-en-el-sector-financiero#:~:text=En%20resumen%2C%20las%20amenazas%20cibern%C3%A9ticas,mitigar%20el%20riesgo%20de%20ciberataques.

https://www.grupoica.com/blog/-/blogs/la-concienciacion-en-ciberseguridad-es-clave-para-garantizar-la-seguridad-en-cualquier-organizacion

https://www.infosecuritymexico.com/es/blog/estrategias-seguridad-fintech.html

https://www.banxico.org.mx/sistema-financiero/seguridad-informacion-banco.html

https://newsroom.accenture.com/news/2023/aligning-cybersecurity-to-business-objectives-helps-drive-revenue-growth-and-lower-costs-of-breaches-accenture-report-finds

https://newsroom.accenture.com/news/2019/cost-of-cybercrime-continues-to-rise-for-financial-services-firms-according-to-report-from-accenture-and-ponemon-institute

https://lurel.io/es/blog/metodos-de-deteccion-de-amenazas-con-ia-en-la-ciberseguridad

https://www.redseguridad.com/actualidad/ciberataques-el-sector-financiero-es-uno-de-los-mas-atacados_20240521.html

https://www.ibm.com/es-es/reports/data-breach

chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://table.media/wp-content/uploads/2024/07/30132828/Cost-of-a-Data-Breach-Report-2024.pdf

https://www.computerworld.es/article/3576875/zero-trust-inteligencia-artificial-y-computacion-cuantica-estas-son-las-claves-en-el-mercado-actual-en-ciberseguridad.html

https://www.segurilatam.com/ciberilatam/el-malware-aumenta-mas-del-doble-en-latinoamerica-en-el-ultimo-ano_20241010.html

https://www.ventasdeseguridad.com/novedades/ultimas-noticias/21-empresas/24044-ataques-ddos-al-sector-financiero-aumentaron-154-akamai.html

Insurgentes Sur No. 64, Torre B, Oficina 501, 502 y 503, Col Juárez, Alcaldía Cuauhtémoc, CDMX, C.P. 06600

praxisglobe.com
55 5080-0048