API-SICHERHEITSSTUDIE 2024

Versicherungsbranche

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

Wenn sich ein Unglück ereignet – von Autounfällen bis hin zu beschädigter Geschäftsausstattung – verlassen sich die Versicherungsnehmer auf digitale Dienste, um Ansprüche einzureichen und Unterstützung von ihren Versicherungsanbietern zu erhalten. Hinter diesen Diensten verarbeiten die APIs von Versicherungsunternehmen sensible Informationen, die die Lebensgeschichte eines Versicherungsnehmers darstellen, die in Datenform erzählt wird.

In einer Branche, in der das Kundenvertrauen von größter Bedeutung ist, stehen Versicherungsunternehmen vor einer wachsenden Herausforderung für die Sicherheit: API-Schwachstellen.

In einer groß angelegten Umfrage von Akamai berichteten 76,7 % der Versicherungsexperten von API-Sicherheitsvorfällen innerhalb der letzten zwölf Monate. Die finanziellen Auswirkungen sind beträchtlich: Allein in den USA geben Versicherungsunternehmen durchschnittlich 625.634 USD für die Bewältigung solcher Vorfälle aus.

Am besorgniserregendsten sind jedoch die Auswirkungen auf das Geschäft: An zweiter Stelle nach API-Angriffen steht „Verlust von Kunden-Goodwill und Abwanderung“ (28 %), was die Bedenken der Versicherungsunternehmen betrifft. Auf einem wettbewerbsorientierten Markt, auf dem Kunden problemlos den Anbieter wechseln können, kann eine solche Rufschädigung über die unmittelbaren Kosten hinaus anhaltende Auswirkungen haben.

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

Obwohl Angriffe zunehmen, bleibt die Sichtbarkeit nach wie vor eine der wichtigsten Herausforderungen

Die finanziellen Kosten von API-Angriffen sind für Versicherungsunternehmen beträchtlich. Die Kosten in den USA (625.634 USD) übersteigen sogar den branchenübergreifenden Durchschnitt (591.404 USD). Was sorgt für den Anstieg dieser Vorfälle?

Nach Angaben der Sicherheitsteams der Versicherungsbranche sind die wichtigsten Ursachen:

1. nicht verwaltete APIs, z. B. ruhende oder Zombie-APIs (22 %)
2. aus Versehen mit dem Internet verbundene APIs (21,3 %)
3. herkömmliche Tools zum Schutz von APIs, die keine Bedrohungen erkennen (20 %)
4. Schwachstellen bei Autorisierung (19,3 %)
5. API-Fehlkonfigurationen (18,7 %)

Viele Unternehmen sind sich der Ursachen ihrer API-Angriffe bewusst, haben aber keinen Einblick in einen wichtigen Risikoindikator: Die Fähigkeit einer API, sensible Daten beim Aufruf zurückzugeben. 56,7 % der Versicherungsunternehmen geben an, dass sie über einen vollständigen Bestand ihrer APIs verfügen (unter dem branchenübergreifenden Durchschnitt von 69,7 %), aber nur 20,7 % wissen, welche APIs sensible Daten zurückgeben.

Diese Sichtbarkeitslücke hat erhebliche Auswirkungen auf Compliance und Sicherheit in einer Branche, in der streng regulierte personenbezogene und finanzielle Daten verarbeitet werden.

76,7 % der Versicherungsunternehmen haben in den letzten zwölf Monaten einen API-Vorfall erlebt.

Nur 20,7 % der Versicherungsunternehmen mit vollständigen API-Beständen wissen, welche APIs vertrauliche Daten zurückgeben

625.634 USD = finanzielle Auswirkungen von API-Sicherheitsvorfällen für US-Versicherungsunternehmen in den letzten zwölf Monaten

Die drei wichtigsten Folgen

1. **Verlust von Kunden-Goodwill und Abwanderung (28 %)**
2. **Beschädigter Ruf der Abteilung bei Führungskräften (25,3 %)**
3. **Kosten für die Behebung des Problems (24,7 %)**

Quelle:
Akamai, API-Sicherheitsstudie, 2024

Akamai

Wir haben verschiedene Trends festgestellt, die den Schutz von APIs erschweren:

- **Kontinuierliche API-Verbreitung**: Mit jeder digitalen Initiative vermehren sich APIs und entwickeln sich ständig weiter, was eine genaue Bestandsaufnahme erschwert.
- **Inkonsistente Standards**: Viele Versicherer verfügen über mehrere Entwicklungsteams, die in Silos über verschiedene Geschäftseinheiten hinweg arbeiten, ohne ein zentrales Playbook für sicheres Design zu verwenden.
- **Unsichtbare Risiken**: APIs übertragen vertrauliche Daten von Versicherungsnehmern, aber die meisten Unternehmen können nicht erkennen, welche spezifischen APIs vertrauliche Informationen zurückgeben.

Stellen Sie sich vor, was mit einer API geschehen kann, die von einer Abteilung ohne angemessene Überwachung durch ein Sicherheitsteam eingesetzt wird. Diese API wurde möglicherweise so entwickelt, dass Datensätze ohne ordnungsgemäße Kontrollen freigegeben oder nach Systemaktualisierungen aktiv bleiben, wodurch potenzielle Risikopunkte für sensible Kundendaten geschaffen wurden.

Auswirkungen von API-Vorfällen auf Compliance, Kundenvertrauen und Mitarbeiterbelastung

Es ist kein Wunder, dass Versicherungsunternehmen sich der finanziellen Folgen von API-Bedrohungen voll und ganz bewusst sind. In unserer Umfrage haben wir die Teilnehmer gebeten, die geschätzten Kosten von API-Sicherheitsvorfällen aus den letzten zwölf Monaten mitzuteilen.

	Versicherungsbranche	Durchschnitt aller Branchen
USA	625.633,70 $	591.404,01 $
Vereinigtes Königreich	493.000,50 £	420.103,18 £
Deutschland	373.918,72 €	403.453,26 €

Auch wenn die finanziellen Auswirkungen beträchtlich sind, haben die Befragten deutlich gemacht, dass die negativen Folgen eine Mischung aus Umsatzeinbußen und Rufschädigung sind. Die wichtigsten Auswirkungen von API-Sicherheitsvorfällen sehen ihrer Erfahrung nach wie folgt aus:

- 28 % haben „Verlust von Kunden-Goodwill und Abwanderung“ angegeben
- 25,3 % haben „Beschädigter Ruf des Teams bei Führungskräften und Vorstand“ angegeben
- 24,7 % haben „Kosten für die Behebung des Problems“ angegeben

Risiken und Stress durch proaktive API-Sicherheit reduzieren

API-Angriffe auf Versicherungsunternehmen 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. 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 Sie unterstützen 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**: 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: Mai 2025.