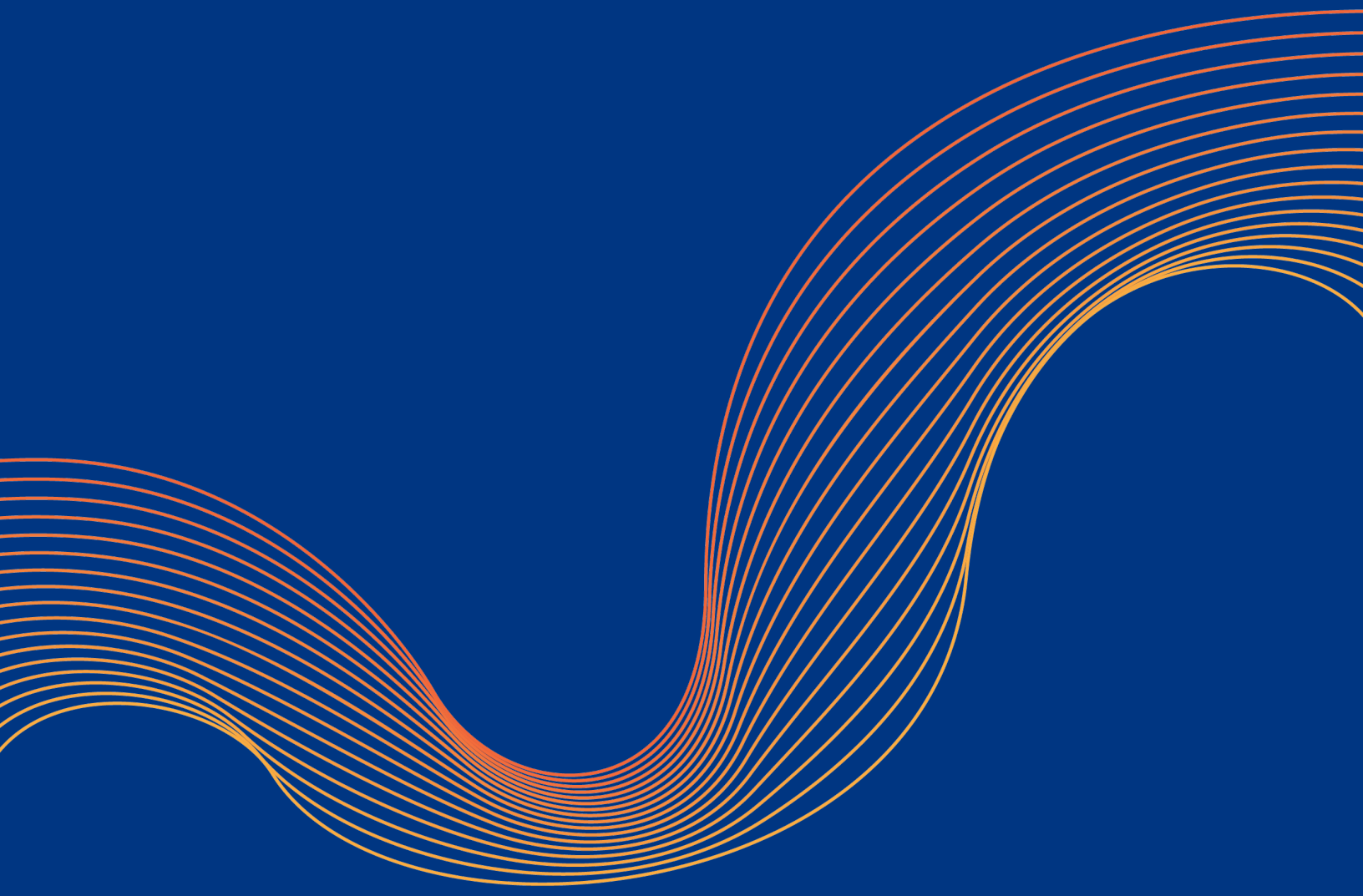
CLOUDFLARE

Effektive Anwendungssicherheit erfordert ganzheitlichen, reaktionsschnellen und kontinuierlichen Schutz



+49 89 2555 2276 | enterprise@cloudflare.com | www.cloudflare.com/de-de/

Was ist Cloudflare?

Cloudflare ist ein globales Netzwerk an der Internet-Edge. Wir bringen Sie Ihren Kunden, Mitarbeitern und Partnern näher, indem wir dafür sorgen, dass Sie sich sicher, vertraulich, schnell und zuverlässig mit dem Internet verbinden können. Ungefähr 25 Millionen Websites – darunter 17 % der Fortune 1000 – nutzen Cloudflare, um öffentlich zugängliche Websites zu schützen und zu beschleunigen, interne Abläufe zu sichern und neue Anwendungen auf unserer Serverless-Plattform zu erstellen.

Unser Netzwerk verfügt über Rechenzentren in über 200 Städten. 99 % aller Internetnutzer können mit einer Latenzzeit von weniger als 100 Millisekunden erreicht werden. Zudem werden durchschnittlich 57 Milliarden Bedrohungen pro Tag blockiert, darunter auch einige der größten DDoS-Angriffe. Jede einzelne Anmeldung, Anfrage und Antwort stärkt die Machine Learning-Modelle, mit denen wir Bedrohungen am Netzwerkrand erkennen und blockieren, bevor sie Ihr Unternehmen überhaupt erreichen.

Zudem ist das Cloudflare-Netzwerk mit Blick auf Datenschutz entwickelt worden. Weil das für uns an erster Stelle steht, setzen wir Ende-zu-Ende Verschlüsselung ein. Wir halten uns an die örtlichen Gesetzesvorgaben zur Datenlokalisierung und -speicherung. Da wir keine Einnahmen aus Werbung erzielen, verzichten wir auf die Erfassung und Speicherung von personenbezogenen Daten, die wir in Ihrem Auftrag verarbeiten.

Der Hauptsitz von Cloudflare befindet sich in San Francisco (Kalifornien). Das Unternehmen unterhält Niederlassungen in Lissabon, London, München, Paris, Peking, Singapur, Sydney, Tokio, Austin (Texas), Champaign (Illinois), Seattle (Washington), New York (New York), San Jos (Kalifornien) und Washington, D.C.

Mehr als 25 Millionen Websites setzen auf die intelligenten Lösungen von Cloudflare. Diese Websites stammen von Unternehmen und Organisationen aus diversen Branchen.

INHALT

EINLEITUNG

Bedrohungen der Anwendungssicherheit sind allgegenwärtig. Im Jahr 2020 meldete die National Vulnerability Database (NVD) über 18.000 Sicherheitslücken und damit einen neuen Rekord. Alarmierend ist dabei die Tatsache, dass mehr als 10.000 dieser Schwachstellen als kritisch oder besonders schwerwiegend eingestuft wurden.

Doch neben neuen Sicherheitslücken machen sich Angreifer auch bereits bekannte Defizite zunutze. Gemeinsame Untersuchungen der US-Behörde für Cybersicherheit und Infrastruktursicherheit (Cybersecurity and Infrastructure Security Agency – CISA), der Sicherheitsbehörde FBI (Federal Bureau of Investigation), des National Cyber Security Center (NCSC) Großbritanniens und des Australian Cyber Security Centre (ACSC) haben ergeben, dass viele der 30 größten Schwachstellen, die von Angreifern im Jahr 2020 (und bis ins Jahr 2021) ausgenutzt wurden, bereits bekannt waren und in diesen Fällen ausnahmslos Patches zur Verfügung standen.

Das von diesen bekannten Sicherheitslücken ausgehende Risiko bleibt bestehen, da die Unternehmen Schwierigkeiten haben, ihre Software zu patchen. Schlimmer noch: Im Durchschnitt dauert es 16 Tage, bis solche Patches wirksam werden, und in der Zwischenzeit sind die betreffenden Anwendungen weiterhin für Angriffe anfällig.

Systeminhärente Schwachstellen stellen leider auch nicht das einzige Sicherheitsproblem für Anwendungsbetreiber dar. APIs bergen ihre eigenen Gefahren und laut Daten aus dem Cloudflare-Netzwerk haben über 50 % der Anfragen einen API-Bezug. Hinzu kommt, dass Bots 40 % des Internet-Traffics ausmachen, weshalb dem Schutz vor Angriffen durch solche Programme entscheidende Bedeutung zukommt. Und schließlich macht Code von Drittanbietern, den viele Websites für korrektes Funktionieren benötigen, Anwendungen anfällig für Supply Chain-Angriffe.

Angesichts des breitgefächerten Angebots an Produkten und Lösungen zum Schutz von Anwendungen vor jeder denkbaren Bedrohung kann die Gewährleistung der Anwendungssicherheit schnell unübersichtlich werden. Abhilfe schaffen lässt sich mit einer ganzheitlichen Strategie, die einen kontinuierlichen Schutz und schnelles Handeln beim Bedrohungen erlaubt.

Gängige Probleme im Bereich der Anwendungssicherheit

Zu den dringlichsten Sicherheitsproblemen der Anwendungsbetreiber zählen:

Schwachstellen von Anwendungen

Schwachstellen in Anwendungen treten unglaublich häufig auf. Laut einem aktuellen Bericht von Veracode zur Software-Sicherheit weisen 83 % der Anwendungen mindestens eine Sicherheitslücke auf, viele auch mehrere. Bei mehr als 20 % der in der Studie untersuchten Applikationen fand sich mindestens eine schwerwiegende Schwachstelle.

API-Angriffe

Anwendungen nutzen immer häufiger Programmierschnittstellen (Application Programming Interfaces – APIs). Kürzlich prognostizierte Gartner, dass „sich API-Missbrauch bis 2022 von einem seltenen zum häufigsten Angriffsvektor entwickeln und Datenlecks bei Webanwendungen von Unternehmen verursachen wird.[1]“

[1]Gartner erwartet, dass „sich API-Missbrauch bis 2022 von einem seltenen zum häufigsten Angriffsvektor entwickeln und Datenlecks bei Webanwendungen von Unternehmen verursachen wird. Quelle: Gartner ‚API Security: What You Need to Do to Protect Your APIs‘“, Mark O'Neill, Dioniso Zumerle, Jeremy D'Hoinne, 1. März 2021, (Gartner-Abonnement erforderlich)

Bot-Angriffe

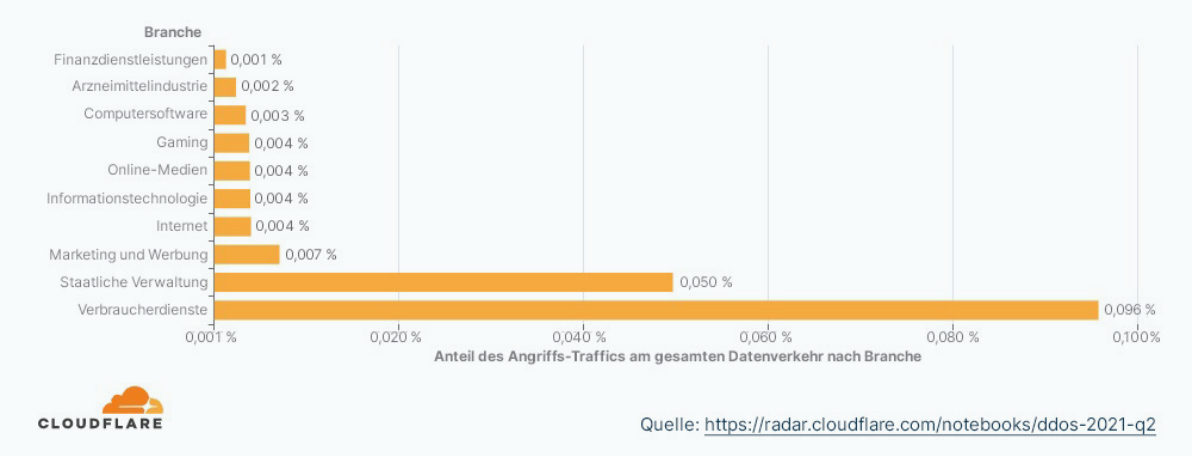
Bot-Angriffe sind sehr verbreitet. Die Angreifer nutzen oft Netzwerke infizierter Geräte – sogenannte Botnetze – für diverse bösartiger Aktionen. Ein Beispiel ist das Credential Stuffing, bei dem Bots Anmeldeseiten mit Hunderten oder Tausenden von gestohlenen Anmeldedatensätzen „füttern", um sich nach Möglichkeit Zugang zu Konten zu verschaffen. Bots werden auch für Content Scraping-Angriffe eingesetzt, bei denen sie die Inhalte einer Website herunterladen und duplizieren, um Vorteile bei der Suchmaschinenoptimierung (SEO) zu erlangen.

Supply Chain-Angriffe

Bei solchen Attacken wird ein Einstiegspunkt über eine externe Quelle gesucht, etwa über Software von vertrauenswürdigen Anbietern, oder Abhängigkeiten von Drittanbieter-Websites oder Dienstleistern. Im Jahr 2015 führte eine Gruppe namens Magecart eine Reihe solcher Angriffe durch, bei denen Zahlungsinformationen von E-Commerce-Websites gestohlen wurden, indem Drittanbieter-Abhängigkeiten auf der Website mit bösartigem Code infiziert wurden. Die Browser der Endnutzer laden die Seite mit den infizierten Abhängigkeiten, was den Angreifern die Möglichkeit gibt, Informationen von der Webseite zu stehlen und sie zu verkaufen. Daraus folgt, dass die Zusammenarbeit mit Dienstleistern und anderen Dritten, auch wenn sich diese auf Abhängigkeiten von anderen Websites beschränkt, die Angriffsfläche erheblich vergrößern kann.

DDoS-Angriffe

Hierbei wird versucht, Anwendungen außer Gefecht zu setzen, indem man sie mit Datenmüll bombardiert. Leider sind DDoS-Angriffe in stetem Wandel begriffen, unter anderem im Hinblick auf Größe und verwendete Vektoren. Und ihr Ende ist nicht in Sicht. Daten aus dem Cloudflare-Netzwerk ergaben, dass unter den im zweiten Quartal 2021 an US-Unternehmen gerichteten HTTP-Anfragen jede zweihundertste Teil eines DDoS-Angriffs war.



Man-in-the-Middle-Angriffe

Anwendungen können auch Opfer von Man-in-the-Middle-Angriffen werden, bei denen man Daten, die beispielsweise zwischen einem Browser und einem Server ausgetauscht werden, zu unlauteren Zwecken abfängt. Der Angreifer kann sich als eine der beiden Parteien ausgeben und deren Kommunikation verändern oder sensible Informationen erbeuten. Man-in-the-Middle-Angriffe können viele Formen annehmen und z. B. auf Domain Name System (DNS)-Server und E-Mail-Server abzielen. Bei DNS-Man-in-the-Middle-Angriffen wird die DNS-Abfrage abgefangen und der Benutzer auf eine andere Website umgeleitet, mit der in der Regel bösartige Absichten verfolgt werden. Ähnlich verhält es sich beim E-Mail-Hijacking, bei dem sich ein Angreifer in die Verbindung zwischen einem E-Mail-Server und dem Internet einschaltet und so die Möglichkeit hat, den E-Mail-Austausch zu lesen und zu stören.

Best Practices zur Abwehr von Bedrohungen für Webanwendungen

Der Schutz vor solchen Angriffen sollte Teil jeder Strategie für Anwendungssicherheit sein. Es kommt aber auch darauf an, auf welche Weise sich Unternehmen dagegen absichern. Eine ausgefeilte Strategie sollte folgende Kriterien erfüllen:

- **Cloudbasiertes Edge-Netzwerk:** Bisher war der lokale Schutz vor Bedrohungen von Webanwendungen die Norm, aber dieser Ansatz ist nur schwer skalierbar. Wenn eine Applikation beispielsweise mit einer hardwarebasierten WAF abgesichert wird, lässt sich dieser Schutz nur durch den Kauf zusätzlicher Hardware skalieren. Dies kann jedoch viel Zeit in Anspruch nehmen, während derer die Anwendung verwundbar bleibt. Bei cloudbasierten Lösungen besteht dieses Problem hingegen nicht. Da die Kapazität beliebig erweiterbar ist, sind der Skalierung keine Grenzen gesetzt.

  Gegen On-Premise-Schutz sprechen außerdem hohe Anschaffungs- und Wartungskosten. Die Hardware ist unter Umständen relativ schnell wieder veraltet, sodass sich die Ausgaben für Reparaturen oder den Austausch von Ausrüstung summieren können. Zusätzlich aufgebläht werden die Gesamtbetriebskosten durch die Fachkräfte, die für die Verwaltung der Hardware eingestellt werden müssen. Mit einer cloudbasierten Lösung lassen sich die Betriebskosten hingegen erheblich senken.

  Ein weiterer Pluspunkt von Cloud-Lösungen ist die Tatsache, dass sie leicht und häufig automatisch aktualisiert werden können. Besonders hilfreich ist das bei Lösungen wie Web Application Firewalls (WAFs), deren Regeln, Abwehrmechanismen und zugrunde liegende Software bei Bereitstellung über die Cloud schnell aktualisierbar sind. On-Premise-Anbieter können ihre Lösungen zwar per Fernzugriff aktualisieren, dies ist jedoch aufwendiger und geschieht im Allgemeinen seltener.

  Bei cloudbasierten Edge-Netzwerken werden diese Vorteile noch ausgeweitet. Dabei handelt es sich um eine Gruppe räumlich verteilter Server, auf denen jeweils dieselben Dienste laufen. Der Schutz erfolgt am Netzwerkrand, sodass nicht nur von der besseren Skalierbarkeit von Cloud-Lösungen, sondern auch von zusätzlichen Performance-Vorteilen gegenüber zentralisierten Modellen profitiert werden kann.

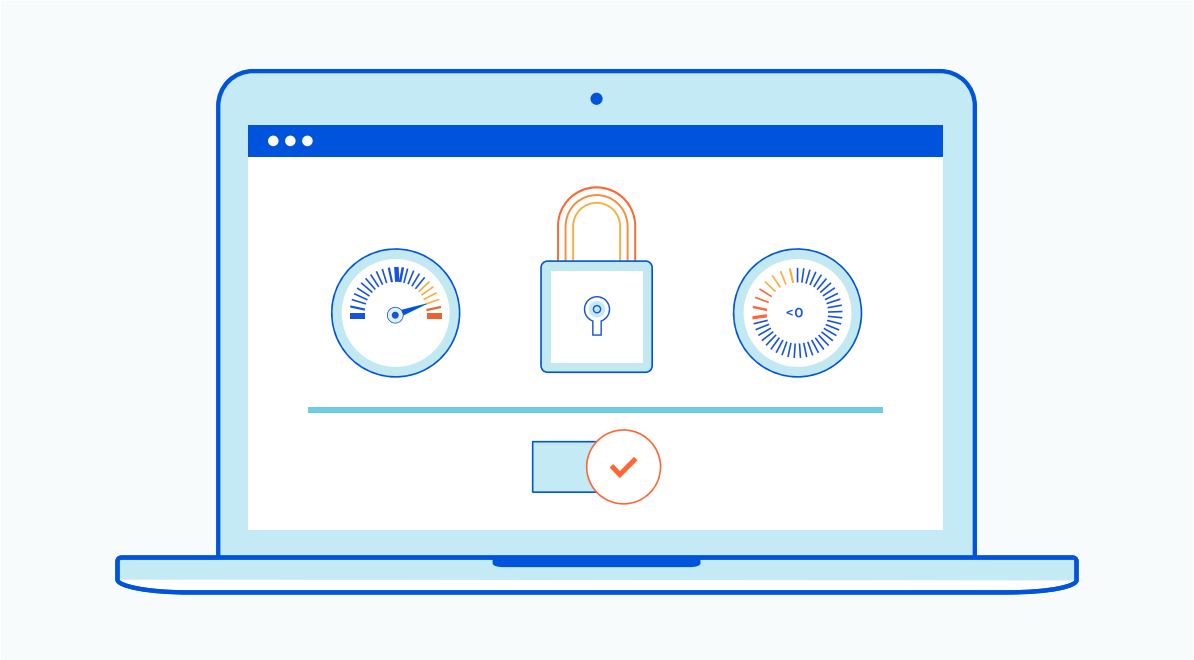
  In einem cloudbasierten Edge-Netzwerk findet der Schutz in größtmöglicher Nähe zum Endnutzer statt, während diese Funktion bei einem zentralisierten Modell in einem einzigen Rechenzentrum gebündelt wird, das von den meisten der auf dem ganzen Globus verstreuten Endanwender erheblich weiter entfernt ist. Für die Absicherung muss der gesamte Traffic des Nutzers – unabhängig von dessen Standort – zu dem zentralen Rechenzentrum zurückgeleitet werden, in dem die Sicherheits-Appliances installiert sind. Wenn sich die Rechenzentren also in Bayern befinden, muss der Datenverkehr zunächst dorthin geleitet werden, bevor er zum Beispiel an einen Endbenutzer in Berlin übermittelt werden kann.

- **Einheitlichkeit:** Wenn versucht wird, mit verschiedenen Tools einen einheitlichen Schutz zu gewährleisten, kann das zu Fehlern führen. Es ist daher empfehlenswerter, ein einziges, einheitliches System zur Angriffsabwehr zu verwenden.

  Werden dagegen mehrere Einzeltools zu Sicherheitszwecken eingesetzt, sind oft unterschiedliche Personen für ihre Verwaltung zuständig. Das kann dazu führen, dass wichtige Informationen nicht auf übergeordneter Ebene weitergegeben werden, wodurch Wissenssilos und Informationslücken entstehen. Außerdem müssen alle Tools selbst konfiguriert und verwaltet werden, was die Beschäftigten belastet und unnötigen Aufwand verursacht.

  Darüber hinaus kann es schwierig sein, alle Warnmeldungen zu analysieren, wenn zu viele verschiedene Lösungen genutzt werden. Jedes Tool folgt seinen eigenen Regeln und seiner eigenen Logik beim Versenden von Warnmeldungen. Wenn mehrere im Einsatz sind, lassen sich deshalb im Zweifelsfall Wichtiges und Unwichtiges nur schwer auseinanderhalten.

  Bei einem einheitlichen System müssen sich die Mitarbeitenden dagegen mit weniger Tools auseinandersetzen. Außerdem haben alle Warnmeldungen denselben Ursprung, sodass viel einfacher zu erkennen ist, worauf gerade besonders geachtet werden muss. Darüber hinaus beziehen sich integrierte Tools häufig auch auf die gleichen Richtlinien, was eine einheitliche Richtlinienanwendung erleichtert. So haben Anwendungsbetreiber beispielsweise die Möglichkeit, Regel für Data Loss Prevention (DLP) nur einmal festzulegen und diese automatisch von ihrer WAF, API und anderen anwendbaren Tools durchsetzen zu lassen.

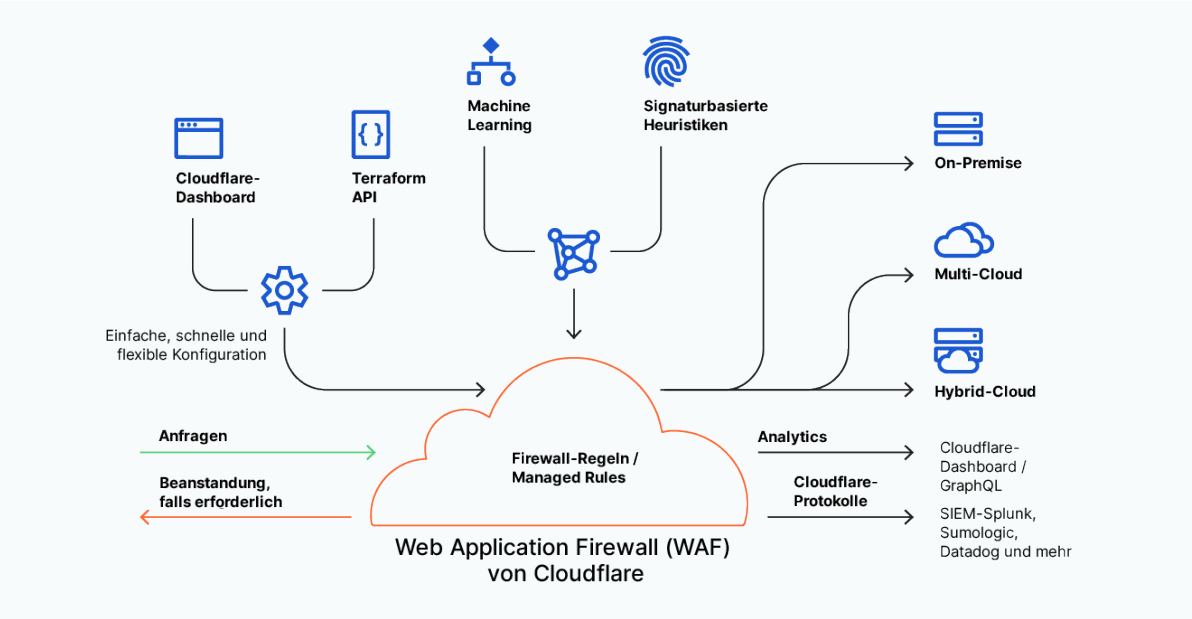


Angriffsspezifische Strategien

Weil sich Anwendungen einer derart hohen Zahl unterschiedlicher Sicherheitsrisiken gegenübersehen, müssen sie auch auf vielfache Weise geschützt werden. Dies sind einige der angriffsspezifischen Strategien, die Anwendungsbetreiber anwenden können:

Schwachstellen von Anwendungen

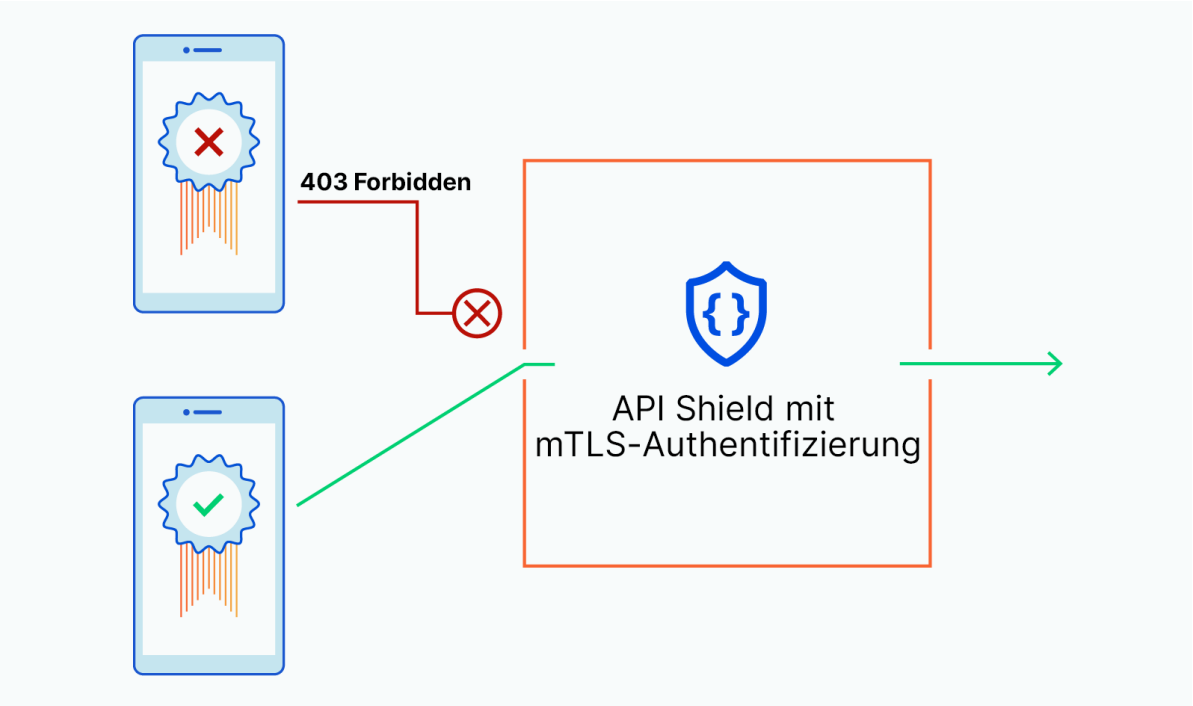
WAFs: Eine WAF zählt zu den besten Mitteln, um Angreifer daran zu hindern, Schwachstellen in Anwendungen auszunutzen. WAFs verwenden eine Reihe von Sicherheitsregeln, die sich aus bekannten Angriffstechniken ableiten, um schädlichen Traffic herauszufiltern und Angriffe zu verhindern. Am effektivsten sind WAFs mit voreingestellten Regeln und Anpassungsoptionen, die Regeländerungen schnell anwenden. Das liegt daran, dass diese Funktionen zwei der größten Probleme vieler WAFs lösen: Fehlalarme und eine langsame Umsetzung von Regeländerungen. Falschmeldungen haben zur Folge, dass durch WAF-Regeln unbeabsichtigt legitimer Web-Traffic blockiert wird. Bei einigen WAFs sind zur Regelfestlegung komplexe Verfahren erforderlich, was es schwierig macht, genaue und aktuelle Listen zu führen und legitimen Traffic freizugeben. Bei WAFs, die zusätzlich zu den verwalteten und benutzerdefinierten Regelsätzen auch OWASP-Regelsätze anbieten, treten daher seltener Fehlalarme auf. Wenn es jedoch zu lange dauert, diese neuen Regeln zu implementieren, bleiben die Anwendungen für Angriffe anfällig.



Data Loss Prevention (DLP): Dabei handelt es sich um eine Strategie, mit der Datenexfiltration (oder das unbefugte Ausschleusen von Daten) verhindert werden soll. DLP-Tools und -Lösungen überwachen Anwendungs- und API-Aktivitäten, um potenzielle Datenlecks frühzeitig zu erkennen und zu unterbinden. Dazu wird der ausgehende Traffic untersucht und mit bekannten Datentypen verglichen, um zu ermitteln, ob es sich um ein Datenleck handelt, das gestopft werden sollte. Ein DLP-Tool kann zum Beispiel eine Zeichenfolge als Benutzernamen identifizieren. Anhand der von dem Unternehmen aufgestellten Regeln kann das Tool die Aktivität als verdächtig kennzeichnen, unterbinden oder weiter zulassen. Einige DLP-Tools können in rollenbasierte Zugriffskontrollen (Role-Based Access Controls – RBAC) integriert werden. Diese legen fest, welche Zugriffsrechte die einzelnen Benutzertypen haben, um die Datenbewegungen innerhalb eines Unternehmens oder einer Anwendung noch besser zu schützen.

API-Sicherheitsrisiken

Schema-Validierung und positive Sicherheitsmodelle: API-Schemata sind Verträge, die das erwartete Verhalten derjenigen beschreiben, die mit einer API interagieren. Schemata legen die Grundregeln dafür fest, was Benutzer bei der Arbeit mit APIs tun dürfen. OpenAPI (oder Swagger) ist das am weitesten verbreitete Schema-Format. Schemata sind gute Vorlagen zur Durchsetzung einer positiven API-Sicherheit. Ein positives Sicherheitsmodell validiert Anfragen anhand des Schemas und lässt nur Anfragen zu, die dem Schema entsprechen, wodurch Missbrauch und Angriffe verhindert werden. Ein positives ist strenger als ein negatives Sicherheitsmodell, das standardmäßig alle Anfragen mit Ausnahme derer zulässt, die es explizit blockieren soll.



Authentifizierung und Autorisierung: Authentifizierung (Sicherstellung, der Legitimität von API-Anfragen) und Autorisierung (Bestätigung der Zugriffsrechte eines Endpunkts oder Clients) sind ebenfalls wichtige Aspekte der API-Sicherheit. Es gibt viele Möglichkeiten, API-Anfragen zu authentifizieren und zu autorisieren. Mutual Transport Layer Security (mTLS) zum Beispiel ist ein Verfahren, bei dem sowohl ein Client als auch ein Server über Authentifizierungszertifikate verfügen, mit denen sie die Identität des jeweils anderen überprüfen.

API-Erkennung: „Schatten"-APIs sind APIs, deren Existenz einem Sicherheitsteam möglicherweise nicht bekannt ist. Sie werden deshalb nicht überwacht und können so zu Datenlecks führen oder entsprechen unter Umständen nicht den Compliance-Standards. Tools zur API-Erkennung überwachen Endpunkte, um Schatten-APIs zwecks besserer API-Verwaltung aufzuspüren.

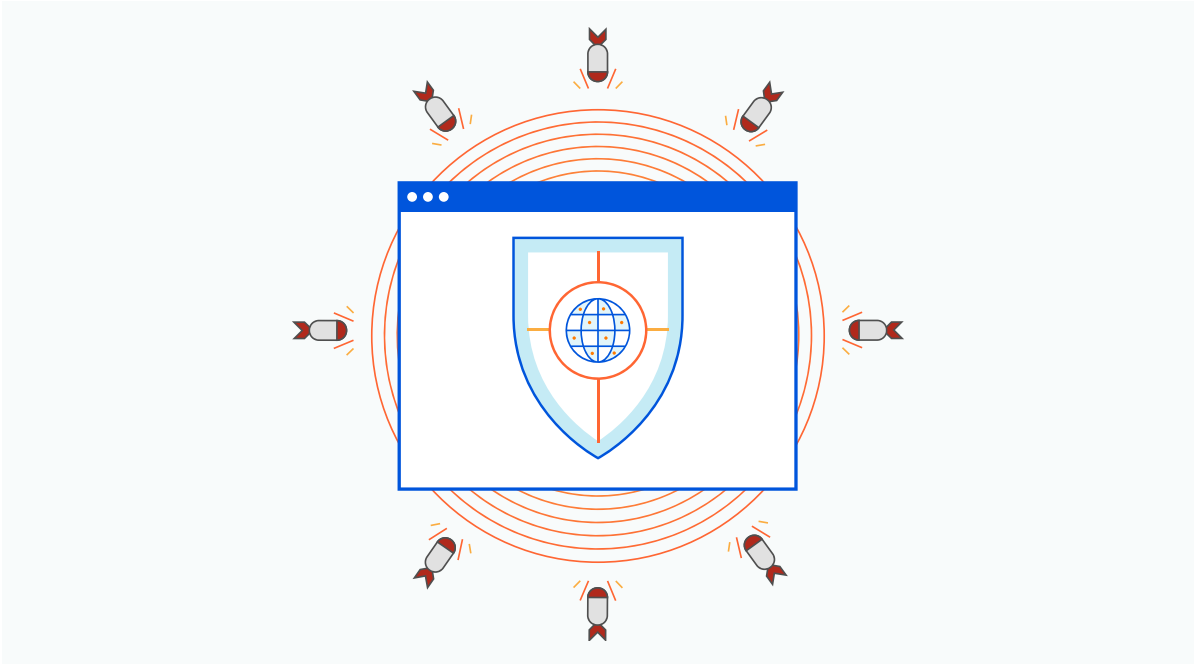
DLP: Die Datenexfiltration kann nicht nur über traditionelle Anwendungen, sondern auch über APIs erfolgen. DLP-Tools lassen sich zur Überwachung des ausgehenden API-Datenverkehrs einsetzen, um potenziell sensible Daten in API-Antworten zu erkennen und zu blockieren.

Bösartige Bots

Bei der Verwaltung des Bot-Traffics kommt es darauf an, schädliche Bots zu erkennen und zu blockieren. Vertrauenswürdige – etwa SEO-Site-Crawler – dürfen hingegen nicht gestoppt werden, da sie zum Verständnis wichtiger Geschäftskennzahlen erforderlich sind. Bösartige Bots können einer Anwendung durch Credential Stuffing, Content Spam und andere Arten von Angriffen Schaden zufügen. Eine Bot-Management-Lösung analysiert den Datenverkehr, um Bot-Aktivitäten zu erkennen und zu ermitteln, ob sie gut- oder bösartig sind, und den Traffic dementsprechend zu blockieren oder zuzulassen. Ein effektives Management von Bots erfordert ausgefeilte Erkennungsmethoden, die Fähigkeit, Trends im Bot-Traffic mithilfe von Analysen über einen längeren Zeitraum hinweg zu verstehen, und die Flexibilität, diese Daten zur Anpassung der Regeln für das Blockieren von Bots zu nutzen.

DDoS-Angriffe

Eine wirksame Bekämpfung von DDoS-Angriffen bedeutet, die Abwehrzeit zu optimieren, ohne dass dabei die Sicherheit auf Kosten der Performance geht. Erreichen lässt sich dies durch einen DDoS-Schutz, der immer im Einsatz ist (Always On). Die Alternative wäre eine Abwehrlösung, die nur auf Abruf aktiv wird (On Demand). Im Gegensatz zum On-Demand-Schutz wird bei der Always-On-Variante nicht gewartet, bis der Traffic einen bestimmten Schwellenwert erreicht, damit der Schutz greift. Vielmehr wird der gesamte Datenverkehr überprüft, was eine höhere Reaktionsschnelligkeit erlaubt. Die DDoS-Abwehr am Netzwerkrand bringt Anwendungsbetreibern Vorteile im Hinblick auf Performance und Sicherheit. Sie erfolgt so nah wie möglich am Ausgangspunkt der Attacke, was sich positiv auf die Performance auswirkt – im Gegensatz zum zentralisierten Schutz, der unabhängig vom Angriffsursprung immer am gleichen vordefinierten Ort stattfindet.



Schwachstellen von Drittanbietern

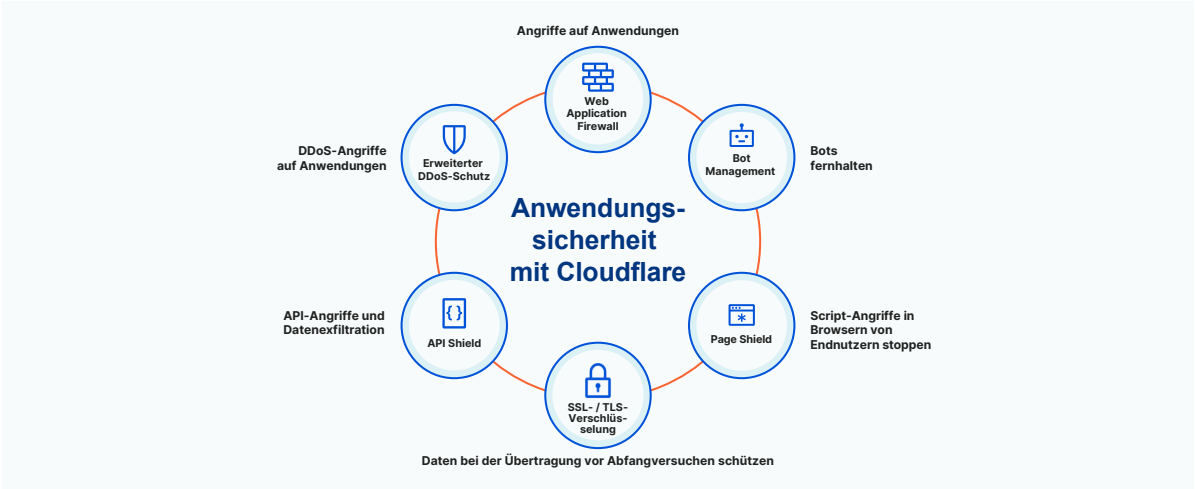
Client-seitige Sicherheitslösungen: Da sich viele Websites auf Drittanbieter stützen, die entsprechenden Abhängigkeiten aber eher selten kontrolliert werden, können sie für Angriffe auf die Supply Chain anfällig sein. Bei Client-seitigen Sicherheitsmodellen werden die Aktivitäten auf Seite des Nutzers abgesichert, in der Regel in seinem Browser. Client-seitige Sicherheit schützt vor Angriffen auf die Supply Chain, indem Änderungen an Drittanbieter-Abhängigkeiten überwacht und die Art der Codeänderungen untersucht werden. Bei dem Verfahren der Content Security Policy (CSP) wird beispielsweise eine Liste zugelassener Ressourcen verwendet und die Ausführung jeder Ressource blockiert, die nicht auf der Liste steht.
Ein Manko der CSP-Technologie ist jedoch, dass sie nicht dynamisch ist. Wenn eine Ressource auf der Zulassungsliste kompromittiert und daher zur Bedrohung wird, weiß die CSP nicht, wie sie sie blockieren kann. Glücklicherweise bauen einige Client-seitige Sicherheitsangebote auf den Vorteilen von CSP auf. Manche Tools sind in der Lage, neue JavaScript-Abhängigkeiten aufzuspüren und Website-Betreiber zu alarmieren, damit sie untersucht werden. Ebenso können einige Angebote bekanntermaßen bösartige URLs erkennen, die JavaScript auf einer Website bereitstellen, oder die Besitzer der Website warnen, um die erkannten Skriptänderungen überprüfen zu lassen.

Man-in-the-Middle-Angriffe

Der Verschlüsselung kommt bei der Abwehr von Man-in-the-Middle-Angriffen, bei denen sich ein Angreifer in die Kommunikation zweier Ressourcen einschaltet, eine entscheidende Rolle zu. Die Verschlüsselung per Secure Sockets Layer (SSL) / Transport Layer Security (TLS) ist eine der besten Methoden zum Schutz des HTTP-Traffics. TLS verschlüsselt Daten, authentifiziert die Parteien, die sie austauschen, und bestätigt, dass die Daten nicht manipuliert wurden. Dieses Verfahren schützt den Datenaustausch zwischen Webdiensten und Endbenutzern. Einige Angreifer können SSL/TLS jedoch umgehen, und hier kommt die HTTP Strict Transport Security – HSTS ins Spiel. Dabei werden alle ungesicherten Verbindungen von Angreifern blockiert und auf diese Weise die Endnutzer vor Man-in-the-Middle-Angriffen geschützt.

Anwendungen mit Cloudflare gegen externe Bedrohungen absichern

Mit Cloudflare lassen sich Anwendungen vor externen Bedrohungen schützen. Das Edge-Netzwerk von Cloudflare erstreckt sich über mehr als 200 Städte in über 100 Ländern und schützt Millionen von Websites unter anderem vor DDoS-Angriffen, Anwendungsschwachstellen, bösartigen Bots und API-Missbrauch. Jeder Cloudflare-Sicherheitsservice läuft auf jedem Server in unserem Netzwerk und profitiert von der gleichen Quelle globaler Bedrohungsdaten.



Cloudflare bietet zur Anwendungssicherheit unter anderem folgende Lösungen:

- **Schwachstellen von Anwendungen**
  - **WAF:** Die Cloudflare-WAF bietet mehrschichtige Regeln – einen verwalteten Regelsatz, der regelmäßig als Reaktion auf die neuesten Angriffe aktualisiert wird, einen Kernregelsatz, der auf den OWASP Top 10 basiert, und benutzerdefinierte Regeln, die von Kunden in Sekundenschnelle konfiguriert und eingesetzt werden können. Da die Cloudflare-WAF mit der gleichen Rust-basierten Regel-Engine wie das Bot-Management von Cloudflare und API Shield arbeitet, gewährleistet sie so einen einheitlichen Schutz.
- **API-Risiken**
  - **API Shield:** API Shield von Cloudflare schützt APIs mit Client-Zertifikat und Schema-basierter Validierung. API Shield verwendet mTLS zur Verifizierung von Geräten bzw. Clients, die versuchen, auf eine API zuzugreifen, scannt den ausgehenden Traffic für DLP und mehr.
    - **DLP:** Cloudflare bietet auch eine DLP-Funktion für APIs, um Antworten zu blockieren, die sensible Daten wie API-Schlüssel oder Kreditkarteninformationen enthalten. Geschützt werden neben APIs aber zum Beispiel auch Anwendungen und Geräte.
- **Schwachstellen von Drittanbietern – Angriffe auf die Browser-Supply-Chain**
  - **Page Shield:** Script Monitor, ein Teil von Cloudflare Page Shield, zeichnet die JavaScript-Abhängigkeiten einer Website im Zeitverlauf auf und unterrichtet Unternehmen von Änderungen oder neuen Abhängigkeiten, damit diese sofort untersucht werden können.
- **Bot-Angriffe**
  - **Bot Management:** Das Bot-Management von Cloudflare nutzt maschinelles Lernen, Verhaltensanalysen und globale Daten, um schädliche Bots zu blockieren. Verwenden Sie Bot Analytics, um Traffic-Muster zu verstehen und die Zugriffsrechte mit benutzerdefinierten Regeln und Genehmigungslisten im Detail festzulegen.
- **DDoS-Angriffe**
  - **DDoS:** Mit einem 90-TBit/s-starken Netzwerk, das durchschnittlich 87 Milliarden Bedrohungen pro Tag blockiert, schützt die DDoS-Abwehr von Cloudflare vom Netzwerkrand aus vor den größten Angriffen.
- **Verschlüsselung**
  - **Cloudflare Free SSL/TLS:** Mit Cloudflare Free SSL/TLS können Sie den Web-Traffic verschlüsseln, um Ihre Anwendung zu schützen. Cloudflare SSL unterstützt auch das HSTS-Protokoll für zusätzlichen Schutz.

Mehr erfahren Sie unter https://www.cloudflare.com/de-de/security.