API-SICHERHEITSSTUDIE 2024

Finanzwesen

API-Angriffe nehmen zu. Erfahren Sie, wie die Finanzdienstleistungsbranche dieses wichtige Sicherheitsproblem angeht – und was Ihr Unternehmen tun kann, um sich zu schützen.

Im letzten Jahr erlebten 88,7 % der Finanzdienstleistungsunternehmen einen Angriff auf die APIs, die ihre Daten verarbeiten und Kunden und Partner mit wichtigen Services verbinden. Mithilfe immer innovativerer Methoden können Bedrohungsakteure auf Daten in ungeschützten APIs zugreifen, um persönliche und finanzielle Informationen zu stehlen, einschließlich Kontostände und Transaktionsverläufe.

Sicherheitsteams bekommen das zu spüren und suchen nach Möglichkeiten, den Schutz zu verbessern. Aber die Fokussierung auf einen weiteren Angriffsvektor kann ernüchternd sein, insbesondere, wenn es sich um APIs handelt, deren fehlerhafte Konfigurationen oder unzulängliche Geschäftslogik sich leicht aufdecken und ausnutzen lässt.

Woher wissen wir das? Akamai hat mehr als 1.200 IT- und Sicherheitsexperten – von Chief Information Security Officers bis hin zu Experten für Anwendungssicherheit – befragt, um mehr über deren Erfahrungen mit API-Bedrohungen zu lernen.

Hier haben wir unsere Ergebnisse nach den Befragten aus der Finanzdienstleistungsbranche gefiltert, die als wichtigste Auswirkungen ihrer API-Sicherheitsvorfälle „Geldbußen von Regulierungsbehörden“ und „erhöhter Stress und/oder Druck für das Team oder die Abteilung“ angaben. Diese miteinander zusammenhängenden Konsequenzen sind leicht nachzuvollziehen, da Ihre Kollegen für die Behebung von API-Vorfällen mit Kosten von 832.800 $ rechnen – 40 % höher als der Durchschnitt in allen acht untersuchten Branchen und höher als in jeder anderen Branche.

Lesen Sie weiter und informieren Sie sich über die Lage in Ihrer Branche mit der API-Sicherheitsstudie 2024.

Die Transparenz nimmt ab, die Angriffe häufen sich

84 % der Unternehmen aller Branchen haben API-Sicherheitsvorfälle erlebt, doch Finanzdienstleister waren mit 88,7 % überdurchschnittlich häufig betroffen. Ihre Kollegen haben zwei wichtige Schwachstellen identifiziert, die diese Angriffe begünstigen: Netzwerk-Firewalls, die Bedrohungen nicht erkennen (26,5 %), und Schwachstellen in APIs in generativen KI-Tools wie große Sprachmodelle (LLMs) (23,2 %).

Trotz zunehmender Beweise für API-Bedrohungen – von häufigen Vorfällen bis hin zu hohen Kosten für die Behebung von Problemen und Geldstrafen – deuten unsere Ergebnisse darauf hin, dass viele Finanzdienstleister die API-Sicherheit noch nicht zu ihrer obersten Priorität gemacht haben. Tatsächlich befindet sich die API-Sicherheit mit 18,5 % nur auf Platz neun der Prioritäten im Bereich Cybersicherheit für das kommende Jahr.

Die Unterscheidung zwischen echten und schadhaften oder betrügerischen API-Aktivitäten stellt für den Finanzsektor eine Herausforderung dar, insbesondere wenn es um die Sichtbarkeit von mit APIs verbundenen Risiken geht. Während 73,5 % Ihrer Kollegen angeben, dass sie eine vollständige Übersicht ihrer APIs haben, wissen nur 28,5 % dieser Teilmenge, welche APIs vertrauliche Daten zurückgeben – einschließlich personenbezogener Daten (PII) sowie Daten, die von der Kredithistorie von Karteninhabern bis hin zu den Finanzdaten von großen Geschäftskunden reichen.

88,7 % der Finanzdienstleister haben in den letzten 12 Monaten einen API-Sicherheitsvorfall erlebt

Nur 28,5 % der Finanzdienstleister mit vollständigen API-Bestandsaufnahmen wissen, welche ihrer APIs sensible Daten zurückgeben

832.800 $ = die finanziellen Folgen von API-Sicherheitsvorfällen, die bei Finanzdienstleistern in den letzten 12 Monaten aufgetreten sind

Die drei wichtigsten Folgen

1. **Erhöhter Stress und/oder Druck** auf das Sicherheitsteam
2. **Geldbußen** von Regulierungsbehörden
3. **Verlust von Vertrauen** und Rufschädigung

Quelle:
Akamai, „API-Sicherheitsstudie“, 2024.

Akamai

Stellen Sie sich vor, was mit einer Shadow-API geschehen kann, die von einer Abteilung oder Tochtergesellschaft eines Finanzdienstleisters ohne Überwachung und ohne Zusammenarbeit mit den zentralen IT- oder Sicherheitsteams des Unternehmens bereitgestellt wird. Diese API könnte:

- so konzipiert sein, dass Transaktionsdaten von Kunden ohne ordnungsgemäße Autorisierungskontrollen ausgegeben und nicht ausreichend auf Fehlkonfigurationen getestet werden
- durch eine neue Version ersetzt, aber nicht deaktiviert worden sein, sodass über das Internet nach wie vor ein Zugriff möglich ist
- von herkömmlichen Tools unbemerkt bleiben, die nicht in der Lage sind, nicht verwaltete APIs zu erkennen
- von Cyberkriminellen ausgenutzt werden, die auf die Konten echter Kunden zugreifen, um ihre Assets zu stehlen

Dieses Szenario ist nicht nur hypothetisch. Laut der Studie „Risk Solutions True Cost of Fraud™“ von LexisNexis® aus dem Jahr 2023 lassen sich 50 % der aus Betrug resultierenden Verluste auf Missbrauch im Zusammenhang mit der Eröffnung neuer Konten zurückführen, bei dem Betrüger APIs verwenden können, um eine Vielzahl von Konten zu eröffnen. Darüber hinaus spiegelt unser Szenario wider, was IT- und Sicherheitsexperten in der Praxis als Hauptursachen für API-Vorfälle anführen.

Auswirkungen von API-Vorfällen auf Compliance, Kosten und Mitarbeiterbelastung

Laut dem im Mai 2024 erschienenen Gartner® Market Guide für API-Schutz* zeigen aktuelle Daten, dass eine durchschnittliche API-Verletzung zu mindestens zehnmal mehr geleakten Daten führt als eine durchschnittliche Sicherheitsverletzung. Es ist also kein Wunder, dass die weithin angewendete PCI DSS v4.0-Verordnung zusätzliche Anforderungen an die API-Sicherheit stellt. Der Standard erfordert nun, dass Unternehmen ihren API-Code vor der Veröffentlichung überprüfen, regelmäßig auf Schwachstellen testen und die sichere Verwendung von API-basierten Komponenten bestätigen. Dies ist besonders wichtig in einer Branche, in der APIs täglich Millionen von Finanztransaktionen ermöglichen.

Verlorenes Vertrauen bei Aufsichtsbehörden kann zu verstärkten Prüfungen und damit zu mehr Arbeit für enorm beanspruchte Teams führen, die Mühe haben, Compliance-Anforderungen zu erfüllen. Auch hohe Geldstrafen können eine Folge sein.

Mit Blick darauf ist klar, dass Finanzdienstleister sich über die Folgen von API-Bedrohungen im Klaren sind. Erstmalig haben wir die Teilnehmer in den drei untersuchten Ländern gebeten, die geschätzten finanziellen Folgen von API-Sicherheitsvorfällen aus den letzten 12 Monaten mitzuteilen.

	Finanzwesen	Durchschnitt aller Branchen
USA	**832.800 $**	**591.404 $**
Vereinigtes Königreich	**297.189 £**	**420.103 £**
Deutschland	**604.405 €**	**403.453 €**

Q3. Wie hoch sind insgesamt die geschätzten finanziellen Auswirkungen von API-Sicherheitsvorfällen, die Sie erlebt haben? Bitte berücksichtigen Sie alle damit verbundenen Kosten wie Systemreparaturen, Ausfallzeiten, Anwaltskosten, Bußgelder und andere damit verbundene Kosten.

* Gartner, Market Guide für API-Schutz, 29. Mai 2024. GARTNER ist eine eingetragene Marke und Dienstleistungsmarke von Gartner, Inc. bzw. seinen Vertragspartnern in den USA und weltweit und wird hierin mit Genehmigung verwendet. Alle Rechte vorbehalten.

Risiken und Stress durch proaktive API-Sicherheit reduzieren

API-Angriffe auf Finanzdienstleister nehmen an Umfang, Ausmaß, Raffinesse und Kosten zu. Dies betrifft auch GenKI-gestützte Bot-Angriffe, die sich schnell anpassen, um herkömmliche API-Sicherheitstools und andere Netzwerkschutzmaßnahmen zu umgehen. Viele Sicherheitsteams in Ihrer Branche erleben diese Bedrohungen an vorderster Front und spüren die Folgen sowohl finanziell als auch bei ihren Mitarbeitern. Doch auch wenn Unternehmen die Bedeutung von API-Bedrohungen verstehen, bleibt die Frage offen: Was können wir dagegen tun?

Wenn Sie jetzt Maßnahmen ergreifen, um Ihre APIs – und die über diese ausgetauschten Daten – besser zu schützen, kann Ihr Unternehmen seine Einnahmen sichern und die Belastungen für Sicherheitsteams verringern. Diese Schritte und der Aufbau von Wissen in Ihren Teams über moderne API-Bedrohungen und die Kompetenzen, die zum Schutz dagegen benötigt werden, können dazu beitragen, das hart verdiente Vertrauen von Kunden und Vorstandsmitgliedern zu erhalten.

Um den vollständigen Bericht zu lesen und mehr über Best Practices für Schutz und Transparenz von APIs zu erfahren, laden Sie die **API-Sicherheitsstudie 2024** herunter.

Wünschen Sie ein Gespräch über Ihre spezifischen Herausforderungen sowie darüber, wie Akamai Ihnen helfen kann?

Individuelle Demo für Akamai API Security anfragen

Die Lösungen von Akamai unterstützen Unternehmen dabei, die Risiken zu reduzieren, die mit den in diesem Artikel beschriebenen Bedrohungen verbunden sind:

- Akamai API Security erkennt Ihre APIs, versteht ihr Risikopotenzial, analysiert ihr Verhalten und hält Bedrohungen von Ihrem Unternehmen fern.
- Akamai Account Protector unterstützt Sie dabei, die missbräuchliche Erstellung von Konten zu verhindern, indem es das Nutzerverhalten in Echtzeit überwacht und sich an sich ändernde Risikoprofile anpasst.

Akamai

Akamai schützt die Anwendungen, die Ihr Unternehmen vorantreiben, an jedem Interaktionspunkt – ohne die Performance oder das Kundenerlebnis zu beeinträchtigen. Unsere globale Plattform liefert Skalierbarkeit sowie transparente Einblicke in Bedrohungen. So können wir mit Ihnen gemeinsam Bedrohungen erkennen und abwehren, damit Sie Markenvertrauen aufbauen und Ihre Vision umsetzen können. Möchten Sie mehr über die Cloud-Computing-, Sicherheits- und Bereitstellungslösungen von Akamai erfahren? Dann besuchen Sie uns unter akamai.com und akamai.com/blog oder folgen Sie Akamai Technologies auf X und LinkedIn. Veröffentlicht: 03/25.