API-SICHERHEITS-STUDIE 2024

Wie sich API-Vorfälle auf Sie und Ihr Team auswirken

Akamai

Eine Partner-Veröffentlichung von
Akamai; Bericht „State of the Internet (SOTI)“

Inhalt

Zusammenfassung

Die bereits im dritten Jahr durchgeführte API-Sicherheitsstudie (ehemals API Security Disconnect Report) untersucht den Stand des API-Schutzes basierend auf einer Befragung von 1.207 Experten aus den USA, dem Vereinigten Königreich und (2024 neu) Deutschland. Die Studie untersucht, wie Unternehmen API-Sicherheitsereignisse erleben – Häufigkeit, Ursachen und Auswirkungen – und wie Sicherheitsabteilungen APIs als Angriffsvektor behandeln.

Um ein vollständiges Bild zu erhalten, haben wir wie folgt ausgewählt:

CISOs, CIOs, CTOs, leitende Sicherheitsexperten und AppSec-Teammitglieder aus Unternehmen mit einer Größe von unter 500 bis über 1.000 Mitarbeitern

Acht Branchen: Finanzdienstleistungen, Einzelhandel/E-Commerce, Gesundheitswesen, Behörden/öffentlicher Sektor, verarbeitendes Gewerbe, Energie/Versorgungsunternehmen und (neu im Jahr 2024) Automobil- und Versicherungswesen

Einführung

APIs werden oft als *aufkommende* Angriffsvektoren angesehen, selbst wenn Daten zeigen, dass sie häufig und schadensanfällig sind. Folgende Statistiken sind hierzu interessant:

- Laut einem kürzlich veröffentlichten „State of the Internet"-Bericht (SOTI) von Akamai wurden von Januar 2023 bis Juni 2024 108 Milliarden API-Angriffe registriert.
- „Aktuelle Daten zeigen, dass ein durchschnittlicher API-Vorfall zu mindestens zehnmal mehr geleakten Daten als eine durchschnittliche Sicherheitsverletzung führt", so der Gartner® Market Guide for API Protection vom Mai 2024.*
- Die Angriffe nehmen ebenfalls zu. Der SOTI-Bericht sagt zudem aus, dass die Angriffe auf Webanwendungen und APIs zwischen dem 1. Quartal 2023 und dem 1. Quartal 2024 um 49 % gestiegen sind.

Viele APIs sind unzureichend geschützt, was sie zu einem attraktiven und kostengünstigen Angriffspunkt für Cyberkriminelle macht.

Diese Zunahme ist nicht überraschend. Hinter den Kulissen erleichtern APIs die Kommunikation und den Datenaustausch zwischen fast allen Technologien, die Ihre digitalen Initiativen unterstützen: GenKI-Tools, kundenorientierte Apps, Cloud-Services und vieles mehr. Viele APIs sind jedoch unzureichend geschützt – unabhängig davon, ob sie ohne Authentifizierung erstellt, falsch konfiguriert oder völlig vergessen wurden – und somit ein attraktiver und kostengünstiger Angriffspunkt für Cyberkriminelle. Sie müssen nur eine anfällige API finden und erhalten *direkten* Zugriff auf alle Daten, die beim Aufruf zurückgegeben werden, also Tausende von Datensätzen.

Unsere Untersuchungen haben gezeigt, dass API-Sicherheit noch nicht zu einem Schlüsselelement einer umfassenden Sicherheitsstrategie geworden ist. Unternehmen behandeln API-Bedrohungen meist als neu, obwohl die Angriffsdaten – sowie die finanziellen Auswirkungen und der Stress für Teams, die in unserer Studie beschrieben wurden – zeigen, dass sie zahlenmäßig wachsen und oft erfolgreich sind. Unsere Ergebnisse aus dem Jahr 2024 bieten einen Einblick in die Auswirkungen von API-Sicherheitsvorfällen auf Ihre Kollegen und deren Abteilungen. Wir hoffen, dass diese Daten Ihrem eigenen Team helfen werden, API-Schutzmaßnahmen besser zu bewerten und bei Bedarf zu verbessern.

Zusammengefasste Ergebnisse: API-Vorfälle beeinträchtigen das Geschäft und verursachen Stress für Teams

Die Ergebnisse unserer Studie aus dem Jahr 2024 haben gezeigt, dass APIs Angriffspunkte sind, die stetig zunehmen und für Teams erhebliche Sicherheitsprobleme mit sich bringen. Unsere Befragten zeigten einen bemerkenswerten Konsens in Bezug auf Folgendes:

- den Anstieg von API-Sicherheitsvorfällen in drei aufeinanderfolgenden Jahren
- durchschnittlich mehr als eine halbe Million US-Dollar Ausgaben für die Behebung und Wiederherstellung nach API-bezogenen Vorfällen (laut unseren Befragten der Führungsebene in den USA liegen die durchschnittlichen finanziellen Auswirkungen bei 943.162 USD)
- eine menschliche Belastung durch API-Vorfälle, wobei die Auswirkungen von Stress und Reputationsschäden auf ihre Teams (insbesondere interne Prüfungen, die diesen Druck verstärken) sogar noch höher sind als der Aufwand für die Behebung der Vorfälle

Die Befragten gaben unterschiedliche Ansichten über die Vollständigkeit ihrer API-Bestandsaufnahmen an, und diese Variabilität war noch stärker ausgeprägt, wenn sie nach Rollen aufgeschlüsselt wurden (siehe Seite 11). Auffallend ist, dass der Anteil von Unternehmen mit vollständigen API-Bestandsaufnahmen, die auch wissen, welche ihrer APIs sensible Daten liefern, von bereits niedrigen 40 % im Jahr 2023 auf nur noch 27 % im Jahr 2024 gesunken ist.

Die Befragten gaben auch an, dass die herkömmlichen Tools, auf die sie zum Schutz von APIs angewiesen sind, Risiken nicht vollständig abdecken. Diese Tools, wie Web Application Firewalls (WAFs), API-Gateways und Netzwerk-Firewalls, sind oft die ersten, die für den Erfolg eines Angriffs verantwortlich gemacht werden (siehe vollständige Liste der Ursachen auf Seite 17 und einen Hinweis zu WAF und WAAP auf Seite 12).

Sicherheitsexperten spüren, welchen menschlichen Tribut API-Vorfälle fordern, wobei die Auswirkungen von Stress und Reputationsschäden auf ihre Teams noch höher sind als die Kosten für die Behebung der Vorfälle.

Unsere Studienergebnisse erlauben uns auch, einige Hauptgründe dafür zu ermitteln, warum API-Sicherheitsstrategien noch immer keine ausreichende Priorität haben, obwohl es nachweislich nötig wäre. Ein Hauptfaktor ist die fehlende Abstimmung zwischen den wichtigsten Sicherheitsrollen hinsichtlich Anzahl, Ort und Risikoattributen von APIs, die geschützt werden müssen – wahrscheinlich aufgrund der schlechten Sichtbarkeit von APIs und der fehlenden zentralen Informationsquelle.

Wir haben auch festgestellt, dass Sicherheitsexperten sich uneinig über die Ursachen von API-Angriffen waren. Sind es die Tools, die sie verwenden, die Fehler, die ihre Programmierer bei der Entwicklung gemacht haben, oder Angriffe auf Schlupflöcher in GenKI-Innovationen? Kommt darauf an, wen Sie fragen.

Der andere Grund, warum die API-Sicherheit strategisch nicht an Bedeutung gewinnt, ist natürlich, dass Teams bereits mit anderen drängenden Bedrohungen vollauf beschäftigt sind, die wahrscheinlich auch den Großteil des Budgets, des Teamfokus und der Anstrengungen beanspruchen. Lassen Sie uns die Ergebnisse genauer untersuchen.

API-Sicherheitsstudie – 2024
Die wichtigsten Ergebnisse in Kürze

84 % der Befragten erlebten einen API-Sicherheitsvorfall in den letzten 12 Monaten

Durchschnittliche Kosten für die Behebung von API-Vorfällen in den letzten 12 Monaten:

USA	Vereinigtes Königreich	Deutschland
591.404 $	420.103 £	403.453 €

Schlechte Sichtbarkeit

Nur 27 % der Unternehmen mit vollständigen API-Bestandsaufnahmen wissen, welche APIs sensible Daten zurückgeben – im Vergleich zu 40 % im Jahr 2023.

Hohe Belastung

Hauptauswirkung von API-Vorfällen *CISOs*: Rufschädigung unserer Abteilung bei Führungskräften und/oder dem Vorstand. *CIOs*: erhöhter Stress und/oder Druck für das Team oder die Abteilung.

Kaum Tests

Nur 13 % bzw. 18 % der Befragten testen ihre APIs in Echtzeit bzw. täglich von der API-Entwicklung bis zur Produktion.

Die finanziellen Kosten von API-Sicherheitsvorfällen verschärfen die Auswirkungen auf Teams und Führungskräfte. Kostspielige Verstöße werden genau untersucht und können bei einflussreichen Interessengruppen wie dem Vorstand den Eindruck erwecken, dass Teams ihre Arbeit nicht erfolgreich erledigen. Das ist stressig. Tatsächlich nannten Teilnehmer aus verschiedenen Regionen Stress für ihre Teams als die wichtigste Auswirkung eines API-Sicherheitsvorfalls.

Der aktuelle Status der API-Sicherheit

In den letzten drei Jahren ist die Zahl der Unternehmen, die API-Sicherheitsvorfälle melden, kontinuierlich gestiegen und erreichte 2024 einen Höchststand von 84 % (siehe unten). Wie wirken sich diese API-Angriffe auf Unternehmen aus? Was tun – oder planen – Unternehmen, um ihr Risiko zu senken? Wir haben unsere Ergebnisse als Antworten auf diese Fragen strukturiert.

Haben API-Angriffe erhebliche Auswirkungen auf Unternehmen und ihre Sicherheitsteams?

Die kurze Antwort lautet: Ja. Dies war das erste Jahr, in dem wir Daten zu den finanziellen Auswirkungen eines API-Sicherheitsvorfalls erhoben haben. Die finanziellen Folgen waren bedeutend: Die durchschnittlichen Kosten für die Behebung von API-Vorfällen (einschließlich Systemreparaturen, Ausfallzeiten, Gerichtsgebühren, Bußgeldern und anderer damit verbundener Ausgaben) für die 84 %, bei denen sie in den letzten 12 Monaten aufgetreten sind, betrugen:

- **591.404** US-Dollar in den USA
- **420.103** Britische Pfund im Vereinigten Königreich
- **403.453** Euro in Deutschland

Bestimmte Rollen sahen die Kosten als viel höher an, insbesondere die Befragten der Führungsebene in den USA, die 943.162 USD angaben, fast 60 % mehr als der Durchschnitt der US-amerikanischen Befragten.

Waren Sie in den letzten 12 Monaten Opfer eines API-Sicherheitsvorfalls?

Jahr	Gesamt	USA	Vereinigtes Königreich	Deutschland
2022	76 %	75 %	77 %	–
2023	78 %	85 %	69 %	–
2024	84 %	83 %	83 %	84 %

Unabhängig von der genauen Zahl verschärfen die finanziellen Kosten von API-Sicherheitsvorfällen die menschlichen Auswirkungen noch. Kostspielige Verstöße werden genau untersucht und können bei einflussreichen Interessengruppen wie dem Vorstand den Eindruck erwecken, dass Teams ihre Arbeit nicht erfolgreich erledigen. Das ist stressig. Tatsächlich nannten Teilnehmer aus verschiedenen Regionen „Stress“ (insbesondere Stress für ihre Teams) als die wichtigste Auswirkung eines API-Sicherheitsvorfalls, gefolgt von „Rufschädigung unserer Abteilung bei Führungskräften und/oder dem Vorstand“ und „Kosten für die Behebung“ an dritter Stelle. Insbesondere treten die internen Auswirkungen, die die Moral am stärksten beeinflussen, wieder auf und dominieren die drei unteren Auswirkungen, die fast gleichauf sind (siehe unten).

Die Ergebnisse waren ähnlich, wenn sie nach Branchen aufgeschlüsselt wurden: „Erhöhter Stress und/oder Druck für das Team nach einem API-Verstoß“ war auch die wichtigste Auswirkung in vier der acht befragten Branchen (siehe Seitenleiste auf Seite 9). Dazu gehören auch Finanzdienstleistungen, die mit 832.801 USD die größten finanziellen Auswirkungen aller Branchen verzeichneten.

Am häufigsten genannte Auswirkungen von API-Sicherheitsvorfällen

1. Erhöhter Stress und/oder Druck für das Team oder die Abteilung – **27,0 %**
2. Rufschädigung unserer Abteilung bei Führungskräften und/oder dem Vorstand – **26,6 %**
3. Kosten für die Behebung des Problems – **25,8 %**
4. Geldbußen von Regulierungsbehörden – **25,4 %**
5. Verlust von Kunden-Goodwill und Abwanderung – **25,0 %**
6. Produktivitätsverlust – **24,1 %**
7. Verlust von Vertrauen und Rufschädigung – **23,8 %**
8. Verlust von Mitarbeiter-Goodwill – **23,8 %**
9. Verstärkte interne Prüfung unseres Teams/unserer Abteilung durch das Unternehmen – **23,5 %**

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

Der Zusammenhang zwischen den finanziellen Kosten und der Belastung der Teammitglieder bei API-Angriffen kam auch in den Antworten von IT- und Sicherheitsexperten zu den Auswirkungen deutlich zum Ausdruck (jeder Befragte durfte bis zu drei Punkte wählen). Ein Bereich, in dem in allen Regionen ein allgemeiner, rollenübergreifender Konsens bestand, war, dass sich API-Sicherheitsvorfälle vor allem auf die Mitarbeiter auswirken.

- Die beiden wichtigsten Punkte, die von CISOs angegeben wurden – „Rufschädigung unserer Abteilung bei Führungskräften und/oder dem Vorstand“ und „Verlust von Kunden-Goodwill und Abwanderung“ –, zeigten mit 31 % einen Gleichstand bei den Auswirkungen auf menschlicher und finanzieller Seite.
- Auch die von den CIOs berichteten größten Auswirkungen zeigten mit 34 % einen Gleichstand bei „Erhöhter Stress und/oder Druck für das Team oder die Abteilung“ und „Kosten für die Behebung“.

Diese Ergebnisse sind für CISOs und CIOs plausibel: Was, wenn die Teams, die sie leiten, immer wieder mit Sicherheitsvorfällen konfrontiert werden, die schlechte Arbeitsbedingungen schaffen, Budgets sprengen und Kunden verärgern? Führungskräfte wollen nicht, dass hochwertige Talente gehen oder der Ruf ihrer Abteilung schlechter wird. Hinzu kommen finanzielle Belastungen wie Sanierungskosten und/oder Kundenabwanderung – der Stress für CISOs und CIOs steigt erheblich. Tatsächlich war „Verlust von Kunden-Goodwill und Abwanderung“ die wichtigste Auswirkung eines API-Sicherheitsvorfalls für die Befragten aus der Versicherungs- und Automobilindustrie (weitere Branchenergebnisse finden Sie in der Seitenleiste auf der nächsten Seite).

Die wichtigsten Antworten für die verbleibenden Rollen waren:

- CTO, 30 %, „Verlust von Mitarbeiter-Goodwill“
- Leitendes Sicherheitspersonal, 27 %, „Rufschädigung unserer Abteilung bei Führungskräften und/oder dem Vorstand“
- AppSec-Team, 31 %, „Erhöhter Stress und/oder Druck für das Team oder die Abteilung“

Am häufigsten genannte Auswirkungen von API-Sicherheitsvorfällen nach Branche	
Automobilindustrie	Verlust von Kunden-Goodwill und Abwanderung – **33 %**
Energie/Versorgungswirtschaft	Rufschädigung unserer Abteilung bei Führungskräften und/oder dem Vorstand – **36 %**
Finanzdienstleistungen	Gleichstand: Erhöhter Stress und/oder Druck für das Team oder die Abteilung und Geldbußen von Regulierungsbehörden – beides **29 %**
Regierung/ öffentlicher Sektor	Erhöhter Stress und/oder Druck für das Team oder die Abteilung – **29 %**
Gesundheitswesen	Gleichstand: Verlust von Vertrauen und Rufschädigung + Produktivitätsverlust – beides **29 %**
Versicherungen	Verlust von Kunden-Goodwill und Abwanderung – **28 %**
Fertigungsindustrie	Erhöhter Stress und/oder Druck für das Team oder die Abteilung – **34 %**
Einzelhandel/ E-Commerce	Erhöhter Stress und/oder Druck für das Team oder die Abteilung – **29 %**

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

Sind APIs und potenzielle Risiken angemessen transparent?

Nein. Die Situation ist sogar schlechter geworden. In diesem Jahr ist der Prozentsatz der Befragten, die über eine vollständige API-Bestandsaufnahme verfügen und auch wissen, welche APIs sensible Daten austauschen, von bereits niedrigen 40 % im Jahr 2023 auf nur noch 27 % im Jahr 2024 gesunken. (Diese Feststellung könnte auch einen positiven Trend bedeuten, wenn wir annehmen, dass mehr Unternehmen versuchen, eine vollständige Bestandsaufnahme durchzuführen, aber die Tools zur Lokalisierung jeder API und zur Identifizierung der Aktivitäten innerhalb der einzelnen API nicht vorhanden sind.)

Der Prozentsatz der Befragten, die über eine vollständige API-Bestandsaufnahme verfügen und auch wissen, welche APIs sensible Daten austauschen, ist **von bereits niedrigen 40 % im Jahr 2023** auf **nur noch 27 % im Jahr 2024** gesunken.

Aktueller Status der API-Bestandsaufnahmen und der Bekanntheit, alle Befragten

	2024	2023
Ja, **und wir wissen**, welche vertrauliche Daten zurückgeben	27 %	40 %
Ja, **aber wir wissen nicht**, welche vertrauliche Daten zurückgeben	43 %	32 %
Wir verfügen über eine unvollständige Bestandsaufnahme unserer APIs **und wissen**, welche vertrauliche Daten zurückgeben	23 %	24 %
Wir verfügen über eine unvollständige Bestandsaufnahme, **wissen aber nicht**, welche sensible Daten zurückgeben	6 %	4 %
Nein, **wir** haben keine Bestandsaufnahme	1 %	–

Basierend auf der Frage: Verfügen Sie über eine vollständige Bestandsaufnahme Ihrer APIs und wissen Sie, welche vertrauliche Daten zurückgeben? (Aus fünf Optionen auswählen); n = 1.207

Werden die Führungspersonen in allen drei Ländern und acht befragten Branchen betrachtet, neigen CIOs zu der Ansicht, dass ihre Unternehmen über vollständige API-Bestandsaufnahmen verfügen – deutlich häufiger als CISOs. Auf der Ebene der Praktiker stimmen sowohl die leitenden Sicherheitsexperten als auch die Mitglieder des AppSec-Teams weitgehend der Ansicht des durchschnittlichen CIOs zu, dass alle APIs bekannt sind.

Aber wie vergleichen sich die fünf Rollen im Durchschnitt, wenn es darum geht, zu wissen (oder nicht zu wissen), welche ihrer APIs sensible Daten zurückgeben, wenn sie aufgerufen werden? Die Antwort ist wichtig, da viele dieser Aufrufe aus bösartigen Quellen stammen, die gängige API-Schwachstellen ausnutzen.

Vier Arten von nicht verwalteten APIs, auf die Angreifer zielen, um auf Daten zuzugreifen

1. **Schatten-APIs** (auch „undokumentierte APIs“ genannt) existieren und arbeiten außerhalb der offiziellen, überwachten Kanäle eines Unternehmens.
2. **Rogue-APIs** sind nicht autorisierte oder bösartige APIs, die ein Sicherheitsrisiko für ein System oder Netzwerk darstellen.
3. **Zombie-APIs** sind alle APIs, die nach dem Ersetzen durch neue Versionen oder andere APIs trotzdem noch ausgeführt werden.
4. **Veraltete APIs** sind APIs, die aufgrund von Änderungen nicht mehr zur Verwendung empfohlen werden.

Diese Ergebnisse bieten einige erstaunliche Erkenntnisse über die Transparenz von API-Risiken. Die Mehrheit der CISOs und CTOs antwortete entweder, dass sie eine vollständige Bestandsaufnahme hätten, *ohne* zu wissen, welche APIs sensible Informationen zurückgeben (nennen wir dieses Wissen „Wissen über sensible Daten"), oder, dass sie eine unvollständige Bestandsaufnahme *mit* Wissen über sensible Daten hätten.

Die Mehrheit der CIOs gab an, über eine vollständige API-Bestandsaufnahme zu verfügen, und von diesen CIOs sagten 42,9 % aus, dass sie auch über vollständiges Wissen über sensible Daten verfügen – während 36,3 % die Angabe machten, dieses Wissen nicht zu haben. Leitende Sicherheitsexperten stimmten mit CIOs überein (75 % berichteten, eine vollständige Bestandsaufnahme zu haben), aber beim Wissen um sensible Daten *kehrten sich die Verhältnisse um*: 32,5 % der leitenden Sicherheitsexperten gaben an, dass sie über das Wissen über sensible Daten verfügen, 42,5 %, dass sie dieses Wissen nicht haben.

Bei den Aussagen der AppSec-Mitarbeiter, wahrscheinlich die Personen mit der meisten Praxis, kam schließlich die höchste einzelne Mehrheit über alle fünf Rollen hinweg zustande. Fast die Hälfte meldete eine vollständige Bestandsaufnahme ohne Wissen um sensible Daten – die andere Hälfte teilte sich grob auf Folgendes auf:

- vollständige Bestandsaufnahme mit vollständigem Wissen um sensible Daten
- unvollständige Bestandsaufnahme mit vollständigem Wissen um sensible Daten bei bekannten APIs

Wir schließen, dass die Messung der Bestände noch nicht standardisiert genug ist, um eine API-Zählung aus einer Quelle zu erhalten. Angesichts der Variabilität ist es auch wahrscheinlich, dass mehr Unternehmen mit vollständigen Bestandsaufnahmen *nicht* über vollständiges Wissen um sensible Daten verfügen. Es ist immer wichtig zu wissen, welche APIs sensible Daten zurückgeben. Eine unvollständige Bestandsaufnahme ist möglicherweise jedoch am gefährlichsten, da Schatten-, Rogue-, Zombie- und veraltete APIs häufig Angriffsziele sind, schlecht geschützt sind und in der Regel von herkömmlichen Sicherheitstools übersehen werden.

Aktueller Status der API-Bestandsaufnahmen und der Bekanntheit, aufgeschlüsselt nach Rolle

	CISO	CIO	CTO	Leitd. Sich.exp.	AppSec
Wir haben eine vollständige Bestandsaufnahme und **wir wissen**, welche APIs sensible Daten zurückgeben	17,2 %	42,9 %	16,5 %	32,5 %	26,4 %
Wir haben eine vollständige Bestandsaufnahme, **aber wir wissen nicht**, welche APIs sensible Daten zurückgeben	41,4 %	36,3 %	34,8 %	42,5 %	47,4 %
Wir verfügen über eine unvollständige Bestandsaufnahme unserer APIs **und wissen**, welche vertrauliche Daten zurückgeben	32,5 %	15,4 %	39,9 %	18,3 %	20,4 %
Wir verfügen über eine unvollständige Bestandsaufnahme, **wissen aber nicht**, welche sensible Daten zurückgeben	8,3 %	5,5 %	8,2 %	5,8 %	5,2 %

Basierend auf der Frage: Verfügen Sie über eine vollständige Bestandsaufnahme Ihrer APIs und wissen Sie, welche vertrauliche Daten zurückgeben? (Aus fünf Optionen auswählen); n = 1.207

In einer Zeit, in der nicht verwaltete APIs sich ausbreiten und herkömmliche Sicherheitstools diese nur schwer erfassen können, zeigen diese Ergebnisse eine häufige Sicherheitslücke auf, die Angriffsvektoren über APIs für Bedrohungsakteure attraktiver macht.

Natürlich sind nicht verwaltete APIs nur einer von mindestens fünf API-Aspekten, die ein Sicherheitsteam sehen und bewerten muss. Weitere Aspekte sind:

- **APIs mit bekannten Sicherheitslücken**, die nicht gepatcht wurden
- **Nicht verwaltete oder vergessene APIs** (Schatten, Rogue, Zombie, veraltet)
- **APIs mit Schnittstellen nach außen** (wie Zugangsdaten, Schlüssel und Variablen außerhalb Ihrer Kontrolle)
- **APIs mit Bedienerfehlern** (falsche Sicherheitskonfigurationen in Infrastruktur und Diensten)
- **APIs mit unentdeckten Sicherheitslücken** und Bugs, die von Bedrohungsakteuren erkannt und ausgenutzt werden

Die Bandbreite der Antworten in Bezug auf API-Bestandsaufnahmen und die Transparenz von API-Schwachstellen lässt mindestens Folgendes vermuten:

- Unternehmen verlassen sich immer noch auf Sicherheitsprodukte, die nicht speziell auf die Erkennung und Sicherung von APIs ausgerichtet sind und noch weniger auf nicht verwaltete, risikoreiche APIs.
- Sicherheitsabteilungen müssen noch die Risikoattribute einer API definieren, die erkannt und bewertet werden müssen, und in ihren vielen Geschäftseinheiten, Entwicklerteams und bei Lieferanten einen Konsens über ihre Strategie für die API-Erkennung und -Bestandsaufnahme schließen.

Das Schließen solcher Lücken kann ein großartiger erster Schritt sein, um effektive Argumente für eine Investition in stärkere Funktionen zur Sicherung aller APIs zu schaffen (siehe „Wie Sie eine ausgereiftere Positionierung der API-Sicherheit erreichen“ auf Seite 18). In der jetzigen Form sind Aufmerksamkeit und Fürsprache, die für eine Budgetzuweisung erforderlich sind, für das Thema API-Sicherheit häufig nicht gegeben. Daher ist die Priorisierung und Finanzierung von Initiativen erschwert, die nicht nur die Verteidigung von APIs und Web-Apps, sondern auch die allgemeine Sicherheitslage eines Unternehmens fördern könnten.

Gemeinsam besser: WAAP + API-spezifischer Schutz

Der Web-Anwendungs- und API-Schutz (WAAP) wurde entwickelt, um Bedrohungen durch mehrere Angriffsvektoren schnell zu erkennen und abzuwehren und den herkömmlichen Schutz einer WAF zu erweitern. **Eine API-Sicherheitslösung, die in Zusammenarbeit den Schutz noch über die Firewall hinaus erweitert und so die bestmögliche Verteidigung schafft**.

Werden APIs oft genug getestet, um das Risiko von Missbrauch oder Sicherheitsverletzungen zu senken?

Nein, nicht oft genug. Öffentliche APIs, die falsch konfiguriert sind, keine Authentifizierungskontrollen aufweisen, mit Programmierfehlern eingebettet sind oder andere vermeidbare Risiken bergen, sind genau das, was Angreifer suchen – und diese Angreifer werden immer besser darin, sie zu finden.

Wenn Ihr Entwicklungsteam APIs wie diese in die Produktion sendet, ohne sie zuerst umfassend zu testen, entspricht das jedes Mal einer Ursache für eine zukünftige Arbeitslast für Ihr Sicherheitsteam. Einer Arbeitslast, die dann zweifellos dringend ist und zu dem beiträgt, was unsere Erkenntnisse über Stress ergeben haben.

Aber wir sprechen von *vermeidbaren* Risiken.

Wenn Sie APIs im Entwicklungsbereich – häufig und effizient durch Automatisierung – testen, *bevor* sie für die Produktion freigegeben werden, geben Sie Ihrem Unternehmen, Ihren Entwicklern und Ihrem Sicherheitsteam einen Vorteil. Und dieser Vorteil liegt unmittelbar in der Reduzierung von Stress, der durch unbekannte Schwachstellen verursacht wird, und in dem Wissen, dass in der Produktion keine Fehler auftreten werden, wo sie exponentiell schwieriger und kostspieliger zu beheben wären.

Wenn Sie APIs im Entwicklungsbereich – häufig und effizient durch Automatisierung – testen, *bevor* sie für die Produktion freigegeben werden, geben Sie Ihrem Unternehmen, Ihren Entwicklern und Ihrem Sicherheitsteam einen Vorteil.

Bisher sind jedoch laut unseren Befragten Tests noch nicht geläufig und wichtig genug. Häufige API-Tests, in Echtzeit und täglich, gingen im Vergleich zum Vorjahr über den gesamten API-Lebenszyklus einschließlich der Produktion zurück.

- Im Jahr 2023 gaben 18 % der Befragten in den USA und im Vereinigten Königreich an, APIs in Echtzeit zu testen. Innerhalb der gleichen Gruppe **sank dieser Wert im Jahr 2024 auf 13 %**.
- Im Jahr 2023 sagten 37 % der Befragten in den USA und im Vereinigten Königreich aus, APIs mindestens einmal täglich zu testen. **2024 führten nur 13 %** der Befragten Tests in dieser Häufigkeit aus, während 26 % der deutschen Befragten einmal täglich testeten.

Wöchentliche API-Tests sind für Teilnehmer über verschiedene Regionen hinweg am häufigsten, erreichten aber in keinem Gebiet 50 %. Darüber hinaus variierte die Häufigkeit von API-Tests in verschiedenen Regionen stark, von *Echtzeit* bis *gar nicht*. Nur 6 % der Befragten antworteten: „Wir testen die Sicherheit von APIs erst kurz bevor sie für die Produktion freigegeben werden." Im Idealfall gehen die Teams dazu über, während des gesamten API-Lebenszyklus kontinuierlich zu testen.

Was bedeutet es, APIs kontinuierlich zu testen?

Schwachstellen können zu jedem Zeitpunkt des API-Lebenszyklus in APIs eingefügt werden, von Programmierfehlern in der Entwicklung bis hin zu Sicherheitslücken, die auftauchen, sobald Benutzer mit der API interagieren. Deshalb werden API-Tests idealerweise in der Entwicklung (Shift-Left) und auch kontinuierlich während der Produktion (Shift-Right) durchgeführt.

Beispiele für API-Tests in der Entwicklung:

- automatisierte Tests, die böswilligen Datenverkehr simulieren
- Prüfung von API-Spezifikationen anhand etablierter Governance-Richtlinien
- Testen von APIs bei Bedarf oder im Rahmen einer CI/CD-Pipeline

Beispiele für API-Tests in der Produktion:

- kontinuierliche Überwachung des API-Datenverkehrs und Bewertung der Metadaten des Datenverkehrs
- Änderungen an Ihren vorhandenen APIs mithilfe einer automatisierten Analyse ermitteln
- Probleme in Echtzeit finden und beheben, bevor Angreifer sie bemerken

Erfüllen Ihre API-Sicherheitsprotokolle die Compliance-Anforderungen?

In vielen Datenschutzvorschriften werden APIs nicht namentlich genannt, aber die Anforderungen beziehen sich eindeutig auf den Schutz der Anwendungen und der Infrastruktur, innerhalb derer APIs betrieben werden. Compliance-Auflagen entwickeln sich ständig weiter, und weitere Vorschriften mit Auswirkungen auf APIs sind auf dem Weg, darunter der American Privacy Rights Act (derzeit noch in der Entwurfsphase) und der EU Cyber Resilience Act.

Zu den Vorschriften und Frameworks mit aktuellen, direkten Auswirkungen auf die API-Sicherheit gehören:

- PCI DSS (derzeit in Version 4.0.1)
- Datenschutz-Grundverordnung (DSGVO)
- Digital Operational Resilience Act (DORA)
- Health Insurance Portability and Accountability Act (HIPAA)
- Richtlinie zur Netz- und Informationssicherheit (NIS2)

API-Sicherheit erhält Aufmerksamkeit, es bleibt aber bei einer geringen Priorität

Wenn API-Angriffe kostspielig sind und Bußgelder verursachen, wenn sie zum Verlust des Kundenvertrauens beitragen, wenn sie die Mitarbeiter zunehmend belasten und die Glaubwürdigkeit bei Unternehmensvorständen gefährden, warum ergreifen die Teams dann nicht entschlossenere Maßnahmen? Die Antworten auf die folgenden Fragen helfen uns, das zu verstehen.

Wie priorisieren verschiedene Unternehmensrollen die API-Sicherheit?

Wir haben unsere Teilnehmer gebeten, ihre wichtigsten Prioritäten für die Cybersicherheit in den nächsten 12 Monaten anzugeben, damit sie bis zu drei aus einer umfangreichen Liste auswählen können (siehe Seitenleiste). Die sechs wichtigsten Prioritäten unterschieden sich nur um je 2 %, und die sechs am wenigsten wichtigen nur um 1 %, was darauf hindeutet, dass die Prioritäten in allen Regionen und Branchen ähnlich sind – und dass Teams oft gezwungen sind, alle miteinander zu vereinbaren.

In einigen Branchen verweisen die für APIs entscheidenden Rangunterschiede jedoch auf einen anderen Zusammenhang. So wird beispielsweise die API-Sicherheit bei Energie-/Versorgungsunternehmen im Vergleich zu allen anderen Sektoren mit 13,2 % (und unter dem Durchschnitt der Teilnehmer aller Befragungen von 18 %) als niedrigste Priorität eingestuft. Gleichzeitig hatten Energie- und Versorgungsunternehmen mit 91 % die höchste Meldung von API-Sicherheitsvorfällen, die höchste aller acht Branchen, deutlich über dem Durchschnitt von 84 %. Wie passt das zusammen? Die niedrige Priorität der API-Sicherheit, trotz der hohen Angriffsrate.

Am häufigsten genannte Sicherheitsprioritäten in den nächsten 12 Monaten

1. Schutz vor GenKI-gestützten Angriffen – 21,2 %
2. Schutz vor Ransomware – 20,5 %
3. Sichere Authentifizierung für Mitarbeiter – 19,7 %
4. Verwaltung und Schutz von Entwicklergeheimnissen – 19,6 %
5. Sicherung von Endpunkten – 19,2 %
6. Lösungen für die Cloudsicherheit – 19,1 %
7. Schutz von privilegiertem IT-Zugriff – 18,6 %
8. Schutz vor Datenverlust – 18,6 %
9. Schutz von APIs vor Bedrohungsakteuren – 17,9 %
10. Schutz von Anwendungen – 17,7 %
11. Integration von Sicherheitsinformationen und Ereignisverwaltung – 17,6 %
12. Reaktion auf Vorfälle und Management – 17,6 %

Basierend auf der Frage: Was sind die wichtigsten Cybersicherheits-Prioritäten Ihres Unternehmens in den nächsten 12 Monaten? (Bis zu 3 auswählen); n = 1.207

Aussagekräftigere Daten entstanden aus der Analyse der Antwortdaten nach Rollen:

- CISOs bewerteten GenKI-gestützte Angriffe und API-Schutz mit **25,5 %** bzw. **24,8 %** am höchsten.
- Die Mitarbeiter von AppSec stimmten mit CISOs überein und nannten GenKI-unterstützte Angriffe mit **22,5 %** als höchste Priorität.
- CIOs und CTOs konzentrierten sich beide auf den privilegierten Zugriff, wobei CTOs der Reaktion auf Vorfälle die gleiche Wichtigkeit zusprachen.
- Leitende Sicherheitsexperten haben Ransomware allein als höchste Priorität eingestuft.

Diese Unterschiede veranlassten uns, weitere Fragen zu stellen, beispielsweise: Warum arbeiten verschiedene Ebenen der IT-Sicherheitsorganisation scheinbar nach unterschiedlichen Playbooks? Und warum sind sich die leitenden Sicherheitsexperten und Mitarbeiter an vorderster Front der wichtigen Rolle und der Risiken von APIs bei GenKI-gestützten Angriffen bewusst, während andere Rollen dies nicht wahrnehmen?

Vielleicht liegt es daran, dass CISOs sehen, dass ihre Geschäftseinheiten Innovationen wie GenKI-basierte Apps hastig einführen, um die Nachfrage zu befriedigen, während die Mitglieder des AppSec-Teams dasselbe sehen. Die *AppSec-Teams* wissen dabei jedoch, in welchem Ausmaß Unwissen über die Schwachstellen von KI-Komponenten (wie LLMs) besteht, die sensible Daten betreffen. Hinzu kommt, dass diese Teams direkt in der ersten Reihe die vielen Warnsignale wahrnehmen, dass Angreifer GenKI in ihre Angriffsmethoden integrieren.

Aber der Hauptgrund könnte der einfachste sein: Top-down- und Bottom-up-Kommunikation findet nicht häufig genug statt – insbesondere in großen Unternehmen –, was zu einer Trennung zwischen Prioritäten der Spitze und dem, was Teams täglich bewältigen *müssen*, führt.

Abschließend vergleichen wir die wichtigsten Prioritäten der Befragten im Bereich Cybersicherheit mit den Ursachen, die sie für ihre API-Sicherheitsvorfälle angegeben haben. Wie auf Seite 17 gezeigt, beziehen sich drei der am häufigsten genannten Ursachen auf herkömmliche Tools zur Anwendungssicherheit, die API-Probleme nicht erkennen konnten. Der Vergleich bietet eine gute Gelegenheit, darüber zu diskutieren, wie Lösungen für die API-Erkennung und API-Tests nicht nur die API-Sicherheit, sondern auch fast alle anderen wichtigen Sicherheitsprioritäten verbessern können.

Mit anderen Worten: Wenn die richtigen API-Sicherheitstools nicht nur APIs schützen, sondern auch die Sicherheit für Bereiche wie Daten, Cloud und Anwendungen verbessern können, wirkt die API-Sicherheit für Ihre Stakeholder weniger wie ein isoliertes Nischenfeld. Wenn Sie mit dem Gesamtbild argumentieren, können Sie leichter eine erhöhte Priorität für APIs durchsetzen.

Wenn die richtigen API-Sicherheitstools nicht nur APIs schützen, sondern auch die Sicherheit für Bereiche wie Daten, Cloud und Anwendungen verbessern können, wirkt die API-Sicherheit für Ihre Stakeholder weniger wie ein isoliertes Nischenfeld.

Lässt die fehlende Übereinstimmung bezüglich API-Sicherheitsvorfällen darauf schließen, dass es keine zentrale Informationsquelle gibt?

Wir haben die Unterschiede in den allgemeinen Sicherheitsprioritäten der Führungsebene und den Mitarbeitern der ersten Linie hervorgehoben, und diese Unterschiede zeigen sich auch bei Problemen, die speziell API-Bedrohungen betreffen. Beispielsweise sehen CIOs und AppSec-Teams die Situation der API-Angriffe ähnlich (etwa 88 % in jeder Rolle berichten, dass es zu Vorfällen gekommen ist). CISOs, CTOs und leitende Sicherheitsexperten gaben jedoch einen um etwa acht Prozentpunkte niedrigeren Wert an, denn etwa 80 % berichteten, dass Vorfälle auftraten.

Die am häufigsten zitierte Ursache für API-Sicherheitsvorfälle variierte auch nach Rolle. Die meisten CISOs und leitenden Sicherheitsexperten gaben an, dass der API-Gateway das Problem nicht erfasst habe, während die anderen drei Rollen jeweils einen anderen Schuldigen nannten:

- CISO: API-Gateway hat sie nicht erfasst – **26,8 %**
- CIO: Unbeabsichtigte Verbindung mit dem Internet – **28,6 %**
- CTO: WAF hat sie nicht erfasst – **25,9 %**
- Leitender Sicherheitsexperte: API-Gateway hat sie nicht erfasst – **23,3 %**
- AppSec-Team: API-Fehlkonfiguration – **23,2 %**

Die häufigsten Ursachen von API-Sicherheitsvorfällen, alle Befragten

1. API war aus Versehen mit dem Internet verbunden – 21,8 %
2. Web Application Firewall hat sie nicht erfasst – 21,8 %
3. API-Gateway hat sie nicht erfasst – 20,2 %
4. APIs in GenKI-Tools/-Technologien, z. B. LLMs – 20,0 %
5. API-Fehlkonfiguration – 19,9 %
6. Netzwerk-Firewall hat sie nicht erfasst – 19,6 %
7. Bekanntes technisches Tool/Service, z. B. Microsoft – 19,2 %
8. Sicherheitsanfälligkeit aufgrund von API-Programmierfehlern – 19,1 %
9. Nicht verwaltete APIs, z. B. ruhende oder Zombie-APIs – 18,9 %
10. Fehlende API-Authentifizierungskontrollen – 18,8 %
11. Schwachstellen bei Autorisierung – 18,7 %
12. Softwarelösung aus dem Internet heruntergeladen – 17,6 %
13. Mid-Tier-Softwarelösung, z. B. Slack – 16,3 %

Basierend auf der Frage: Was sind Ihrer Meinung nach die Ursachen für die API-Sicherheitsvorfälle in Ihrem Unternehmen? (Bis zu 3 auswählen); n = 1.207

Bei den gemeldeten Kosten von API-Sicherheitsvorfällen ließ sich ebenso eine mangelnde Übereinstimmung von den Führungsrollen abwärts feststellen. Es ist jedoch wichtig zu beachten, dass eine Segmentierung der Daten nach Rolle *und* Region natürlich zu einer geringeren Stichprobengröße führt. Dennoch sind die Unterschiede in diesen Untergruppen bemerkenswert. Insbesondere in den USA schätzten CIOs und CTOs die Kosten von Vorfällen auf etwa 1 Mio. USD und CISOs auf etwa 737.000 USD, während leitende Sicherheitsexperten und AppSec-Mitarbeiter sie bei etwa 375.000 USD bzw. 444.000 USD sahen.

Im Vereinigten Königreich wurden die Kosten in der Regel über rollenspezifische Teilmengen hinweg ähnlich geschätzt; hier fielen Mitglieder der AppSec-Teams mit der höchsten Angabe von 749.000 GBP und CISOs mit 190.000 GBP als niedrigster Summe auf. (Die mittleren Rollen reichten von oben nach unten von 374.000 GBP bis 222.000 GBP.) Deutschlands Diskrepanz bei der Kostenberichterstattung fiel ähnlich aus wie im Vereinigten Königreich, wobei die höchste Schätzung von den hierarchisch am niedrigsten angesiedelten Mitarbeitern mit der meisten Praxis stammte – 345.000 EUR – und die niedrigste Schätzung von einem Teil der Führungsebene, den CISOs, mit 197.000 GBP (gegenläufig zu den Ergebnissen aus den USA). Ein Aspekt, bei dem sich alle Rollen in allen Regionen einig waren, war, dass die größten Auswirkungen von API-Sicherheitsvorfällen die Mitarbeiter betreffen (siehe Auswirkungen, Seite 7).

Wie Sie eine ausgereiftere Positionierung der API-Sicherheit erreichen

Wie bereits erwähnt, zeigen unsere Ergebnisse, dass Mitglieder von Sicherheitsteams auf verschiedenen Unternehmensebenen die API-Sicherheit nicht durch dieselbe Brille sehen. Aber es gibt eine Kehrseite: Klar ist auch, dass sie gemeinsame Grundlagen haben, auf denen sie aufbauen können. Sie kennen die Kosten (finanziell und personell) und haben erkannt, dass die Tools, auf die sie sich verlassen, nicht ausreichen.

Da die API-Sicherheit so große Auswirkungen auf Unternehmen hat, könnten Ihre nächsten Schritte darin bestehen, zu entscheiden, worauf Sie aufbauen und was geändert werden soll, und Führungskräften zu zeigen, wie der Schutz von APIs das Ergebnis unterstützen kann. Ein Konsens in der Sicherheitsabteilung, vom CISO bis zum AppSec-Team, über die Priorisierung der API-Sicherheit ist ein guter Ausgangspunkt. Anschließend sollte eine offene Kommunikation zwischen Führungskräften und AppSec-Teammitgliedern sowie den dazwischen liegenden Managementebenen gefördert werden.

Schritte, die Sie ergreifen können

Zum Abschluss unserer Studie haben wir eine Reihe progressiver Schritte zusammengestellt, die Ihr Sicherheitsteam ergreifen kann, um Ihre API-Sicherheitsstrategie einzuführen oder darauf aufzubauen und einen ausgereiften API-Schutz zu erreichen.

1 Der Startpunkt: API-Erkennung und API-Transparenz

Um eine vollständige Bestandsaufnahme Ihres gesamten API-Bestands durchzuführen, suchen Sie nach Tools mit einem automatisierten Ansatz zur Erkennung von APIs und den von ihnen unterstützten Microservices. Die Breite der Abdeckung ist von entscheidender Bedeutung, da nicht verwaltete APIs (siehe Seitenleiste auf Seite 10) ein Hauptziel für Bedrohungsakteure sind.

2 In Tests investieren

Wählen Sie eine API-Sicherheitslösung, mit der Sie einfach testen können, ob APIs für die beabsichtigte Funktion korrekt programmiert sind. Idealerweise werden Tests vor der Bereitstellung durchgeführt. Es ist jedoch auch wichtig, alle bereits in Produktion befindlichen APIs mit Echtzeitanalyse des Datenverkehrs und potenziellen Schwachstellen zu testen.

3 Vollständige API-Dokumentation erstellen

Es ist entscheidend, Ihre gesamte API-Umgebung kontinuierlich zu prüfen, um falsch konfigurierte APIs oder andere Fehler zu identifizieren. Ihr Audit sollte außerdem eine angemessene Dokumentation jeder API gewährleisten und ermitteln, ob die APIs sensible Daten enthalten und ob sie über geeignete Sicherheitskontrollen verfügen. Dies hilft Ihnen auch, sich auf Compliance-Anforderungen vorzubereiten, die die API-Sicherheit implizit oder explizit betreffen (siehe Seite 14).

4 Laufzeiterkennung verwenden

Mit einer API-Sicherheitslösung mit automatisierter Laufzeiterkennung können Sie zwischen „normaler“ und „nicht normaler“ API-Aktivität unterscheiden. Durch diese Überwachung von API-Interaktionen können Sie in Echtzeit Verhaltensweisen erkennen, die auf eine Bedrohung hinweisen, und auf sie reagieren.

5 Auf verdächtiges Verhalten reagieren

Durch die Integration einer API-Sicherheitslösung in Ihren vorhandenen Sicherheits-Stack (z. B. WAF oder WAAP) können Sie risikoreiche Verhaltensweisen erkennen und verdächtigen Datenverkehr blockieren, bevor ein Zugriff auf kritische Ressourcen erfolgt.

6 Bedrohungen untersuchen und verhindern

Im höchsten Stadium der API-Sicherheit führen Sie regelmäßig forensische Analysen vergangener Bedrohungsdaten durch, um zu erfahren, ob Warnungen Bedrohungen korrekt erkannt haben und ob Muster aufgetreten sind, die eine proaktive Bedrohungssuche mithilfe einer Kombination aus ausgeklügelten Tools und menschlicher Intelligenz möglich machen.

Fazit

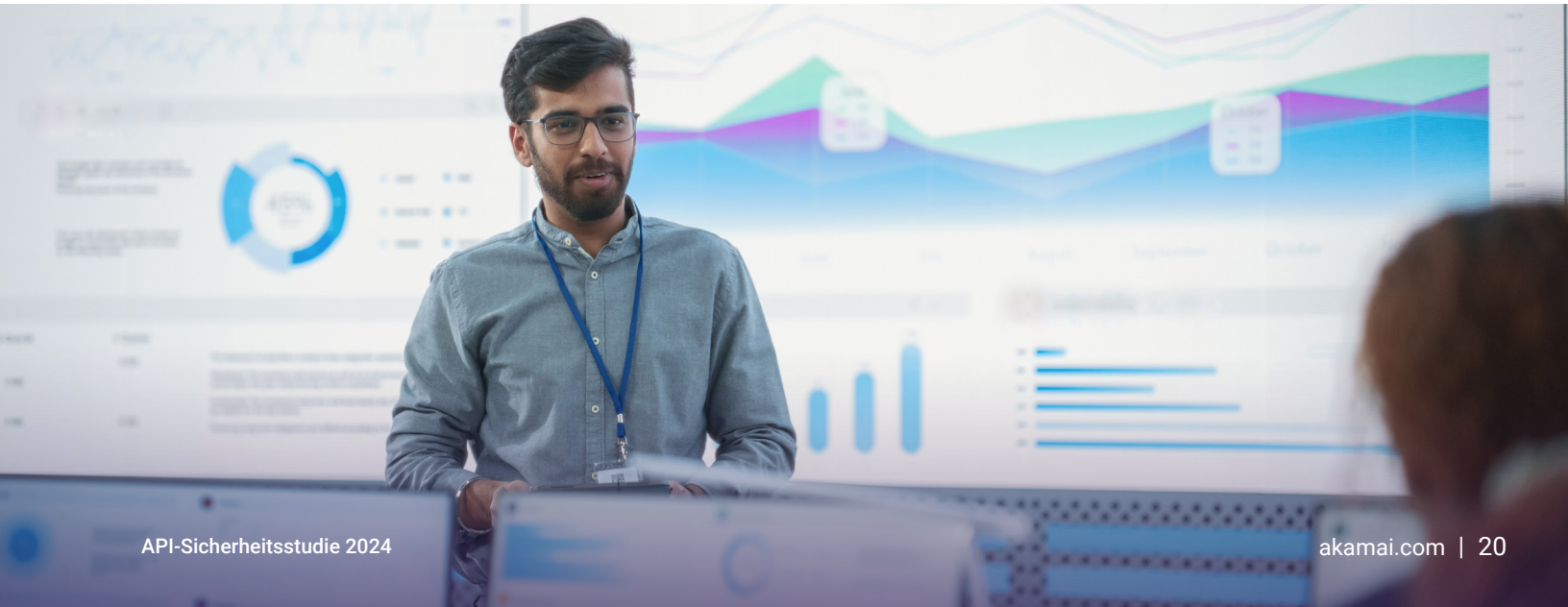
Der diesjährige Bericht machte deutlich, dass es bei der Sicherheit – in diesem Fall bei der API-Sicherheit – nicht nur um Bedrohungslisten oder Tools geht, sondern um Menschen.

Unsere Studie bestätigt, dass Sicherheitsteams überlastet sind und dass die Aussicht, die Arbeitslast Ihres Teams durch eine völlig neue Angriffsmethode zu steigern, erschreckend erscheint. Die Verbreitung von APIs wird jedoch nicht nachlassen, und Maßnahmen zur Sicherung Ihrer APIs haben einen starken Einfluss auf weitere hohe Prioritäten wie GenKI-Schwachstellen (zum Schutz der APIs, die Daten mit LLMs austauschen) und Cloudsicherheit (zur Verringerung des Risikos in jeder API, die in migrierten Workloads enthalten ist).

Wir sind fest davon überzeugt, dass die proaktive Arbeit an der API-Sicherheit nicht nur Ihr Unternehmen schützt, sondern auch die Perspektive Ihres Teams auf diesen kritischen Angriffsvektor viel glaubwürdiger und vertrauenswürdiger werden lässt – gegenüber Kollegen, Führungskräften und dem Vorstand. Dies hat den enormen Vorteil, dass die Stressbelastung in Ihrem Team verringert wird. Unsere Studie sagt aus, dass Teams stark von API-Sicherheitsvorfällen und der Skepsis und dem Goodwill-Verlust betroffen sind, die diese bei Kollegen und Kunden auslösen.

Wenn Sie jetzt Maßnahmen ergreifen, vereinfachen Sie auch präventiv Ihre Compliance-Planung und -Berichterstattung, ganz zu schweigen von der rechtzeitigen Vermeidung von Bußgeldern. Warum also nicht anfangen?

- Wenn Sie bereit für die nächsten Schritte auf Ihrem Weg zu einer ausgereiften API-Sicherheit sind, empfehlen wir Ihnen, mit unserem Whitepaper Grundlagen der API-Sicherheit zu beginnen.
- Wenn Sie gerne ein Gespräch über Ihre Herausforderungen führen und erfahren möchten, wie wir Ihnen helfen können, können Sie ganz einfach eine individuelle API-Sicherheitsdemo von Akamai anfordern.



Informationen zur API-Sicherheitsstudie

Die Umfrage für die API-Sicherheitsstudie wurde vom 12. Juni 2023 bis 7. Juli 2024 von Opinion Matters durchgeführt. Insgesamt wurden 1.207 Teilnehmer mit folgender Aufschlüsselung nach Sitz des Unternehmens befragt: 404 aus dem Vereinigten Königreich, 402 aus den USA und 401 aus Deutschland. Ein Drittel der Befragten waren CIOs oder CISOs, ein Drittel leitende Sicherheitsexperten und ein Drittel stammte aus Teams für Anwendungssicherheit, die alle in Unternehmen mit einer Größe von unter 500 bis über 1.000 Mitarbeitern in acht Schlüsselbranchen tätig sind: Automobilindustrie, Finanzdienstleistungen, Einzelhandel/E-Commerce, Gesundheitswesen, Versicherungen, Staat/öffentlicher Sektor, verarbeitende Industrie und Energie/Versorgungsunternehmen.

Opinion Matters beschäftigt Mitglieder der Market Research Society und hält ihre Regeln sowie den MRS-Verhaltenskodex und die ESOMAR-Grundsätze ein. Opinion Matters ist auch Mitglied des British Polling Council.

Mitwirkende

Lead Writer
Annie Brunholzl

Managing Editor
John Natale

Research Director
Mitch Mayne

Copy Editor
Randi Kravitz

Werbung
Barney Beal

Marketing und Veröffentlichung
Georgina Morales Hampe

Prüfung und fachliche Expertise
Pam Cobb
Jim Lubinskas
Kimberly Gomez
Stas Neyman

„State of the Internet“-Sicherheitsbericht

Lesen Sie vorherige Ausgaben und informieren Sie sich über bevorstehende Veröffentlichungen der renommierten „State of the Internet“-Sicherheitsberichte von Akamai. **akamai.com/soti**

Bedrohungsforschung bei Akamai

Halten Sie sich unter diesem Link zu neuesten Threat-Intelligence-Analysen, Sicherheitsberichten und Cybersicherheitsforschung auf dem Laufenden **akamai.com/security-research**

Akamai API Security

Erfahren Sie, wie Akamai APIs während ihres gesamten Lebenszyklus von der Entwicklung bis zur Produktion schützt – mit wichtigen Funktionen für API-Erkennung, Positionierung, Laufzeitschutz und API-Sicherheitstests. **https://www.akamai.com/products/api-security**