API-SICHERHEITSSTUDIE 2024

# Einzelhandel und E-Commerce

## So bewerten Ihre Branchenkollegen die wachsenden Bedrohungen für APIs

APIs, die für digitale Initiativen von Einzelhandels- und E-Commerce-Unternehmen maßgeblich sind, sind zur Zielscheibe für Angriffe geworden. Cyberkriminelle verwenden immer raffiniertere Methoden, um auf Daten in ungeschützten APIs zuzugreifen und Kreditkartendaten zu stehlen, Geld von Treueprogrammen abzubuchen, Credential-Stuffing-Angriffe durchzuführen und vieles mehr. 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 CISOs bis hin zu AppSec-Mitarbeitern – befragt, um mehr über deren Erfahrungen mit API-Bedrohungen zu erfahren.

Diese Übersicht filtert die Ergebnisse für Ihre Branche, für die 68 % der Befragten in den vergangenen 12 Monaten API-Sicherheitsvorfälle gemeldet haben. Welche Auswirkungen wurden beobachtet? Zu den häufigsten Antworten Ihrer Kollegen zählten ein steigender Stresspegel für ihre Teams sowie beschädigte Glaubwürdigkeit bei Führungskräften und Vorständen. Angesichts der berichteten Kosten in Höhe von 526.531 US-Dollar, die laut Einzelhandels- und E-Commerce-Experten für die Behebung von API-Vorfällen anfielen, ist diese Antwort nachvollziehbar.

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

## Immer mehr Angriffe bei schlechterer Transparenz

Während bei einer deutlichen Mehrheit der Befragten in Einzelhandels- und E-Commerce-Unternehmen API-Sicherheitsvorfälle aufgetreten sind, lag der Branchendurchschnitt mit 68 % unter dem Anteil von 84 %, der für die Gesamtheit aller acht befragten Branchen zu verzeichnen war. Zugleich zählen für Ihre Branchenkollegen in den nächsten 12 Monaten der „Schutz vor GenKI-gestützten Angriffen“ sowie der „Schutz von APIs vor Cyberkriminellen“ zu den wichtigsten Sicherheitsprioritäten.

Gibt es einen Zusammenhang zwischen der Priorisierung von APIs und der Verhinderung von Angriffen? Möglicherweise haben Sicherheitsteams von Einzelhandels- und E-Commerce-Unternehmen die Bedeutung des API-Schutzes erkannt und ihre Maßnahmen haben zur Reduzierung von Vorfällen beitragen. Unsere Ergebnisse deuten jedoch auch darauf hin, dass diese Teams nicht jede Instanz von API-Missbrauch erkennen.

Die Unterscheidung zwischen echten und schadhaften oder betrügerischen API-Aktivitäten ist für Handels- und E-Commerce-Unternehmen nach wie vor eine Herausforderung. Die Risikotransparenz ist ebenfalls eine Herausforderung. 67 % Ihrer Branchenkollegen geben an, dass sie über vollständige API-Bestandsaufnahmen verfügen. Dennoch wissen in dieser Gruppe nur *29 %*, welche ihrer unzähligen APIs vertrauliche Daten zurückgeben. Dazu gehören auch personenbezogene Daten (PII) oder Kreditkartendaten.

Stellen Sie sich vor, was mit einer API geschehen kann, die von einer Geschäftseinheit ohne Überwachung und ohne Zusammenarbeit mit den zentralen IT- oder Sicherheitsteams des Händlers bereitgestellt wird. Diese API könnte:

- so konzipiert sein, dass Kundendaten ohne ordnungsgemäße Autorisierungskontrollen ausgegeben und nicht ausreichend auf Fehlkonfigurationen getestet werden
- durch eine neue Version ersetzt aber nicht deaktiviert worden sein, so dass 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 Betrügern ausgenutzt werden, die auf Treuekonten echter Kunden zugreifen und Bargeld auszahlen

**68 %** der Einzelhandels- und E-Commerce-Unternehmen haben in den letzten 12 Monaten einen API-Sicherheitsvorfall erlebt.[1]

**Nur 29 %** der Einzelhandels- und E-Commerce-Unternehmen mit vollständigen API-Bestandsaufnahmen wissen, welche ihrer APIs sensible Daten zurückgeben.[1]

**526.531 US-Dollar** = die finanziellen Folgen von API-Sicherheitsvorfällen, die bei Einzelhandels- und E-Commerce-Unternehmen in den letzten 12 Monaten aufgetreten sind[1]

### Die drei wichtigsten Folgen[1]

1. **Erhöhter Stress** und/oder Druck für das Team oder die Abteilung
2. **Anfallende Kosten** für die Behebung des Problems
3. **Rufschädigung unserer Abteilung** bei Führungskräften und/oder dem Vorstand

**44 %** der Webangriffe auf Handelsorganisationen zielten auf APIs ab.[2]

Quellen:
1. Akamai, „API-Sicherheitsstudie“, 2024.
2. Akamai State of the Internet (SOTI), „Verborgen im Schatten: Angriffstrends bringen API-Bedrohungen ans Licht“, 2024.

Akamai

Dieses Szenario ist nicht nur hypothetisch. Laut der Studie von LexisNexis® Risk Solutions True Cost of Fraud™ 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.

**Hauptursachen für API-Vorfälle, die von Sicherheitsteams im Einzelhandel/E-Commerce angegeben werden**

1. APIs in generativen KI-Tools, z. B. LLMs: **24,7 %**
2. API hatte unbeabsichtigte Verbindung mit dem Internet: **24,0 %**
3. API-Fehlkonfiguration: **22,0%**
4. Web Application Firewall hat sie nicht erfasst: **21,3%**
5. API-Gateway hat sie nicht erfasst: **20,7%**
6. Sicherheitsanfälligkeit aufgrund von API-Programmierfehlern: **20,0%**
7. Bekanntes technisches Tool/Service: **20,0 %**
8. Netzwerk-Firewall hat sie nicht erfasst: **18,7%**
9. Schwachstellen bei Autorisierung: **17,3%**
10. Aus dem Internet heruntergeladene Softwarelösung: **16,7%**
11. Fehlende API-Authentifizierungskontrollen: **16,0%**
12. Mid-Tier-Softwarelösung: **14,7 %**
13. Nicht verwaltete APIs (z. B. Zombie): **13,3 %**

*F: Was sind Ihrer Meinung nach die Ursachen für API-Sicherheitsvorfälle in Ihrem Unternehmen? (Bis zu 3 auswählen), n = 1.207*

## Auswirkungen von API-Vorfällen auf Compliance, Kosten und Mitarbeiterbelastung

Laut dem Gartner® Market Guide for API Protection vom Mai 2024 zeigen aktuelle Daten, dass ein durchschnittlicher API-Verstoß zu mindestens zehnmal mehr geleakten Daten führt als ein gewöhnlicher Sicherheitsverstoß.[3] Es ist daher nicht verwunderlich, dass Anforderungen zur API-Sicherheit in die weithin angewendete PCI DSS v4.0-Verordnung aufgenommen wurden. Unternehmen – und deren Aufsichtsbehörden – müssen wissen, welche Arten von Daten nicht nur über ihre eigenen APIs, sondern auch über die APIs ihrer Partner und Lieferanten übertragen werden. Dies stellt eine weitere Herausforderung für die Kontrolle von Risiken Dritter für E-Commerce dar.

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 auf die Kosten ist klar, dass Einzelhandels- und E-Commerce-Unternehmen sich über die finanziellen 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.

[3] 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.

| | Einzelhandel/E-Commerce | Durchschnitt für alle Branchen |
|---|---|---|
| USA | **526.531 $** | **591.404 $** |
| Vereinigtes Königreich | **258.815 £** | **420.103 £** |
| Deutschland | **348.467 €** | **403.453 €** |

*F: 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. n = 1.207*

Auch wenn die finanziellen Auswirkungen beträchtlich sind, haben die Befragten deutlich gemacht, dass zu den negativen Folgen nicht nur anfallende Kosten gehören. Die wichtigsten Auswirkungen von API-Sicherheitsvorfällen sind anderer Natur. Die Befragten aus der Einzelhandels- und E-Commerce-Branche haben insbesondere auf die persönlichen Belastungen hingewiesen: Stress und Druck für ihre Teams.

**Die fünf wichtigsten Auswirkungen von API-Sicherheitsvorfällen für Einzelhandels- und E-Commerce-Unternehmen**

1. Erhöhter Stress und/oder Druck für das Team oder die Abteilung: **28,7 %**
2. Kosten für die Behebung des Problems: **28,0 %**
3. Rufschädigung unserer Abteilung bei Führungskräften und/oder dem Vorstand: **25,3 %**
4. Verstärkte interne Prüfung unseres Teams/unserer Abteilung durch das Unternehmen: **23,3 %**
5. Geldbußen von Regulierungsbehörden: **25,3 %**

*F: Welche Kosten und/oder Auswirkungen hatten API-Sicherheitsvorfälle auf Ihr Unternehmen, falls zutreffend? (Bis zu 3 auswählen), n = 1.207*

## Nächste Schritte: Risiken und Stress durch proaktive API-Sicherheit reduzieren

API-Angriffe auf Einzelhandels- und E-Commerce-Unternehmen werden immer umfassender, weitreichender und raffinierter. 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. Gleichzeitig wird das hart erarbeitete Vertrauen von Vorständen und Kunden gewahrt. Zu diesen Schritten gehören der Aufbau von Wissen in Ihrem Teams über moderne API-Bedrohungen und die Kompetenzen, die zum Schutz dagegen benötigt werden.


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**

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. Gemeinsam mit Ihnen können wir auf diese Weise 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 (ehemals Twitter) und LinkedIn. Veröffentlicht: November 2024.