Akamai

WHITE PAPER

Seguridad de las API en el ecosistema de banca abierta

Equilibrar la innovación y la seguridad de los bancos europeos en la era digital

Resumen ejecutivo

En 2023, los bancos de Europa, Oriente Medio y África (EMEA) disfrutaron de una buena rentabilidad, y se prevé que esa rentabilidad se mantenga en el próximo año. Las interfaces de programación de aplicaciones (API), que constituyen el 31 % de todo el tráfico web, han desempeñado un papel fundamental en este crecimiento, ya que han facilitado diversos servicios, como transacciones bancarias, depósito remoto de cheques y ubicación de cajeros automáticos asistida por GPS, junto con servicios de terceros. Sin embargo, la rápida adopción de las API ha ampliado el panorama de ciberamenazas, lo que ha generado importantes inversiones en ciberseguridad por parte de las instituciones financieras.

La Directiva sobre Servicios de Pago de la Unión Europea (PSD2) y la directiva PSD3 prevista han desempeñado un papel fundamental en la configuración de los intercambios de datos entre los bancos tradicionales y las empresas de tecnología financiera. Las normas técnicas de regulación (NTR) imponen un uso seguro de las API al incorporar una autenticación reforzada del cliente (SCA) y estándares de comunicación abiertos comunes y seguros (SCA-NTR). La directiva PSD2, aunque se centra principalmente en los pagos, ha popularizado el término "banca abierta" en el Reino Unido, haciendo hincapié en el intercambio de datos de cuentas autorizado por los clientes y allanando el camino para el uso de soluciones más amplias de "finanzas abiertas". En el centro de estas soluciones de finanzas abiertas se encuentran las API.

La transformación digital en curso en el sector de los servicios financieros de EMEA, impulsada por las API, demuestra la capacidad de adaptación y el compromiso del sector para satisfacer las necesidades cambiantes de los clientes. Sin embargo, a medida que tiene lugar esta transformación, la vigilancia es esencial para fortalecer la ciberseguridad, abordar las vulnerabilidades y garantizar que los beneficios de la innovación digital prevalezcan sobre la amenaza siempre presente de los ciberataques. McKinsey informa de que los principales bancos planean asignar un 14 % a programas de API, lo que refleja el aumento del uso de las API y genera importantes inversiones en ciberseguridad. Las instituciones financieras ahora priorizan la protección de los sistemas internos y de los datos y activos de los clientes, prestando especial atención a la detección de amenazas, las estrategias de respuesta y la colaboración para contrarrestar eficazmente los riesgos cibernéticos.

La creciente importancia de las API

La región EMEA está experimentando una revolución digital basada en el deseo de proporcionar servicios y productos más eficientes y personalizados a sus clientes de servicios financieros. Las API desempeñan un papel fundamental, ya que ofrecen comodidad, velocidad y seguridad sin precedentes a los clientes que acceden a productos bancarios. Las API permiten que las aplicaciones de terceros se conecten con las herramientas, los servicios y los activos valiosos de un banco, lo que optimiza las conexiones para ambas partes. Los clientes disfrutan ahora de una amplia gama de actividades financieras, lo que ha transformado su experiencia y ha llevado al sector financiero directamente a la era digital. Las API, que han evolucionado desde simples herramientas de comunicación, se han convertido en la columna vertebral del tráfico de Internet y sirven de soporte para numerosas aplicaciones.

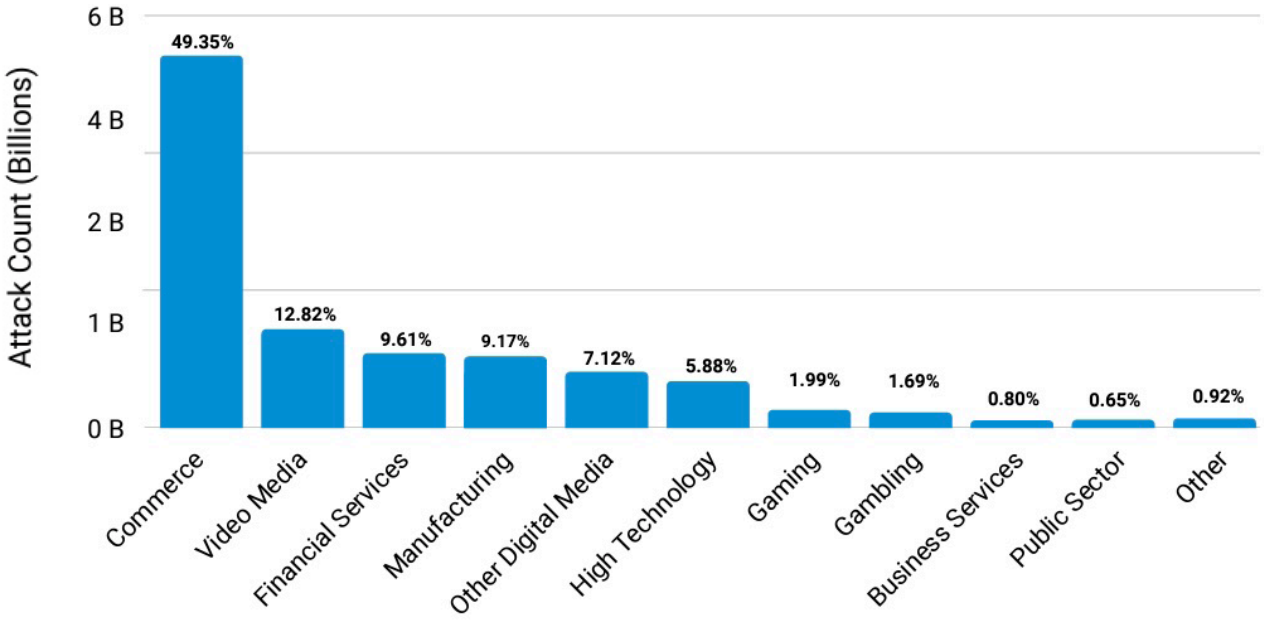
Según Allied Market Research, el mercado europeo de banca abierta alcanzó los 6140 millones de dólares en 2020 y se espera que alcance los 48 300 millones de dólares en 2030, con una tasa de crecimiento anual compuesto del 23,18 % entre 2021 y 2030. Iniciativas como el Open Bank Project, liderado por TESOBE, con sede en Berlín, aceleran esta adopción.
En colaboración con más de 40 bancos de todo el mundo, el Open Bank Project permite a los bancos ofrecer aplicaciones y servicios de terceros a sus clientes a través de una API abierta y una tienda de aplicaciones. En Francia, la consolidación en torno a la API de STET, proporcionada por el centro de compensación Systèmes technologiques d'échange et de traitement (STET), está ayudando a la implementación de pagos de banca abierta. Las API están a la vanguardia de la rápida remodelación del panorama financiero en EMEA y en el resto del mundo.

Amenazas relacionadas con las API en EMEA

El sector de los servicios financieros emerge como el tercero más atacado en la región EMEA; fue el objetivo de casi el 10 % de los ataques a aplicaciones web y API entre enero de 2022 y junio de 2023. Esto se traduce en la escalofriante cifra de 1000 millones de ataques web, del total de 11 000 millones sufridos por los distintos sectores en EMEA, y supone un aumento interanual del 119 % entre el segundo trimestre de 2022 y el segundo trimestre de 2023. Al profundizar en los datos, descubrimos que el Reino Unido lideró el ranking con el 59,2 % de los ataques a aplicaciones web, experimentando el mayor crecimiento interanual, con un 79 %, seguido de los Países Bajos, con un 16,2 %, y Alemania, con un 10,7 %.

EMEA: Principales sectores víctimas de ataques a aplicaciones web y API

Del 1 de enero de 2022 al 30 de junio de 2023



Los servicios financieros son el tercer sector que recibe más ataques en EMEA.

Riesgos clave sobre seguridad de las API

Las API pueden ser vulnerables a una amplia gama de riesgos de seguridad, lo que puede dar lugar a filtraciones de datos, accesos no autorizados y otras formas de abuso. Entre los principales riesgos de seguridad de las API se incluyen las API en la sombra, las API vulnerables, el abuso de API, el uso compartido excesivo de información confidencial y los ataques de Credential Stuffing.

- **API en la sombra.** En muchas instituciones financieras, ninguna persona o equipo es responsable de gestionar todas las API. Esta falta de supervisión crea una importante brecha de seguridad. Detectar y catalogar las API en toda la organización es crucial para gestionarlas y protegerlas. Es importante tender un puente entre los desarrolladores y los equipos de seguridad para detectar las API en la sombra en su entorno. La detección continua le mantiene informado sobre las API recién detectadas o los cambios en las existentes, lo que puede eliminar las API en la sombra.

- **API vulnerables.** Una vez detectadas las API, las instituciones financieras deben evaluar su posición de riesgo e identificar vulnerabilidades, especialmente en el caso de aquellas que contienen datos confidenciales. Este paso es vital para priorizar las iniciativas de seguridad de forma eficaz.

- **Abuso de API.** A medida que se acelera la digitalización, el número de ataques web en EMEA sigue aumentando. Los atacantes dirigen sus ataques sin descanso a las API, lo que requiere medidas de seguridad sólidas para impedir el abuso y el uso indebido.

- **Uso compartido excesivo de información confidencial.** Las aplicaciones modernas suelen compartir datos confidenciales en exceso, lo que presenta un nuevo vector de ataque. Los atacantes pueden interceptar el tráfico y obtener acceso no autorizado a información confidencial.

- **Ataques de Credential Stuffing.** Los atacantes dirigen sus ataques a las instituciones financieras mediante las API para automatizar los ataques de Credential Stuffing.

Desafíos de seguridad de las API

Inventario de API

Según una reciente encuesta de SANS, el inventario de API sigue siendo un problema crítico para las instituciones financieras. Es posible que dichas instituciones financieras ni siquiera conozcan todas las API de su infraestructura, lo que crea un punto ciego de control y seguridad. Esta falta de visibilidad puede ser uno de los factores clave que contribuyen al hecho de que los ataques de API a menudo no se detecten ni se notifiquen. El primer paso para proteger las API es detectarlas y catalogarlas de forma exhaustiva.

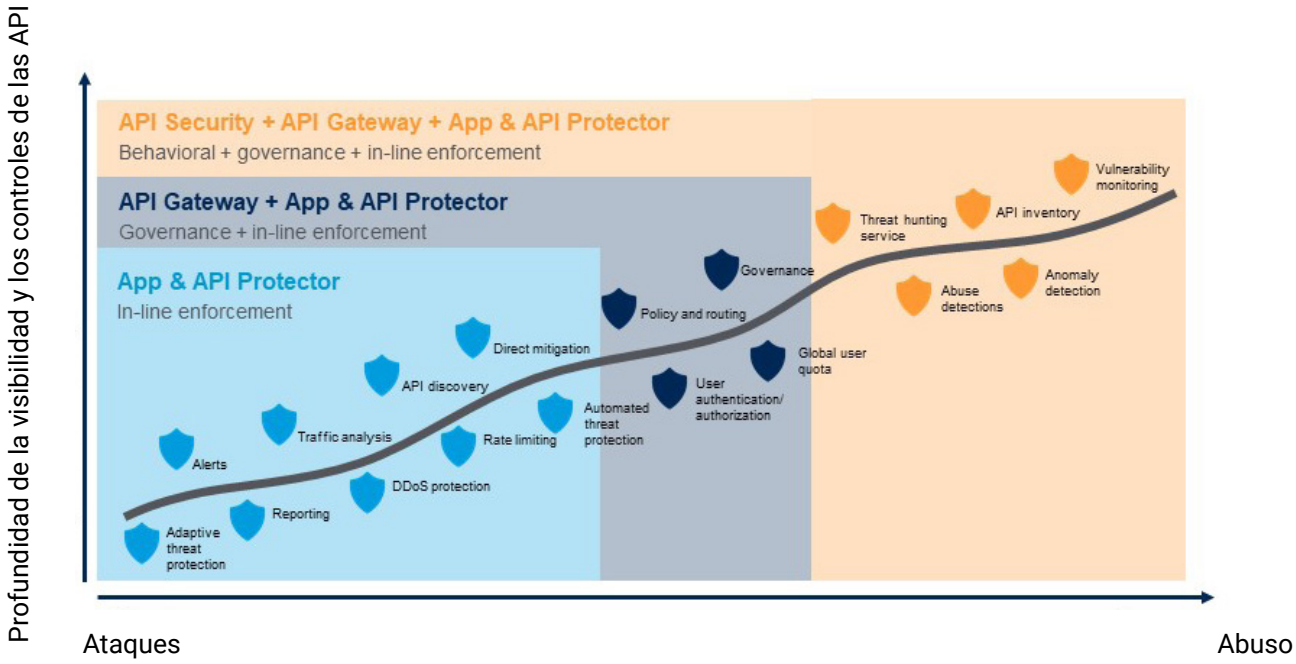
El impacto disruptivo de los ataques a las API

Las interrupciones en la disponibilidad de las aplicaciones web y las API pueden afectar de manera significativa a la satisfacción del cliente y a la fidelidad a la marca. Con la creciente adopción de un enfoque centrado en la digitalización, las API se han vuelto aún más esenciales para el éxito de las instituciones financieras, especialmente en el contexto de la banca abierta que han adoptado las empresas de tecnología financiera y los bancos tradicionales.

Crecimiento rápido del tráfico de API

El tráfico de API en el sector financiero ha experimentado un crecimiento rápido, con un volumen de tráfico que ha aumentado exponencialmente. Este crecimiento desafía la capacidad de los controles de seguridad para seguir el ritmo del cambiante panorama de las amenazas relacionadas con las API.

Los ataques de API evolucionan



Normativas y seguridad

Las instituciones financieras que aprovechan el potencial de las API y otras tecnologías innovadoras se encuentran en el cruce de caminos entre los objetivos de la política pública y los objetivos de estabilidad financiera. El importante papel que desempeñan las API en la mejora de los resultados de los clientes las ha convertido en el método de conectividad e intercambio de datos predeterminado en los entornos de servicios financieros modernos, y lo seguirán siendo en el futuro. Los objetivos generales son ampliar la gama de opciones financieras, fomentar una mayor competencia y accesibilidad, y promover la inclusión financiera. Los organismos reguladores de toda la región EMEA se esfuerzan por ampliar el alcance de los servicios financieros, lo que beneficiará tanto a los particulares como a las organizaciones.

El papel que desempeñan las normativas en la seguridad de las API

Normativas como la directiva PSD2 (y, pronto, la directiva PSD3) promueven la transparencia al exigir que las instituciones tradicionales compartan datos con entidades externas, priorizando la privacidad y la seguridad de los usuarios finales. Las instituciones financieras deben cumplir con estas normativas al mismo tiempo que buscan activamente la innovación.

Aunque las normativas promueven el uso compartido de los datos, también especifican cómo deben las organizaciones almacenar y proteger los datos. Las instituciones financieras necesitan un partner tecnológico que garantice el cumplimiento de las normativas sin obstaculizar la innovación. Dicho partner debe abordar las preocupaciones relativas a la calidad de las API y proporcionar a las autoridades las herramientas necesarias para evaluar las interfaces de API dedicadas de los bancos y otras entidades financieras.

Según la Autoridad Bancaria Europea, "La experiencia adquirida con la implementación de la directiva PSD2 pone de manifiesto la ausencia de un único estándar de API, lo que da como resultado diversas soluciones de API en toda la UE. Esto plantea importantes desafíos a los proveedores de servicios externos, ya que exige esfuerzos sustanciales para conectarse a las diferentes API de los proveedores de servicios de pago gestores de cuentas y adaptar las conexiones a la evolución de las API". Se espera que la directiva PSD3 incorpore las lecciones aprendidas con la directiva PSD2.

6 pasos para crear una estrategia de seguridad de API sólida

La estrategia de prevenir los ataques basados en API mediante la protección de terminales y la comprobación de credenciales ya no es suficiente. Hoy en día, una estrategia de seguridad de las API sólida debe incluir los seis pasos siguientes.

1. Colaboración con partners

Las instituciones financieras y sus partners de seguridad deben colaborar estrechamente y coordinar personas, procesos y tecnologías para establecer una defensa sólida contra los riesgos de seguridad de las API. Esta colaboración incluye a equipos de desarrollo, equipos de operaciones de redes y seguridad, equipos de gestión de identidades, responsables de los riesgos, arquitectos de seguridad y equipos jurídicos o de cumplimiento.

2. Detección y catalogación de API

El primer paso para proteger las API es detectarlas y catalogarlas en toda la organización. Este proceso permite a los ingenieros de seguridad comprender el alcance de la superficie de ataque y la posible exposición de la información confidencial.

3. Pruebas de vulnerabilidad y evaluación del riesgo

Una vez detectadas las API, las instituciones financieras deben realizar pruebas de vulnerabilidad y evaluaciones de riesgos para identificar y abordar las vulnerabilidades de forma oportuna. Este proceso debe integrarse en los ciclos de desarrollo y actualización de las API para garantizar una seguridad continua.

4. Implementación de la detección del comportamiento

Las protecciones de API son componentes esenciales del marco de seguridad general de las aplicaciones. La detección del comportamiento es una estrategia clave para evitar que se exploten las API vulnerables. Este enfoque implica la supervisión y el análisis continuos del comportamiento de las API para identificar posibles amenazas.

5. Priorización de los controles sobre los 10 principales riesgos según OWASP

Las instituciones financieras deben priorizar los 10 principales riesgos de seguridad de las API según el Proyecto Abierto de Seguridad de Aplicaciones Web (OWASP) para garantizar una protección completa. Estos controles cubren las vulnerabilidades y los vectores de ataque más críticos que afectan a las API.

OWASP API Top 10 coverage by Akamai

- **API1:2023 — Broken Object Level Authorization:** BOLA vulnerabilities can occur when a client's authorization is not properly validated to access specific object IDs.
- **API2:2023 — Broken Authentication:** BA refers to broad vulnerabilities in the authentication process, exposing the system to attackers that can exploit these weaknesses to compromise API object protection.
- **API3:2023 — Broken Object Property Level Authorization:** BOPLA is a security flaw where an API endpoint unnecessarily exposes more data properties than required for its function, neglecting the principle of least privilege.
- **API4:2023 — Unrestricted Resource Consumption:** This is a type of vulnerability, sometimes called API resource exhaustion, where APIs do not limit the number of requests or the volume of data they serve within a given time.
- **API5:2023 — Broken Function Level Authorization:** BFLA can occur when access control models for API endpoints are incorrectly implemented.
- **API6:2023 — Unrestricted Access to Sensitive Business Flows:** This risk arises when an API exposes critical operations like business logic without sufficient access control.
- **API7:2023 — Server Side Request Forgery:** SSRF allows an attacker to induce the server-side application to make HTTPS requests to an arbitrary domain of the attacker's choosing.
- **API8:2023 — Security Misconfiguration:** This refers to the improper setup of security controls, which can leave a system vulnerable to attacks.
- **API9:2023 — Improper Inventory Management:** This is a challenge for every organization managing APIs. API security solutions can protect known APIs, but unknown APIs — including deprecated, legacy, and/or outdated APIs — may be left unpatched and vulnerable to attack.
- **API10:2023 — Unsafe Consumption of APIs:** This refers to the risks associated with the use of third-party APIs without putting proper security measures in place.

6. Aprendizaje de los homólogos

Las instituciones financieras deben aprender de las lecciones que han extraído otras empresas del sector y compartir las prácticas recomendadas. La pertenencia al Centro de Análisis e Intercambio de Información sobre Servicios Financieros (FS-ISAC) permite a las instituciones financieras aprovechar su plataforma de inteligencia, sus recursos y su red de confianza en la que colaboran distintos expertos para ayudarles a anticipar, mitigar y responder a las ciberamenazas. Una comprensión clara de cómo otras organizaciones abordan los desafíos de seguridad de las API puede ayudar a mejorar las medidas de seguridad para el sector en su conjunto.

Conclusión

En esta era de rápida transformación digital y adopción generalizada de las API, que se diseñaron para facilitar una integración flexible, rápida y rentable en una amplia gama de software, dispositivos y fuentes de datos, proteger las API es de vital importancia para las instituciones financieras de EMEA. No obstante, la seguridad de las API representa un complejo juego de malabarismos en el que están implicadas varias características, funciones y exigencias del negocio. Ignorar la seguridad de las API puede acarrear graves consecuencias, como ciberataques, filtraciones de datos, infracciones de las normativas y daños a la reputación de una institución.

Nuestros datos indican que la funcionalidad de las API se encuentra entre los principales objetivos de los atacantes, cuyos métodos de ataque evolucionan y se adaptan continuamente. Por lo tanto, es imprescindible que la seguridad de las API se desplace hacia el Edge: la estrategia consiste en alejarla de la infraestructura de una organización y acercarla a los puntos de contacto digitales en los que los clientes interactúan con los datos y las aplicaciones. Este ajuste estratégico es crucial para garantizar una protección sólida de sus activos digitales.

Obtenga más información sobre Akamai para el sector de los servicios financieros. También puede hablar con su contacto de Akamai para obtener más información sobre este tema y cómo afecta a su organización.