SOTI

B10 AUSGABE 01

10 YEARS
OF SECURITY INSIGHT

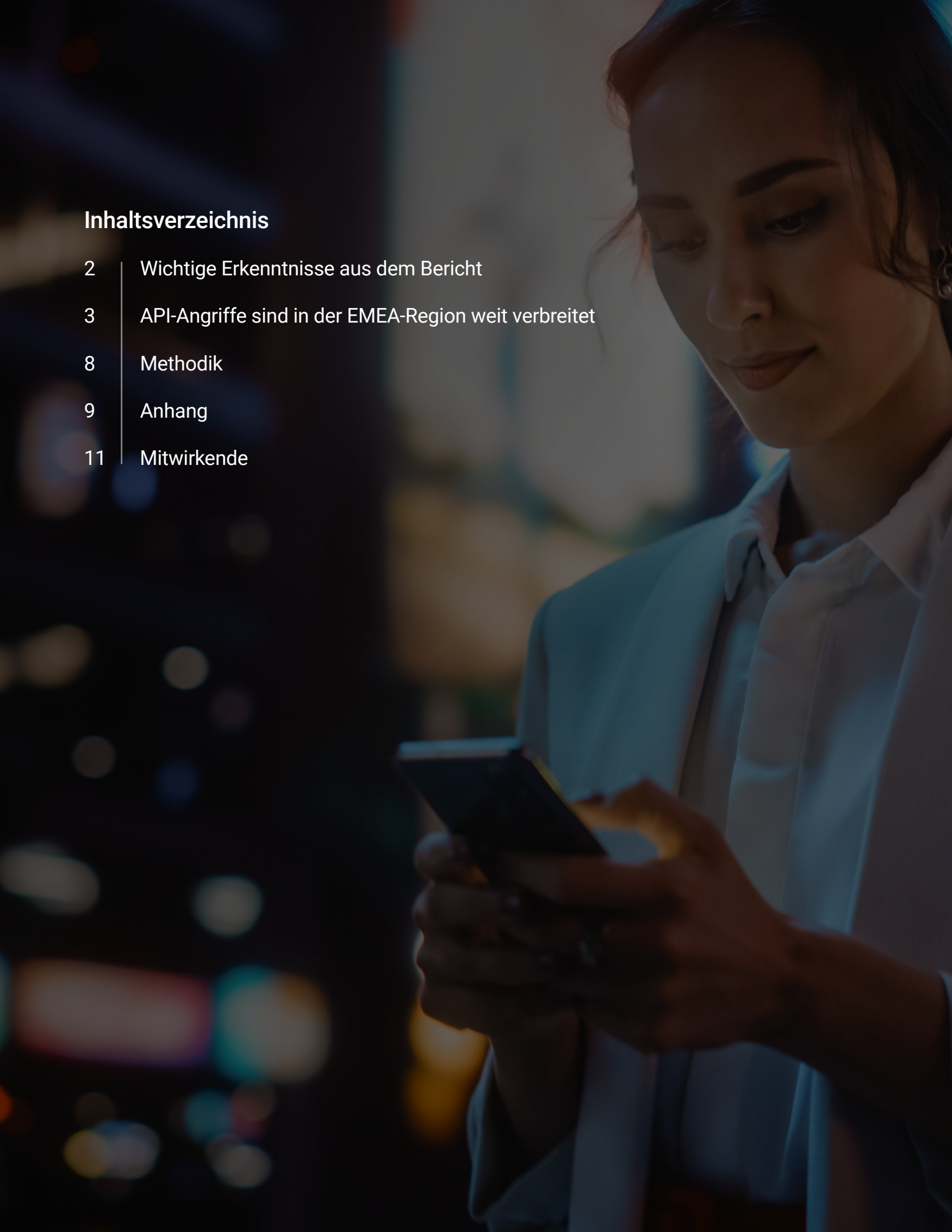
Angriffstrends bringen API-Bedrohungen ans Licht

EMEA Snapshot

Akamai

„State of the Internet“-Sicherheitsbericht

Inhaltsverzeichnis



Wichtige Erkenntnisse aus dem Bericht

Der EMEA Snapshot ist eine Ergänzung zu unserem umfassenderen SOTI-Sicherheitsbericht Verborgen im Schatten: Angriffstrends bringen API-Bedrohungen ans Licht (nur in englischer Sprache verfügbar). In diesem Bericht finden Sie detaillierte Beschreibungen dazu, wie Angreifer die in diesem Snapshot beschriebenen Angriffsvektoren ausnutzen, Empfehlungen, um Ihr Unternehmen zu schützen, sowie eine Erklärung zu unseren Forschungsmethoden und neuen Daten.

Übersicht

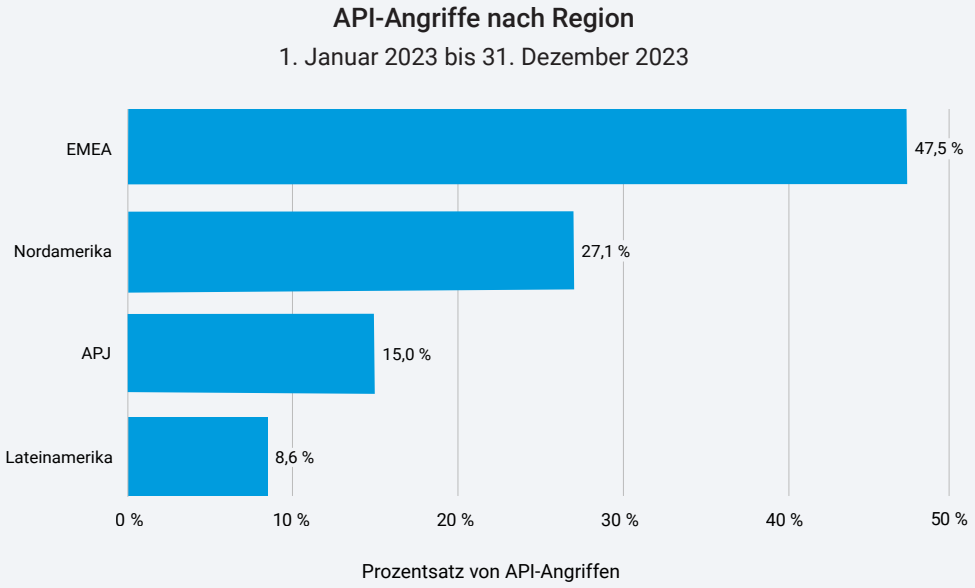
Digitale Innovationen und die API-Wirtschaft verbessern das Mitarbeiter- und Kundenerlebnis. Gleichzeitig bieten sie Cyberkriminellen neue Exploit-Möglichkeiten. Auf APIs abzielende Angriffe können zu finanziellen, Marken- und Reputationsschäden sowie zum Verlust vertraulicher Daten und des Kundenvertrauens führen. Da APIs zunehmend für den Austausch sensibler Finanzdaten genutzt werden, ist die API-Sicherheit angesichts des zu erwartenden Anstiegs des Volumens von API-Angriffen und der zunehmenden Aufsichts- und Meldepflichten im Bereich der Cybersicherheit wichtiger denn je.

Um die API-Bedrohungslandschaft besser verstehen zu können, verwenden wir 2024 einen neuen Datensatz, der es den Forschern von Akamai ermöglicht, zwischen den beiden Angriffstypen zu unterscheiden und sich auf den Anteil der Angriffe zu konzentrieren, die auf APIs abzielen. In diesem EMEA Snapshot, der die 12 Monate von Januar bis Dezember 2023 abdeckt, befassen wir uns mit den Angriffstrends und was sie für Sie bedeuten.

- Auf globaler Ebene wies die EMEA-Region (Europa, Naher Osten und Afrika) mit 47,5 % den höchsten Prozentsatz an Webangriffen auf, die auf APIs abzielten – deutlich mehr als die nächstfolgende Region, Nordamerika, mit 27,1 %.
- In Übereinstimmung mit dem globalen Trend waren HTTP-Protokoll- (HTTP) und SQLi-Angriffe (Structured Query Language Injection) in den letzten 12 Monaten die dominierenden Angriffsvektoren für APIs in EMEA.
- Bot-Anfragen sind ebenfalls ein Problembereich: 40 % der fast vier Billionen verdächtigen Bot-Anfragen zielten auf APIs ab.
- Im Handel waren fast drei Viertel (74,6 %) aller Webangriffe, die sich schädlich auf Unternehmen auswirkten, API-Angriffe – mehr als doppelt so viel wie in der nächstfolgenden Branche, der Hightech-Industrie (35,5 %).

API-Angriffe sind in der EMEA-Region weit verbreitet

Durch die Nutzung eines neuen Datensatzes, der speziell den API-Angriffstraffic verfolgt, hat die Akamai-Forschung ergeben, dass die EMEA-Region mit 47,5 % den höchsten Prozentsatz an API-Angriffen weltweit aufweist – und damit die nächstfolgende Region, Nordamerika, mit 27,1 % bei Weitem übertrifft (EMEA, Abbildung 1). Dies basiert auf der Gesamtzahl der Webangriffen in jeder Region und zeigt, dass APIs in EMEA stärker gefährdet sind als in anderen Regionen.

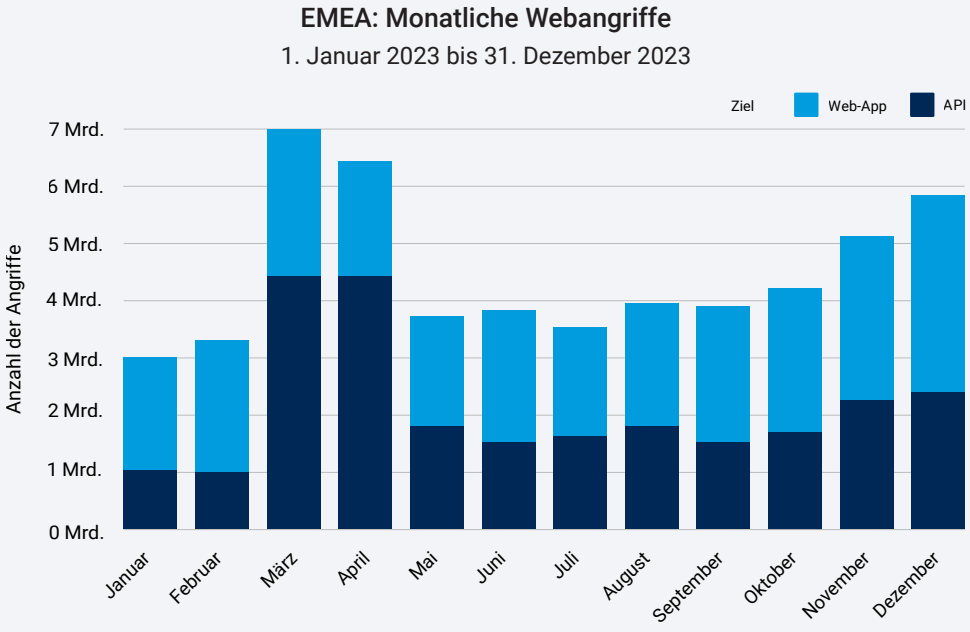


EMEA-Abb. 1: Webangriffe zielen in der EMEA-Region deutlich häufiger auf APIs ab als in jeder anderen Region

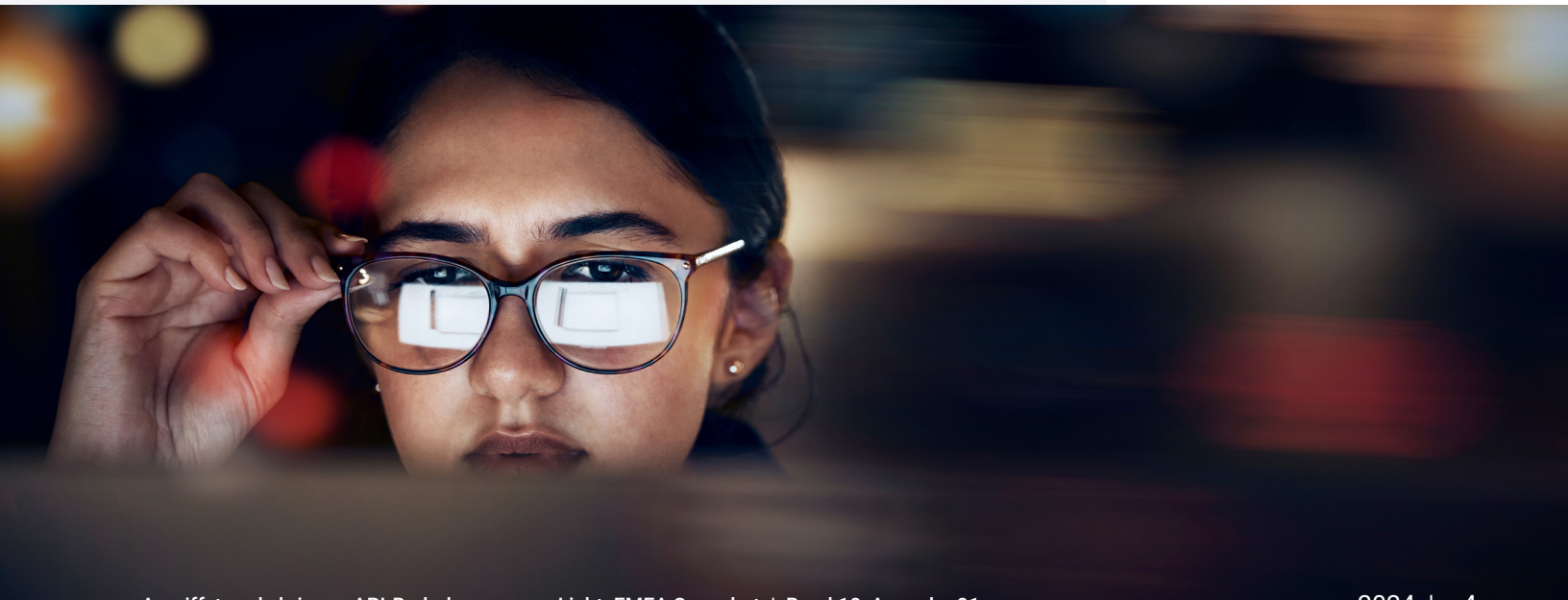
Dieser relativ hohe Prozentsatz von Angriffen in der EMEA-Region (im Vergleich zum Prozentsatz der Angriffe in anderen Regionen) kann zum Teil auf die relativ große Größe des offenen API-Marktes im Vergleich zu Nordamerika und dem asiatisch-pazifischen Raum zurückgeführt werden, was die höhere API-Nutzung in der EMEA-Region widerspiegelt, sowie auf Open Banking und den PCI DSS (Payment Card Industry Data Security Standard) v4.0, die die Nutzung von APIs beschleunigen und die im globalen Bericht diskutierten Sicherheitsrisiken mit sich bringen können.

Innerhalb der Region EMEA sind Spanien (94,8 %), Portugal (84,5 %), die Niederlande (71,9 %) und Israel (67,1 %) die Länder mit dem höchsten Anteil an Angriffen auf APIs. Das bedeutet nicht, dass die Zahl der Webangriffe in diesen Ländern insgesamt höher ist als in anderen EMEA-Ländern. Vielmehr sind diese Länder durch den API-Missbrauch viel stärker gefährdet, da sich die Angreifer auf diesen Vektor konzentrieren.

Die monatlichen Trends im Berichtszeitraum von Januar bis Dezember 2023 zeigen, dass Webangriffe, die auf APIs in EMEA abzielten, ziemlich stetig zunahmen, beginnend mit 34 % im Januar und ansteigend auf 41 % bis zum Ende des Jahres (EMEA, Abbildung 2). Ausnahmen waren März und April, in denen Akamai-Forscher einen Anstieg der API-Angriffe feststellten, da der Handelssektor in Spanien – einem Land mit einer ohnehin schon hohen Konzentration von API-Angriffen – groß angelegten, gezielten Angriffen ausgesetzt war. Diese Spitze zeigt, wie schnell Angreifer ihren Fokus auf andere Regionen und Branchen verlagern können, so dass es sich lohnt, breitere Trends zu verfolgen.

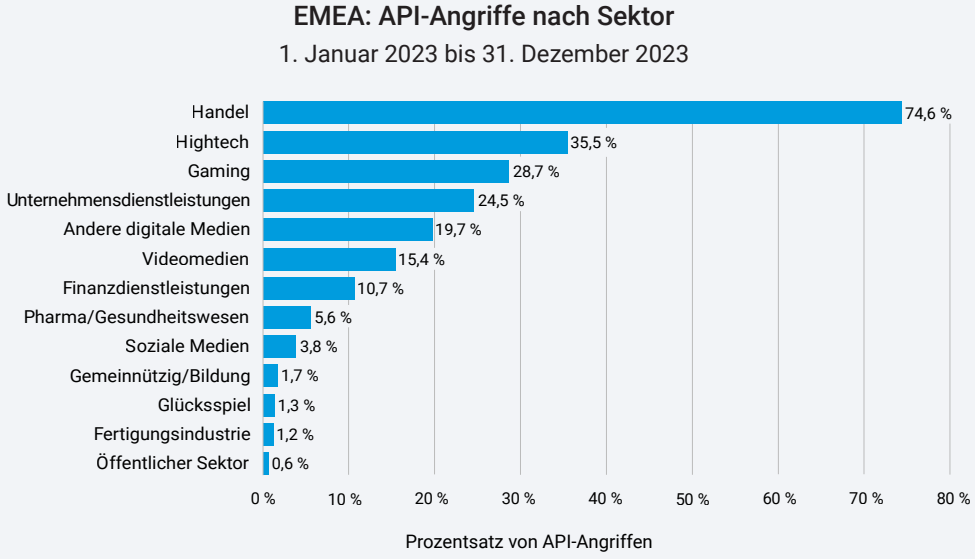


EMEA-Abb. 2: Mit Ausnahme der Monate März und April, in denen API-Angriffe Spitzen erlebten, nahmen API-Angriffe im Jahr 2023 langsam zu und machten am Ende des Jahres 41 % aller Angriffe aus.



API-Angriffe in allen Branchen

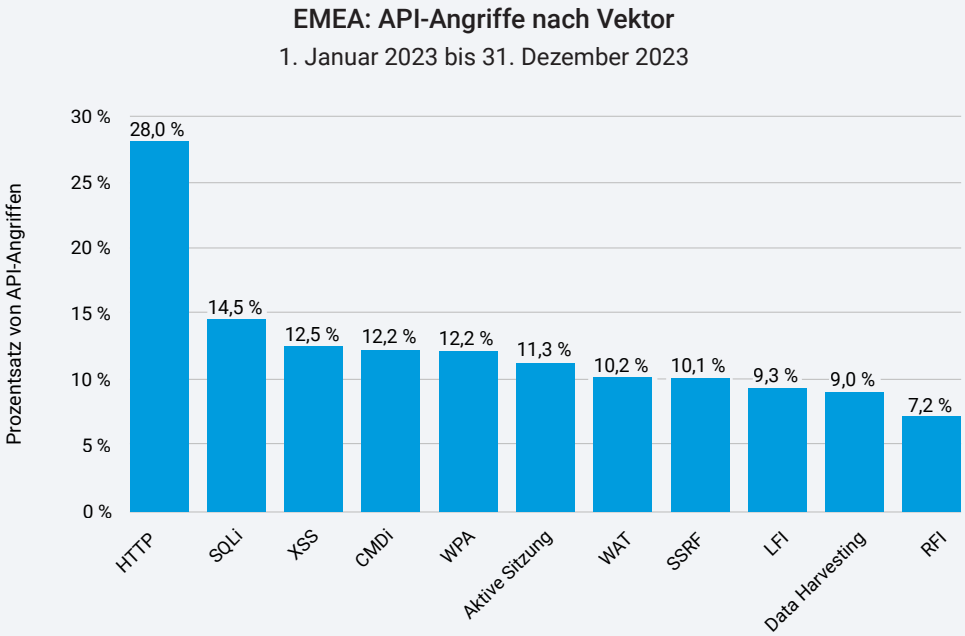
Forscher von Akamai haben im Berichtszeitraum herausgefunden, dass Unternehmen in der Handelsbranche mit 74,6 % die meisten Webangriffe von allen betroffenen Unternehmen verzeichneten. Dieser Prozentsatz ist mehr als doppelt so hoch wie der Anteil der am zweitstärksten betroffenen Branche, der Hightech-Branche (35,5 %). Es folgten Gaming mit 28,7 %, Geschäftsdienstleistungen mit 24,5 % und andere digitale Medien mit 19,7 % (EMEA, Abbildung 3).



EMEA-Abb. 3: Der Anteil an API-Angriffen war im Handel am höchsten, was teilweise auf die Komplexität des Ökosystems, die starke Nutzung von APIs und die wertvollen Daten der Unternehmen in diesem Sektor zurückzuführen ist.

APIs unter Beschuss: Trafficanalyse

Im Einklang mit dem weltweiten Trend waren HTTP und SQLi in den letzten 12 Monaten die vorherrschenden Methoden, mit denen Angreifer in der EMEA-Region APIs ins Visier nahmen. LFI (Local File Inclusion) hingegen ist im Vergleich zu seiner Dominanz bei Angriffen auf Webanwendungen nach hinten abgerutscht (EMEA, Abbildung 4).



EMEA-Abb. 4: HTTP, SQLi und XSS sind die relevantesten Vektoren für API-Angriffe. LFI ist weniger verbreitet für API-Angriffe, wird aber immer noch aktiv für Angriffe auf Webanwendungen genutzt.

Cross-Site Scripting (XSS) ist in EMEA nach wie vor eine beliebte Technik auch für API-Angriffe, und Command Injection (CMDi) ist ebenfalls weit verbreitet. Unser neuer Datensatz ermöglicht es uns, zusätzliche Angriffsvektoren in APIs zu überwachen. So ist SSRF (Server-Side Request Forgery, besprochen in unserem Bericht für 2023) beispielsweise ein aufstrebender Vektor. (Eine vollständige Liste der Definitionen der Angriffsvektoren finden Sie im Anhang.)

Unsere Untersuchungen haben auch ergeben, dass Bot-Anfragen ein Problembereich sind. In diesem 12-monatigen Berichtszeitraum waren 40 % der fast vier Billionen verdächtigen Bot-Anfragen auf APIs gerichtet.

Fazit

Der Schutz von APIs ist aus Sicherheits- und Risikomanagement-Perspektive absolut notwendig. Darüber hinaus machen die bestehenden Gesetze und Vorschriften sowie die sich abzeichnenden Reformen zur Anpassung der Cybersicherheitsgesetze an die Bedrohungslage den Schutz von APIs unabdingbar.

So konzentriert sich beispielsweise die Datenschutz-Grundverordnung (DSGVO) der Europäischen Union auf den Schutz personenbezogener Daten, und APIs stehen nun an vorderster Front bei der Verwendung und Weitergabe dieser Daten. Darüber hinaus wird in der neuen Richtlinie zur Netz- und Informationssicherheit (NIS2) ausdrücklich die Einrichtung eines zuverlässigen API-Sicherheitsprogramms gefordert. Außerhalb der EU haben Länder wie Saudi-Arabien Datenschutzgesetze erlassen, die der DSGVO ähneln und Verpflichtungen für Unternehmen im Hinblick auf personenbezogene Daten umfassen. Darüber hinaus enthält Abschnitt 6 des kommenden PCI DSS (Payment Card Industry Data Security Standard) v4.0 eigens neue Standards für die Verwendung von APIs bei der Entwicklung und Pflege von Systemen und Software, um das Risiko von Datenmissbrauch zu verringern.

Vor dem Hintergrund der Einführung von Initiativen und Richtlinien durch die Regulierungsbehörden zur Stärkung der Cybersicherheitsstandards für APIs ist es wichtig, Best Practices und Richtlinien zu kennen, damit Sie APIs in Ihr Sicherheitsprogramm integrieren können, um die Transparenz zu verbessern, Schutzmaßnahmen zu stärken und die Compliance-Anforderungen zu erfüllen.

Weitere Informationen finden Sie im globalen SOTI-Sicherheitsbericht Verborgen im Schatten: Angriffstrends bringen API-Bedrohungen ans Licht.

Methodik

Webanwendungs- und Bot-Angriffe

Diese Daten beschreiben Warnungen auf Anwendungsebene über Traffic, der unsere Web Application Firewall (WAF) und unser Bot-Management-Tool durchläuft. Die Anwendungsangriffswarnungen werden ausgelöst, wenn wir innerhalb einer Anfrage an eine geschützte Website, Anwendung oder API eine schädliche Payload erkennen. Die Warnungen werden ausgelöst, wenn wir innerhalb einer Anfrage an eine geschützte Website, Anwendung oder API eine schädliche Bot-Payload erkennen. Diese Bot-Warnungen können sowohl von schädlichen als auch von gutartigen Bots ausgelöst werden. 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 Connected Cloud, einem globalen Netzwerk mit mehr als 4.000 Edge Points of Presence in über 130 Ländern, festgestellt wurden. 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.

Die Daten in diesem Bericht decken den Zeitraum von 12 Monaten vom 1. Januar 2023 bis zum 31. Dezember 2023 ab.

Datenaktualisierung 2024

Wir freuen uns, anlässlich unseres 10-jährigen Jubiläums einige Updates unserer Datensätze ankündigen zu können! Unsere Datensätze für Webanwendungen und Bot-Angriffe haben einige Updates erhalten. Die Erfassungsmethode wurde jeweils umgestaltet, gestrafft und optimiert. Umfang und Tiefe unserer Einblicke wurden erweitert. Klassifizierungen für zusätzliche Angriffsvektoren, wie z. B. SSRF, wurden hinzugefügt. Die Erkennung von Angriffen auf API-Endpunkte wurde ebenfalls zu jedem Datensatz hinzugefügt. Es war uns ein Vergnügen, einige dieser neuen Verbesserungen in diesem Bericht hervorzuheben, und wir freuen uns darauf, diese Updates im Laufe des Jahres – und darüber hinaus – zu veröffentlichen, während wir diesen State of the Internet“-Sicherheitsbericht mit unseren Lesern feiern.

Einblicke aus Akamai API Security

Besonderer Dank gilt unserem Akamai API Security Solution Engineering-Team für seine Beiträge zu realen Einblicken in API-Risiken und deren mögliche Auswirkungen auf der Grundlage unserer Warnungen in API Security.

Anhang

Angriffsvektor	Definition
Aktive Sitzung	Angriffstraffic wurde kürzlich für den Client markiert, und wiederholte Anfragen werden für die Dauer der Sitzung blockiert.
Command Injection (CMDi)	Ein Angreifer fügt neue Elemente in einen bestehenden Befehl ein, um die Interpretation des Befehls abzuändern und ihn in Richtung der von ihm gewünschten Aktionen zu lenken.
Cross-Site Scripting (XSS)	Ein Angreifer bettet bösartige Skripte in Inhalte ein, sodass die Zielsoftware die Skripte mit den Berechtigungsstufen des Nutzers ausführt, wenn der Inhalt an Webbrowser übermittelt wird.
Data Harvesting	Ein Angreifer nutzt Schwachstellen im Design oder in der Konfiguration des Zielobjekts und seiner Kommunikation aus, um es dazu zu bringen, mehr Informationen als beabsichtigt preiszugeben. Dies wird oft durchgeführt, um Daten zur Vorbereitung einer anderen Art von Angriff zu sammeln, der Zugriff auf die Informationen kann aber auch das eigentliche Ziel des Angreifers sein.
HTTP-Protokoll (HTTP)	Ein Angreifer nutzt Schwachstellen in dem Protokoll aus, über das ein Client und ein Server kommunizieren, um unerwartete Aktionen durchzuführen. Die Ausnutzung verschiedener Protokolltypen kann unterschiedlichen Angriffszielen dienen.
Local File Inclusion (LFI)	Ein Angreifer manipuliert die Eingaben in die Zielsoftware, um Zugriff auf Bereiche des Dateisystems, die eigentlich nicht zugänglich sein sollten, zu erhalten und diese möglicherweise zu verändern.

Angriffsvektor	Definition
Remote File Inclusion (RFI)	Der Angreifer lädt und führt aus der Ferne beliebigen Code aus, übernimmt anschließend die Kontrolle über die Zielanwendung und veranlasst sie, seine eigenen Anweisungen auszuführen.
Serverseitig manipulierte Anforderungen (SSRF)	Der Angreifer missbraucht die Funktionalität des Servers, um interne Ressourcen zu lesen oder zu aktualisieren.
Structured Query Language Injection (SQLi)	Ein Angreifer manipuliert Eingabezeichenfolgen, sodass, wenn die Zielsoftware SQL-Anweisungen anhand von Nutzereingaben erstellen will, die resultierende SQL-Anweisung stattdessen die vom Angreifer beabsichtigten Aktionen ausführt. Erfolgreiche Injektionen können zur Offenlegung von Informationen führen und die Möglichkeit bieten, Daten in der Datenbank hinzuzufügen oder zu ändern.
Web Attack Tool (WAT)	Ein Angreifer sucht das Ziel aktiv in einer Art und Weise ab, die darauf abzielt, Informationen zu erhalten, die für böswillige Zwecke genutzt werden können. Als Ergebnis dieser Suchen ist der Angreifer in der Lage, Informationen vom Ziel zu erhalten, die ihm helfen, Rückschlüsse auf dessen Sicherheit, Konfiguration oder potenzielle Schwachstellen zu ziehen.
Web Platform Attack (WPA)	Ein Angriff auf eine Softwareplattform (Cloud-, Web- oder Anwendungsebene), die nicht in eine andere Angriffsgruppe eingestuft ist

Mitwirkende

Redaktion und Text

Badette Tribbey – Editor in Chief
Charlotte Pelliccia – Lead Writer (regional)

Redaktionelle Beiträge

James Casey
Edward Roberts
Steve Winterfeld

Prüfung und Fachleute

Tom Emmons
Reuben Koh
Rob Lester
Richard Meeus
Abigail Ojeda
Menachem Perlman
Yariv Shivek

Datenanalyse

Chelsea Tuttle

Marketing und Veröffentlichung

Georgina Morales Hampe
Emily Spinks

Weitere „State of the Internet“-Sicherheitsberichte

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

Weitere Informationen zur Bedrohungsforschung von Akamai

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

Greifen Sie auf Daten aus diesem Bericht zu

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

Weitere Informationen zu Akamai-Lösungen

Weitere Informationen zu den Akamai-Lösungen zum Schutz vor API-Angriffen finden Sie auf unserer **Seite zu Anwendungs- und API-Sicherheit**.

Veröffentlicht: März 2024.