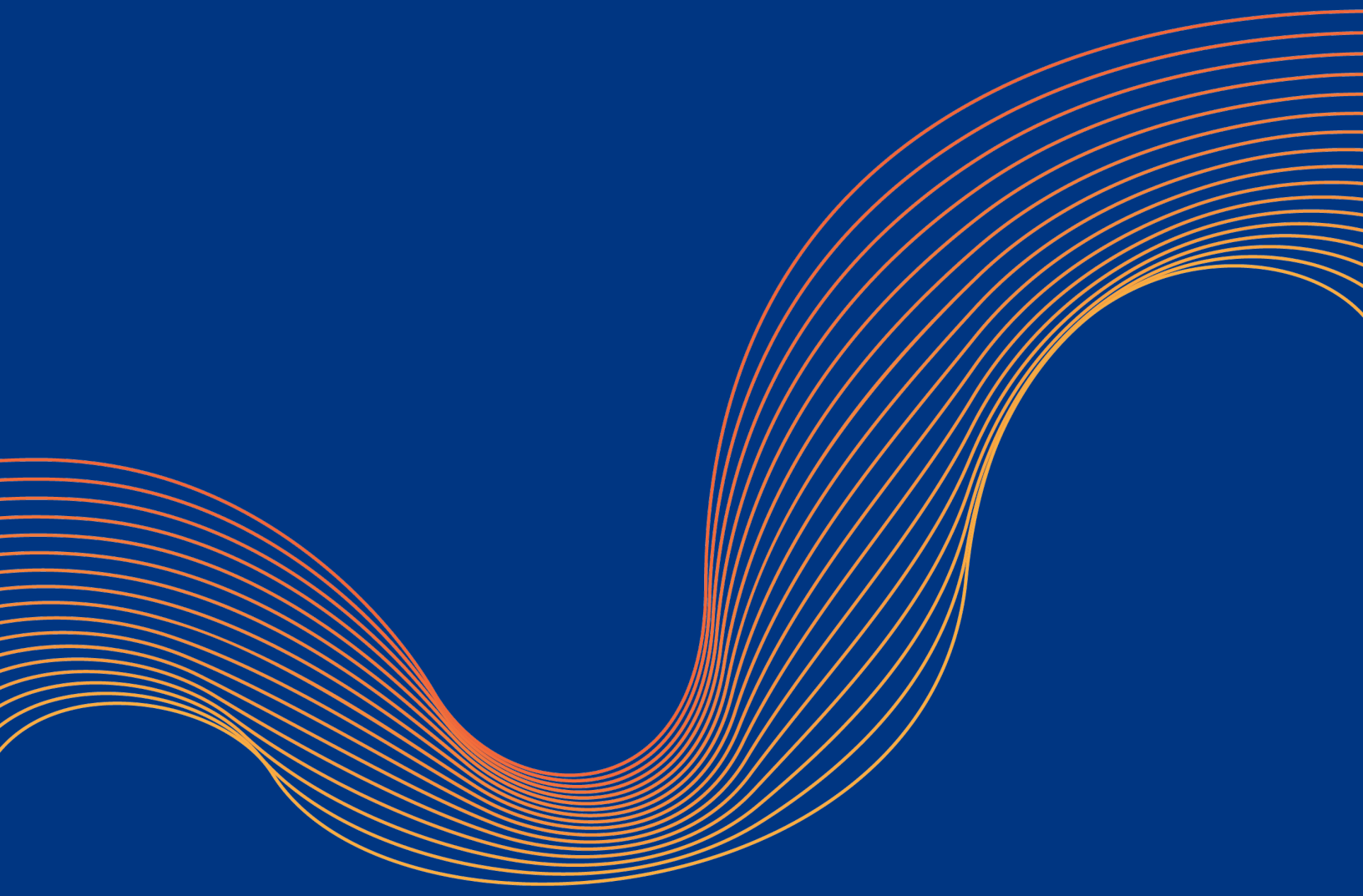
WHITEPAPER

CLOUDFLARE

Mehr Performance und Sicherheit für Ihre Internetpräsenz in China

Strategien zur Erschließung eines enormen und rapide wachsenden Online-Markts mit komplexen Rahmenbedingungen



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

Kurzfassung

In keinem anderen Land sind so viele Menschen online wie in China. Doch eine komplexe Netzwerklandschaft und die permanente Gefahr, ins Fadenkreuz von Cyberangriffen zu geraten, erschweren die Erschließung dieses Marktes. Um Kunden bei der Überwindung dieser Hürden zu unterstützen und die Online-Erfahrung chinesischer Nutzer zu optimieren, hat Cloudflare dafür gesorgt, dass die globalen Performance- und Sicherheitsservices des Unternehmens auch in China in gewohnter Weise verfügbar sind.

Die Herausforderungen bei der Erschließung des chinesischen Online-Marktes

Mit seinen Wachstumsraten und seiner schieren Größe stellt das chinesische Online-Geschäft einen attraktiven Markt für Unternehmen aus den verschiedensten Branchen dar. In der Volksrepublik sind mehr als 900 Millionen Menschen mit dem Internet verbunden – so viele wie in keinem anderen Land der Welt. Über 749 Millionen chinesische Bürger haben im ersten Halbjahr 2020 auch online eingekauft. Im Vergleich zu den Vorjahren war der dabei generierte Umsatz in diesem Zeitraum leicht rückläufig, was größtenteils einer von der Covid-19-Pandemie verursachten Phase allgemeiner wirtschaftlicher Instabilität geschuldet war. Dennoch verzeichnen nun viele Sektoren eine erste Erholung.

Global aufgestellte Unternehmen müssen stets darauf achten, dass sie ihre Dienstleistungen und die gebotene Online-Erfahrung an die vor Ort herrschenden Erwartungen anpassen – das gilt natürlich auch für den chinesischen Markt. Allerdings sehen sie sich dort angesichts Internetregulierung, der infrastrukturellen Voraussetzungen und der Bedrohungslage verschiedenen besonderen Herausforderungen gegenüber. Deshalb fällt es ihnen nicht immer leicht, auch in China Online-Erlebnisse zu bieten, die den lokalen Ansprüchen genügen. Unter anderem treten folgende Schwierigkeiten auf:

- Durch eine fragmentierte Netzwerklandschaft und eingeschränktes lokales Peering verursachte Latenz
- Reduzierte Performance beim mobilen Zugriff auf Websites
- Permanente Bedrohung durch lokale Cyberangriffe

Dieses Whitepaper geht im Detail auf diese Herausforderungen ein, beschreibt Strategien zu ihrer Überwindung und zeigt, welche Unterstützung Cloudflare dafür anbietet.

Latenz aufgrund von Datenengpässen und eingeschränktem lokalem Peering

Wie überall auf der Welt haben auch in China die Verbraucher hohe Ansprüche, wenn es um ihre Online-Erfahrung geht. Laut einem kürzlich veröffentlichten Bericht von PwC ist die Entwicklung hin zu E-Commerce nirgendwo sonst so weit fortgeschritten wie in der Volksrepublik. Im Vergleich zum globalen Durchschnitt hat man dort eine deutlich höhere Bereitschaft der Verbraucher festgestellt, beim Bezahlen, bei der Produktrecherche und bei anderen Schritten des Kaufprozesses das Internet zu nutzen und auf den persönlichen Kontakt zu verzichten.

Doch leider tun sich Unternehmen häufig schwer damit, ihren chinesischen Kunden eine angemessene Performance und Zuverlässigkeit ihrer Websites zu bieten.

Ein Grund dafür sind Netzwerkengpässe: Der gesamte Austausch von Internetdaten mit dem Ausland läuft über nicht mehr als drei Internet Exchange Points (IXPs) in Peking, Shanghai und Guangzhou. Wenn hoher Datenverkehr auftritt, kann es zu einer Überlastung dieser IXPs kommen, was die Ladezeiten von außerhalb Chinas gehosteten Websites erheblich verlängert. Im Rahmen einer Testreihe brauchte die TED-Website in Shanghai während einer solchen Phase acht bis 38 Sekunden, um sich vollständig aufzubauen. In New York mussten die Besucher in einem vergleichbaren Zeitraum hingegen nur fünf bis acht Sekunden warten.

Zur Vermeidung dieser Engpässe haben sich einige globale Unternehmen entschieden, ihre Websites in Rechenzentren in möglichst geringer Entfernung zu einem der drei chinesischen IXPs – zum Beispiel in Hongkong und damit nahe Guangzhou – oder sogar innerhalb der chinesischen Landesgrenzen zu hosten. Die Netzwerklandschaft birgt allerdings noch eine andere große Herausforderung, die mit diesem Ansatz noch nicht aus der Welt geschafft ist: Es gibt nur wenige lokale Internet Service Provider (ISPs), die zudem nur eingeschränkt miteinander verbunden sind.

Wer schon einmal mit der chinesischen Internetlandschaft zu tun hatte, weiß vielleicht schon, dass drei staatliche ISPs den Markt beherrschen und geografisch unter sich aufgeteilt haben: China Telecom, China Mobile und China Unicom. Die „Peering" genannte Praxis, über IXPs Verbindungen zwischen separaten Netzwerken herzustellen, wird von diesen drei ISPs nur mit Einschränkungen angewandt. Eine Studie von MIytics aus dem Jahr 2017 ergab, dass damals das jeweilige Netzwerk mit den meisten Peerings in China nur mit zwei, in Nordamerika aber mit 66 und in Europa gar mit 71 IXPs verbunden war.

In der Praxis bedeutet das, dass in China selbst inländischer Internetverkehr im Netzwerk oft eine große Distanz zurücklegen muss, um relativ kurze geografische Entfernungen zu überwinden. Das führt zu zusätzlicher Latenz beim Endbenutzer.

Ansätze zur Überwindung von Datenengpässen und der Einschränkungen des lokalen Peerings

Angesichts dieser Probleme bei der Web-Performance entscheiden sich viele globale Player, die in China geschäftlich aktiv sind, für den Einsatz eines Content Delivery Network (CDN), mit dem sie statische (oder nicht benutzerspezifische) Inhalte ihrer Websites in Rechenzentren in der Nähe der Endbenutzer zwischenspeichern können. Damit ist bei einem Großteil der Anfragen kein Datenaustausch mit den weit entfernten Ursprungsservern mehr nötig. Bei der Wahl eines CDN sollten Unternehmen darauf achten, dass folgende Kriterien erfüllt sind:

- **Ein großes und gut verbundenes Netzwerk:** Je mehr Rechenzentren ein CDN hat, desto näher ist es am Endnutzer, und je besser es mit den drei großen ISPs in China verbunden ist, desto weniger Netzwerk-Hops müssen die Anfragen der Nutzer durchlaufen.
- **Auflösung von DNS-Abfragen innerhalb Chinas:** Auch wenn andere Inhalte einer Website lokal zwischengespeichert werden, kann Latenz immer noch durch den DNS-Auflösungsprozess entstehen, wenn für die Umwandlung der Domain-Namen in IP-Adressen Datenverkehr mit dem Ausland hergestellt werden muss.
- **Möglichkeit der Minimierung von HTML-, CSS- und Javascript-Codes:** Quelltext in diesen Sprachen bestimmt den Aufbau der meisten Websites und gibt den Browsern der Endbenutzer vor, wie die angezeigte Seite aussehen soll. Beim Minifizieren werden überflüssige Zeichen aus dem Code entfernt – der Quelltext verkürzt sich und nimmt somit bei der Übertragung über das Netzwerk auch weniger Bandbreite in Anspruch. Das führt dazu, dass die entsprechende Seite schneller lädt.
- **Einsatzmöglichkeit für serverlosen Code am Netzwerkrand zur Erstellung benutzerdefinierter Regeln für die Beantwortung von Anfragen:** Serverloser Code ist Quelltext, der nicht an einen bestimmten, vom Entwickler kontrollierten Server gebunden ist. Wenn er am Netzwerkrand ausgeführt wird, existiert serverloser Code in einem ganzen Netzwerk von Rechenzentren. Das bedeutet, dass man mit diesem Quelltext einfach und schnell spezielle Regeln auf bestimmten Endbenutzer-Traffic anwenden kann. Beispielsweise könnte ein Unternehmen in einem chinesischen Netzwerk serverlosen Code einsetzen, um Sonderregeln für mobile Benutzer, langsamere Internetverbindungen und viele andere Anwendungsfälle durchzusetzen.

Mit JD Cloud, dem neuen Netzwerkpartner von Cloudflare, und unseren globalen Performance-Services unterstützen wir unsere Kunden bei der Überwindung von Datenengpässen und der Folgen des eingeschränkten Peerings in China. Im nächsten Abschnitt dieses Whitepapers erfahren Sie, wie uns das gelingt.

Permanente Bedrohung durch lokale Cyberangriffe

Wie überall auf der Welt sind Websites auch in China einer Vielzahl von Sicherheitsbedrohungen ausgesetzt.

Unter anderem kommt es zu DDoS-Angriffen (Distributed Denial-of-Service), bei denen Server oder Netzwerkinfrastrukturen mit so viel Datenmüll bombardiert werden, dass sie nicht mehr in der Lage sind, auf legitime Anfragen zu reagieren. Schon 2017 ging aus einem Bericht von Talos Intelligence hervor, dass die Zahl der in China verfügbaren DDoS-for-Hire-Dienste, mit denen sich auch Laien ohne Weiteres die infizierten Geräte von Botnetzen für Angriffe zunutze machen können, rapide zugenommen hat.

Seitdem ist es den Strafverfolgungsbehörden des Landes gelungen, mehrere große DDoS-Botnetze stillzulegen, unter anderem eines, das bis zu seiner Zerschlagung im Jahr 2019 über 200.000 Geräte infiziert und seine Ziele mit bis zu 200 Gbit/s an Anfragen traktiert hatte. Andere Botnetze sind aber nach wie vor aktiv – zum Beispiel DoubleGuns, dessen Betreiber zum Zeitpunkt der Veröffentlichung dieses Artikels noch nicht gefasst werden konnten.

Betreiber von Websites in China müssen sich auch verschiedener Zugriffsversuche auf vertrauliche Daten- und Entwicklungsumgebungen erwehren. 2018 bedienten sich Angreifer in dem Bestreben, auf die Server von über 45.000 chinesischen Websites zuzugreifen, einer Schwachstelle in einem beliebten PHP-Framework. Zwischen der Veröffentlichung der Schwachstelle und dem Beginn der Attacken auf das Framework waren dabei weniger als 24 Stunden vergangen. Und 2020 wurden zwei Hacker in China beschuldigt, sich zehn Jahre lang illegalen Zugriff auf Hunderte von privaten Firmennetzwerken verschafft zu haben. Auch sie nutzten verschiedene Schwachstellen von Webanwendungen aus.

Erschwerend kommt hinzu, dass Unternehmen, die ihre vertraulichen Daten in China schützen wollen, möglicherweise nicht auf ihr gewohntes Verteidigungsarsenal zurückgreifen können: Chinesische Netzwerke unterstützen keine modernen Verschlüsselungsstandards wie TLS 1.3 oder Encrypted Server Name Identification (ESNI), sodass Unbefugte mehr Möglichkeiten haben, den Datenverkehr auszuspionieren.

Maßnahmen zum Schutz vor der permanenten Bedrohung durch Cyberangriffe in China

Angesichts der zunehmenden DDoS-Angriffe in aller Welt führt auch in China an entsprechenden Abwehrdiensten und anderen Anwendungssicherheitstools wie Web Application Firewalls (WAFs) kein Weg mehr vorbei, wenn man eine aktive Website sicher betreiben will. Bei der Suche nach einem geeigneten Schutz auf diesem Markt sollten Unternehmen darauf achten, dass die folgenden Kriterien erfüllt sind:

- **DDoS-Abwehr am Netzwerkrand und nicht mithilfe einiger weniger „Scrubbing Center“:** Fast jeder moderne DDoS-Abwehrdienst wird zwar mittlerweile in der Cloud betrieben, aber viele stützen sich auf eine begrenzte Anzahl von Rechenzentren, um bösartigen Datenverkehr zu filtern („Scrubbing“). Das Backhauling zur Prüfung des Traffics in diesen „Scrubbing Centern“ macht möglicherweise zusätzliche Netzwerk-Hops erforderlich, erhöht somit die Latenz und führt bei den Benutzern zu Störungen – insbesondere in China angesichts der dort herrschenden Netzwerkbeschränkungen. Für eine DDoS-Abwehr ohne Beeinträchtigung der Internet-Performance in China sollten Unternehmen Cloud-Services den Vorzug geben, die in der Lage sind, den entsprechenden Schutz in jedem Rechenzentrum am Netzwerkrand anzubieten und auf diese Weise unnötige Netzwerk-Hops zu vermeiden.

- **WAFs, die sich automatisch – und schnell – aktualisieren:** Chinesische Hacker haben bewiesen, dass sie keine Zeit verlieren, wenn es darum geht, neue Schwachstellen in Webanwendungen auszunutzen. Viele Unternehmen möchten unter Umständen selbst WAF-Regeln erstellen können. Allerdings sollten sie sich nicht nur auf ihre eigenen Bedrohungsdaten und internen Updates verlassen, sondern darauf achten, dass sich ihre Web Application Firewall automatisch und auf der Grundlage einer breit angelegten Beobachtung der Bedrohungslage aktualisiert. Und wenn das Unternehmen den Regelsatz ergänzend selbst aktualisieren möchte, sollte es sich darauf verlassen können, dass seine Änderungen schnell übertragen werden.
- **Anpassbare Verschlüsselungsoptionen:** Um Daten auch ohne TLS 1.3 und ESNI sicher übertragen zu können, sollten Unternehmen nur Sicherheitsservices in Betracht ziehen, die eine große Auswahl an konfigurierbaren Verschlüsselungsmethoden zu bieten haben.

Die Sicherheitsservices von Cloudflare sind integraler Bestandteil unseres China-Netzwerks und bieten DDoS-Abwehr ohne Latenz sowie eine WAF, die anhand von Bedrohungsinformationen aus aller Welt schnell aktualisiert wird. Im nächsten Abschnitt dieses Whitepapers erfahren Sie mehr.

Wie Cloudflare den Betrieb globaler Websites in China unterstützt

Cloudflare betreibt ein weltumspannendes Netzwerk mit Rechenzentren in 200 Städten und 100 Ländern. Jedes dieser Zentren bietet eine breite Palette von Diensten zur Verbesserung von Sicherheit, Performance und Zuverlässigkeit – von der Content-Bereitstellung und DNS-Auflösung über DDoS-Abwehr und WAF-Durchsetzung bis hin zur Ausführung von serverlosem Code. Dadurch, dass jeder dieser Dienste in jedem einzelnen Rechenzentrum zur Verfügung steht, kann es den Endnutzer aus nächster Nähe bedienen. Dies wirkt sich positiv auf die Latenz aus und sorgt gleichzeitig dafür, dass wir mit unserem Netzwerk einen detaillierten und aktuellen Überblick über die Bedrohungslage und Netzwerkbedingungen haben. Außerdem haben unsere Firmenkunden die Möglichkeit, alle diese Services über ein zentrales Dashboard zu verwalten.

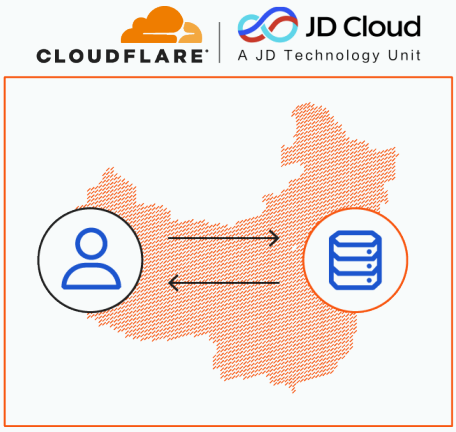
Cloudflare unterstützt Unternehmen seit 2015 dabei, den chinesischen Besuchern ihrer Internetpräsenzen eine sichere, schnelle und zuverlässige Nutzererfahrung zu bieten. Um diese Services weiter zu verbessern, arbeiten wir seit Kurzem mit JD Cloud zusammen, dem Geschäftsbereich für Clouds und intelligente Technologie des chinesischen Internetriesen JD.com. Im Rahmen dieser Partnerschaft können wir in Festlandchina ein eigenes Netzwerk anbieten, das Ende 2023 aus 150 Rechenzentren bestehen wird.

Im Folgenden erfahren Sie, wie wir Unternehmen mithilfe dieses Netzwerks bei der Bewältigung der oben beschriebenen Herausforderungen unterstützen werden.

Wie Cloudflare zu einer Verringerung der Latenz beiträgt

In Verbindung mit dem chinesischen Netzwerk von JD Cloud bieten wir Folgendes an:

- **Zwischenspeicherung und Bereitstellung statischer Inhalte mithilfe einer Reihe von Rechenzentren innerhalb Chinas:** Dadurch sinken die Latenz und die Ladezeiten der Internetseiten, unabhängig davon, wo sich die Endbenutzer befinden. Dank der engen Verbindungen unseres Netzwerks zu allen chinesischen ISPs verringert sich die Anzahl der Netzwerk-Hops, die der Datenverkehr nehmen muss.



Austausch zwischengespeicherter Inhalte zwischen chinesischen Besuchern und einem Rechenzentrum vor Ort

- **Optionale DNS-Auflösung innerhalb Chinas:** Auch dies verkürzt die Reaktionszeiten.
- Einsatzmöglichkeit für **Internet Protocol Version 6 (IPv6):** Höhere Effizienz beim Routing und bei der Paketverarbeitung.
- Optionale **Minimierung von Website-Quelltext:** Dies erledigt unsere Auto Minify-Funktion, die ganz einfach über ein Markierungsfeld im Cloudflare-Dashboard aktiviert werden kann.
- **Serverless-Computing:** Mithilfe von Cloudflare Workers, einem in jedem Rechenzentrum unseres China-Netzwerks betriebenen Dienst, können Sie auf bestimmte Anfragen individuell reagieren und vorhandene Anwendungen erweitern oder sogar Applikationen komplett neu erstellen, ohne dafür Infrastruktur konfigurieren oder warten zu müssen.

Wie Cloudflare die Abwehr der permanenten Bedrohung durch lokale Cyberangriffe unterstützt

Dank der Sicherheitsservices unseres China-Netzwerks stehen folgende Abwehrmöglichkeiten zur Verfügung:

- **Verteidigung gegen DDoS-Angriffe:** Weil jedes unserer Rechenzentren in China für sich genommen in der Lage ist, Angriffe abzuwehren, verfügen wir in unserem Netzwerk über immense Kapazitäten, um selbst die größten Attacken zu parieren, ohne legitime Anfragen zu verlieren – und ohne auf Cloudflare-Rechenzentren außerhalb Chinas angewiesen zu sein. Da die Prüfung des Datenverkehrs nahe am Endbenutzer stattfinden kann, entfällt für dessen Anfragen der langwierige Prozess einer Umleitung zu einem unter Umständen weit entfernten „Scrubbing Center". Angesichts der Herausforderungen der chinesischen Netzwerklandschaft bietet Cloudflare zudem einzigartige Mechanismen zur Optimierung des Datenverkehrs (Traffic Engineering), die ein automatisches Rerouting von Angriffs-Traffic ermöglichen. Alle diese Funktionen tragen dazu bei, Performance-Einbußen für legitimen Datenverkehr innerhalb und außerhalb Chinas zu verhindern.
- **Schutz vor Schwachstellen in Webanwendungen:** Die Cloudflare WAF schützt nicht nur vor den laut OWASP zehn wichtigsten Bedrohungen (OWASP Top 10), sondern wird zudem kontinuierlich mit Bedrohungsinformationen aus unserem gesamten Netzwerk versorgt, um auch brandneue Gefahren automatisch abwehren zu können. Darüber hinaus können Unternehmen ganz einfach eigene Regeln erstellen und sie im gesamten Netzwerk innerhalb weniger Minuten durchsetzen.
- **Verschlüsselung von Daten mit TLS 1.2:** Dabei können Unternehmen ihre eigenen Zertifizierungen unkompliziert über das Cloudflare-Dashboard verwalten.

MEHR DAZU

Angesichts des anhaltenden Wachstums der chinesischen Internetwirtschaft ist es nur eine Frage der Zeit, bis neue Schwierigkeiten in Sachen Sicherheit und Leistung auftreten. Doch Cloudflare hat die Weichen für dieses kontinuierliche Wachstum in China richtig gestellt und versetzt die Unternehmen in unserem Netzwerk damit in die Lage, schnell auf diese neuen Herausforderungen zu reagieren und die Messlatte für reibungslose Benutzererfahrungen höher zu legen.

Besuchen Sie cloudflare.com/network/china/ oder wenden Sie sich direkt an Ihren Ansprechpartner bei Cloudflare, um mehr über unser China-Netzwerk zu erfahren.