

The logo consists of the letters 'FOS' in a large, white, sans-serif font. The 'F' and 'O' are connected, and the 'S' is positioned below the 'O'. The background of the entire cover features a digital landscape with blue and purple wavy terrain and a starry sky.

B11.AUSGABE 02

Der Zustand der Anwendungs- und API-Sicherheit **2025**

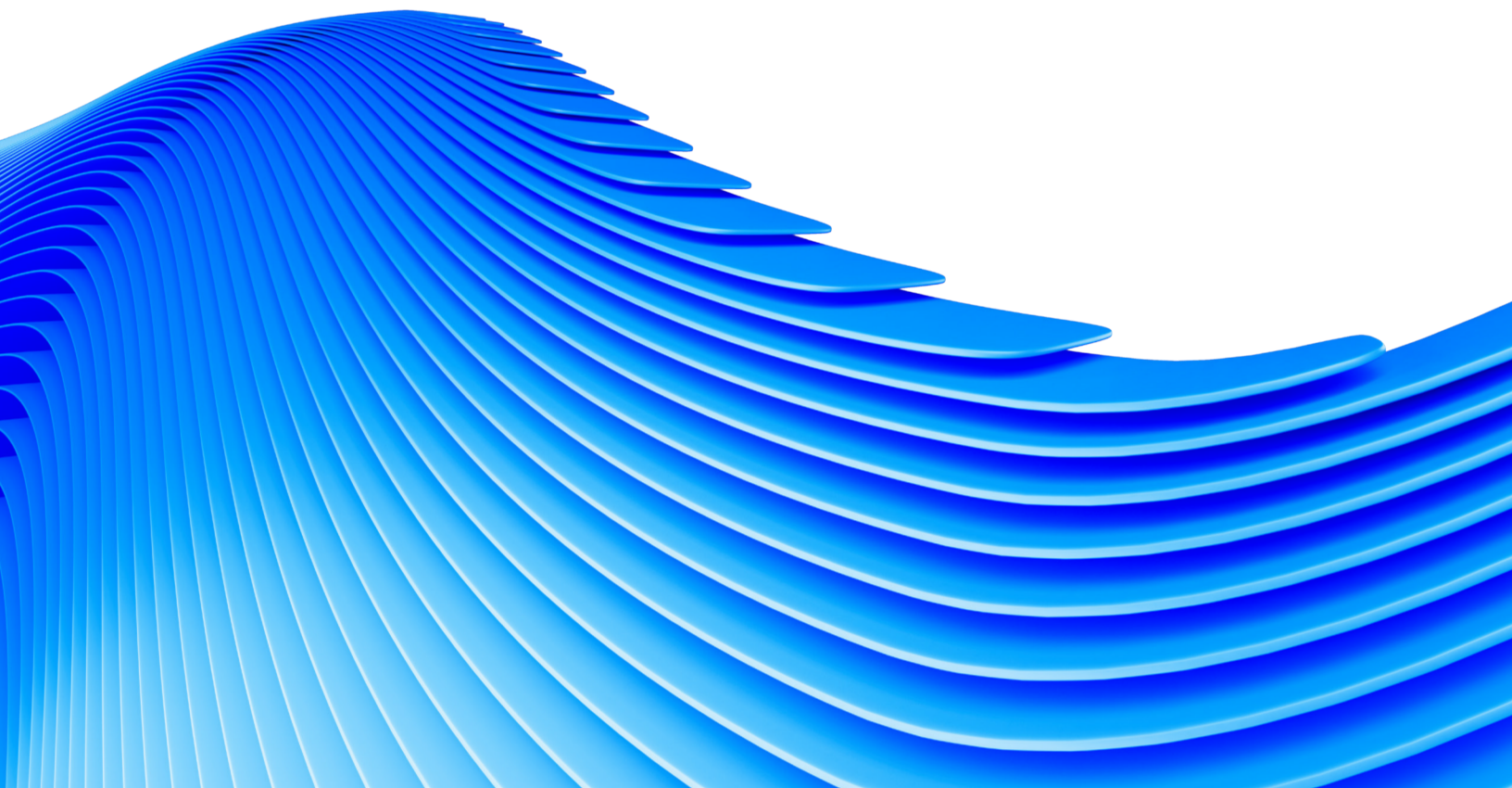
Wie künstliche Intelligenz das digitale Terrain verändert



„State of the Internet“-**Sicherheitsbericht**

Inhalt

02	Einführung
04	Wichtige Erkenntnisse aus dem Bericht
06	Weiterentwicklung unserer API-Bedrohungsinformationen
13	Webangriffe: Jahresvergleich und Trends
17	Layer-7-DDoS-Angriffe: Jahresvergleich und Trends
21	Branchentrends
27	Regionale Trends
39	Compliance
44	Abwehr
46	Methodik
47	Mitwirkende



Einführung

Die Landschaft der Webanwendungssicherheit ist Anfang 2025 von einer beispiellosen Komplexität und Raffinesse der Bedrohungsvektoren geprägt. Unternehmen sehen sich mit einer deutlichen Zunahme von Angriffen auf Webanwendungen konfrontiert. Allein 2024 beobachtete Akamai mehr als 311 Milliarden Angriffe auf Webanwendungen und APIs, was einem Anstieg von 33 % gegenüber dem Vorjahr entspricht. Dieser Anstieg steht in direktem Zusammenhang mit der beschleunigten Einführung von Cloud-Services, Microservices-Architekturen und KI-basierten Anwendungen. Geopolitische [Faktoren](#) haben die Probleme weiter verschärft: So hat die Hightech-, Handels- und Social-Media-Industrie das größte Volumen von DDoS-Angriffen (Distributed Denial-of-Service) auf Layer 7 (Anwendungsschicht) erlebt. Insbesondere setzen Cyberkriminelle heute [KI-generierte Kill Chains](#) ein, die den gesamten Angriffslebenszyklus automatisieren.

Gleichzeitig sind auch APIs zu primären Zielen geworden: Akamai dokumentierte mehr als 150 Milliarden API-Angriffe zwischen Januar 2023 und Dezember 2024. Indem KI-gestützte SaaS-Tools (Software-as-a-Service) per APIs in zentrale Plattformen integriert wurden, wurde die Angriffsfläche erheblich erweitert. Die finanziellen [Auswirkungen](#) sind gravierend: Probleme mit der API-Sicherheit kosten derzeit rund 87 Milliarden US-Dollar jährlich. Prognosen deuten darauf hin, dass diese Zahl ohne angemessene Intervention bis 2026 auf über 100 Milliarden US-Dollar wachsen könnte. Shadow- und Zombie-APIs stellen besonders anfällige Angriffsvektoren in zunehmend komplexen API-Umgebungen dar.



Die Rolle von KI bei der Sicherheit von Webanwendungen und APIs

KI transformiert sowohl die Webanwendungs- als auch die API-Sicherheit, indem sie die Funktionen zur Erkennung und Reaktion von Bedrohungen verbessert – sie bringt aber auch neue Herausforderungen mit sich. In Webanwendungen wird KI **verwendet**, um die Erkennung von Bedrohungen zu automatisieren, potenzielle Sicherheitsverstöße vorherzusagen und die Vorfallsreaktion zu beschleunigen. Doch KI **ermöglicht** es Angreifern auch, KI-basierte Malware und ausgeklügelte Web-Scraper zu erstellen und den gesamten Angriffslebenszyklus mithilfe dynamischer Methoden zu automatisieren.

Im Bereich der APIs spielt KI eine entscheidende **Rolle** für die Verwaltung und Sicherung der riesigen Anzahl von API-Interaktionen. KI-basierte Tools sind unerlässlich, um Anomalien und unzulässige Verhaltensmuster zu erkennen und die Bedrohungsreaktion in Echtzeit zu automatisieren. Und KI-gestütztes API-Management wird sich noch **weiterentwickeln** – durch die Integration prädiktiver Analysen und automatisierter Sicherheitsmaßnahmen zum Schutz vor immer komplexeren Angriffen. Trotz dieser Fortschritte stellen KI-basierte **Angriffe** auf APIs – darunter Credential Stuffing oder die Ausnutzung der Geschäftslogik – nach wie vor ein erhebliches Problem dar. Und es braucht leistungsstarke Sicherheitsframeworks, um diesen Bedrohungen effektiv entgegenzuwirken.

Anders, aber doch mit Gemeinsamkeiten: Strategien gegen Angriffe auf Webanwendungen und APIs

Angriffe auf Webanwendungen und APIs stehen zwar miteinander in Verbindung, richten sich aber auf verschiedene Aspekte der Anwendungsinfrastruktur:



Angriffe auf Webanwendungen zielen auf nutzerseitige Komponenten von Webanwendungen ab, z. B. öffentliche Anmeldeseiten, und setzen häufig weniger ausgeklügelte Techniken ein.



API-Angriffe konzentrieren sich auf die Ausnutzung von Schwachstellen in den API-Endpunkten und der Backend-Logik einer Anwendung, was ein tieferes Verständnis der Struktur und des Verhaltens der API erfordert.

Die Hauptunterschiede liegen in der Angriffsfläche und der Komplexität. Angriffe auf Webanwendungen zielen in der Regel auf die sichtbaren Teile einer Anwendung ab, während API-Angriffe die Kommunikationskanäle zwischen verschiedenen Softwarekomponenten ausnutzen. Wenn sie erfolgreich sind, können sie jedoch beide unbefugten Zugriff auf vertrauliche Daten und Systemressourcen gewähren.

Es ist entscheidend, die nötigen Cybersicherheitsmaßnahmen sowohl für Webanwendungs- als auch für API-Angriffe zu kennen – denn moderne Anwendungen sind zunehmend auf APIs angewiesen, um zu funktionieren. Unternehmen erwarten, dass Webanwendungen in den nächsten zwei Jahren um 39 % **zunehmen** werden, weshalb das Zusammenspiel von Web- und API-Sicherheit heute so wichtig ist. Wenn Unternehmen einen dieser Aspekte vernachlässigen, sind sie **anfällig** für ausgeklügelte Angriffe mit mehreren Vektoren, die Schwachstellen sowohl im Frontend als auch im Backend von Anwendungen ausnutzen.

Die einzigartige Perspektive von Akamai: Aufdeckung von Bedrohungsmustern

Bei der Analyse all dieser Komplexität profitiert Akamai von seiner Netzwerkinfrastruktur, die mehr als ein Drittel des globalen Webverkehrs verarbeitet und so einen unübertroffenen Einblick in Bedrohungsmuster bietet. Diese Perspektive und die Erkenntnisse seiner Forschungs- und Data-Science-Teams ermöglichen es Akamai, umfassende und aussagekräftige Informationen bereitzustellen. Die Ergebnisse liefern Sicherheitsexperten die nötigen strategischen Erkenntnisse, um zu entscheiden, wo sie sich auf die Risikominderung konzentrieren sollen, um die Rendite aus Sicherheitsinvestitionen zu maximieren.

Wichtige Erkenntnisse aus dem Bericht



KI-basierte APIs sind unsicherer als ihre Gegenstücke.

Der Großteil der KI-gestützten APIs ist extern zugänglich und viele von ihnen verfügen über nur unzureichende Authentifizierungsmechanismen. Diese Schwachstelle wird durch die wachsende Anzahl KI-gestützter Angriffe noch vergrößert.



KI fördert den technischen Fortschritt von Cyberkriminellen.

Dazu gehören Verbesserungen wie KI-basierte Malware, Schwachstellenscans, Angriffe auf KI-integrierte Systeme oder ausgeklügelte Web-Scraper.

32 %

Prozentuale Zunahme von Zwischenfällen in Bezug auf die OWASP API Security Top 10

API-Sicherheitsvorfälle nehmen zu, wobei die OWASP (Open Worldwide Application Security Project) API Security Top 10 darauf hindeuten, dass Authentifizierungs- und Autorisierungsfehler, die vertrauliche Daten und Funktionen offenlegen, die größten Probleme darstellen.

30 %

Zunahme der Sicherheitswarnungen im Zusammenhang mit dem MITRE-Sicherheitsframework

Angreifer nutzen fortschrittliche Techniken, einschließlich Automatisierung und KI, um APIs auszunutzen. Das MITRE-Framework kann Verteidiger dabei unterstützen, diese Angriffe schneller und genauer zu erkennen.

33 %

Prozentuale Zunahme globaler Webangriffe im Jahresvergleich

Die Zunahme der Angriffe steht in direktem Zusammenhang mit der schnellen Einführung von Cloud-Services, Microservices und KI-Anwendungen, die die Angriffsflächen erweitern und neue Sicherheitsherausforderungen mit sich bringen.

Über 230 Milliarden

Anzahl der Webangriffe, die Handelsorganisationen getroffen haben

Damit ist der Handel die am stärksten betroffenen Branche. Er verzeichnete fast dreimal so viele Angriffe wie die Hightech-Branche (die am zweithäufigsten angegriffene Branche).

73 %

Zunahme der Gesamtzahl von Webangriffen im Jahresvergleich in der APJ-Region

Angriffe stiegen von 29 Milliarden im Jahr 2023 auf 51 Milliarden im Jahr 2024.

37 %

Prozentsatz der Webangriffe in der EMEA-Region, die auf APIs abzielten

Das ist die höchste Konzentration solcher Angriffe in allen Regionen.

94 %

Anstieg der vierteljährlichen Layer-7-DDoS-Angriffe

(zwischen Q1 2023 und Q4 2024)

11,9 Billionen

Anzahl der Layer-7-DDoS-Angriffe, die auf Nordamerika abzielten

(im 2-Jahres-Zeitraum zwischen Q1 2023 und Q4 2024)

7 Billionen

Anzahl der Layer-7-DDoS-Angriffe, die auf den Hightech-Sektor abzielten

(Januar 2023 bis Dezember 2024.) Damit ist Hightech die am stärksten betroffene Branche.

7,4 Billionen

Anzahl der Layer-7-DDoS-Angriffe, die auf die APJ-Region abzielten

(im 2-Jahres-Zeitraum zwischen Q1 2023 und Q4 2024)

20 %

Prozentsatz der Layer-7-DDoS-Angriffe auf APIs, die auf die EMEA-Region abzielten

Das stellt die höchste Konzentration dieses Angriffstyps in allen Regionen dar.

Weiterentwicklung unserer API-Bedrohungsinformationen

Durch die Integration von Noname Security hat Akamai seine Fähigkeiten zur API-Bedrohungsforschung und -Berichterstattung erheblich verbessert und liefert eine neue Sicht auf API-spezifische Risiken. Akamai nutzt diesen neuen Datensatz (der sich noch in der Anfangsphase der Datenintegration befindet), um unsere vorhandenen Bedrohungsinformationen zu verbessern und eine erweiterte Ansicht von API-Sicherheitsproblemen zu ermöglichen.

Zuordnen von Warnungen zu Sicherheitsframeworks

Im Laufe der Zeit können wir mit diesem neuen Datensatz immer mehr Details zu Sicherheitswarnungen zuordnen und mit kritischen Cybersicherheitsframeworks und Compliance-Standards in Verbindung bringen, darunter:

- MITRE Adversarial Tactics, Techniques and Common Knowledge (ATT&CK)
- Datenschutz-Grundverordnung (DSGVO)
- Payment Card Industry Data Security Standard (PCI DSS)
- Internationale Organisation für Normung (ISO)
- Open Worldwide Application Security Project (OWASP)

Durch diese Verbesserungen kann Akamai seinen Kunden einen leistungsstarken Schutz anbieten. Durch die Abstimmung mit diesen Frameworks können Unternehmen ihre Sicherheitslage besser verstehen, gesetzliche Auflagen erfüllen und ihre Sicherheitsmaßnahmen effektiv priorisieren. Mit diesem umfassenden Ansatz können Unternehmen Ressourcen strategisch zuweisen und gezielte Strategien zum Schutz ihrer APIs und sensiblen Daten entwickeln.

Analyse einer 30-Tage-Datenprobe

Für diesen Bericht haben wir eine 30-Tage-Datenprobe analysiert, um die allgemeine Aktivität der Cyberkriminellen in jedem Cybersicherheitsframework und Compliance-Standard hervorzuheben (Abbildung 1). Wir bieten auch eine tiefere Perspektive auf MITRE- und OWASP-Warnungen. Außerdem untersuchen wir, wie sich diese Risiken und Sicherheitsvorfälle auf Compliance-Standards auswirken können.

	30-Tage-Aktivität	Monatlicher Anstieg
OWASP	5.907.000	32 %
MITRE	2.817.000	30 %
ISO	832.000	22 %
DSGVO	669.000	21 %
PCI DSS	881.000	16 %

Abb. 1: Aufschlüsselung der Sicherheitswarnungen nach Sicherheitsframeworks und Compliance-Standards

MITRE-Warnungen

Über einen Zeitraum von 30 Tagen konnten wir bei unseren Kunden einen Anstieg der Vorfälle im Zusammenhang mit MITRE-Techniken um 30 % feststellen. Vor allem haben Angreifer häufig T1078 (gültige Konten) eingesetzt, indem sie legitime Anmeldedaten ausgenutzt haben, um unbefugten Zugriff auf Systeme oder Netzwerke zu erhalten. Da APIs häufig Token für die Autorisierung benötigen, können Angreifer, die diese Token erhalten, auf vertrauliche Daten zugreifen, ohne hierbei erkannt zu werden.

Wir haben auch T1566 (Phishing) identifiziert, bei dem Angreifer Phishing-Kampagnen starteten, um API-Token oder Anmeldeinformationen für künftige Angriffe zu stehlen. Da APIs die Angriffsfläche erweitern, nutzen Cyberkriminelle diese zunehmend aus, um sich Zugang zu verschaffen. Darüber hinaus haben Warnungen im Zusammenhang mit T1190 (Ausnutzung öffentlich zugänglicher Anwendungen) Angreifer aufgedeckt, die Anwendungsfehler nutzten, um Netzwerke zu infiltrieren. Eine weitere beobachtete Technik war T1580 (Cloud-Infrastruktur-Erkennung), bei der Angreifer APIs für die Aufklärung verwendeten, indem sie öffentlich zugängliche Cloud-Endpunkte über API-Aufrufe sondierten.

Obwohl MITRE über keine spezielle Sicherheitsmatrix für APIs verfügt, bleibt sein Framework für Sicherheitsteams und Organisationen, die Einblicke in API-orientierte Angreifertechniken suchen, von entscheidender Bedeutung. Indem die Taktiken von Angreifern API-spezifischen Verhaltensweisen zugeordnet werden, können Sicherheitsteams die Vorfälle und Bedrohungserkennung verbessern, indem sie Angriffsphasen und zugehörige Taktiken, Techniken und Verfahren identifizieren. Dieser Ansatz ermöglicht es Verteidigern, Risiken effektiver zu mindern.

OWASP-Warnungen

Die OWASP API Security Top 10 ist eine wichtige Ressource, die verwertbare Einblicke in die Auswirkungen und den Schweregrad von Sicherheitslücken bietet. Hiermit können Entwickler und Sicherheitsteams Initiativen effektiv priorisieren, da sie Updates erhalten, mit denen sie stets über aktuelle Informationen über die dynamische Bedrohungslandschaft verfügen.

Während des 30-tägigen Stichprobenzeitraums ergab unsere Analyse einen Anstieg der OWASP-bezogenen Vorfälle um 32 %. Besonders durch Sicherheitsanfälligkeiten wie Broken Object Property Level Authorization (BOPLA), Autorisierung auf Funktionsebene und fehlerhafte Authentifizierung konnten Angreifer direkt auf sensible Daten oder kritische Funktionen zugreifen. Unzureichende Autorisierungsmechanismen ermöglichen es Angreifern, Berechtigungen zu eskalieren, Konten zu übernehmen und auf vertrauliche Informationen zuzugreifen. Das macht sie zu den gefährlichsten Angriffsmethoden für APIs.

Broken Object Level Authorization (BOLA) ist nach wie vor eine kritische Sicherheitslücke für APIs, die aufgrund ihrer Abhängigkeit von Geschäftslogikfehlern nur schwer zu erkennen ist. Das führt häufig zu einer unzureichenden Berichterstattung oder zu niedrigen Erkennungsraten. Um diesem Problem gerecht zu werden, sollten Unternehmen API-Sicherheitslösungen einsetzen, die klare Beziehungen herstellen: zwischen Nutzern und den Ressourcen, auf die sie normalerweise zugreifen. Hierfür müssen über ausgeklügelte ML-Algorithmen (maschinelles Lernen) Verhaltens-Baselines festgelegt werden, die in der Lage sind, anomale Zugriffsmuster zu erkennen.

BOPLA nutzt kleinste Zugriffsprobleme im API-Betrieb aus, die bei Sicherheitstests oft übersehen werden. Im Gegensatz zu BOLA, wo ganze Objekt-IDs geändert werden müssen, zielen BOPLA-Angriffe auf bestimmte Eigenschaften innerhalb von Objekten ab. So stellt beispielsweise ein DELETE-API-Aufruf, der vertrauliche personenbezogene Daten in seiner Antwort offenlegt, eine BOPLA-Sicherheitsanfälligkeit dar. Aufgrund dieser Subtilität sind BOPLA-Probleme stärker verbreitet als BOLA-Angriffe.

Ein praktisches Beispiel ist eine E-Mail-Abmeldung, bei der lediglich die E-Mail-Adresse verwendet wird und die API-Antwort versehentlich den vollständigen Namen und die Adresse des Nutzers enthält. Diese Offenlegung sensibler Daten gegenüber nicht autorisierten Parteien erfolgt, weil Sicherheitstests in der Regel auf ganze Objekte statt auf einzelne Eigenschaften ausgerichtet sind. Diese Tatsache trägt zur besseren Erkennung von BOPLA-Sicherheitsanfälligkeiten in API-Sicherheitsbewertungen bei.

Eine weitere kritische Sicherheitsanfälligkeit ist uneingeschränkte Ressourcennutzung, mit der Angreifer Ressourcen erschöpfen oder DDoS-ähnliche Angriffe durchführen können, um Serviceunterbrechungen zu verursachen. Doch diese Schwachstelle birgt Risiken, die über bloße Serviceauswirkungen hinausgehen: darunter höhere Betriebskosten aufgrund der übermäßigen Nutzung von Cloud-Ressourcen oder auch das erhöhte Risiko von Brute-Force-Angriffen. Ohne angemessene Ratenbegrenzung können Angreifer schnell APIs ermitteln, was die Sicherheit gefährden kann. Darüber hinaus erzeugen diese Angriffe viel Datenverkehr, was zu erheblichen Kostensteigerungen für Unternehmen führt.

Die unsichere Nutzung von APIs – die auf unzureichende Validierung, Datenfilterung und fehlende Sicherheitsmechanismen bei API-Integrationen von Drittanbietern zurückzuführen ist – stellt eine weitere wichtige Bedrohungsquelle dar. Dieses Problem wird immer besorgniserregender, da Unternehmen bei der digitalen Transformation immer stärker auf APIs von Drittanbietern angewiesen sind. Eine [kürzlich durchgeführte Studie](#) ergab, dass mehr als 80 % der befragten Unternehmen Probleme mit APIs von Drittanbietern hatten. Das unterstreicht die Bedeutung der Einführung eines Zero-Trust-Sicherheitsmodells. Obwohl diese Schwachstelle allein nicht sofort katastrophal ist, kann sie sich in Kombination mit anderen Schwachstellen, wie unzureichender Validierung oder unsicheren Abhängigkeiten, zu einer großen Sicherheitsbedrohung entwickeln. Wenn beispielsweise eine Finanz-API nicht verifizierten Transaktionen von Dritten vertraut, kann das zu Sicherheitsverstößen führen.



Die Sicherheitswarnungen im Zusammenhang mit PCI DSS und DSGVO stiegen um 16 bzw. 21 %, während die Warnmeldungen im Zusammenhang mit ISO 27001 um 22 % zunahmen.

Gewährleisten der API-Compliance

Zu den Best Practices für die Gewährleistung der API-Compliance gehört das Kennzeichnen jeder Warnung mit den spezifischen Compliance- und Regulierungsstandards, die sie verletzt. So erhalten Unternehmen sofort Einblicke in kritische Compliance-Probleme sowie Handlungsempfehlungen für deren Behebung. Dieser proaktive Ansatz unterstützt Unternehmen bei der Einhaltung gesetzlicher Vorschriften, wodurch das Risiko von Bußgeldern, rechtlichen Auswirkungen und Reputationsschäden verringert wird, die ansonsten zu erheblichen finanziellen Verlusten führen können. Beispielsweise [musste eine Fluggesellschaft eine Geldstrafe von 20 Millionen Pfund zahlen](#), nachdem eine API-Schwachstelle die Daten von 400.000 Kunden offengelegt hatte. Das verdeutlicht die schwerwiegenden Folgen unzureichender API-Sicherheit im Rahmen der DSGVO.

Compliance-Standards dienen Unternehmen als unverzichtbare Sicherheitsvorkehrungen zum Schutz vertraulicher Daten, zum Schutz von Kunden und zur Einhaltung gesetzlicher und behördlicher Auflagen. Standards wie PCI DSS, DSGVO und Health Insurance Portability and Accountability Act (HIPAA) erfordern den sicheren Umgang mit sensiblen Informationen wie Zahlungs- oder personenbezogenen Daten. Laut unserer Datenanalyse stiegen die Sicherheitswarnungen im Zusammenhang mit PCI DSS und DSGVO um 16 bzw. 21 %, während die Warnmeldungen im Zusammenhang mit ISO 27001 um 22 % zunahmen.

DSGVO

Die DSGVO legt den Schwerpunkt auf die Integration von Datensicherheit und Kundendatenschutz über den gesamten API-Lebenszyklus hinweg. Dazu gehören sicheres Design, starke Authentifizierung und Autorisierung, Ratenbegrenzung, regelmäßige Schwachstellentests, Verschlüsselung und laufende Risikobewertungen – auch in frühen Entwicklungsphasen. Diese Maßnahmen gewährleisten die Vertraulichkeit, Integrität und Verfügbarkeit von Daten.

PCI DSS

Auf ähnliche Weise betont [PCI DSS](#) den Schutz von APIs, die Zahlungskartendaten verarbeiten, indem Sicherheit in die Entwicklungs-, Codierungs- und Testphasen integriert wird. Der Standard erfordert Schutz vor Sicherheitslücken im Internet sowie regelmäßige Tests, um Schwachstellen zu erkennen und zu beheben.

Die Anforderungen 10 und 11 erfordern insbesondere eine umfassende Protokollierung und Überwachung von API-Aktivitäten, einschließlich Anfragen, Antworten, Authentifizierungsversuchen und Systemänderungen. Die Protokolle müssen mindestens zwölf Monate lang aufbewahrt werden, wobei die letzten drei Monate für die Analyse leicht zugänglich sein müssen. Außerdem wird empfohlen, dass Unternehmen nach umfangreichen Änderungen externe Schwachstellenscans durchführen. Um die PCI-Compliance zu gewährleisten, müssen Unternehmen strenge Kontrollen implementieren, darunter Ratenbegrenzung, Protokollierung, rollenbasierte Zugriffskontrollen und Sitzungsverwaltung, um sicherzustellen, dass APIs gegen Bedrohungen und Risiken geschützt sind.



ISO 27001

Der ISO-27001-Standard bietet ein solides Framework für das effektive Management von Informationssicherheitsrisiken, die Verbesserung der Unternehmenssicherheit und die Förderung des Vertrauens von Kollegen und Kunden. Hier einige empfohlene Best Practices:

- Implementieren von Zugriffskontrollen (z. B. API-Schlüssel) zur Überprüfung der Nutzeridentität
- Durchgängige Datenverschlüsselung
- Überwachung von APIs auf anomales Verhalten
- Gründliche Risikobewertungen, um potenzielle API-Schwachstellen zu identifizieren

Diese Compliance-Anforderungen verdeutlichen den kritischen Schnittpunkt zwischen API-Sicherheit und regulatorischen Frameworks. Eine ordnungsgemäße Implementierung schützt nicht nur sensible Daten, sondern erfüllt auch mehrere Compliance-Anforderungen gleichzeitig. Weitere Informationen zu bestehenden und neuen globalen Standards finden Sie im Abschnitt [Compliance](#) dieses Berichts.

API-Transparenzlücken: die verborgenen Pfade zu Daten

API-Missbrauch

Im November 2024 [meldete Bleeping Computer](#) einen erheblichen Angriff auf einen Anbieter von E-Signatur-Lösungen. Hierbei nutzten Cyberkriminelle eine Kernkomponente der Dokumentenverwaltungs- und -verfolgungs-API des Anbieters aus, wodurch sie betrügerische Rechnungen an zahlreiche potenzielle Opfer senden konnten. Wenn Empfänger diese Dokumente unwissentlich unterschrieben, konnten Angreifer anschließend Zahlungen von verschiedenen Organisationen anfordern.

Dieser Vorfall unterstreicht die schädlichen Auswirkungen einer API-Ausnutzung – Cyberkriminelle können APIs über ihr beabsichtigtes Design hinaus ausnutzen und in unbeabsichtigte Angriffsvektoren verwandeln. Die Entstehung generativer KI hat diese Risiken weiter verschärft, indem die Schwachstellensuche automatisiert und Ratenbegrenzungen umgangen werden, was schnellere und ausgefeiltere Angriffe ermöglicht.

Quelle: [bleepingcomputer/Wallarm](#)

Please Review & Act on These Documents



Elaine Harris
Symantec

Norton
Receipts & Invoice
[View More](#)

Norton
Internet Security
Powered by [docusign](#)

Please review the documents below.

CONTINUE

OTHER ACTIONS ▾

Signature
 Initial
 Stamp
 Date Signed

Name
 First Name
 Last Name
 Email Address
 Company
 Title

- Comprehensive protection against viruses and malware
- Identity theft protection
- Performance optimization tools
- 24/7 customer support

DETAILS:

PRODUCT	TENURE	AMOUNT
Norton LifeLock 360	2 Users/1 Year	249.00 USD
	Activation Charges	49.00 USD
TOTAL		298.00 USD

POLICY:

We understand that circumstances can change and you may need to cancel your subscription. We

Herausforderungen bei der Erkennung von API-Missbrauch

Sicherheitsteams stoßen bei der Erkennung von API-Missbrauch auf erhebliche Hindernisse – vor allem aufgrund der Notwendigkeit, eine Baseline für normales Verhalten festzulegen, um anhand dieser Baseline verdächtiges Verhalten zu erkennen. Diese Herausforderung unterstreicht die Notwendigkeit einer Echtzeit-Verhaltensüberwachung, um Anomalien und Bedrohungen präventiv zu erkennen.

Unsere [Studie zur Auswirkung auf die API-Sicherheit 2024](#) zeigt einen besorgniserregenden Trend: Nur 13 % der befragten Unternehmen testen ihre APIs täglich – ein deutlicher Rückgang gegenüber 37 % im Jahr 2023. Dieser Rückgang ist angesichts der aktuellen Bedrohungslage besonders alarmierend. Die drastische Reduzierung täglicher API-Tests setzt Unternehmen erhöhten Sicherheitsrisiken aus. Denn hierdurch wird ihre Fähigkeit, schnell wachsende Bedrohungen zu erkennen und darauf zu reagieren, erheblich eingeschränkt, wodurch kritische Schwachstellen potenziell über längere Zeiträume nicht behoben werden.

Durch häufige automatisierte Tests während der Entwicklungszyklen können Unternehmen Probleme frühzeitig erkennen und beheben. Hierdurch werden kostspielige Abhilfemaßnahmen in Produktionsumgebungen vermieden. In einer Zeit, in der die API-Ausnutzung zunehmend automatisierte und verdeckte Methoden verwendet, spielen proaktive Tests eine entscheidende Rolle bei der Risikominderung.

Nicht verwaltete APIs: Zombie- und Schatten-APIs

Die Transparenz von API-Assets bleibt eine entscheidende Herausforderung für Unternehmen – sie umfasst sowohl die offizielle API-Verfolgung als auch die Identifizierung sensibler Daten. Unsere [Studie zur Auswirkung auf die API-Sicherheit 2024](#) hat eine erhebliche Lücke aufgedeckt: 47 % der AppSec-Teams führen vollständige API-Bestände, identifizieren jedoch nicht die APIs, die vertrauliche Daten verarbeiten. Leitende Sicherheitsexperten berichten von ähnlichen Einschränkungen: 42 % von ihnen haben mit diesem Problem zu kämpfen. Alarmierend ist, dass der Anteil der Unternehmen, die vollständige API-Bestände führen und wissen, wo sensible Daten verarbeitet werden, von 40 % im Jahr 2023 auf 27 % im Jahr 2024 zurückgegangen ist. In der Sicherheitsstudie werden Zombie- und Schatten-APIs als eine der Hauptursachen für API-Sicherheitsvorfälle hervorgehoben.

In unvollständigen Beständen fehlen in erster Linie Zombie- und Schatten-APIs. Zombie-APIs (also veraltete Schnittstellen, die aufgrund unvollständiger Stilllegung, Personalfluktuations oder anderer Gründe aktiv bleiben) erzeugen anfällige Angriffsvektoren. Schatten-APIs (die als schnelle Lösungen außerhalb der standardmäßigen Genehmigungsprozesse entwickelt wurden) stellen eine vergleichbare Bedrohung dar. [Untersuchungen zeigen](#), dass ein Drittel der schädlichen API-Transaktionen auf Schatten-APIs abzielt.

Herkömmliche Sicherheitsmaßnahmen wie Web Application Firewalls (WAFs) erweisen sich als unzureichend gegen diese Bedrohungen. Unternehmen benötigen fortschrittliche API-Erkennungs- und -Überwachungslösungen, um anfällige Endpunkte effektiv zu identifizieren.

Ein umfassender API-Bestand bildet den Eckpfeiler einer effektiven Sicherheitsstrategie, mit der Unternehmen Nutzungsmuster überwachen, den Versionsverlauf verfolgen, Schwachstellen identifizieren und Compliance- und regulatorische Anforderungen erfüllen können. Dieser strategische Ansatz bietet einen klaren Einblick in die digitale Infrastruktur des Unternehmens, was letztendlich das Risikomanagement und die allgemeine Sicherheitslage verbessern kann.

Sicherheit im Fokus

Im ersten Quartal 2025 haben wir einen API-basierten Angriff auf ein E-Commerce-Unternehmen festgestellt: Die Unternehmens-API für den SMS-Versand verfügte nicht über eine ordnungsgemäße Authentifizierung, sodass Angreifer diese API mithilfe von mehr als 200 verschiedenen IP-Adressen, einem einzigen Authentifizierungstoken und zahlreichen zufälligen Mobiltelefonnummern (sowohl legitimen als auch gefälschten) ausnutzen konnten.

Die Angriffsstrategie war einfach, aber effektiv: Es galt, das Unternehmen zu überwinden, indem Angreifer mehrere Handynummern registrierten und SMS-Nachrichten an betrügerische Nummern sendeten, um direkt finanziellen Schaden anzurichten. Wenn die Angreifer eine Mobiltelefonnummer registrierten, entstanden dem betroffenen Unternehmen – das für einen SMS-Gateway-Dienst bezahlt, um Textnachrichten zwischen seinen Anwendungen und mobilen Geräten zu ermöglichen – hierdurch unerwartete Kosten, die potenziell seine Marke oder seinen Ruf schädigen konnten. Eine mehrschichtige Verteidigungsstrategie mit mehreren Ebenen von Sicherheitsmaßnahmen kann dieser Art von Angriffen entgegenwirken und die damit verbundenen Risiken erheblich mindern.

Unsere Warnungen haben gezeigt, dass Cyberkriminelle während dieses Angriffs 11.057 POST-Anfragen gestartet hatten – mit 5.659 erfolgreichen Antworten (Abbildung 2).

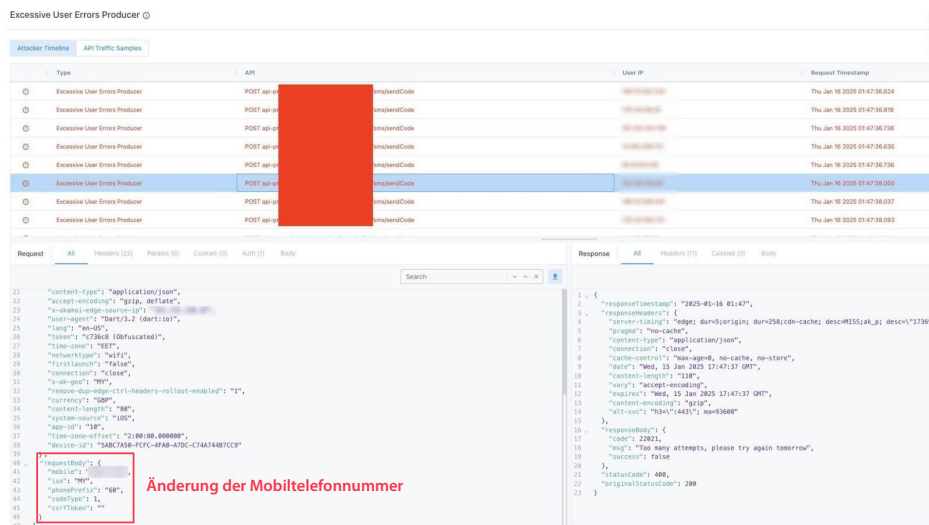


Abb. 2: Cyberkriminelle fluten die unsichere API mit Anfragen.

Diese automatisierten Anfragen waren identisch, mit Ausnahme eines kritischen Parameters:

Body-Parameter **mobile**: Folgendes Muster wurde erkannt – **<Nummer>**

Solche Anfragen können den Server überlasten und zu Serviceunterbrechungen führen – oder sie deuten auf einen erfolgreichen, nicht autorisierten Zugriff auf die API hin. Herkömmliche WAFs sind nicht in der Lage, diese ausgeklügelten Angriffe zu erkennen. Fortschrittliche API-Sicherheitslösungen, die eine Baseline für normales API-Verhalten schaffen, können solche Angriffe jedoch durch Verhaltensanalysen identifizieren, Risiken proaktiv mindern und Angreifer daran hindern, Schäden zu eskalieren.

Webangriffe: Jahresvergleich und Trends

Die Studie von Akamai stellte im Berichtszeitraum von Januar 2023 bis Dezember 2024 eine erhebliche Zunahme von Webangriffen fest, die auf Webanwendungen und APIs gerichtet waren (Abbildung 3). Das monatliche Angriffsvolumen stieg von fast 14 Milliarden Anfang 2023 auf über 29 Milliarden im Oktober 2024. Das entspricht einem Wachstum der Webangriffe von 65 % zwischen Q1 2023 und Q4 2024.

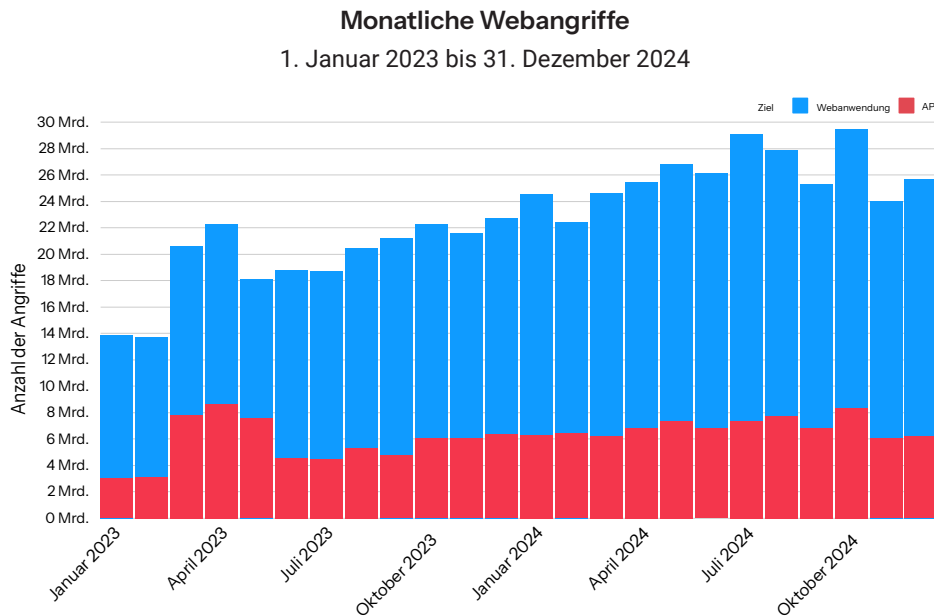


Abb. 3: Herkömmliche Webangriffe auf Webanwendungen und APIs nehmen weiter zu; das zeigt auch der Anstieg von 65 % zwischen Q1 2023 und Q4 2024.

Top-Vektoren: eine Mischung aus traditionellen und modernen verhaltensbasierten Risiken

Cybersicherheitsexperten haben mit zunehmender Komplexität zu kämpfen, während sie die digitale Infrastruktur ihres Unternehmens vor vielfältigen Bedrohungen schützen: von traditionellen Webangriffen bis hin zu modernen Exploits, die auf inhärente Schwachstellen und Fehlkonfigurationen abzielen.

Verletzung von API-Anfragebeschränkungen: eine wachsende Bedrohung

Eine umfassende Analyse der API-Endpunkte über einen Zeitraum von zwei Jahren zeigt, dass Verstöße gegen API-Anfragebeschränkungen Anlass zur Sorge geben (Abbildung 4). Diese Verletzungen treten auf, wenn Anfragen oder Antworten vordefinierte Parameter oder festgelegte Anforderungen nicht erfüllen, wie z. B. die Überschreitung von Ratenbegrenzungen oder die Weiterleitung ungültiger Dateneingaben.

API-Angriffe nach Vektor

1. Januar 2023 bis 31. Dezember 2024

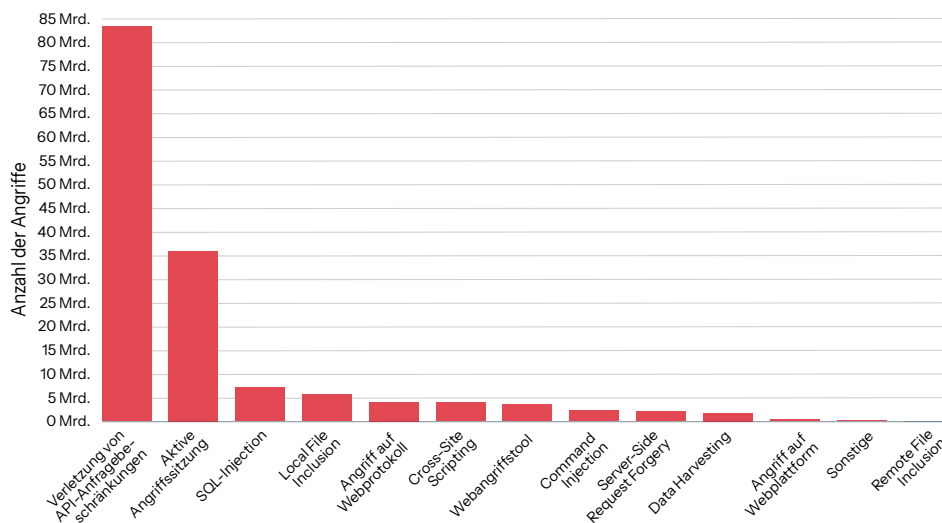


Abb. 4: Innerhalb von zwei Jahren wurden mehr als 83 Milliarden Verstöße gegen die Anfragebeschränkungen festgestellt.

Verstöße gegen API-Anfragebeschränkungen stellen eine wachsende Bedrohung dar: Mehr als 83 Milliarden Angriffe wurden innerhalb von zwei Jahren registriert. Dieser Angriffsvektor verzeichnete von 2023 bis 2024 einen erheblichen Anstieg von 24 %, was die Gefahren eines API-Missbrauchs unterstreicht. Die Verbreitung dieser Verstöße ist ein kritischer Indikator für potenziellen API-Missbrauch, der eine Welle negativer Auswirkungen auslösen kann, einschließlich einer Verschlechterung der Systemperformance, Serviceunterbrechungen und einer erhöhten Anfälligkeit für gezielte Angriffe.

Aktive Angriffssitzungen: einzigartige Angriffe, die eine kreative Lösung erfordern

Die Lösungen von Akamai nutzen innovative Sicherheitstools, um die einzigartigen Herausforderungen zu meistern, die durch API-spezifische Angriffe entstehen. Im Kern dieser Lösungen steht ein eigens entwickelter Mechanismus zur Erkennung aktiver Angriffssitzungen, der als strategisches Abwehrtool dient. Dieses System nutzt die Threat Intelligence von Akamai, um verdächtiges Verhalten zu erkennen und zu verfolgen, sodass Unternehmen Bedrohungen proaktiv abwehren können, bevor sie zu umfassenden Angriffen eskalieren.

Das System kennzeichnet Cyberkriminelle und setzt einen „Strafbank“-Ansatz ein. Bei modernen Attacken nutzen Angreifer überwiegend Automatisierung, um ihre Aufklärung und Angriffe auszuführen. Akamai identifiziert diese Sitzungen schnell, reagiert, indem der Client vorübergehend blockiert wird, und kennzeichnet diese Sitzungen als aktive Angriffssitzungen. Diese Strategie hält potenzielle Kriminelle effektiv davon ab, Aufklärungen durchzuführen und Netzwerkschwachstellen auszunutzen.

Durch die Einschränkung der Möglichkeiten, die Cyberkriminellen zur Verfügung stehen, können Unternehmen ihre API-Sicherheit erheblich verbessern. Dieser Ansatz bietet zuverlässigen Schutz vor einer Vielzahl potenzieller Angriffe und verbessert die allgemeine Resilienz der Cybersicherheit deutlich.

Wie wichtig diese Strategie ist, zeigen unsere Daten: Aktive Angriffssitzungen belegten sowohl bei Webanwendungen als auch bei APIs die oberste Position im Gesamt-Ranking (Abbildung 5). Im Jahr 2023 waren es mehr als 69 Milliarden Angriffe. Diese Zahl stieg 2024 auf über 113 Milliarden, was einem bemerkenswerten Anstieg von 63 % gegenüber dem Vorjahr entspricht.

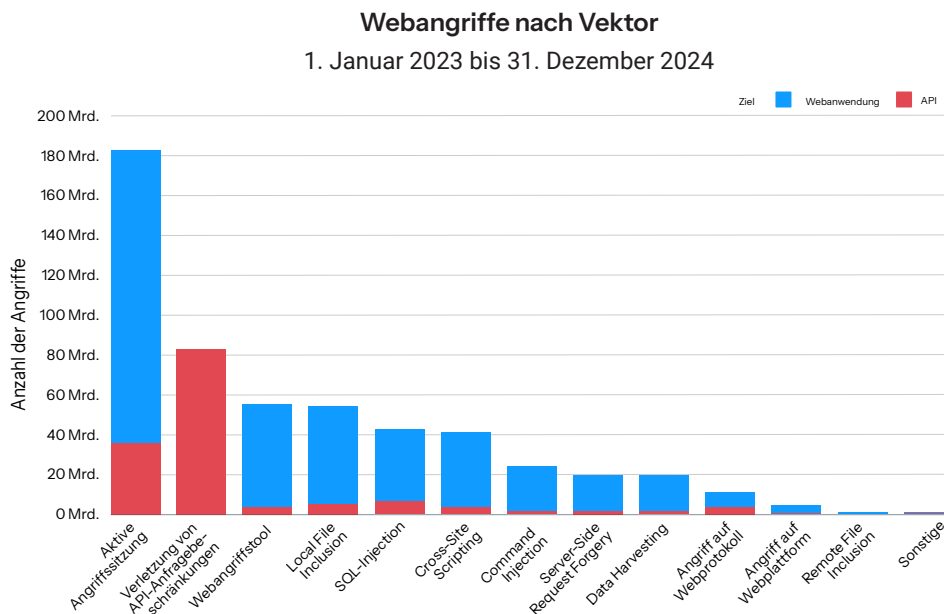


Abb. 5: Die aktive Angriffssitzung übertrifft alle anderen Vektoren sowohl für Webanwendungen als auch für APIs. Das verdeutlicht die unerbittliche Suche der Angreifer nach Schwachstellen in den Netzwerken ihrer Ziele.

Warum wir herkömmliche Webschwachstellen in modernen Infrastrukturen nicht ignorieren dürfen

Auch wenn mittlerweile ausgeklügelte, verhaltensbasierte Angriffsmethoden eingesetzt werden und ein stärkeres Bewusstsein für herkömmliche Webschwachstellen herrscht, sind Injection-Angriffe weiterhin äußerst wirksam. Unsere Daten von Januar 2023 bis Dezember 2024 deuten auf einen erheblichen Anstieg des Angriffsvolumens hin, wobei Structured Query Language Injection (SQLi) und Command Injection im Jahresvergleich ein Wachstum von 60 % bzw. 34 % verzeichnen. Diese Schwachstellen ermöglichen es Cyberkriminellen, unbefugte Befehle auszuführen, die Systemintegrität zu gefährden und ohne ordnungsgemäße Authentifizierung auf vertrauliche Daten zuzugreifen. All das unterstreicht die fortwährende Relevanz dieser Schwachstellen für die Cybersicherheit.

Die anhaltende Verbreitung von SQL-Datenbanken – die für ihre Zuverlässigkeit und Skalierbarkeit bei der Datenspeicherung bekannt sind – trägt weiter dazu bei, dass diese Systeme ständig angegriffen werden. So verwenden [die vier am häufigsten verwendeten Datenbanken](#) SQL-basierte Architekturen, was die kritische Natur dieses Angriffsvektors unterstreicht.

Obwohl die OWASP API Security Top 10 überarbeitet wurden – z. B. wurden Injection-Angriffe im Update 2023 durch falsche Sicherheitskonfigurationen ersetzt –, bleibt das Risiko, das mit Injection-Angriffen verbunden ist, von größter Bedeutung. Gleichzeitig werden auch andere etablierte Vektoren wie Local File Inclusion (LFI) und Cross-Site Scripting (XSS) weiterhin in großem Maßstab genutzt. Unser [Leitfaden für Abwehrspezialisten 2025](#) erläutert die Raffinesse der XSS-Ausnutzungstechniken, einschließlich Remote Resource Injection, Cookie-Diebstahl, Website Defacement und Session Riding, basierend auf realen Angriffen aus dem Jahr 2024.

Diese Ergebnisse unterstreichen die Notwendigkeit, eine mehrschichtige Verteidigungsstrategie zu verfolgen. Cybersicherheitsexperten müssen eine Kombination aus korrekter Ausgabecodierung, leistungsstarken Sicherheitsrichtlinien für Inhalte und fortschrittlichen WAFs einsetzen, um diesen immer ausgefeilteren Angriffen effektiv entgegenzuwirken.

Layer-7-DDoS-Angriffe: Jahresvergleich und Trends

Von Januar 2023 bis Dezember 2024 dokumentierte die Studie von Akamai einen dramatischen Anstieg der DDoS-Angriffe auf Webanwendungen und APIs, die auf Layer 7 (der Anwendungsschicht) stattfanden (Abbildung 6). Das monatliche Angriffsvolumen stieg von etwas über 500 Milliarden Anfang 2023 auf über 1,1 Billionen Angriffe im Dezember 2024. Das entspricht einem Wachstum der Layer-7-DDoS-Angriffe von 94 % zwischen Q1 2023 und Q4 2024.

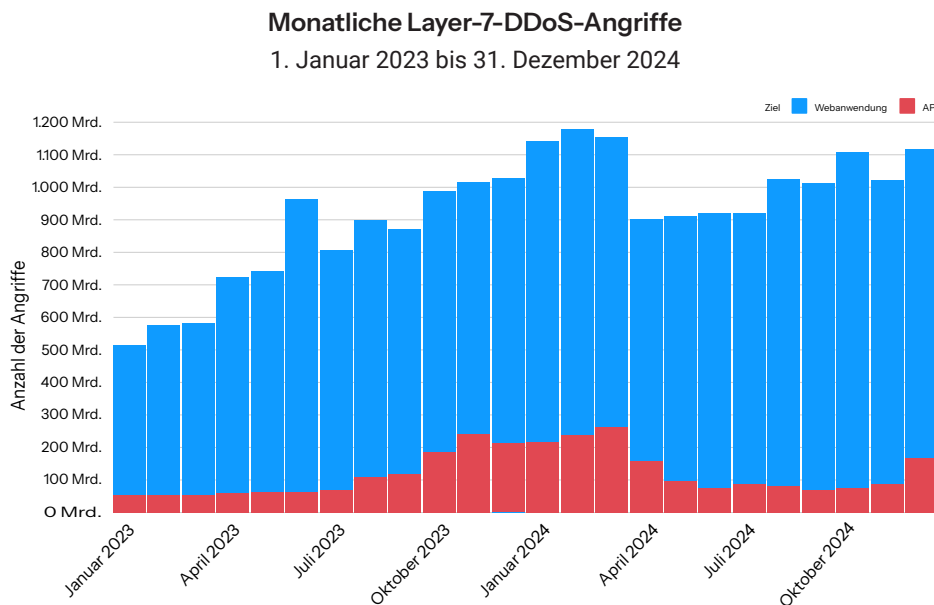


Abb. 6: Die Anzahl der Layer 7-DDoS-Angriffe auf Webanwendungen und APIs steigt weiter an. Das zeigt der Anstieg von 94 % zwischen Q1 2023 und Q4 2024.

Layer-7-DDoS-Angriffe auf Anwendungen und APIs

HTTP-Floods sind nach wie vor eine primäre Bedrohungsquelle in der kontinuierlichen Entwicklung von Layer-7-DDoS-Angriffen, die auf Webanwendungen und API-Endpunkte abzielen. Diese Angriffe überfordern API-Ressourcen, indem sie sie mit großen Mengen scheinbar legitimer Anfragen überfluten, die sich auf ressourcenintensive Vorgänge konzentrieren. Angreifer haben ihre Techniken verfeinert und mittlerweile Layer-7-DDoS-Angriffe entwickelt, die bestimmte Schwachstellen in der Logik von Webanwendungen oder APIs ausnutzen. Hierdurch werden die Erkennung und Abwehr dieser Angriffe erschwert. Darüber hinaus sind Bot-gestützte Angriffe immer ausgefeilter geworden und erzeugen heute Trafficmuster, die eine legitime API-Nutzung genau nachahmen.

KI-gestützte API-Angriffe, manuell oder automatisch

GenAI-Technologien (generative KI) haben die Unternehmensintegration über APIs revolutioniert – und das treibt auch die breite Einführung und praktische Anwendung von APIs voran. Der Markt für KI-APIs wird ein **explosives Wachstum** von 44,41 Mrd. USD im Jahr 2025 auf 179,14 Mrd. USD im Jahr 2030 verzeichnen, was einer durchschnittlichen jährlichen Wachstumsrate von 32,2 % entspricht. Doch der vermehrte Einsatz von KI fällt mit einem deutlichen Anstieg der **KI-gestützten Angriffe auf APIs** und Webanwendungen zusammen. Der Anstieg der offengelegten API-Schwachstellen ist größtenteils darauf zurückzuführen, dass Angreifer KI als Tool sowohl zur Aufklärung als auch zur Ausnutzung verwenden, sei es manuell oder automatisch.

KI-basierte API-Angriffsstrategien

-  **Strategische Ausrichtung:** Angreifer verwenden KI-Tools, um bestimmte Komponenten in Ziel-APIs zu identifizieren und zu analysieren und maßgeschneiderte Exploits mit **KI-generiertem schädlichem Code** für bestimmte Schwachstellen zu erstellen. Dieser Ansatz ermöglicht präzise und effektive Angriffe auf API-Schwachstellen.
-  **Automatisierte Angriffe:** Durch die Automatisierung des Angriffsprozesses reduzieren Cyberkriminelle ihren Zeit- und Arbeitsaufwand erheblich und können Schwachstellen in der API-Sicherheit schnell erkennen und ausnutzen. Diese Automatisierung umfasst häufig **KI-basierte Bots**, die sowohl für Unternehmen als auch für Privatpersonen eine kritische Bedrohung darstellen.
-  **Volumetrische Angriffe:** Angreifer nutzen KI, um APIs mit Traffic zu überlasten und Sicherheitssysteme mit erheblichem Volumen und Tempo zu überfluten. **Automatisierte DDoS-Angriffe** sind ein Ergebnis dieser Strategie: Hier starten KI-basierte Bots kontinuierliche Angriffe und passen sich dynamisch an Verteidigungsmaßnahmen an.
-  **Verhaltensbasierte Angriffe:** KI analysiert Datenverkehrsmuster, um **kleine, langsame Angriffe zu generieren**, die die Erkennung umgehen, indem sie unterhalb der typischen Alarmschwellenwerte arbeiten. Diese Angriffe richten sich häufig gegen gängige API-Schwachstellen wie BOLA und Broken Authentication.

Die Ironie KI-gestützter APIs

Paradoxerweise haben sich APIs, die von KI unterstützt werden, als besonders unsicher erwiesen. Die Mehrheit der **KI-gestützten APIs** ist extern zugänglich und ein erheblicher Teil von ihnen nutzt unzureichende Authentifizierungsmechanismen, wodurch sie anfälliger für Angriffe sind. Unsere **API-Sicherheitsstudie 2024** ergab, dass APIs in GenAI-Tools die Hauptursache für API-Vorfälle waren, die von Sicherheitsteams im Einzelhandel/E-Commerce gemeldet wurden.

KI-Bedrohungslandschaft entwickelt sich weiter

Die Fortschritte in der KI-Technologie haben erheblich zur Entwicklung der API-Bedrohungslandschaft beigetragen. Im vergangenen Jahr wurden [Rekordzuwächse](#) bei Schwachstellen KI-gestützter APIs gemeldet. Quellen behaupten sogar, dass zum ersten Mal die Mehrheit aller von der CISA (U.S. Cybersecurity and Infrastructure Security Agency) registrierten [ausgenutzten Schwachstellen](#) API-bezogen waren.

KI-gestützte Webanwendungsangriffe und Verteidigungsstrategien

KI hatte auch erheblichen Einfluss auf die Sicherheit von Webanwendungen – durch die Einführung neuer Angriffsvektoren, aber auch neuer Verteidigungsfunktionen. Zu den wichtigsten Bereichen, in denen KI die Cybersicherheitslandschaft für Angriffe auf Webanwendungen erheblich verändert hat, gehören KI-gestützte Malware, KI-gestützte Schwachstellenscans, Angriffe auf KI-gestützte Systeme, hoch entwickeltes Web-Scraping und KI-gestützte WAF-Systeme.

KI-gestützte Malware

Cybersicherheitsexperten haben beobachtet, dass hoch entwickelte Malware KI nutzt, um Webanwendungen anzugreifen. In einer E-Mail-Kampagne von 2024, die französische Nutzer angriff, implementierten Angreifer schädlichen Code, der wahrscheinlich mit GenAI-Unterstützung entwickelt wurde, um die [AsyncRAT-Malware auszuführen](#). Dieses Beispiel zeigt den wachsenden Trend bei der Erstellung und Bereitstellung KI-gestützter Malware – und er bringt neue Herausforderungen für Sicherheitsexperten im Bereich Webanwendungen mit sich.

KI-gestützte Schwachstellenscans

KI hat [Schwachstellenscans](#) für Webanwendungen revolutioniert und bietet sowohl defensive als auch offensive Funktionen – unabhängig davon, ob es sich um eine legitime oder böswillige Nutzung handelt. Diese KI-basierten Tools automatisieren die Suche nach häufig auftretenden Sicherheitslücken wie SQLi, XSS, Cross-Site Request Forgery und Server-Side Request Forgery (SSRF). Darüber hinaus führen sie KI-basierte Analysen potenzieller Auswirkungen durch und generieren KI-gestützte Empfehlungen für Abhilfemaßnahmen.

Angriffe auf KI-gestützte Systeme

Durch die Integration von KI, insbesondere von LLMs (Large Language Models), in Webanwendungen wurden [neue Sicherheitslücken geschaffen](#). *Prompt-Injection-Angriffe* zielen auf KI-Systeme und sollen die Sicherheitsmaßnahmen von Modellen außer Kraft setzen. Ein bemerkenswertes Beispiel ist eine mittlerweile gepatchte [Slack-KI-Sicherheitslücke](#), die es per indirekter Prompt Injection ermöglichte, Daten aus privaten Kanälen zu sammeln. *Data-Poisoning-Angriffe* verändern das Verhalten von KI-Modellen, indem ein kleiner Prozentsatz von Datensätzen manipuliert wird, was potenziell zu einer Beeinträchtigung der Systemintegrität führen kann. *Jailbreaking-Techniken* umgehen LLM-Sicherheitsvorkehrungen und ermöglichen es Angreifern, Beschränkungen außer Kraft zu setzen, sensible Daten zu extrahieren und schädliche Ergebnisse zu generieren. Diese neuen Angriffsvektoren erfordern erhöhte Wachsamkeit und neue Verteidigungsstrategien.

Fortschrittliches Web-Scraping

KI verfügt über verbesserte Web-Scraping-Funktionen, was neue Herausforderungen für die Sicherheit von Webanwendungen mit sich bringt. Diese KI-gestützten Scraping-Tools bieten jetzt effizientere Datenextraktionsmethoden und eine bessere Umgehung von Anti-Scraping-Maßnahmen. Seit den frühen 2020er Jahren nutzt [hoch entwickeltes Web-Scraping](#) KI zur Verarbeitung von Daten, doch in letzter Zeit ist die Häufigkeit von LLM-Scraping erheblich gestiegen. Ein Großteil davon ist auf die Zunahme agentenbasierter Abfragen zurückzuführen, die den Bedarf an (nicht statischen) Echtzeitdatenquellen erhöhen.

Leider hat das dazu geführt, dass die durchschnittliche Webanwendungsanfrage (abhängig von Faktoren wie Komplexität der Anfrage, Hosting-Infrastruktur usw.) zwischen 0,01 und 0,50 US-Dollar pro Anfrage kostet. Und während der Handel ursprünglich die Branche war, die am stärksten von der Zunahme von LLM-Scraping betroffen war, hat sich die Situation gewendet: Heute erleben andere Branchen (z. B. Finanzdienstleistungen, Glücksspiel, digitale Medien und Videomedien) die Hauptlast dieses Wandels.

KI-gestützte WAF-Systeme

Positiv ist, dass fortschrittliche WAF-Systeme durch KI unterstützt werden, um eine Reihe von Cyberbedrohungen effektiver zu erkennen und abzuwehren, darunter Bots, DDoS-Angriffe, Scraper und Scanner. [KI-gestützte WAF-Systeme](#) helfen bei der Bekämpfung komplexer Cyberangriffe, da herkömmliche WAFs mit ihren statischen Regelsätzen mit Zero-Day-Bedrohungen zu kämpfen haben und manuelle Updates erfordern.

Die mehrschichtige ML-Strategie (maschinelles Lernen) ermöglicht Mustererkennung, adaptives Lernen, Anomalieerkennung und verbesserte Reaktionszeiten. Indem KI-gestützte WAF-Systeme Modelle mit Milliarden täglicher Ereignisse trainieren und einen mehrschichtigen Ansatz mit kontinuierlicher Überwachung verfolgen, zielen sie darauf ab, neue Bedrohungen proaktiv zu verhindern und Kunden zu schützen.

Branchentrends

Unter den Branchen überstieg der Handel alle anderen, wobei sich die Zahl der Webangriffe im Bereich der Hightech-Branche (die zweithäufigste attackierte Branche) vom 1. Quartal 2023 bis zum 4. Quartal 2024 fast verdreifacht hat (Abbildung 7). Darüber hinaus überstieg die Anzahl der API-Angriffe, die in der Handelsbranche im selben Zeitraum verzeichnet wurden, die Gesamtzahl der API-Angriffe der verbleibenden Top-10-Branchen.

Webangriffe nach Branche
1. Januar 2023 bis 31. Dezember 2024

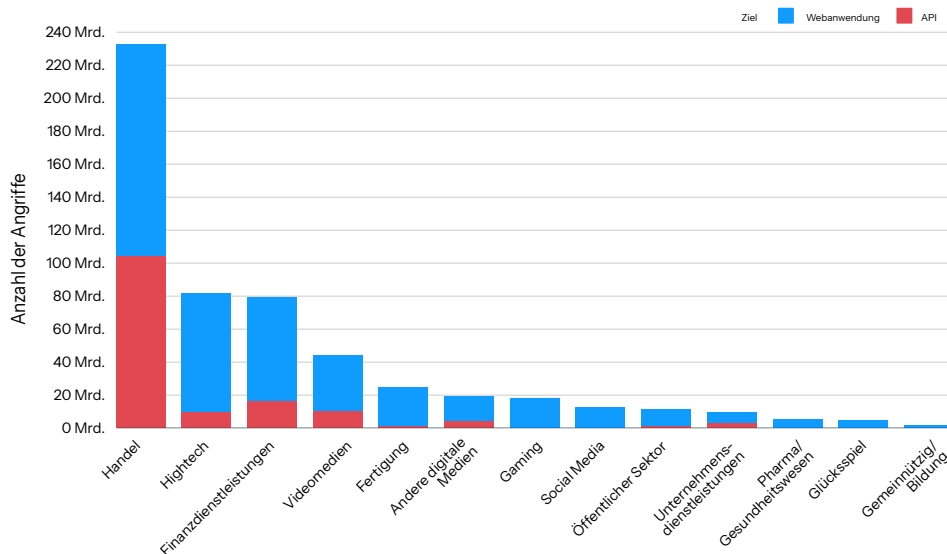


Abb. 7: Handel, Hightech und Finanzdienstleistungen waren die drei Branchen, die am meisten von Webangriffen betroffen waren.

Bei DDoS-Angriffen auf Layer 7 (Anwendungsschicht) wurde die Hightech-Branche stärker als jede andere Branche angegriffen. Im Zeitraum vom 1. Quartal 2023 bis zum 4. Quartal 2024 wurden mehr als 7 Billionen Angriffe verzeichnet. Auf Hightech folgten Social Media und Handel (Abbildung 8). Im gleichen Zeitraum übertraf die Anzahl der API-orientierten Layer-7-DDoS-Angriffe auf die Handelsbranche jedoch erneut deutlich die aller anderen Branchen zusammen.

Layer-7-DDoS-Angriffe nach Branche

1. Januar 2023 bis 31. Dezember 2024

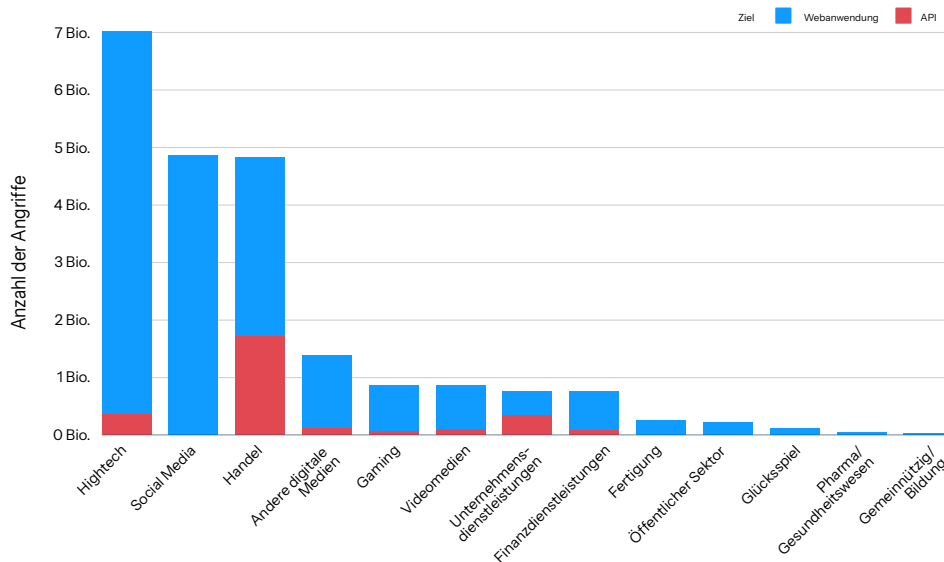


Abb. 8: Layer-7-DDoS-Angriffe nach Branche

Handel

Zusätzlich zu mehr als 230 Milliarden Webangriffen – das sind mehr als 40 % aller Webangriffe – zwischen 2023 und 2024 war die Handelsbranche auch mit einer beispiellosen Menge von Layer-7-DDoS-Angriffen konfrontiert: So verzeichnete Akamai in den Jahren 2023 und 2024 mehr als 4,8 Billionen Angriffe.

Dieses kombinierte Volumen stellt ein strategisches Targeting-Muster dar, bei dem Webanwendungen etwa 64,25 % der Angriffe abbekommen, während APIs die restlichen 35,75 % ausmachen. Diese Verteilung spiegelt die dualen Vektoren wider, die Angreifer einsetzen, um Handelsplattformen zu kompromittieren, und unterstreicht die Vielschichtigkeit der modernen Bedrohungslandschaft.

Handelsunternehmen stellen aufgrund ihrer vielen sensiblen Kundendaten, Zahlungsinformationen und Finanztransaktionen besonders lukrative Ziele dar. Der direkte Weg zur Monetarisierung durch gestohlene Zahlungsdaten, kompromittierte Kundenkonten und vertrauliche personenbezogene Daten schafft einen direkten finanziellen Anreiz für Cyberkriminelle. Im Gegensatz zu anderen Branchen – in denen es zusätzliche Schritte erfordert, aus kompromittierten Daten finanzielle Gewinne zu schlagen – stoßen Angreifer bei Handelsplattformen häufig auf direkt ausnutzbare Ressourcen.

Handel als primäres Ziel

Der Einzelhandel ist das am stärksten angegriffene Branchensegment innerhalb der breiteren Handelsbranche. Hier wird aufgrund verschiedener Besonderheiten eine unverhältnismäßig hohe Angriffsmenge verzeichnet:

Einzelhandelsunternehmen pflegen in der Regel komplexe digitale Ökosysteme, die verschiedene Plattformen und Systeme umfassen. Bei ihren aggressiven Initiativen zur digitalen Transformation hat das Markteinführungstempo oft Vorrang vor umfassender Sicherheit, wodurch Sicherheitslücken entstehen. Die Einführung von Omnichannel-Strategien erhöht unbeabsichtigt die Komplexität der Angriffsfläche. Darüber hinaus entsteht durch die starke Abhängigkeit von Drittanbietern eine komplexe Lieferkette mit zahlreichen potenziellen Angriffspunkten.

Saisonale Verkehrsschwankungen schaffen vorhersehbare Zeiträume mit hohem Datenaufkommen, die Angreifer gezielt ausnutzen. So gibt beispielsweise das FBI-Zentrum für Internetkriminalität an, dass Cyberkriminalitätsfälle während der Winterferien um **25 bis 30 %** zunehmen. E-Commerce-Plattformen sind ebenfalls mit erhöhten Bedrohungen konfrontiert, wobei die Zahl der Cyberangriffe im Dezember im Vergleich zum Jahresdurchschnitt um **31 %** gestiegen ist.

Die Entwicklung von Webanwendungsangriffen

Angriffe auf Webanwendungen durchlaufen eine erhebliche Transformation, die durch technologische Fortschritte und neue Angriffsmethoden angetrieben wird. Cyberkriminelle nutzen immer ausgefeiltere Techniken, um Schwachstellen in Webanwendungen auszunutzen, und passen ihre Strategien an, um neue Sicherheitsmaßnahmen zu umgehen. Die Verbreitung automatisierter Angriffstools in Verbindung mit der Integration von ML-Algorithmen hat es Angreifern ermöglicht, präzisere und gezieltere Attacken auf die Webanwendungen von Einzelhändlern zu starten.

Darüber hinaus hat der Wandel hin zu Microservices-Architekturen und API-orientierter Entwicklung die Angriffsfläche erweitert, was eine Neubewertung traditioneller Sicherheitsansätze erforderlich macht. Diese Entwicklung erfordert einen proaktiven Ansatz von Cybersicherheitsexperten, der sich auf kontinuierliche Überwachung, adaptive Abwehrmechanismen und ein tiefgreifendes Verständnis der neuen Angriffsvektoren in der Webanwendungslandschaft konzentriert.

Die Bot-Bedrohungslandschaft

Die Bot-Bedrohungslandschaft entwickelt sich durch den technologischen Fortschritt rasant weiter, insbesondere da Angreifer GenAI-Funktionen integrieren. Diese Entwicklung hat Angriffsstrategien durch schnellere Zero-Day-Exploits und ausgeklügelte Ausweichtechniken verbessert, die herkömmliche Abwehrmaßnahmen umgehen. Es gibt Hinweise darauf, dass KI-basierte Bot-Betrugsangriffe auf Einzelhändler zwischen August 2022 und April 2024 kontinuierlich **zugenommen** haben, wobei im Januar 2024 ein markanter Anstieg von 137 % verzeichnet wurde. Erkennungsprobleme verschärfen diese Bedrohungen noch weiter: Unternehmen benötigen in der Regel vier Monate, um Bot-Angriffe zu erkennen – und während dieser Zeit erleiden sie konstant finanzielle und Reputationsschäden.

Bots fungieren jetzt als zentrale Vektoren in der Cyberlandschaft des Einzelhandels und erleichtern Kontoübernahmen, Kreditkartenbetrug und den Missbrauch von Geschenkkarten. Sie dienen als Grundlage für umfassendere Angriffskampagnen, indem sie mit den Daten, die von einer kompromittierten Website gestohlen wurden, Credential-Stuffing-Angriffe auf andere Opfer starten. So entsteht eine Art Dominoeffekt in den Ökosystemen des Einzelhandels. Diese Tätigkeit trägt zur „Industrialisierung“ von Onlinebetrug bei, da in globalen Kriminalitätskreisen automatisierte Tools eingesetzt werden können, um die Vorgänge weit über das hinaus zu skalieren, was sie mit manuellen Methoden erreichen könnten.

Eine Liste mit Empfehlungen zum besseren Schutz der Webanwendungen und APIs Ihres Einzelhandelsbetriebs vor KI- und Bot-bezogenen Angriffen finden Sie im Abschnitt [Abwehr](#).

Finanzdienstleistungen

Die Finanzdienstleistungsbranche hat sich zu einem Hauptziel für Webangriffe entwickelt und erlebt weiterhin Layer-7-DDoS-Angriffe. Webangriffe summierten sich zwischen Januar 2023 und Dezember 2024 auf mehr als 79 Milliarden, während Layer-7-DDoS-Angriffe im selben Zeitraum mehr als 761 Milliarden Webanwendungen und APIs trafen.

Dieses beispiellose Volumen unterstreicht die Anfälligkeit und Attraktivität der Branche für Cyberkriminelle. Dieser Anstieg wird durch mehrere Faktoren vorangetrieben, darunter die entscheidende Rolle der Branche in der globalen Wirtschaftsinfrastruktur, der hohe Wert von Finanzdaten und das Potenzial für erhebliche [Störungen](#).

Die Digitalisierung von Finanzdienstleistungen

Die Digitalisierung von Finanzdienstleistungen hat die Angriffsfläche für Cyberkriminelle deutlich erweitert. Durch die Einführung von KI-gestützten Personalisierungslösungen, Banking-as-a-Service und Embedded-Finance-Lösungen wurden neue Schwachstellen geschaffen. Geopolitische Konflikte, insbesondere der Krieg zwischen Russland und der Ukraine, haben „hacktivistische“ Aktivitäten angeheizt, die auf Finanzinstitute [abzielen](#). Wirtschaftliche Faktoren wie der Anstieg von Kryptowährungen und die mögliche Einführung einer Kryptoreserve haben das [Interesse](#) der Cyberkriminellen an der Finanzbranche verstärkt.

Angriffe auf Webanwendungen verändern sich rasant, passen sich an neue Technologien an und nutzen neue Schwachstellen aus. Angreifer nutzen heute ausgeklügelte KI- und ML-Algorithmen, um herkömmliche Sicherheitsmaßnahmen zu umgehen und gezieltere, beharrlichere Angriffe zu starten. Durch die Zunahme serverloser Architekturen und Microservices wurden neue Angriffsvektoren geschaffen, während die zunehmende Nutzung von APIs die potenziellen Einstiegspunkte für Cyberkriminelle erweitert hat. Darüber hinaus hat die Umstellung auf mobile und cloudbasierte Anwendungen eine Neubewertung der Sicherheitsstrategien erforderlich gemacht, da diese Plattformen einzigartige Herausforderungen in Bezug auf Datenschutz und Zugriffskontrolle mit sich bringen.

Das Banksegment als beliebtes Angriffsziel

In der Finanzdienstleistungsbranche ist das Bankwesen das Segment, das am häufigsten von Webanwendungsangriffen getroffen wird (Abbildung 9). Wie in der Handelsbranche entwickeln sich **Credential-Stuffing-Angriffe** auch im Bankwesen zu einem der führenden Angriffsvektoren.

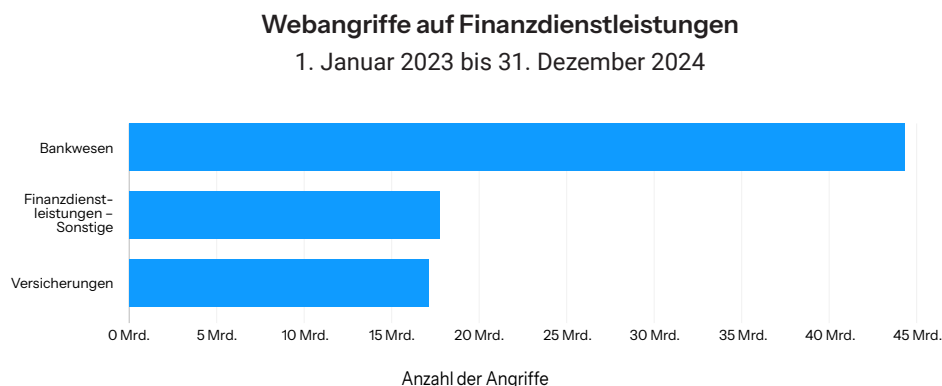


Abb. 9: Banking ist das am stärksten anvisierte Branchensegment unter den Webangriffen auf Finanzdienstleistungen.

Die Verbreitung von Onlinebanking-Services in Verbindung mit der kritischen Natur eines Kontozugriffs zieht zahlreiche Cyberkriminelle an. Die finanziellen Anreize für erfolgreiche Angriffe sind beträchtlich: Selbst eine kleine Anzahl kompromittierter Konten kann erhebliche Gewinne bringen. Die Zurückhaltung des Bankensektors, strenge Sicherheitsmaßnahmen einzuführen, die das Nutzererlebnis beeinträchtigen könnten (wie z. B. Multi-Faktor-Authentifizierung), hat unbeabsichtigt zur Anfälligkeit des Sektors **beigetragen**.

Die Beliebtheit des Banksegments als Angriffsziel wird durch mehrere Faktoren noch verstärkt: Die Sensibilität gegenüber Ausfällen bietet eine Möglichkeit zur Erpressung, indem Cyberkriminelle **Bedenken** über Serviceunterbrechungen ausnutzen. Darüber hinaus stellt die zunehmende Ausgereiftheit der Angriffstechniken – einschließlich der Verwendung von KI und maschinellem Lernen, um der Erkennung zu entgehen – eine erhebliche **Herausforderung** für herkömmliche Verteidigungsmechanismen dar. Die regulatorische Landschaft – mit ihren strengen Compliance-Anforderungen und potenziellen Geldstrafen für Sicherheitsverstöße – erhöht die Komplexität der Cybersicherheit im Banksegment weiter.

Hightech

Hightech ist nach wie vor eine der am häufigsten angegriffenen Branchen, was Web- und Layer-7-DDoS-Angriffen angeht. Für den Zweck unseres Berichts umfasst Hightech die Branchen Telekommunikation, Unternehmenssoftware und -hardware sowie Verbrauchersoftware und -hardware. Unsere Daten zeigen, dass diese Branche mit über 81,7 Milliarden Angriffen im Zeitraum von 2023 bis 2024 hinter dem Handel an zweiter Stelle stand. Darüber hinaus war die Hightech-Branche das Ziel der meisten Layer-7-DDoS-Angriffe: über 7 Billionen in den zwei Jahren.

Hightech-Webanwendungen nutzen häufig komplexe Datenbankabfragen und dynamische Inhalte. Das schafft Schwachstellen, die Angreifer einfach ausnutzen können, um [Server zu überfordern](#). Diese Schwachstellen tragen zur hohen Rate von Layer-7-DDoS-Angriffen bei, die in der Branche auftreten. Insbesondere haben [Blockchain-Netzwerke](#) einen deutlichen Anstieg der DDoS-Angriffe verzeichnet. Hierbei setzen Angreifer Methoden wie HTTP-Flooding und Spam-Transaktionen ein, um legitime Transaktionen zu behindern – trotz der dezentralen Architektur der Blockchain. Die kritischen finanziellen Auswirkungen von Betriebsausfällen in der Hightech-Branche motivieren Angreifer dazu, DDoS-Angriffe einzusetzen, die wichtige Services außer Betrieb setzen können. Die Abhängigkeit moderner Softwareentwicklung von API-orientierten Architekturen birgt zusätzliche Risiken, da Angreifer häufig unsicher codierte Endpunkte bei HTTP-Flood-Angriffen ausnutzen.

Das Telekommunikationssegment steht vor ähnlichen Herausforderungen

Das Telekommunikationssegment, das von einer erheblichen Anzahl von API-Angriffen betroffen ist, steht vor ähnlichen Herausforderungen im Bereich der Cybersicherheit. Zu den Bedrohungen für Webanwendungen und API in diesem Hightech-Sektor gehören Datenmissbrauch, DDoS-Angriffe und Schwachstellen in der Lieferkette. Diese Schwachstellen haben zu mehreren hochgradigen Datenschutzverletzungen geführt.

So entdeckten Forscher im Januar 2025 kritische API-Schwachstellen in einem [großen Telekommunikationsnetzwerk](#), wodurch 3.000 Unternehmen Sicherheitsrisiken ausgesetzt waren. Die Untersuchung ergab erhebliche Sicherheitslücken, darunter Schwachstellen im „Know Your Customer“-Verifizierungsprozess und eine Schwachstelle im Backend-API-Pfad, die Zugriff auf interne Systeme gewährte.

Das Internet der Dinge führt neue Angriffsmethoden ein

In einer Zeit des rasanten technologischen Fortschritts muss sich die Hightech-Branche immer stärker mit den wachsenden Schwachstellen von Webanwendungen und APIs auseinandersetzen. Diese Entwicklung umfasst die weitverbreitete Einführung von IoT-Geräten (Internet of Things), die neue Angriffsmethoden mit sich bringen, da viele Geräte nicht über starke Sicherheitsmaßnahmen verfügen. Die beschleunigte Einführung von Multi-Cloud-Infrastrukturen führt häufig zu falsch konfigurierten Umgebungen und schafft potenzielle Einstiegspunkte, die ausgenutzt werden können.

Sicherheitslücken in unsicher entwickelten IoT-Geräten und Cloud-Systemen werden zunehmend von ausgeklügelten [KI-gestützten Angriffen](#) ausgenutzt. [SaaS-Plattformen](#) sind aufgrund ihrer großen Angriffsfläche einem erhöhten Risiko von API-Angriffen ausgesetzt. Die zunehmende Verbreitung von KI-Lösungen und die zunehmende Abhängigkeit externer SaaS-Plattformen haben die gesamte API-Angriffsfläche in der Hightech-Branche erheblich erweitert. Wenn Unternehmen diese Technologien weiterhin einsetzen, wird eine Ausnutzung immer wahrscheinlicher, weshalb es leistungsstarke Sicherheitsmaßnahmen und eine sorgfältige Überwachung braucht.

Regionale Trends

HINWEIS: Wir haben das Format für unsere regionalen Berichte geändert, um die Daten für Leser zugänglicher zu machen und Angriffstrends in verschiedenen Regionen zu präsentieren, darunter Nordamerika (NOAM), Asien-Pazifik und Japan (APJ), Europa, Naher Osten und Afrika (EMEA) und Lateinamerika (LATAM). Außerdem haben wir ein Diagramm für einen kurzen Überblick über die Daten hinzugefügt, die wir in diesem Abschnitt besprechen (Abbildung 10).

Region	Anzahl der Webangriffe	Anzahl der Layer-7-DDoS-Angriffe	Top-Webangriffsvektoren	Webangriffsdaten Layer-7-DDoS-Angriffsdaten	
				Top-Zielgebiete	Top-Zielbranchen
APJ	80 Mrd., 14 % API	7,4 Bio., 6 % API	Aktive Angriffssitzung, LFI, XSS	Australien (20,3 Mrd.), Indien (17,3 Mrd.), Singapur (15,9 Mrd.)	Finanzdienstleistungen, Handel, Social Media
				Singapur (4,7 Bio.), Indien (607 Mrd.), Südkorea (283 Mrd.)	Social Media, andere digitale Medien, Handel
EMEA	116 Mrd., 37 % API	2,6 Bio., 20 % API	Aktive Angriffssitzung, Verletzung von API-Anfragebeschränkungen LFI	Vereinigtes Königreich (30,3 Mrd.), Niederlande (19,5 Mrd.), Spanien (14,2 Mrd.), Deutschland (12,8 Mrd.)	Handel, Videomedien, Finanzdienstleistungen
				Deutschland (569 Mrd.), Vereinigtes Königreich (506 Mrd.)	Handel, andere digitale Medien, Videomedien
LATAM	3 Mrd., 12 % API	258 Mrd., 18 % API	Aktive Angriffssitzung, WAT, SSRF	Brasilien (19,3 Mrd.), Mexiko (2 Mrd.)	Handel, Finanzdienstleistungen
				Brasilien (175 Mrd.), Mexiko (39 Mrd.)	Handel, Finanzdienstleistungen
NOAM	327 Mrd., 29 % API	11,9 Bio., 16 % API			

Abb. 10: Regionen auf einen Blick, Januar 2023 bis Dezember 2024 (LFI steht für die Local File Inclusion; XSS für Cross-Site Scripting; WAT für Webangriffstool; SSRF für Server-Side Request Forgery)



Zwei Anwendungs- und API-Angriffstrends

Unsere regionalen Vergleiche von Webanwendungs-, API- und Layer-7-DDoS-Angriffen während des 24-monatigen Berichtszeitraums von Januar 2023 bis Dezember 2024 zeigen zwei übergreifende Trends (Abbildung 11).

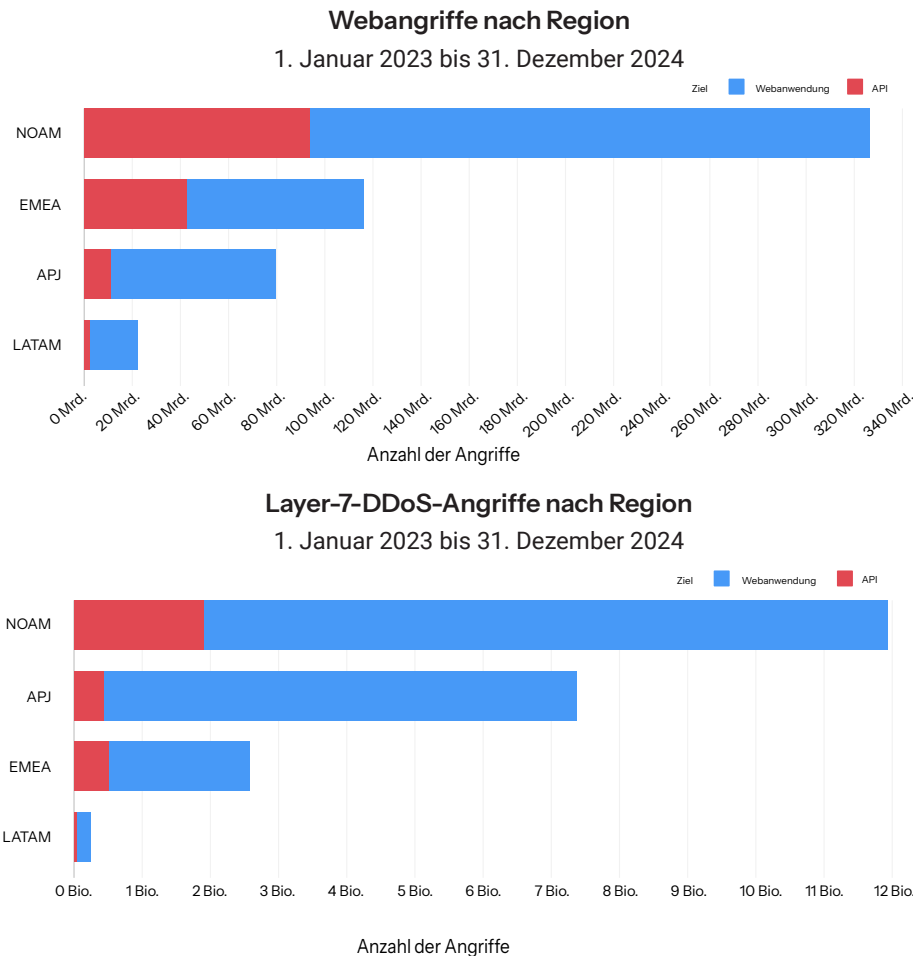


Abb. 11: Während des Berichtszeitraums verzeichnete EMEA weltweit den höchsten Prozentsatz an API-Angriffen, während APJ die zweithöchste Anzahl an Layer-7-DDoS-Angriffen verzeichnete.

Angriffstrend 1: API-Angriffe waren in EMEA weitverbreitet, was auf [höhere API-Einführungsraten als in anderen Regionen](#) sowie auf Open Banking und [PCI DSS 4.0](#) zurückzuführen ist. Sie beide treiben die Verwendung von APIs voran und können neue Sicherheitsrisiken mit sich bringen. (Eine ausführliche Erläuterung der API-spezifischen Risiken finden Sie im Abschnitt [Weiterentwicklung unserer API-Bedrohungsinformationen](#).)

Der Trend, den wir erstmals [2023 beobachtet](#) haben, setzt sich fort: EMEA verzeichnete erneut die höchste Konzentration von Webangriffen auf APIs während der 24 Monate: Von den insgesamt 116 Milliarden Webangriffen in der Region zielten 37 % auf APIs ab. Im Gegensatz dazu verzeichnete Nordamerika insgesamt 327 Milliarden Webangriffe, 29 % davon auf APIs. In APJ zielten 14 % der 80 Milliarden Webangriffe auf APIs ab, gefolgt von LATAM mit 12 % von insgesamt 3 Milliarden.

EMEA verzeichnete auch die höchste Konzentration von Layer-7-DDoS-Angriffen, die auf APIs abzielten (20 %), gefolgt von LATAM (18 %), Nordamerika (16 %) und APJ (6 %). Im Allgemeinen machten Layer-7-DDoS-Angriffe auf APIs einen relativ geringen Prozentsatz der gesamten Webangriffe in jeder Region aus. Wir gehen davon aus, dass diese Prozentsätze im Laufe der Zeit aus verschiedenen Gründen steigen werden, darunter fortschrittlichere Bot-basierte Angriffe und eine Zunahme KI-basierter Angriffe auf API-Schwachstellen.

Angriffstrend 2: APJ erlebte mit 7,4 Billionen (gegenüber 11,9 Billionen in Nordamerika) die zweithöchste Menge von Layer-7-DDoS-Angriffen. EMEA folgte mit 2,6 Billionen und LATAM mit 258 Milliarden. Dieser Trend wurde zunächst in unserem [SOTI-Bericht „Digitale Festungen unter Beschuss“](#) beobachtet. Er ist nach wie vor auf eine hohe Konzentration von Social-Media-Angriffsversuchen in APJ zurückzuführen.

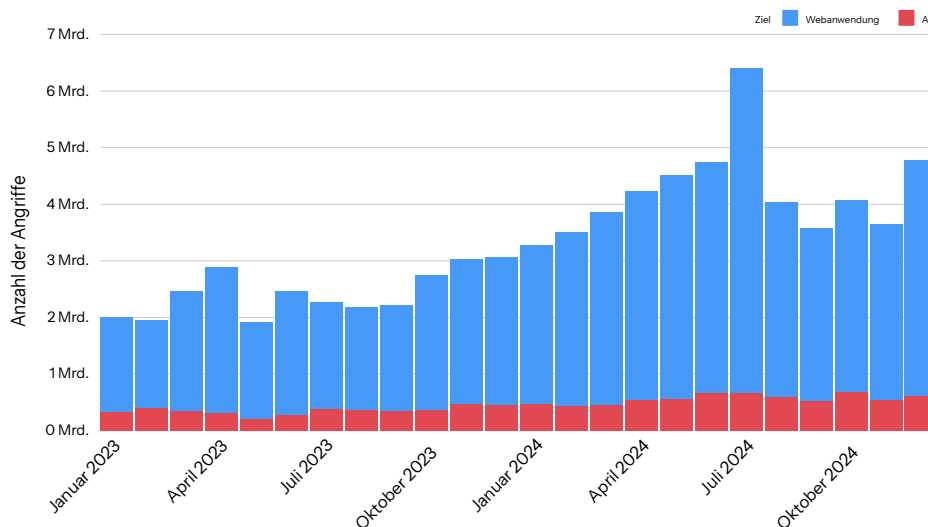
Ein tieferer Einblick in APJ, EMEA und LATAM

In diesem Abschnitt werden wir einige wichtige Trends in APJ, EMEA und LATAM hervorheben. Bei diesen Regionen beziehen wir auch Daten für Gebiete ein, in denen wir über ausreichende Daten zu Angriffsereignissen verfügen, um statistisch signifikante Erkenntnisse zu liefern.

Angriffe auf Webanwendungen und APIs: Trafficanalyse

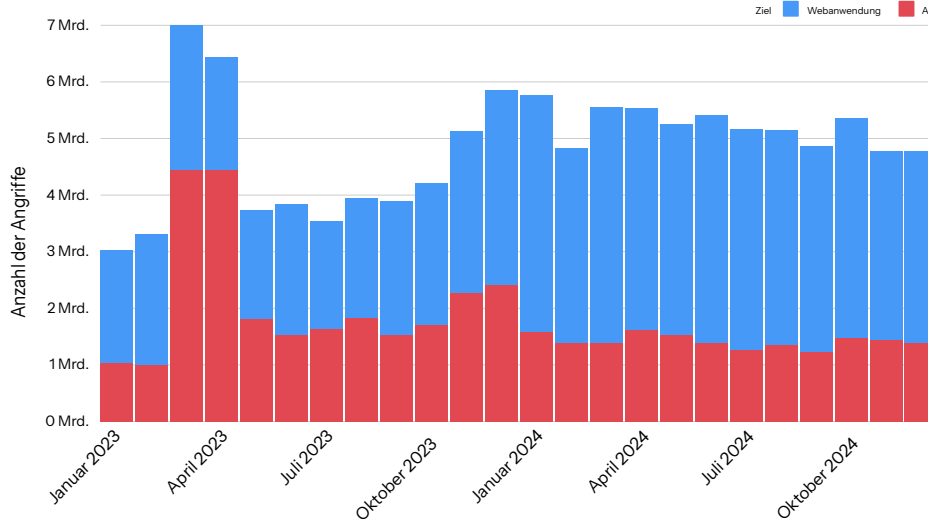
Ein Vergleich der monatlichen Trends bei Webangriffen zwischen den Regionen zeigt starke Unterschiede (Abbildung 12).

APJ: Monatliche Webangriffe
1. Januar 2023 bis 31. Dezember 2024



EMEA: Monatliche Webangriffe

1. Januar 2023 bis 31. Dezember 2024



LATAM: Monatliche Webangriffe

1. Januar 2023 bis 31. Dezember 2024

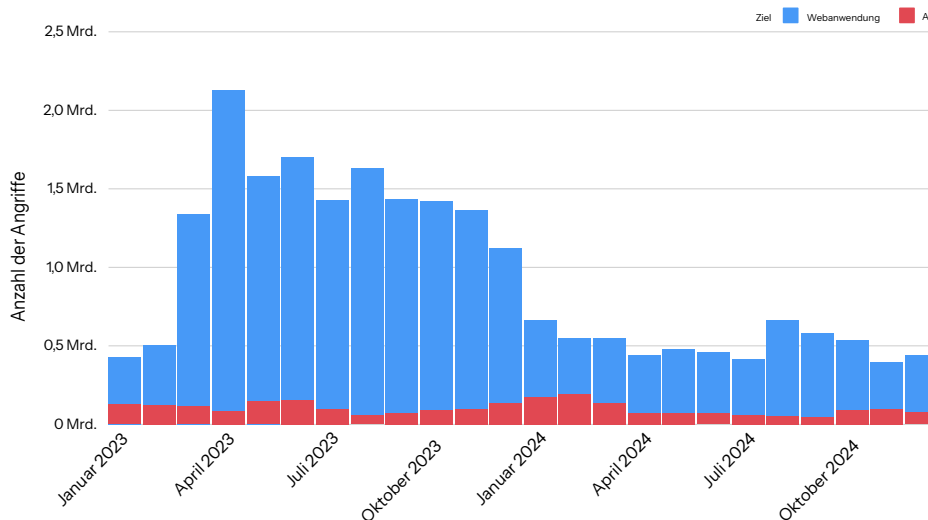


Abb. 12: Angriffe auf Webanwendungen führten zu einer Zunahme der Gesamtzahl von Webangriffen in APJ und EMEA, während Angriffe in LATAM stark zurückgingen.

APJ verzeichnete im Jahresvergleich einen deutlichen Anstieg der Gesamtzahl der Webangriffe um 73 %: von 29 Mrd. im Jahr 2023 auf 51 Mrd. im Jahr 2024. In EMEA betrug der Anstieg im Jahresvergleich moderate 16 % (von 54 auf 62 Mrd.). Dieser kleinere Anstieg ist jedoch auf ein Ausreißer-Ereignis in den Daten zurückzuführen. Würde es entfernt, würde die Zahl eher bei 33 % liegen. In LATAM gingen die Webangriffe erheblich zurück – von insgesamt 16 Milliarden im Jahr 2023 auf 6 Milliarden im Jahr 2024 – was einem Rückgang von 61 % gegenüber dem Vorjahr entspricht.

Die Zunahme der Webanwendungsangriffe scheint zu einer Zunahme der Gesamtzahl von Webangriffen zu führen, da API-Angriffe auf einem niedrigen Niveau blieben, insbesondere in APJ und LATAM.

In der EMEA-Region gingen die API-Angriffsraten nach dem Anstieg im ersten Halbjahr 2023 (der auf [groß angelegte, gezielte Angriffe auf den Handelssektor in Spanien](#) zurückzuführen war) zurück und blieben 2024 auf niedrigem Niveau – auch wenn sie im Vergleich zu anderen Regionen immer noch vergleichsweise hoch waren.

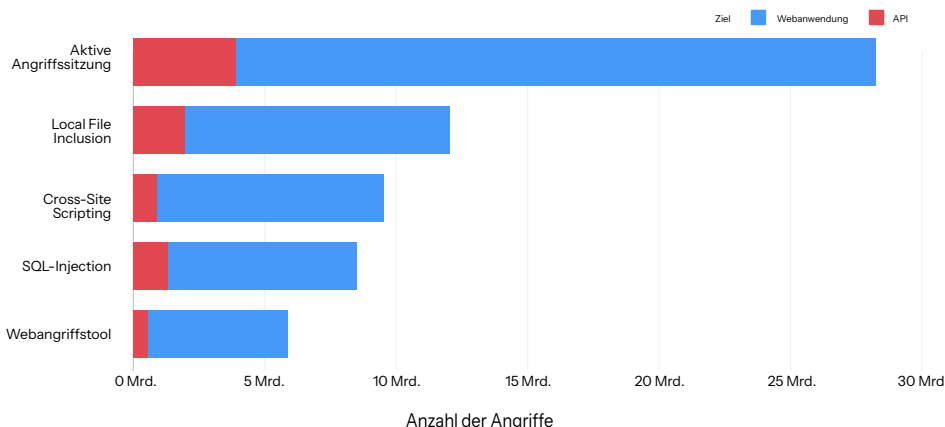
In LATAM gingen Webangriffe zurück, da Cyberkriminelle ihren Fokus vom Handelssektor auf andere Branchen verlagerten, einschließlich Pharmazeutika und Unternehmensdienstleistungen, und sich auf andere Angriffstypen wie [Ransomware](#) konzentrierten.

Angriffe auf Webanwendungen und APIs: beliebte Taktiken

In den letzten zwei Jahren haben sich Cyberkriminelle weiterhin auf traditionelle, bewährte Methoden verlassen, aber auch moderne, verhaltensbasierte Webangriffsvektoren wurden stark genutzt (Abbildung 13).

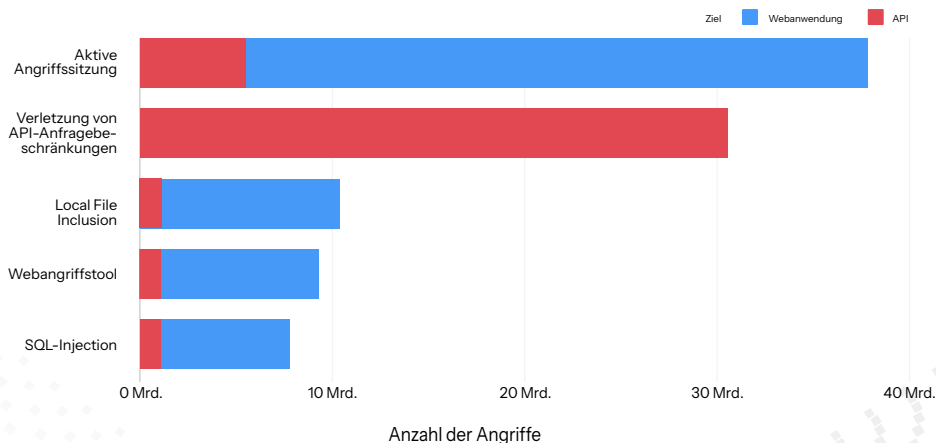
APJ: Webangriffe nach Vektor

1. Januar 2023 bis 31. Dezember 2024



EMEA: Webangriffe nach Vektor

1. Januar 2023 bis 31. Dezember 2024



LATAM: Webangriffe nach Vektor 1. Januar 2023 bis 31. Dezember 2024

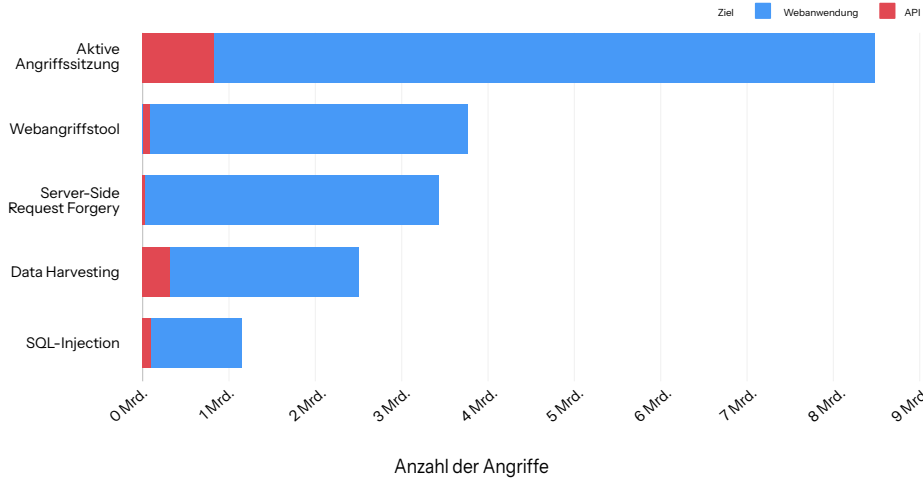


Abb. 13: In allen Regionen umfassten die Top-Angriffsvektoren traditionelle Methoden und moderne verhaltensbasierte Methoden, die speziell auf API-Missbrauch ausgerichtet waren.

In Übereinstimmung mit globalen Trends kommen in allen Regionen weiterhin traditionelle Angriffsvektoren zum Einsatz, einschließlich LFI, SQLi und XSS (sowie SSRF in LATAM). In unserem [Leitfaden für Abwehrspezialisten 2025](#) haben wir die Beständigkeit von XSS und seine anhaltende Relevanz für den Schutz vor herkömmlichen Websicherheitslücken im Internet betont.

Was sich im aktuellen Zeitraum unterscheidet, in dem sich Cyberkriminelle zunehmend auf API-Missbrauch konzentrieren, ist die Zunahme moderner, verhaltensbasierter Angriffsvektoren. Cyberkriminelle nutzen diese Vektoren, um Schwachstellen zu erkennen, die ausgenutzt werden können. Nach der Verfolgung dieser Vektoren auf regionaler Ebene haben die Forscher von Akamai Folgendes beobachtet:

- Der wichtigste Angriffsvektor in jeder Region waren aktive Angriffssitzungen. Hier kommen unsere intelligenten Kontrollen zum Einsatz, um Anfragen bekannter Cyberkrimineller proaktiv über einen längeren Zeitraum zu blockieren.
- Die Verletzung von API-Anforderungsbeschränkungen war der zweithäufigste Vektor in EMEA, wo die Konzentration von API-orientierten Angriffen am größten ist. Angreifer versuchen, APIs auszunutzen, indem sie Anforderungen wie Ratenbegrenzungen und Dateneingaben umgehen.
- In jeder Region war das Webangriffstool unter den Top 5. Cyberkriminelle nutzen diesen Vektor, um das Ziel zu untersuchen und so Informationen über seine Sicherheit, seine Konfigurationen oder potenzielle Schwachstellen zu erhalten, die für böswillige Zwecke ausgenutzt werden könnten.

Weitere Informationen zu diesen Top-Vektoren finden Sie im Abschnitt [Webangriffe](#).

Angriffe auf Webanwendungen und APIs: Top-Ziele

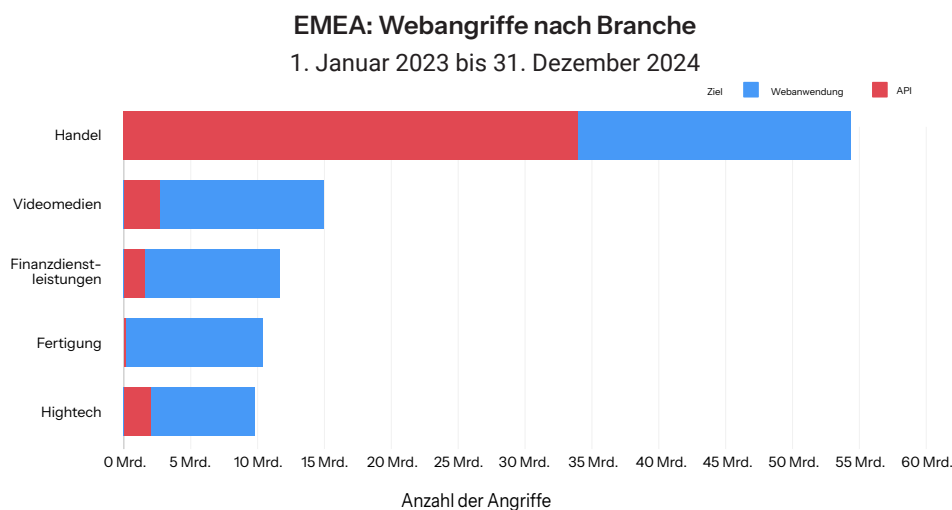
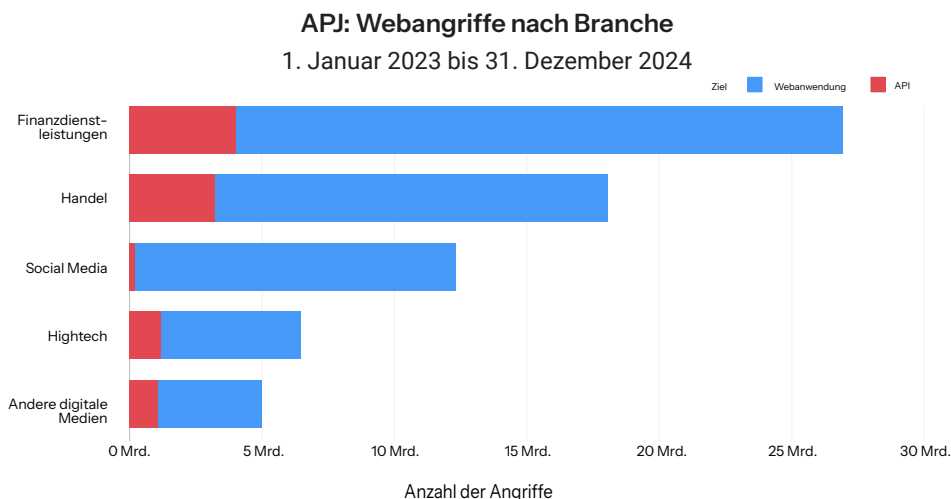
Betrachtet man die Schwerpunkte der Angreifer in den einzelnen Regionen, so zeigt sich, dass APJ, Australien (20,3 Mrd.), Indien (17,3 Mrd.) und Singapur (15,9 Mrd.) die Hauptlast der Angriffe auf Webanwendungen und APIs tragen, gefolgt von Japan (6,3 Mrd.), China (6,2 Mrd.), Südkorea (4,9 Mrd.), Neuseeland (2,9 Mrd.) und Hongkong SAR (2,2 Mrd.).

In EMEA waren die drei Länder, die am stärksten von Angriffen auf Webanwendungen und APIs betroffen waren, das Vereinigte Königreich (30,3 Mrd.), die Niederlande (19,5 Mrd.), Spanien (14,2 Mrd.) und Deutschland (12,8 Mrd.). Österreich folgte mit 8,2 Mrd., dann Frankreich (7,5 Mrd.), Italien (4,1 Mrd.), die Schweiz (3,7 Mrd.), Belgien (3,5 Mrd.) und Israel (3,3 Mrd.).

In LATAM konzentrierte sich das Volumen von Webanwendungs- und API-Angriffen auf Brasilien (19,3 Mrd.) – die nachfolgenden Länder Mexiko (2,0 Mrd.) und Chile (0,4 Mrd.) erlebten nur einen Bruchteil der Angriffe in der Region.

Branchenziele

Die Analyse nach Branchentrends ergab, dass Handel und Finanzdienstleistungen in APJ, EMEA und LATAM durchweg zu den drei Branchen gehören, die am stärksten von Webangriffen betroffen waren (Abbildung 14).



LATAM: Webangriffe nach Branche

1. Januar 2023 bis 31. Dezember 2024

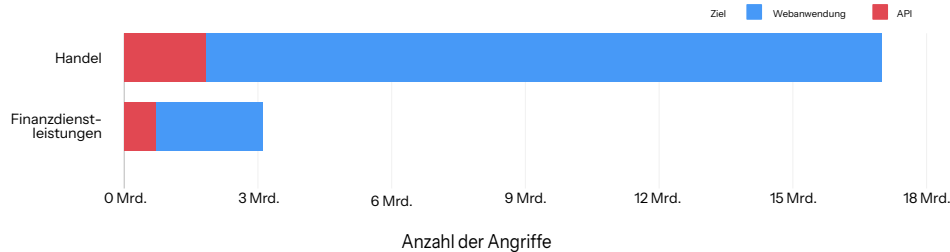


Abb. 14: Handel und Finanzdienstleistungen gehörten zu den drei wichtigsten Zielbranchen in den Regionen APJ, EMEA und LATAM.

In APJ verzeichnete die Finanzdienstleistungsbranche mit 27 Milliarden die höchste Anzahl an Webangriffen, während der Handel mit 18 Milliarden an zweiter Stelle stand. Das entspricht einem Wachstum im Jahresvergleich von 52 % bzw. 161 %. Andere digitale Medien waren mit 22 % die am häufigsten angegriffene Branche für API-Angriffe, gefolgt von Handel (18 %) und Finanzdienstleistungen (15 %).

In der EMEA-Region war der Handel mit 54 Milliarden die Branche, die am stärksten von Webangriffen betroffen war – das sind mehr als dreimal so viele Angriffe wie die nächstgelegene Branche. Trotz der hohen Konzentration gingen die Gesamtangriffe auf Handelsunternehmen im Jahr 2023 um 10 % zurück. Das ist auf einen Anstieg 2023 zurückzuführen, durch den die Daten in der Region verzerrt wurden. Allerdings verzeichnete EMEA im Vergleich zum Vorjahr immer noch einen Anstieg der Webangriffe um 16 %, was auf eine Zunahme der Angriffe auf andere Branchen zurückzuführen ist, darunter Finanzdienstleistungen (152 %) und Fertigung (96 %). Wenn wir uns die API-gerichteten Angriffe in der Region genauer ansehen, stellen wir fest, dass 63 % der gesamten Webangriffe auf Handels-APIs abzielten.

Einen ähnlichen Trend sehen wir auch in LATAM: Hier erreichte die Gesamtzahl der Webangriffe auf den Handel 17 Milliarden und übertraf damit alle anderen Branchen. Angriffe auf den Handel gingen jedoch im Jahresvergleich um 76 % zurück. Die Pharma- und Unternehmensdienstleistungsbranche verzeichneten im Jahresvergleich Zuwächse von 107 % bzw. 129 %. Darüber hinaus konzentrierten sich 11 % der Angriffe im Handel auf APIs – bei Finanzdienstleistern war die Konzentration von API-Angriffen sogar noch höher (23 %).

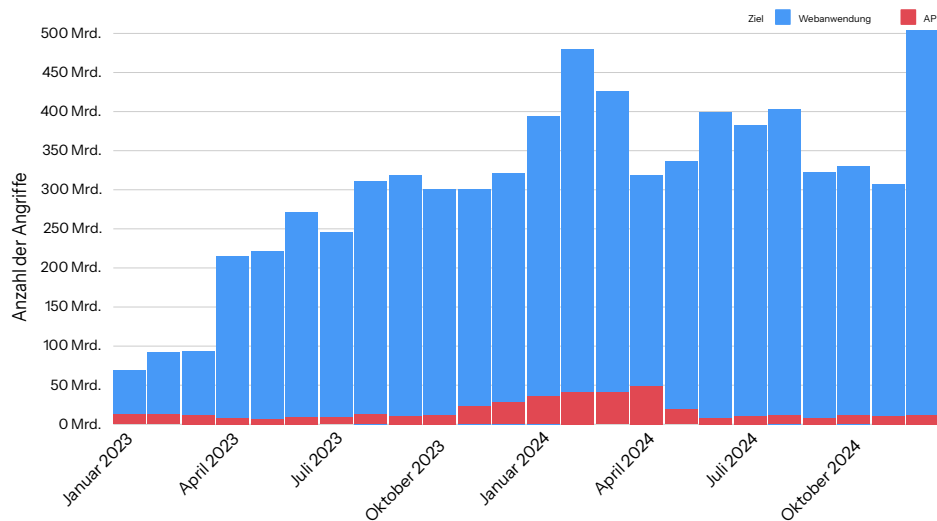
Finanzdienstleistungs- und Handelsbranchen haben gemeinsame Attribute, die sie zu attraktiven Zielen für Webanwendungs- und API-Angriffe machen: Beide arbeiten innerhalb komplexer Ökosysteme, sind stark auf APIs angewiesen und verfügen über wertvolle Daten. Cyberkriminelle nutzen eine Mischung aus traditionellen und neuen Angriffstechniken, um ihre Ziele zu erreichen.

Layer-7-DDoS-Angriffe: Trafficanalyse

Ein Vergleich der monatlichen Layer-7-DDoS-Angriffstrends zwischen den Regionen zeigt, dass APJ ein Hotspot war und dass EMEA und LATAM eine Ebbe und Flut von Angriffen verzeichneten (Abbildung 15).

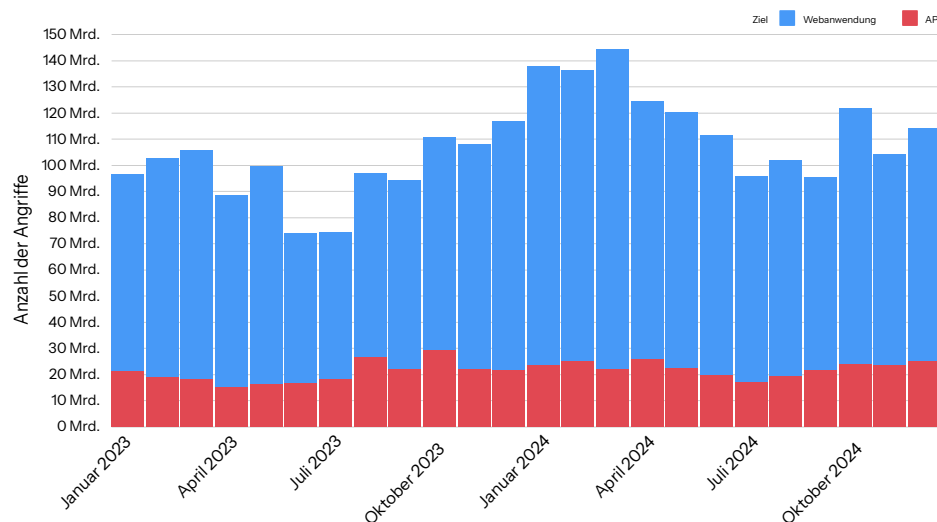
APJ: Monatliche Layer-7-DDoS-Angriffe

1. Januar 2023 bis 31. Dezember 2024



EMEA: Monatliche Layer-7-DDoS-Angriffe

1. Januar 2023 bis 31. Dezember 2024



LATAM: Monatliche Layer-7-DDoS-Angriffe

1. Januar 2023 bis 31. Dezember 2024

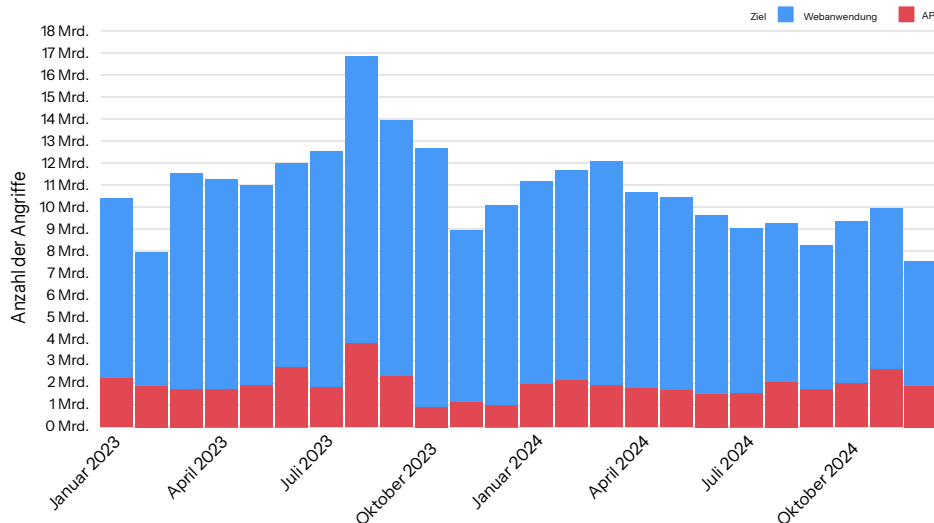


Abb. 15: Layer-7-DDoS-Angriffe nahmen in APJ und EMEA zu, während die Angriffe in LATAM 2024 zurückgingen.

APJ verzeichnete im Jahresvergleich ein Wachstum von 66 % bei Layer-7-DDoS-Angriffen und erreichte im Dezember 2024 mit 504 Milliarden den höchsten Wert der letzten 24 Monate. Das Wachstum wurde in erster Linie durch Angriffe auf die Social-Media-Branche angetrieben.

In der EMEA-Region erreichten Layer-7-DDoS-Angriffe im März 2024 ihren Höchststand von fast 145 Milliarden. Nach einem Rückgang stiegen sie wieder an und erzielten im Jahresvergleich ein Wachstum von 20 %. Das ist auf das Zusammenspiel geopolitischer und technologischer Faktoren zurückzuführen. Die anhaltenden Spannungen in der Region haben „haktivistische“ Aktivitäten angeheizt. Dieser Trend wird durch die Zunahme von KI-gestützten Tools und DDoS-as-a-Service-Plattformen noch verstärkt, die die Zugangsbarriere für Cyberkriminelle verringert haben.

LATAM verzeichnete bereits zu Beginn des Berichtszeitraums eine deutliche Zunahme der Layer-7-DDoS-Angriffsversuche. Sie fielen mit einer Zunahme von [HTTP-Flood-Angriffen](#) zusammen, die auf die Überlastung von API-Ressourcen abzielten (ein Angriffsvektor, der ausführlicher im Abschnitt [Layer-7-DDoS-Angriffe: Jahresvergleich und Trends](#) besprochen wird). Die Aktivität erreichte im August 2023 ihren Höchststand von 16,8 Milliarden, ging dann im restlichen Zeitraum zurück und erreichte einen Tiefststand von 7,5 Milliarden. Das entspricht einem Rückgang der Angriffe im Jahresvergleich um 15 %.

Layer-7-DDoS-Angriffe: Top-Ziele

Innerhalb der einzelnen Regionen haben wir im Vergleich zu unserer [vorherigen Layer-7-DDoS-Angriffsanalyse](#) kaum bis gar keine Änderungen beobachtet, was die Gebiete und Branchen angeht, die von Cyberkriminellen angegriffen wurden.

In APJ erlebte Singapur mit 4,7 Billionen die höchste Angriffskonzentration, gefolgt von Indien (1,1 Bio.), Südkorea (607 Mrd.), Indonesien (283 Mrd.), China (246 Mrd.), Japan (111 Mrd.), Australien (108 Mrd.) und Taiwan (81 Mrd.).

In EMEA waren Deutschland (569 Mrd.) und das Vereinigte Königreich (506 Mrd.) die Gebiete mit der höchsten Anzahl von DDoS-Angriffen auf Layer 7, gefolgt von Israel (205 Mrd.), Schweden (193 Mrd.) und Malta (160 Mrd.). Italien (158 Mrd.), die Schweiz (147 Mrd.), Frankreich (129 Mrd.), die Niederlande (111 Mrd.) und Spanien (96 Mrd.) rundeten die Top 10 ab.

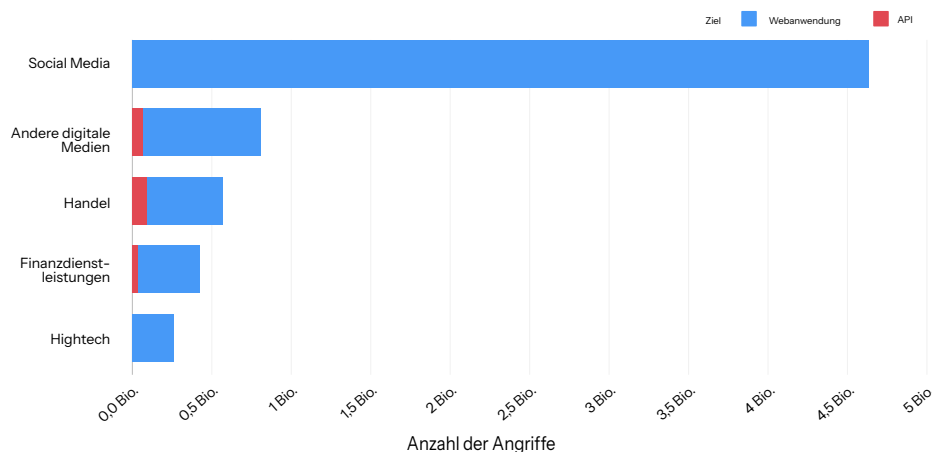
In LATAM verzeichnete Brasilien mit 175 Milliarden die höchste Konzentration von Layer-7-DDoS-Angriffen, gefolgt von Mexiko (39 Mrd.) und Costa Rica (19 Mrd.).

Branchenziele

Die Top-Branchen, die von Layer-7-DDoS-Angriffen in APJ und EMEA betroffen sind (Abbildung 16), haben sich seit unserem [vorherigen SOTI-Bericht zur Anwendungssicherheit](#) nicht verändert. Wie wir in diesem Bericht ausführlicher besprochen haben, stiegen die Layer-7-DDoS-Angriffe auf Social-Media-Plattformen in APJ von Januar 2023 bis Juni 2024. Dieser Anstieg korrelierte mit umfassenderen weltweiten militärischen Konflikten und Wahlereignissen mit hoher Medienpräsenz. Das ist nicht überraschend, da Social-Media-Plattformen in Zeiten geopolitischer Umwälzungen ein hohes Verkehrsaufkommen aufweisen. Wie erwartet hat sich der Trend im weiteren Verlauf von 2024 aufgrund der Wahlen sowohl in APJ als auch in den USA weiter verschärft. Diese Faktoren trugen zum Wachstum der Angriffe auf den Sektor um 130 % im Jahresvergleich bei.

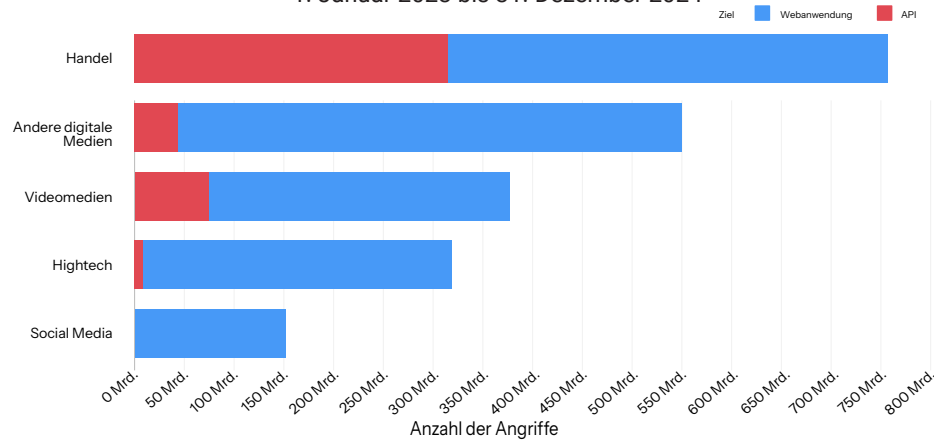
APJ: Layer-7-DDoS-Angriffe nach Branche

1. Januar 2023 bis 31. Dezember 2024



EMEA: Layer-7-DDoS-Angriffe nach Branche

1. Januar 2023 bis 31. Dezember 2024



LATAM: Layer-7-DDoS-Angriffe nach Branche

1. Januar 2023 bis 31. Dezember 2024

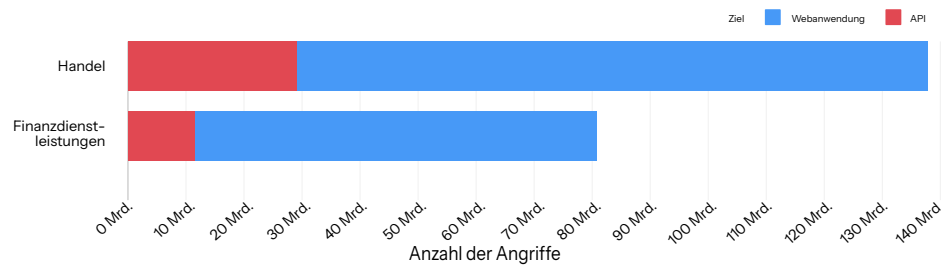


Abb. 16: Die am stärksten betroffenen Branchen pro Region blieben seit unserer Analyse unverändert. Der Handel war durchweg die Branche, die von Layer-7-DDoS-Angriffen auf APIs am stärksten betroffen war.

In der EMEA-Region blieb der Handel die am stärksten betroffene Branche für Layer-7-DDoS-Angriffe, gefolgt von anderen digitalen Medien und Videomedien. Zu den Branchen, in denen diese Angriffe im Jahresvergleich am stärksten zugenommen haben, zählten Hightech (70 %), Social Media (23 %) und Handel (14 %). Diese Verschiebungen zeigen, wie schnell Angreifer ihren Fokus auf andere Regionen und Branchen verlagern können und dass es sich lohnt, breitere Trends zu verfolgen.

Der Handel war auch in LATAM die am häufigsten angegriffene Branche, was Layer-7-DDoS-Angriffe angeht. Finanzdienstleistungen standen hier an zweiter Stelle. Während des Berichtszeitraums blieb die Aktivität von Layer-7-DDoS-Angriffen in allen Branchen relativ konstant.

Unter den Branchen, die am häufigsten von Layer-7-DDoS-Angriffen betroffen waren, hat die Handelsbranche in jeder Region die höchste Konzentration von API-Angriffen erlebt. In der EMEA-Region zielten 43 % der Angriffe im Handel auf APIs ab, in LATAM 21 % und in APJ 16 %.

Aus Gründen wie den geopolitischen Umwälzungen und den potenziellen wirtschaftlichen Auswirkungen von Unterbrechungen stark präsenter Services waren Handel, Medien und Finanzdienstleistungen in den letzten zwei Jahren in EMEA und LATAM die Hauptziele von Layer-7-DDoS-Angriffen. Im Abschnitt [Branchentrends](#) finden Sie eine ausführliche Beschreibung der Faktoren und Methoden, die hinter der hohen Angriffsaktivität in der Handels- und Finanzdienstleistungsbranche stehen.

Compliance

Globale und nordamerikanische Perspektive

Die globale Cybersicherheitslandschaft im Jahr 2025 zeichnet sich durch beispiellose Komplexität und Volatilität aus. Geopolitische Spannungen, insbesondere die anhaltenden Konflikte in der Ukraine und im Nahen Osten, haben Cyberbedrohungen und staatlich unterstützte Angriffe verstärkt. Die Verbreitung von „Hacktivismus“ – insbesondere von prorussischen Gruppen, die westliche Nationen ins Visier nehmen – hat die Bedrohungslandschaft weiter verkompliziert. Aus wirtschaftlicher Sicht hat die rasante digitale Transformation über alle Branchen hinweg die Angriffsfläche erweitert. Cyberkriminelle greifen zunehmend auf kritische Infrastrukturen zu und nutzen fortschrittliche Technologien wie KI, um ihre Fähigkeiten zu erweitern.

Diese Faktoren haben zusammen mit dem globalen wirtschaftlichen Druck und politischen Veränderungen in wichtigen Ländern die Komplexität für Cybersicherheitsexperten weltweit gesteigert. Der Schutz von Webanwendungen und APIs ist eine wesentliche Herausforderung für Unternehmen. Die Bemühungen von ethischen Hackern, Cybersicherheitsexperten und Unternehmen wie Akamai, den nötigen Schutz dieser Einstiegspunkte zu fördern, ergänzen zunehmende Compliance-Überlegungen.

Aufsichtsbehörden auf der ganzen Welt implementieren strengere Compliance-Anforderungen für die Cybersicherheit von Anwendungen. In Nordamerika hat sich der Schwerpunkt auf umfassende Risikomanagementstrategien und obligatorische Vorfallsberichte verlagert. Der [Cyber Incident Reporting for Critical Infrastructure Act](#) in den USA, der voraussichtlich 2026 in Kraft treten wird, schreibt vor, dass Unternehmen mit kritischen Infrastrukturen mindestens einmal jährlich eine Bestandsaufnahme ihrer Informationssysteme vornehmen, Cyberrisiken kategorisieren und ihre Cybersicherheit bewerten müssen. Dieses Gesetz unterstreicht die Notwendigkeit leistungsstarker Sicherheitsmaßnahmen in Anwendungen, insbesondere in kritischen Sektoren wie Energie, chemische Fertigung und Informationstechnologie.

Auf ähnliche Weise passen Kanada und Mexiko ihre Vorschriften an internationale Standards an, wobei der Schwerpunkt auf Datenschutz und der Sicherheit kritischer Infrastrukturen liegt. Obwohl die spezifischen Vorschriften unterschiedlich ausfallen, geht der globale Trend hin zu strengeren Sicherheitsanforderungen für Anwendungen. Das umfasst verbesserte Eingabevalidierung, sichere Entwicklungspraktiken und regelmäßige Sicherheitsprüfungen.

Die API-Sicherheitslandschaft ist mit ähnlichen Herausforderungen konfrontiert: Hier werden APIs aufgrund ihrer entscheidenden Rolle für Serviceintegration und -datenaustausch zu den wichtigsten Zielen für Cyberkriminelle. Aufsichtsbehörden weltweit reagieren darauf mit [strengeren Vorschriften](#), die Unternehmen verpflichten, leistungsstarke API-Sicherheitsmaßnahmen zu implementieren.

Dazu gehören obligatorisch die kontinuierliche API-Erkennung und -Überwachung sowie der Schutz vor neuen Bedrohungen. In Nordamerika liegt der Schwerpunkt auf gründlichen Risikobewertungen in API-Ökosystemen. Dabei werden sichere Entwicklungspraktiken, starke Authentifizierungsmechanismen sowie Funktionen zur Echtzeiterkennung von Bedrohungen hervorgehoben. Die schnelle Einführung KI-basierter SaaS-Tools, die häufig über APIs integriert werden, hat die Angriffsfläche erheblich erweitert und Regulierungsbehörden dazu veranlasst, ausgefeiltere Sicherheitsansätze zu verlangen.

Mit der zunehmenden Komplexität von API-Umgebungen – insbesondere mit der Zunahme von KI- und ML-Anwendungen – entwickeln sich die Compliance-Anforderungen weiter, um Risiken im Zusammenhang mit Datenschutzverletzungen, nicht autorisiertem Zugriff und Serviceunterbrechungen zu minimieren. Während Regionen wie APJ, LATAM und EMEA ihre eigenen spezifischen Vorschriften entwickeln, geht der globale Trend hin zu einer Harmonisierung der API-Sicherheitsstandards, um der Vernetzung moderner digitaler Architekturen Rechnung zu tragen.

APJ-Perspektive

Die APJ-Region erlebt einen erheblichen Wandel in der regulatorischen Landschaft – mit neuen Compliance-Auflagen, die Unternehmen in verschiedenen Sektoren betreffen. In Singapur haben die jüngsten Änderungen des [Cybersicherheitsgesetzes](#) den Anwendungsbereich auf physische und virtuelle kritische Informationsinfrastruktursysteme ausgeweitet. Das umfasst auch Systeme, die auf Cloud-Plattformen gehostet werden und sich [im Ausland](#) befinden. Japan hat sein [nationales Zentrum für Vorfallbereitschaft und Cybersicherheitsstrategie](#) aktualisiert, während Indien sein IT-Gesetz mit der Verabschiedung des [Gesetzes zum Schutz digitaler personenbezogener Daten](#) überarbeitet hat. Australien hat seine Cybersicherheitsstrategie 2023–2030 eingeführt, die den Fokus der Region auf die Stärkung der Cybersicherheitsmaßnahmen unterstreicht. Im Rahmen dieser Strategie wurden Ende 2024 Änderungen am Australian Security of Critical Infrastructure Act vorgenommen und es ist ein neues [Cybersicherheitsgesetz 2024](#) in Kraft getreten. Die Durchsetzung wird nun sekundäre Assets wie IoT-Geräte, Anwendungen und APIs umfassen, die sensible Daten verarbeiten. Diese gesetzlichen Änderungen zwingen Unternehmen dazu, ihre Sicherheitspraktiken für Webanwendungen neu zu bewerten und zu verbessern. Hierbei liegt ein besonderer Schwerpunkt auf dem Schutz kritischer Infrastrukturen und sensibler Daten.

[PCI DSS 4.0.1](#) wird erhebliche Auswirkungen auf Unternehmen haben, die Zahlungskartendaten verarbeiten. Die Frist für die Einhaltung der Vorschriften war der 31. März 2025. Mit dieser neuen Version werden strengere Anforderungen an Webanwendungen eingeführt, darunter Kontrollen für alle Skripte auf Zahlungsseiten, die in den Browsern der Nutzenden ausgeführt werden, sowie der Einsatz automatisierter technischer Lösungen zur kontinuierlichen Erkennung und Verhinderung webbasierter Angriffe. Unternehmen in der APJ-Region müssen nun gründliche Lückenanalysen durchführen, ihre Sicherheitsrichtlinien aktualisieren und die erforderlichen technischen Änderungen implementieren, um diese erweiterten Sicherheitsstandards für ihre Webanwendungen zu erfüllen.

In Bezug auf APIs wird in der APJ-Region zunehmend die API-Sicherheit betont, was teilweise auf die zunehmende Einführung von Open-Banking-Initiativen zurückzuführen ist. Zwar hat die Region Open-Banking-Vorschriften noch nicht in vollem Umfang akzeptiert, wie es in der EMEA zu beobachten ist. Doch für APJ-Länder besteht die Möglichkeit, proaktiv auf [Sicherheitsbedenken](#) zu APIs einzugehen. Eine [Umfrage im August 2024](#) zu API-Sicherheitseinblicken aus dieser Region zeigt, dass interne APIs am häufigsten eingesetzt werden. Dennoch bleibt der externe Nutzerzugriff das Hauptanliegen bei der API-Zugriffskontrolle. Das deutet darauf hin, dass Unternehmen leistungsstarke API-Sicherheitsmaßnahmen implementieren müssen, einschließlich strenger Authentifizierungs- und Autorisierungsprotokolle, Datenverschlüsselung und kontinuierlicher API-Erkennung und -Überwachung. Während sich die Region hin zu [Open-Banking](#)-Vorschriften entwickelt, müssen Unternehmen die API-Sicherheit priorisieren, um die Einhaltung der neuen Vorschriften zu gewährleisten und sich vor neuen Bedrohungen zu schützen.

EMEA-Perspektive

Die Cybersicherheitslandschaft in EMEA durchläuft einen erheblichen Wandel, der auf ein komplexes Zusammenspiel von geopolitischen Spannungen, technologischen Fortschritten und regulatorischen Veränderungen zurückzuführen ist. Die Region steht vor einzigartigen Herausforderungen: Anhaltende Konflikte in der Ukraine und im Nahen Osten verschärfen Cyberbedrohungen und staatlich geförderte Angriffe. Darüber hinaus hat der Anstieg von „Hacktivismus“ – insbesondere von prorussischen Gruppen, die auf europäische Länder abzielen – die Region zu einem Hauptfokus für politisch motivierte Cyberangriffe gemacht.

Die API-Landschaft in EMEA ist mit ähnlichen Herausforderungen konfrontiert. APIs sind aufgrund ihrer entscheidenden Rolle für Serviceintegration und -datenaustausch zu einem Hauptziel von Cyberkriminellen geworden. Und die schnelle Einführung KI-basierter SaaS-Tools, die häufig über APIs integriert werden, hat die Angriffsfläche deutlich erweitert.

Als Reaktion auf diese eskalierenden Bedrohungen hat die Europäische Union eine Reihe umfassender Cybersicherheitsvorschriften eingeführt. Die aktualisierte [Netz- und Informationssystemrichtlinie \(NIS2\)](#), die im Januar 2025 in Kraft trat, erweitert ihren Geltungsbereich erheblich: auf 18 kritische Sektoren. Sie schreibt strenge Cybersicherheitsmaßnahmen für mittlere und große Unternehmen vor.

Für den Finanzsektor tritt der [Digital Operational Resilience Act \(DORA\)](#), der seit 17. Januar 2025 durchgesetzt wird, an die Stelle des NIS2. DORA verlangt starke Frameworks für das Risikomanagement hinsichtlich Informations- und Kommunikationstechnologien, Mechanismen für die Meldung von Vorfällen sowie Programme für digitale betriebliche Resilienztests für Anwendungen in Finanzdienstleistungen. Darüber hinaus führt [PCI DSS 4.0.1](#), das am 31. März 2025 verbindlich wurde, neue Compliance-Anforderungen ein, die sich auf neue Sicherheitsanforderungen, kontinuierliche Sicherheitsprozesse, flexible Methoden und erweiterte Validierungsverfahren konzentrieren. Die anstehende überarbeitete [EU-Zahlungsdienstleistungsrichtlinie \(PSD3\)](#) zielt darauf ab, Mängel in der PSD2 zu beheben – durch strengere Regulierung der Mechanismen für die gemeinsame Nutzung von Daten, durch Verschärfung der Sicherheitsanforderungen und durch Verbesserung der Aufsicht im Finanzdienstleistungssektor.

Der Cyber Resilience Act (CRA), der am 10. Dezember 2024 in Kraft trat, führt verbindliche Cybersicherheitsstandards für Produkte mit digitalen Elementen ein, die in der Europäischen Union verkauft werden. Und er verpflichtet Hersteller, während des gesamten Lebenszyklus eines vernetzten Produkts Sicherheitsmaßnahmen zu ergreifen. Für Anwendungsentwickler und -nutzer umfasst der CRA auch Smartphones und Tablets als signifikante Risikovektoren. Diese Tatsache macht es erforderlich, dass Unternehmen mobile Endgeräte als grundlegende Komponenten ihrer gesamten Cybersicherheitsstrategie betrachten und während des gesamten Anwendungslebenszyklus rigorose Sicherheitsmaßnahmen implementieren.

Im Vereinigten Königreich wird das bevorstehende [Gesetz für Cybersicherheit und -resilienz](#) die Cyberabwehr verbessern und wichtige öffentliche Dienste schützen. Die wichtigen Aktualisierungen des alten Rechtsrahmens werden den Anwendungsbereich erweitern, um mehr digitale Dienstleistungen und Lieferketten zu schützen, die Durchsetzung zu stärken und die Meldepflichten zu erhöhen.

LATAM-Perspektive

Die Cybersicherheitslandschaft in LATAM entwickelt sich rasant weiter, sowohl durch globale technologische Trends als auch durch wirtschaftliche und politische Herausforderungen, die in der Region einzigartig sind. In diesem Zusammenhang hat die schnelle digitale Transformation in den LATAM-Ländern – zusammen mit den Schwachstellen zunehmend vernetzter Systeme – die Region zu einem attraktiven Ziel für Cyberkriminelle und staatlich geförderte Angreifer gemacht. Die Handels- und Finanzdienstleistungsbranchen haben sich zu den wichtigsten Zielen für Cyberangriffe entwickelt. Online-Einzelhändler, Zahlungsabwickler, Banken, Versicherungen, Fintech-Start-ups und Kryptobörsen sind besonders [anfällig](#) für Bedrohungen, die auf die digitale Infrastruktur dieser Unternehmen abzielen, insbesondere auf ihre Webanwendungen und APIs.

LATAM-Länder sind sich dieser Herausforderungen bewusst und machen bei der Entwicklung und Implementierung von Cybersicherheitsvorschriften erhebliche Fortschritte, wobei der Schwerpunkt zunehmend auf der Sicherheit von Webanwendungen und APIs liegt. Brasilien hat mit der Umsetzung des Lei Geral de Proteção de Dados Pessoais (LGPD) eine führende Rolle übernommen – das mittlerweile in Kraft getretene Gesetz schreibt strenge [Anforderungen](#) an Datenschutz und -sicherheit vor. Obwohl das LGPD nicht speziell auf Webanwendungen oder APIs abzielt, hat es Unternehmen dazu veranlasst, ihre Cybersicherheit insgesamt zu verbessern, einschließlich der Sicherheit ihrer digitalen Schnittstellen.

Auf ähnliche Weise hat Chile sein [Rahmengesetz für Cybersicherheit](#) erlassen, das am 1. Januar 2025 in Kraft trat. Mit diesem Gesetz wird die National Cybersecurity Agency eingerichtet und es werden umfassende Maßnahmen zur Verhinderung, Meldung und Lösung von Cybersicherheitsvorfällen in verschiedenen Sektoren vorgeschrieben, einschließlich solcher, die stark von Webanwendungen und APIs abhängig sind. Ebenfalls im Januar 2025 veröffentlichte Argentinien seinen [Regierungsplan für die Verhinderung von Cyberkriminalität und die strategische Verwaltung der Cybersicherheit \(2025–2027\)](#).

Im Bereich der API-spezifischen Vorschriften gibt es vielversprechende Entwicklungen. Mexiko beispielsweise hat [Gesetze](#) eingeführt, die sich auf den Finanzsektor konzentrieren, einschließlich Fintech, und detaillierte Anforderungen an Auskunftsteien und Clearingstellen stellen, was die Entwicklung sicherer APIs angeht. Dieser Ansatz zeigt, dass die entscheidende Rolle von APIs in modernen digitalen Ökosystemen und die Notwendigkeit gezielter Sicherheitsmaßnahmen immer breitere Anerkennung finden. Darüber hinaus regelt das [Bundesgesetz zum Schutz personenbezogener Daten im Besitz privater Parteien](#) in Mexiko die Verarbeitung personenbezogener Daten und legt Verpflichtungen für Unternehmen und Organisationen fest.

Auch Kolumbien hat seinen [Rechtsrahmen](#) weiter ausgebaut und damit seinen rechtlichen Anwendungsbereich erweitert. Hierzu wurden Cybersicherheitsrichtlinien für öffentliche Einrichtungen eingeführt und es wurde ein digitales Risikomanagementsystem mit unterschiedlichen Meldeebenen für die Vorfallsreaktion geschaffen. Diese Maßnahmen konzentrieren sich zwar nicht ausschließlich auf APIs, wirken sich aber zwangsläufig auf die API-Sicherheitsverfahren in Unternehmen aus.

In der gesamten Region gibt es einen zunehmenden Trend zur Einführung branchenspezifischer [Initiativen](#), wie z. B. Open-Finance-Frameworks, die API-Sicherheitsstandards zum Schutz von Kundendaten festlegen. Diese Frameworks sind besonders im Finanzsektor von Bedeutung, wo die Sicherheit von APIs entscheidend ist, um die Integrität von Finanztransaktionen zu wahren und vertrauliche Kundendaten zu schützen. Während LATAM-Länder weiterhin Sicherheitsverbesserungen priorisieren und ihre Cybersicherheitsvorschriften an internationale Standards anpassen, können wir erwarten, dass auch umfassendere und spezifischere Richtlinien für die Sicherheit von Webanwendungen und APIs entwickelt werden.

Abwehr

In der äußerst dynamischen Bedrohungslandschaft mit ihren immer komplexeren Angriffstechniken stellt der Schutz von Webanwendungen und APIs eine wesentliche Herausforderung für Unternehmen dar. Einige der von uns empfohlenen Sicherheits- und Abwehrtechniken umfassen folgende Punkte:

- **Erstellen Sie einen umfassenden API-Sicherheitsplan:** Implementieren Sie einen Shift-Left- und DevSecOps-Ansatz, der Sicherheit vom API-Design bis zur Postproduktion integriert. Sorgen Sie für kontinuierliche [Erkennung](#) und Transparenz, um die gesamte Angriffsfläche zu verstehen, einschließlich versteckter APIs (Schatten-, Legacy- und Zombie-APIs). Erhöhen Sie die Sicherheit durch strenge Authentifizierung und Autorisierung (OAuth 2.0, mTLS, rollen-/attributbasierte Zugriffskontrolle), Ratenbegrenzung und Bot-Abwehr, um Missbrauch zu verhindern. Implementieren Sie Echtzeit-Bedrohungserkennung, Anomalieüberwachung und Laufzeitschutz, um Angriffe sofort zu erkennen und zu stoppen. Gewährleisten Sie die Einhaltung von Vorschriften wie DORA, DSGVO, HIPAA, NIS2 und PCI DSS, während Sie Ihre API-Governance-Richtlinien durchsetzen, um die Sicherheit flächendeckend zu garantieren.
- **Implementieren Sie leistungsstarke Cybersicherheitsmaßnahmen:** Verwenden Sie eine [adaptive Sicherheits-Engine](#), die Bedrohungen kontinuierlich überwacht und in Echtzeit darauf reagiert und darüber hinaus Bedrohungsinformationen und [Laufzeitschutz](#) bietet. Verwenden Sie auch [API-Testtools](#) wie Dynamic Application Security Testing (DAST), um sicherzustellen, dass die Sicherheitsanforderungen erfüllt sind, einschließlich sicherer Zugriff, Verschlüsselung und Authentifizierung.
- **Schützen Sie sich proaktiv vor Bedrohungen:** Verwenden Sie [spezielle DDoS-Schutztools](#), konfigurieren Sie Ratenbegrenzungen und CDN-Caching und implementieren Sie Maßnahmen wie Patch Management, Zugriffssteuerungsrichtlinien und Netzwerksegmentierung. Schützen Sie außerdem die DNS-Infrastruktur mit kontinuierlicher Datenverkehrsüberwachung und hybriden Plattformen.
- **Minimieren Sie API-Schwachstellen:** Befolgen Sie etablierte Sicherheitsrichtlinien, wie z. B. die von [OWASP](#), um starke API-Sicherheit zu gewährleisten und die Risiken von schlechten Programmierpraktiken und Fehlkonfigurationen in der API-Architektur zu beseitigen. Denn diese können ansonsten ausnutzbare Schwachstellen verursachen, über die Hacker unbefugten Zugriff erlangen oder Daten manipulieren können.

- **Schützen Sie sich vor Ransomware-Bedrohungen:** Nutzen Sie einen mehrschichtigen Ansatz, um Ransomware zu bekämpfen. Implementieren Sie Zero-Trust-Lösungen, um schädlichen Datenverkehr zu blockieren, verwenden Sie Mikrosegmentierung für detaillierte Transparenz und präzise Zugriffskontrolle und nutzen Sie das [MITRE ATT&CK Framework](#), um Angriffsmuster zu verstehen und Reaktionsstrategien zu verbessern.
- **Seien Sie auf KI vorbereitet:** Setzen Sie eine umfassende Verteidigungsstrategie ein, die [Bot-Verteidigungslösungen](#), KI-gestützte Sicherheitstools, spezialisierte Firewalls und proaktive Maßnahmen wie kontinuierliche Bewertungen und Zero-Trust-Modelle umfasst. So können Sie die neuen Sicherheitsrisiken bewältigen, die durch den [zunehmenden Einsatz von KI](#) entstehen. Schützen Sie KI-Systeme mit einem vielseitigen Ansatz: Gehen Sie spezifische Bedrohungen wie Prompt Injection und Data Poisoning an, indem Sie sich der Modelle und Datensätze bewusst sind. Führen Sie außerdem proaktive Schwachstellentests durch und implementieren Sie starke Abwehrmechanismen wie Verhaltensüberwachung, Inhaltsvalidierung und automatisierte Angriffsreaktionen, die sowohl in Entwicklungs- als auch Laufzeitumgebungen integriert sind.

Methodik

Angriffe auf Webanwendungen und Layer-7-DDoS-Angriffe

Diese Daten beschreiben Warnungen auf Anwendungsebene über Traffic, der unsere Web Application Firewall (WAF) durchläuft. Die Anwendungsangriffswarnungen werden ausgelöst, wenn wir innerhalb einer Anfrage an eine geschützte Website, Anwendung oder API eine schädliche Payload erkennen. Die Layer-7-DDoS-Warnungen werden ausgelöst, wenn wir volumetrische Anomalien bei der Anzahl der Anfragen an eine geschützte Website, Anwendung oder API erkennen. Diese Warnungen können sowohl von schädlichen als auch von gutartigen Anfragen ausgelöst werden. In der Regel sind die Anfragen selbst harmlos, aber ihre hohe Anzahl weist auf eine böswillige Absicht hin. Die Warnungen zeigen nicht an, ob ein Angriff erfolgreich war. Obwohl diese Produkte ein hohes Maß an Anpassung ermöglichen, haben wir die hier dargestellten Daten auf eine Weise erfasst, bei der keine nutzerdefinierten Konfigurationen der geschützten Ressourcen berücksichtigt werden.

Die Daten stammen aus einem internen Tool zur Analyse von Sicherheitsereignissen, die in der Akamai Cloud erkannt wurden, einem Netzwerk aus ca. 340.000 Servern an mehr als 4.000 Standorten in fast 1.300 Netzwerken in über 130 Ländern. Diese Daten werden in Petabyte pro Monat gemessen und von unserem Sicherheitsteam verwendet, um Angriffe zu untersuchen, schädliches Verhalten aufzudecken und zusätzliche Informationen in die Lösungen von Akamai einzuspeisen.

Diese Daten decken den Zeitraum von 24 Monaten vom 1. Januar 2023 bis zum 31. Dezember 2024 ab.

API-Angriffsdaten

Durch die Integration von Noname Security hat Akamai seine Fähigkeiten zur API-Bedrohungsforschung und -Berichterstattung erheblich verbessert. Dieser Datensatz befindet sich noch in der Anfangsphase der Integration und Analyse. Für diesen Bericht haben wir eine 30-Tage-Datenprobe aus dem 1. Quartal 2025 verwendet, um die Aufschlüsselung der API-Sicherheitswarnungen gemäß den entsprechenden Sicherheitsframeworks und Compliance-Standards zu analysieren. Dieser Datensatz wird sich weiterentwickeln und in Zukunft eine breitere Ansicht der API-Sicherheitsprobleme bieten.



Mitwirkende

Forschungsleitung

Mitch Mayne

Redaktion und Text

Charlotte Pelliccia

Badette Tribbey

Lance Rhodes

Maria Vlasak

Prüfung und fachliche Expertise

Tom Emmons

Stas Neyman

Reuben Koh

Steve Winterfeld

Richard Meeus

Datenanalyse

Chelsea Tuttle

Werbematerialien

Barney Beal

Ashley Linares

Marketing und Veröffentlichung

Georgina Morales Hampe

Emily Spinks

„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/de/security-research

Greifen Sie auf Daten aus diesem Bericht zu

Sehen Sie sich die hochauflösenden Versionen der Diagramme und Grafiken an, die in diesem Bericht aufgeführt sind. Diese Bilder können kostenlos verwendet und referenziert werden, vorausgesetzt, Akamai wird ordnungsgemäß als Quelle genannt und das Akamai-Logo wird beibehalten. akamai.com/sotidata

Akamai-Sicherheitsforschung

Lesen Sie den Blog zur Sicherheitsforschung von Akamai, um eine schnelle Einordnung der wichtigsten aktuellen Forschungsergebnisse zu erhalten. akamai.com/blog/security-research



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: 04/25.