CLOUDFLARE

Der Stand der Dinge bei API-Sicherheit und -Verwaltung

Programmierschnittstellen (Application Programming Interfaces – API) bilden die Grundlage neuer Anwendungserlebnisse: von der Erfassung von Gesundheitsdaten bis hin zu personalisiertem Online-Gaming. Außerdem unterstützen sie unzählige geschäftliche Vorteile: Sie ermöglichen die Analyse von Kundendaten, SaaS-Integrationen, den Einsatz bestimmter Funktionen generativer KI und mehr.

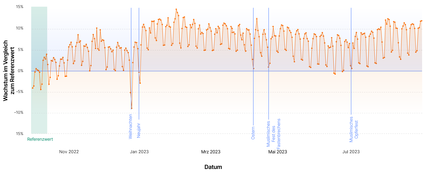
Sie sind zugleich aber umständlich zu verwalten und werden pausenlos angegriffen. Informieren Sie sich über die Trends bei der Absicherung und Verwaltung des API-Traffics, auf den inzwischen **mehr als die Hälfte (57 %) des gesamten dynamischen Internet-Datenverkehrs*** entfällt.

30,7 %

Mittels Machine Learning wurden knapp 31 % mehr API REST-Endpunkte aufgespürt als anhand von Session-Identifikationsmerkmalen, die von Kunden angegeben wurden

Alles dreht sich um API

Insgesamt hat sich der API-Datenverkehr 2023 weltweit stetig erhöht.



Die zehn Branchen, bei denen API den größten Anteil am gesamten Web-Traffic haben:

1. IoT-Community-Plattformen
2. Zug-, Bus- und Taxiverkehr
3. Rechtsdienstleistungen
4. Multimedia, Gaming und Grafiksoftware
5. Logistik, Lieferketten und Transport
6. Unterhaltungselektronik
7. Finanzsoftware
8. Sicherheit und Ermittlungen
9. Bank-, Finanz- und Versicherungsdienste
10. Medizinische Geräte

Ungeschützte API

Wenn Unternehmen keinen umfassenden Überblick über ihren API-Bestand haben, besteht die Gefahr von „Schatten-API". Dabei handelt es sich im Wesentlichen um versteckte Einfallstore:

59,2 %

Der falschen Person Schreibzugriff einzuräumen, kann ein Sicherheitsrisiko darstellen. Viele Unternehmen (59,2 %) räumen Schreibzugriff (die Möglichkeit, Updates durchzuführen) mindestens für die Hälfte ihrer API ein.

Über 15.000

Bei über 15.000 Konten, die Cloudflare nutzen, wurden bestimmte API-Endpunkte ausschließlich mittels Machine Learning-Methoden aufgespürt.

Weit verbreitete API-Schwachstellen

Die Nachfrage nach Sicherheits- und Verwaltungsmöglichkeiten für API ist parallel zum Anstieg von API-Traffic, -Fehlern und -Angriffen regelrecht explodiert.

Größte API-bezogene Bedrohung
HTTP-Anomalien – die am stärksten verbreitete API-bezogene Bedrohung – sind häufig Hinweise auf bösartige API-Aufrufe.

Am stärksten verbreiteter API-Traffic-Fehler
Mehr als die Hälfte (51,6 %) aller auf API zurückgehender Traffic-Fehler umfasste **die Fehlermeldung „429" („Zu viele Anfragen.")**.

Wichtigste Abwehrmethode
Ein Drittel der API-bezogenen Abwehrmaßnahmen umfasste die Blockierung von DDoS (Distributed Denial of Service)-Angriffen.

Herausforderungen beim Schutz vom API im Vergleich zu Webanwendungen

Eine Webanwendung

- Ist für den Endnutzer **sichtbar**
- Wird über einen Webbrower **von Endnutzern verwendet**
- **Stellt Daten** aus dem Backend (mittels HTML, CSS und JavaScript) mit verschiedenen Nutzerinteraktionen **bildlich dar**.
- Wird normalerweise mittels eines **„negativen" Sicherheitsmodells** geschützt, bei dem bekannter schädlicher Traffic blockiert wird

Eine API

- Ist für den Anwendungsnutzer **unsichtbar**
- Erlaubt den Datenaustausch zwischen **Systemen und Anwendungen**
- **Übermittelt Daten** durch den Zugriff auf Server und Anwendungen in einem definierten Format (meistens RESTful JSON, gRPC, XML, GraphQL)
- Wird auf effektivere Weise durch ein **„positives Sicherheitsmodell"** geschützt, das nur bestätigten und authentifizierten Traffic zulässt

Drei wirkungsvolle API-Schutzmaßnahmen

Umstellung von einem „negativen" auf ein „positives" Sicherheitsmodell

Bei einem positiven Sicherheitsmodell wird nur API-Traffic akzeptiert, der bekanntermaßen gutartig ist (was durch API-Schemas definiert ist). Das funktioniert besser als ein negatives Sicherheitsmodell, bei dem der Fokus ausschließlich darauf liegt, bekanntermaßen bösartigem API-Traffic fernzuhalten.

Anwendung von Machine Learning zur Entlastung von Ressourcen und Kostensenkung

Mithilfe von Machine Learning lässt sich der gesamte API-basierte Datenverkehr (einschließlich aller Angriffsvariationen) sichtbar machen sowie zwischen legitimen Traffic-Spitzen und bösartigem Bot-Datenverkehr unterscheiden. Außerdem können damit andere Ressourcen-intensive API-Verwaltungsaufgaben organisiert werden.

Entwicklung, Übersicht, Performance und Sicherheit von Anwendungen an einem Ort

Eine Connectivity Cloud ermöglicht Any-to-Any-Verbindungen zwischen Netzwerken, Clouds, Anwendungen und Nutzern. Damit bildet sie das Fundament für die Vernetzung von Diensten für die Anwendungsentwicklung und die mehrschichtige Verteidigung (Defense in Depth) von API.

CLOUDFLARE

Sie möchten mehr erfahren?

Bericht lesen

Vollständigen Cloudflare-Bericht zu API-Sicherheit und -Verwaltung 2024 aufrufen

* Die Erkenntnisse aus dieser Infografik beruhen auf zusammengefassten Traffic-Mustern, die im weltumspannenden Cloudflare-Netzwerk (was unsere Web Application Firewall, unseren DDoS-Schutz, unsere Bot-Verwaltung und unsere API Gateway-Dienste umfasst) zwischen dem 1. Oktober 2022 und dem 31. August 2023 registriert wurden.