Akamai

WHITEPAPER

API-Sicherheit im Open-Banking-Ökosystem

Innovation und Sicherheit für europäische Banken im digitalen Zeitalter

Zusammenfassung

Im Jahr 2023 verzeichneten Banken in Europa, dem Nahen Osten und Afrika (EMEA) eine erhebliche Rentabilität, die voraussichtlich auch 2024 anhalten wird. Programmierschnittstellen (APIs), die 31 % des gesamten Webtraffics ausmachen, waren maßgeblich an diesem Wachstum beteiligt, da sie verschiedene Services wie Banktransaktionen, Remote-Scheckeinzahlungen und GPS-gestützte Standorte von Geldautomaten sowie Services von Drittanbietern ermöglichten. Die rasche Einführung von APIs hat jedoch auch die Cyberbedrohungslandschaft erweitert und so Finanzinstitute zu umfassenden Investitionen in die Cybersicherheit veranlasst.

Die überarbeitete EU-Zahlungsdiensterichtlinie (PSD2) und die erwartete PSD3 haben eine entscheidende Rolle beim Datenaustausch zwischen traditionellen Banken und FinTech-Unternehmen gespielt. Technische Regulierungsstandards (RTS) sorgen für eine sichere API-Nutzung, die eine starke Kundenauthentifizierung (SCA) und gemeinsame, sichere und offene Kommunikationsstandards (SCA-RTS) umfasst. Die PSD2, die sich in erster Linie auf Zahlungen konzentriert, hat im Vereinigten Königreich den Begriff „Open Banking“ vorangetrieben, was den Austausch von Kundendaten betont und den Weg für umfassendere „Open Finance“-Lösungen ebnet. Das Herzstück dieser Open-Finance-Lösungen sind APIs.

Die laufende digitale Transformation in der Finanzdienstleistungsbranche im EMEA-Raum, die von APIs vorangetrieben wird, zeigt die Anpassungsfähigkeit und das Engagement der Branche für die Erfüllung der sich wandelnden Kundenanforderungen. Im Zuge dieser Transformation ist jedoch Wachsamkeit gefragt: Die Cybersicherheit muss gestärkt und Schwachstellen beseitigt werden, und es muss sichergestellt werden, dass die Vorteile digitaler Innovationen die allgegenwärtige Bedrohung durch Cyberangriffe überwiegen. McKinsey berichtet, dass große Banken planen, 14 % Ihres IT-Budgets für API-Programme zu verwenden. Dies spiegelt den Anstieg der API-Nutzung wider und führt zu erheblichen Investitionen in die Cybersicherheit. Finanzinstitute legen nun den Schwerpunkt auf den Schutz interner Systeme und die Sicherheit von Kundendaten und -Assets. Dabei legen sie den Schwerpunkt auf die Erkennung von Bedrohungen, Reaktionsstrategien und Zusammenarbeit, um Cyberrisiken effektiv zu bekämpfen.

Die wachsende Bedeutung von APIs

Der EMEA-Raum erlebt derzeit eine digitale Revolution, die auf dem Wunsch beruht, Finanzkunden effizientere und maßgeschneiderte Services und Produkte anzubieten. APIs spielen dabei eine zentrale Rolle, da sie Kunden, die auf Bankprodukte zugreifen, ein unvergleichliches Maß an Komfort, Geschwindigkeit und Sicherheit bieten. APIs ermöglichen es Drittanbieteranwendungen, sich mit den Tools, Services und Assets einer Bank zu verbinden, wodurch die Verbindungen für beide Parteien optimiert werden. Kunden profitieren nun von einer breiten Palette an Finanzaktivitäten, die das Kundenerlebnis verändert und die Finanzbranche in das digitale Zeitalter gebracht hat. APIs, die sich aus einfachen Kommunikationstools entwickelt haben, sind zum Rückgrat des Internettraffics geworden und unterstützen verschiedene Anwendungen.

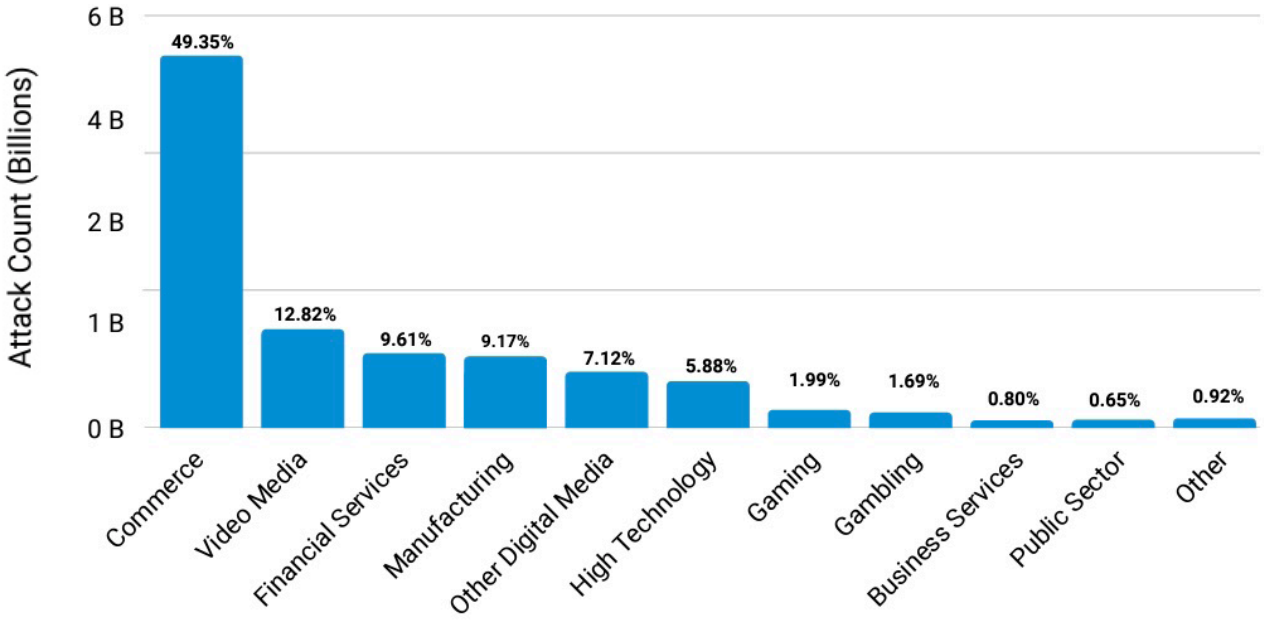
Laut Allied Market Research erreichte der europäische Open-Banking-Markt 2020 einen Wert von 6,14 Milliarden US-Dollar und dürfte mit einer jährlichen Wachstumsrate von 23,18 % bis 2030 auf 48,3 Milliarden US-Dollar wachsen. Initiativen wie das Open Bank Project unter der Leitung des Berliner TESOBE beschleunigen diese Umsetzung. Das Open Bank Project arbeitet mit mehr als 40 Banken weltweit zusammen und ermöglicht Banken, ihren Kunden Anwendungen und Services von Drittanbietern über eine offene API und einen App Store anzubieten. In Frankreich trägt die Konsolidierung von STET-API, die von der Verrechnungsstelle Systèmes technologiques d'échange et de traitement (STET) bereitgestellt wird, zur Umsetzung von Open-Banking-Transaktionen bei. APIs sorgen für eine rasante Neugestaltung der Finanzlandschaft im EMEA-Raum und der übrigen Welt.

API-Bedrohungen im EMEA-Raum

Die Finanzdienstleistungsbranche ist in der EMEA-Region zum drittgrößten Angriffsziel geworden: Auf sie zielten zwischen Januar 2022 und Juni 2023 fast 10 % der Angriffe auf Webanwendungen und APIs ab. Dies entspricht einer erstaunlichen Milliarde der insgesamt 11 Milliarden Webangriffe auf Branchen im EMEA-Raum, was von Q2 2022 bis Q2 2023 einem deutlichen Anstieg von 119 % im Jahresvergleich entspricht. Wenn wir noch genauer hinsehen, stellen wir fest, dass das Vereinigte Königreich mit 59,2 % der Angriffe auf Webanwendungen am häufigsten betroffen ist und mit 79 % das größte Wachstum im Jahresvergleich verzeichnet, gefolgt von den Niederlanden mit 16,2 % und Deutschland mit 10,7 %.

EMEA: Die am stärksten von Angriffen auf Webanwendungen & APIs betroffenen Branchen

1. Januar 2022 bis 30. Juni 2023



Die Finanzdienstleistungsbranche ist die am dritthäufigsten angegriffene Branche in EMEA

Wichtigste API-Sicherheitsrisiken

APIs können für eine Vielzahl von Sicherheitsrisiken anfällig sein, die zu Datenschutzverletzungen, unbefugtem Zugriff und anderen Formen des Missbrauchs führen können. Zu den wichtigsten API-Sicherheitsrisiken gehören Shadow-APIs, anfällige APIs, API-Missbrauch, das Teilen vertraulicher Informationen und Credential-Stuffing-Angriffe.

- **Shadow-APIs.** In vielen Finanzinstituten ist keine einzelne Person oder einzelnes Team für die Verwaltung aller APIs verantwortlich. Dieser Mangel an Überwachung ist eine erhebliche Sicherheitslücke. Die Erkennung und Katalogisierung von APIs im gesamten Unternehmen ist entscheidend für die Verwaltung und Sicherung dieser APIs. Es ist wichtig, die Lücke zwischen Entwicklern und Sicherheitsteams zu schließen und Shadow-APIs in ihrer Umgebung zu erkennen. Mit permanenter Erkennung bleiben Sie immer über neu entdeckte APIs oder Änderungen an bestehenden APIs auf dem Laufenden, sodass Shadow-APIs eliminiert werden können.

- **Anfällige APIs.** Sobald APIs erkannt wurden, müssen Finanzinstitute ihre Risikolage bewerten und Schwachstellen identifizieren, insbesondere bei APIs, die vertrauliche Daten verarbeiten. Dieser Schritt ist für eine effektive Priorisierung von Sicherheitsmaßnahmen unerlässlich.

- **API-Missbrauch.** Mit zunehmender Digitalisierung steigt auch die Zahl der Webangriffe im EMEA-Raum weiter an. Cyberkriminelle greifen unermüdlich APIs an, weshalb leistungsstarke Sicherheitsmaßnahmen unverzichtbar sind, um Missbrauch und Ausnutzung zu verhindern.

- **Übermäßiges Teilen vertraulicher Informationen.** Moderne Anwendungen teilen oft zu viele vertrauliche Daten, was einen neuen Angriffsvektor darstellt. Angreifer können den Traffic abfangen und so unbefugten Zugriff auf vertrauliche Informationen erlangen.

- **Credential-Stuffing-Angriffe.** Cyberkriminelle zielen auf Finanzinstitute ab, die APIs verwenden, um Credential-Stuffing-Angriffe zu automatisieren.

Herausforderungen bei der API-Sicherheit

API-Bestandsaufnahme

Laut einer kürzlich durchgeführten SANS-Umfrage ist der API-Bestand für Finanzinstitute nach wie vor ein kritisches Problem. Finanzinstituten sind möglicherweise nicht einmal alle APIs in ihrer Infrastruktur bekannt, was zu einem blinden Fleck bei Governance und Sicherheit führt. Dieser Mangel an Transparenz kann einer der Hauptfaktoren dafür sein, dass API-Angriffe oft unerkannt bleiben und nicht gemeldet werden. Der erste Schritt bei der Sicherung von APIs besteht darin, diese umfassend zu entdecken und zu katalogisieren.

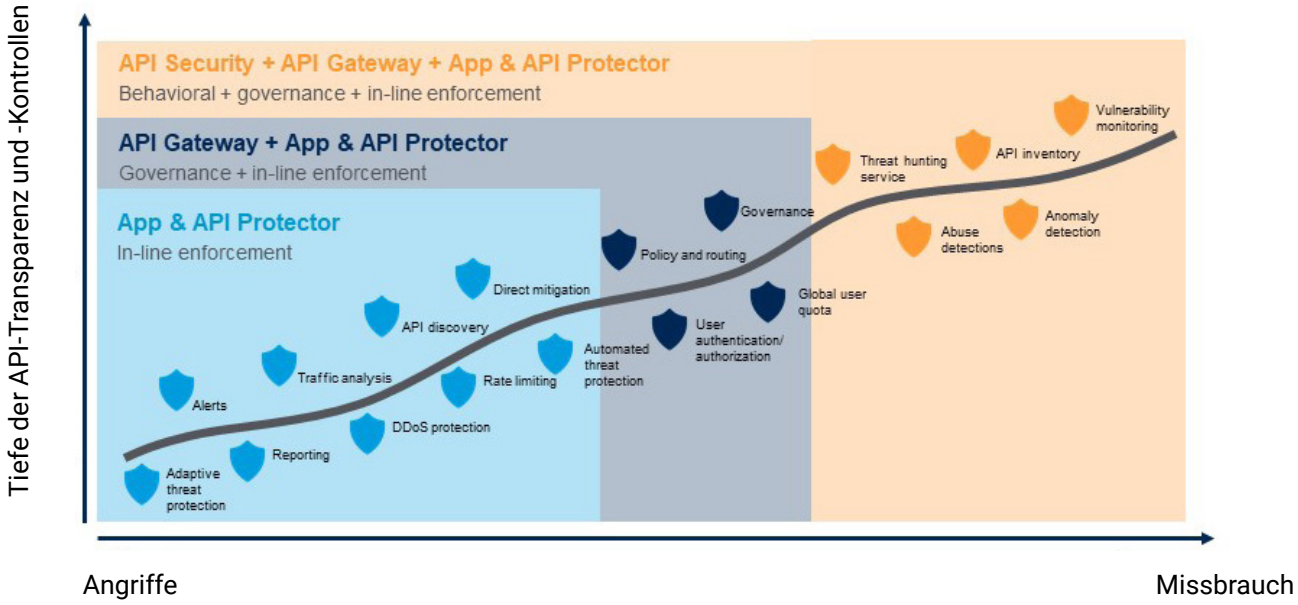
Die Auswirkungen disruptiver API-Angriffe

Unterbrechungen bei der Verfügbarkeit von Webanwendungen und APIs können die Kundenzufriedenheit und die Markentreue erheblich beeinträchtigen. Mit der zunehmenden Einführung eines digital fokussierten Ansatzes sind APIs für den Erfolg von Finanzinstituten noch wichtiger geworden, insbesondere im Kontext von Open Banking, auf das sowohl FinTech-Unternehmen als auch traditionelle Banken immer mehr setzen.

Schneller Anstieg des API-Traffics

Der API-Traffic im Finanzsektor hat rasant zugenommen, wobei das Trafficvolumen in den dreistelligen Bereich gestiegen ist. Dieses Wachstum stellt die Sicherheitskontrollen vor Herausforderungen, da sie mit der sich wandelnden API-Bedrohungslandschaft Schritt halten müssen.

API-Angriffe entwickeln sich weiter



Vorschriften und Sicherheit

Finanzinstitute, die die Leistungsfähigkeit von APIs und anderen innovativen Technologien nutzen, befinden sich an der Schnittstelle zwischen den Zielvorgaben der öffentlichen Politik und der Finanzstabilität. Die wichtige Rolle von APIs bei der Verbesserung der Kundenergebnisse hat sie zur Standardmethode für Konnektivität und Datenaustausch in modernen Finanzdienstleistungsumgebungen gemacht, und dies wird auch in Zukunft weiterhin der Fall sein. Übergeordnete Ziele sind die Erweiterung der Angebotspalette für Finanzdienstleistungen, die Förderung von mehr Wettbewerb und Zugänglichkeit sowie finanzieller Inklusion. Die Regulierungsbehörden im gesamten EMEA-Raum bemühen sich um eine Ausweitung des Angebots an Finanzdienstleistungen, von denen sowohl Einzelpersonen als auch Organisationen profitieren.

Die Rolle von Vorschriften bei der API-Sicherheit

Vorschriften wie die PSD2 (und demnächst die PSD3) fördern Transparenz, indem sie vorgeben, dass traditionelle Institutionen Daten mit externen Stellen austauschen und dabei den Daten, dem Datenschutz und der Sicherheit der Endnutzer Priorität einräumen. Die Finanzinstitute müssen diese Vorschriften einhalten und gleichzeitig aktiv an Innovationen arbeiten.

Vorschriften fördern zwar die gemeinsame Nutzung von Daten, legen aber auch fest, wie Unternehmen Daten speichern und schützen müssen. Finanzinstitute benötigen einen Technologiepartner, der die Einhaltung gesetzlicher Vorschriften gewährleistet, ohne dabei Innovationen zu behindern. Ein solcher Partner sollte Bedenken hinsichtlich der API-Qualität angehen und den Behörden Tools zur Bewertung dedizierter API-Schnittstellen von Banken und anderen Finanzinstituten zur Verfügung stellen.

Laut der Europäischen Bankenaufsichtsbehörde „zeigen die Erfahrungen mit der Umsetzung der PSD2, dass es keinen einheitlichen API-Standard gibt, was zu unterschiedlichen API-Lösungen in der gesamten EU führt. Dies stellt für Drittanbieter erhebliche Herausforderungen dar, da große Anstrengungen unternommen werden müssen, um sich mit den APIs verschiedener Account Servicing Payment Service Provider zu verbinden und diese Verbindungen an die sich entwickelnden APIs anzupassen.“ Es ist zu erwarten, dass die PSD3 die aus der PSD2 gewonnenen Erkenntnisse miteinbeziehen wird.

6 Schritte zum Aufbau einer zuverlässigen API-Sicherheitsstrategie

Die Strategie, API-basierte Angriffe durch das Überwachen von Endpunkten und das Überprüfen von Anmeldedaten zu verhindern, reicht heute nicht mehr aus. Eine zuverlässige API-Sicherheitsstrategie muss die folgenden sechs Schritte umfassen:

1. Zusammenarbeit mit Partnern

Finanzinstitute und ihre Sicherheitspartner müssen eng zusammenarbeiten, indem sie Mitarbeiter, Prozesse und Technologien aufeinander abstimmen, um eine solide Abwehr gegen API-Sicherheitsrisiken zu schaffen. Diese Zusammenarbeit umfasst Entwicklungsteams, Netzwerk- und Sicherheitsteams, Identitätsteams, Risikomanager, Sicherheitsarchitekten sowie Rechts- und Compliance-Teams.

2. Erkennung und Katalogisierung von APIs

Der erste Schritt bei der Sicherung von APIs besteht darin, diese unternehmensweit zu erkennen und zu katalogisieren. Dieser Prozess ermöglicht es Sicherheitstechnikern, den Umfang der Angriffsfläche und die potenzielle Offenlegung vertraulicher Informationen nachzuvollziehen.

3. Testen von Schwachstellen und Bewertung von Risiken

Sobald APIs erkannt wurden, müssen Finanzinstitute Schwachstellentests und Risikobewertungen durchführen, um Sicherheitslücken rechtzeitig zu erkennen und zu beheben. Dieser Prozess sollte in die Entwicklungs- und Upgradezyklen der APIs integriert werden, um kontinuierliche Sicherheit zu gewährleisten.

4. Implementierung einer Verhaltenserkennung

API-Schutzmaßnahmen sind wichtige Komponenten des gesamten Frameworks für Anwendungssicherheit. Die Verhaltenserkennung ist eine bedeutende Strategie, die verhindert, dass anfällige APIs ausgenutzt werden. Dieser Ansatz umfasst die kontinuierliche Überwachung und Analyse des API-Verhaltens, um potenzielle Bedrohungen zu identifizieren.

5. Priorisierung der OWASP Top 10-Kontrollen

Finanzinstitute sollten die Top 10 API-Sicherheitsrisiken des Open Worldwide Application Security Project (OWASP) priorisieren, um einen umfassenden Schutz zu gewährleisten. Diese Kontrollen decken die kritischsten Sicherheitslücken und Angriffsvektoren ab, die APIs betreffen.

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. Von Kollegen lernen

Finanzinstitute sollten voneinander lernen und Best Practices austauschen. Die Mitgliedschaft im Financial Services Information Sharing and Analysis Center (FS-ISAC) bietet Finanzinstituten Zugriff auf eine Informationsplattform, zahlreiche Ressourcen und ein vertrauenswürdiges Peer-to-Peer-Netzwerk von Experten, um Cyberbedrohungen zu antizipieren, abzuwehren und darauf zu reagieren. Ein klares Verständnis dafür, wie andere Unternehmen die Herausforderungen der API-Sicherheit bewältigen, kann dazu beitragen, die Sicherheitsmaßnahmen für die gesamte Branche zu verbessern.

Fazit

In einer Zeit der schnellen digitalen Transformation und der weit verbreiteten Einführung von APIs, um eine flexible, schnelle und kosteneffiziente Integration über ein breites Spektrum von Software, Geräten und Datenquellen hinweg zu ermöglichen, ist der Schutz von APIs für Finanzinstitute im EMEA-Raum von größter Bedeutung. Dennoch stellt die API-Sicherheit einen komplexen Balanceakt dar, der verschiedene Funktionen und Anforderungen des Unternehmens umfasst. Die Missachtung der API-Sicherheit kann schwerwiegende Folgen haben, darunter Cyberangriffe, Datenschutzverletzungen, Verstöße gegen gesetzliche Vorschriften und Rufschädigungen.

Unsere Daten zeigen, dass die API-Funktionalität zu den wichtigsten Angriffszielen für Cyberkriminelle zählt, die ihre Angriffsmethoden kontinuierlich weiterentwickeln und anpassen. Daher ist es unerlässlich, dass die API-Sicherheit sich an die Edge verlagert, sich von der Infrastruktur des Unternehmens entfernt und näher an die digitalen Touchpoints heranbewegt, an denen Kunden mit Daten und Anwendungen interagieren. Diese strategische Anpassung ist entscheidend, um einen leistungsstarken Schutz Ihrer digitalen Assets zu gewährleisten.

Erfahren Sie mehr über Akamai-Services im Finanzwesen. Oder wenden Sie sich an Ihren Ansprechpartner bei Akamai, um dieses Thema und seine Auswirkungen auf Ihr Unternehmen weiter zu besprechen.