CLOUDFLARE®

Überlebenshandbuch für SaaS-Anbieter

Performance-, Sicherheits- und Verschlüsselungsgrundlagen für Online-Anwendungen

1 888 99 FLARE | enterprise@cloudflare.com | www.cloudflare.com/de/

Kurzfassung

Zwischen 2016 und 2020 wird der SaaS-Markt Schätzungen zufolge um 196 % wachsen.[1] Bei der Zunahme des SaaS-Marktes wird er immer mehr zu einem integralen Bestandteil von Geschäftsinfrastrukturen. Sicherheit und Performance stehen dabei sowohl für SaaS-Anbieter als auch für deren Kunden weiterhin an erster Stelle. Mit diesem Wachstum steigt die Konkurrenz für SaaS-Anbieter beim Bereitstellen der sichersten und leistungsfähigsten Anwendungen für Kunden. Weniger leistungsstarken und angriffssicheren Anwendungen stehen unvermeidlich negative Auswirkungen auf den Umsatz, die Endbenutzerbindung, den Ruf der Marke und die Kundentreue bevor. Für eine wichtige Untergruppe unter den SaaS-Anbietern bedeutet die Anforderung, markenbezogene Vanitydomains von Kunden verschlüsseln zu müssen, dass der SSL-Lebenszyklus manuell verwaltet werden muss. Das führt zu langen Bereitstellungszeiten und hohen finanziellen Aufwendungen. Die Alternative, eine komplexe automatisierte interne Lösung zu entwickeln, nimmt technische Ressourcen in Anspruch, die dann nicht mehr für die Kernkompetenzen zur Verfügung stehen.

Durch die Performance- und Sicherheitslösungen für SaaS-Anbieter von Cloudflare wird das Kundenerlebnis für SaaS-Anbieter, Endkunden und Endbesucher gesichert und beschleunigt. Durch das Cloudflare Content Delivery Network (CDN) mit 10 Tbit/s in Kombination mit Argo Smart Routing, Lastenausgleich und Performanceoptimierungen wird die Besucherlatenz bis um das Zweifache reduziert. Der erweiterte DDoS-Schutz von Cloudflare schwächt in Verbindung mit der Ratenbegrenzung und einer Web Application Firewall (WAF) sowohl große volumetrische als auch komplexe Angriffe auf die Netzwerk-, Übertragungs- und Anwendungsebene ab. Außerdem haben die SaaS-Anbieter die Möglichkeit, die Übertragung von Kundendaten durch eine leicht einzurichtende und vollständig verwaltete SSL-Lösung für individuelle Vanitydomains abzusichern.

Auswirkungen von Latenz und unzureichender Sicherheit auf das Unternehmen

SaaS-Anwendungslatenz und unzureichende Sicherheit jeglicher Art können zu negativen Kundenerlebnissen sowie schlechten Konvertierungsraten und Suchmaschinenergebnissen führen, die ihrerseits Umsatzeinbußen und die Abwanderung von Kunden nach sich ziehen können.

Auswirkungen von Performance und Verfügbarkeit auf die SaaS-Anwendungsnutzung

Die Kunden verlangen nach schnellen und hochgradig verfügbaren Angeboten, wenn sie Websites, Anwendungen und APIs nutzen. Wenn es bei Online-Assets zu Latenz kommt oder sie nicht verfügbar sind, hat dies deutliche negative Auswirkungen auf die SaaS-Anwendungsnutzung und die Konvertierungsraten.

So berichtet beispielsweise Google, dass eine um gerade einmal 100 bis 400 Millisekunden längere Latenz der Website messbare Auswirkungen auf das Verbraucherverhalten hat[1]. Walmart bemerkte einen plötzlichen Rückgang der Konvertierungsrate, nachdem sich die Ladezeit seiner Website um wenige Sekunden verlängerte[2], und auch Amazon hat festgestellt, dass jede Verkürzung der Latenz um 100 Millisekunden jeweils eine Umsatzsteigerung von 1 % bewirkte.[3]

Meist hängen Schwierigkeiten bei der SaaS-Anwendungsperformance mit internen Faktoren zusammen, die sich nachteilig auf die Shared-Hosting-Infrastruktur oder das Anwendungs-Setup eines SaaS-Anbieters auswirken. Einer dieser Faktoren ist die geografische Distanz zwischen den Besuchern und den ursprünglichen Serverstandorten der SaaS-Anwendung. Man geht davon aus, dass pro 100 Meilen Distanz 0,82 Millisekunden Latenz hinzukommen.[4] In Verbindung mit zahlreichen nicht optimierten statischen Inhalten führt diese Distanz dann zu einer weiteren Latenz für die Besucher.

Die Performance hängt jedoch nicht allein von Servern, Netzwerken und Anwendungen ab. Sie kann auch von Datenverkehrsspitzen oder saisonal bedingt höherem Datenverkehr abhängen, der die gemeinsame Infrastruktur überlasten und dazu führen kann, dass Anwendungen Latenz entwickeln oder gar nicht mehr verfügbar sind.

SaaS-Anwendungen, die nur langsam geladen werden oder nicht verfügbar sind, können dramatische Auswirkungen auf Umsätze, Konvertierungsraten, Absprungragen, Suchmaschinenrankings (SEO-Rankings), den Ruf der Marke, die Kundenzufriedenheit und Service Level Agreements (SLA) haben.

[1] http://www.sfgate.com/business/article/Google-s-speed-need-instantaneous-Internet-3251049.php
[2] https://www.slideshare.net/devonauerswald/walmart-pagespeedslide
[3] https://blog.gigaspaces.com/amazon-found-every-100ms-of-latency-cost-them-1-in-sales/
[4] http://www.smartinsights.com/mobile-marketing/mobile-marketing-analytics/mobile-marketing-statistics/

Auswirkungen gezielter Angriffe auf SaaS-Anwendungen

Ganz gleich, ob ein neuer SaaS-Anbieter in den Markt eintritt oder ein etabliertes Softwareunternehmen eine bislang lokale Anwendung in die Cloud migriert, die Auswirkungen im Hinblick auf die Sicherheit müssen in jedem Fall berücksichtigt werden.

Die Angriffsfläche von SaaS-Anwendungen und -Diensten wird größer, wenn sie mit dem öffentlichen Internet in Kontakt kommen. Hinzu kommt, dass die Auslastung oft auf mehrere Infrastrukturen verteilt ist. Beispiele für Angriffsvektoren für SaaS-Anbieter sind Login-Portale, ein gemeinsames DNS bzw. Shared Hosting sowie komplexe Anwendungsschwachstellen. Man muss bedenken, dass viele SaaS-Anbieter mehrere Clientanwendungen in einer gemeinsamen Infrastruktur hosten. Dabei können sich Datenlecks, Beeinträchtigungen der Zuverlässigkeit oder Angriffe auf die gemeinsame Infrastruktur negativ auf andere Kunden auswirken.

Spezifische Angriffe, die auf die oben genannten Vektoren abzielen, sind beispielsweise volumetrische und komplexe DDoS-Angriffe, Brute-Force-Anmeldeversuche, Ausnutzen der Schwachstellen einer Anwendung und Abfangen nicht verschlüsselter Kundendaten. Alle diese Angriffe richten sich über unterschiedliche Geräte gegen Websites, Anwendungen und APIs. Ist so ein Angriff erfolgreich, kann dies zu einer ganzen Reihe von geschäftlichen Auswirkungen führen, von Unterbrechungen der Dienste über die Abwertung der Marke und den Verlust von Kunden bis hin zu hohen Umsatzeinbußen und Kosten für die Schadensbegrenzung.

2013 infiltrierten Hacker Adobe und verschafften sich Zugang zu Kreditkarteninformationen und anderen persönlichen Daten von 2,9 Millionen Kunden.[5] Brad Arkin, der Chief Security Officer von Adobe, nahm die Risiken im Online-Geschäft mit den Worten zur Kenntnis: „Cyberangriffe gehören zu den traurigen Tatsachen der heutigen Geschäftswelt."

Am 16. Oktober 2016 waren Airbnb, Amazon.com, Netflix, The New York Times, Paypal, Pinterest, Reddit, Tumblr, Twitter, Verizon, Visa, The Wall Street Journal, Yelp, Zillow und viele weitere Unternehmen für längere Zeit nicht erreichbar, weil sie Opfer des berüchtigten Botnet Mirai geworden waren. Dabei waren gar nicht die Anwendungen selbst die direkten Angriffsziele, sondern Dyn, der gemeinsame DNS-Anbieter dieser Websites und Anwendungen. Nach 11 Stunden gelang es Dyn, den Schaden zu beheben und dafür zu sorgen, dass die Dienste auf allen betroffenen Websites wieder normal funktionierten.[6]

Die Wahl zwischen Verschlüsselung und individuellen Vanitydomains

Die Verwendung der SSL-/TLS-Verschlüsselung für Online-Organisationen hat sich zu einer Best Practice in Sachen Sicherheit entwickelt und wird immer mehr zur Voraussetzung, weil große Technologieunternehmen sich das Ziel gesetzt haben, das Internet sicherer zu machen, und entsprechend Druck ausüben. So hat beispielsweise der Webbrowser Google Chrome Ende 2016 begonnen, Websites, die HTTPS nicht verwenden, für die Benutzer deutlich erkennbar als „Nicht sicher" zu kennzeichnen.[7] Außerdem schreibt Apple mittlerweile vor, dass alle iOS-Anwendungen HTTPS-Verbindungen verwenden müssen, um in den Appstore des Unternehmens aufgenommen zu werden.[8]

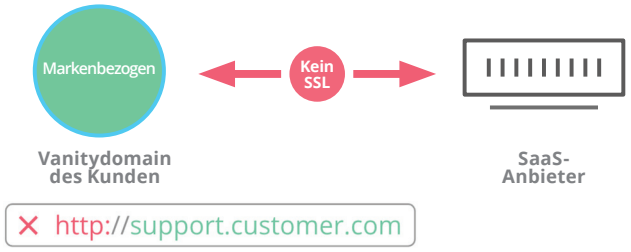
In den Anfangstagen von SSL mussten sich Online-Organisationen entscheiden, ob sie Datenverkehr mit HTTPS verschlüsseln oder die Erwartungen der Besucher an die Performance erfüllen wollten. Noch vor wenigen Jahren verursachte das SSL-Protokoll eine Steigerung der Latenz und beeinträchtigte die Performance von Website und Anwendungen. Selbst wenn eine Organisation sich zulasten der Performance für mehr Sicherheit entschied, verhinderten die betrieblichen Schwierigkeiten, die damals mit SSL einhergingen, die Umsetzung auf breiter Front. Heute ist die Performance dank moderner SSL-Verbesserungen wie der Entwicklung von HTTP/2 (der Nachfolger von HTTP 1.1), bei dem der Datenverkehr über HTTPS mit SSL verschlüsselt wird, höher als beim unverschlüsselten HTTP.

Ebenso wie Organisationen sich früher zwischen Verschlüsselung und Performance entscheiden mussten, muss sich heute eine wichtige Untergruppe unter den SaaS-Anbietern zwischen der Verschlüsselung des Datenverkehrs ihrer Kunden und der Möglichkeit entscheiden, dass diese Kunden ihre eigenen markenbezogenen Vanitydomains mitbringen können. Beides ist unverzichtbar, um von den kombinierten Vorteilen einer angemessenen Markendarstellung, Sicherheit, Suchmaschinenrankings und der bestmöglichen Performance zu profitieren.

[5] http://www.nytimes.com/2013/10/04/technology/adobe-announces-security-breach.html
[6] http://dyn.com/blog/dyn-analysis-summary-of-friday-october-21-attack/
[7] https://techcrunch.com/2016/06/14/apple-will-require-https-connections-for-ios-apps-by-the-end-of-2016/
[8] https://techcrunch.com/2016/06/14/apple-will-require-https-connections-for-ios-apps-by-the-end-of-2016/

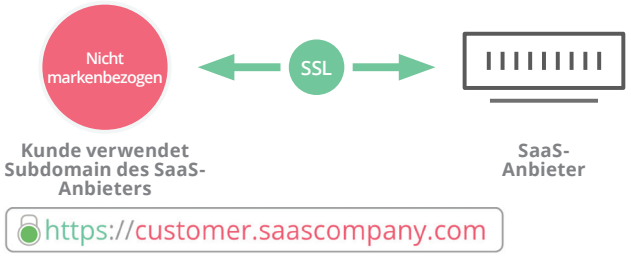
Diese Untergruppe der SaaS-Anbieter bietet ihren Kunden in der Regel die Möglichkeit, öffentliche Online-Assets wie Startseiten, Websites, Supportportale usw. zu erstellen. Gewöhnlich hostet der SaaS-Anbieter diese neu erstellten Kundenassets auf einer Subdomain seiner primären Domain. So kann z. B. die URL eines Assets, den ein Kunde des SaaS-Anbieters erstellt hat, **customercompany.saasprovider.com** anstelle einer markenbezogenen Vanity-URL wie **customercompany.com** oder **support.customercompany.com** lauten. Dies ist eine Herausforderung für die Kunden, weil ohne markenbezogene Vanitydomain der Wiedererkennungswert ihrer Marke, die SEO-Rankings und das Besuchervertrauen beeinträchtigt werden.

SaaS-Anbieter und ihre Kunden haben die Herausforderungen beim Domain Branding überwunden, indem sie die URL der Kundendomain customercompany.com bzw. support.customercompany.com per CNAME mit customercompany.saasprovider.com verknüpfen. Dadurch kann der Kunde seine eigene markenbezogene Vanitydomain verwenden. Der SaaS-Anbieter kann dadurch jedoch SSL nicht mehr so leicht aktivieren und steht vor der Herausforderung, einen kompletten SSL-Lebenszyklusprozess verwalten zu müssen. Die manuelle Verwaltung des SSL-Lebenszyklusprozesses oder der Versuch, eine interne Lösung für Endkunden zu entwickeln, führt dazu, dass hierfür viel Zeit, manueller Aufwand und Geld aufgewendet werden muss.



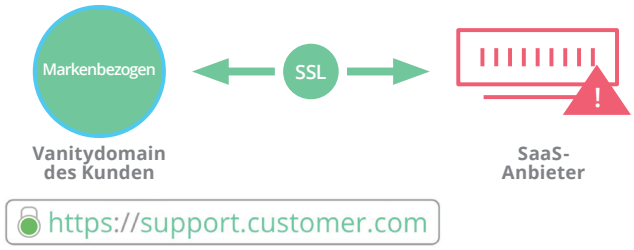
UNVERSCHLÜSSELTE ABER MARKENBEZOGENE VANITYDOMAIN

Bei Vanitydomains von Kunden ohne SSL fehlen die Performancevorteile von SSL und der sicheren Datenübertragung, wodurch sie anfälliger dafür werden, dass Inhalte ausgespäht oder verändert werden, bevor sie die Besucher erreichen.



VERSCHLÜSSELTE ABER NICHT MARKENBEZOGENE DOMAIN

Domains, bei denen ein SaaS-Anbieter SSL aktiviert hat, verfügen nicht über eine individuelle Vanitydomain. Dadurch wird die Marke abgewertet und die SEO-Rankings verschlechtern sich.

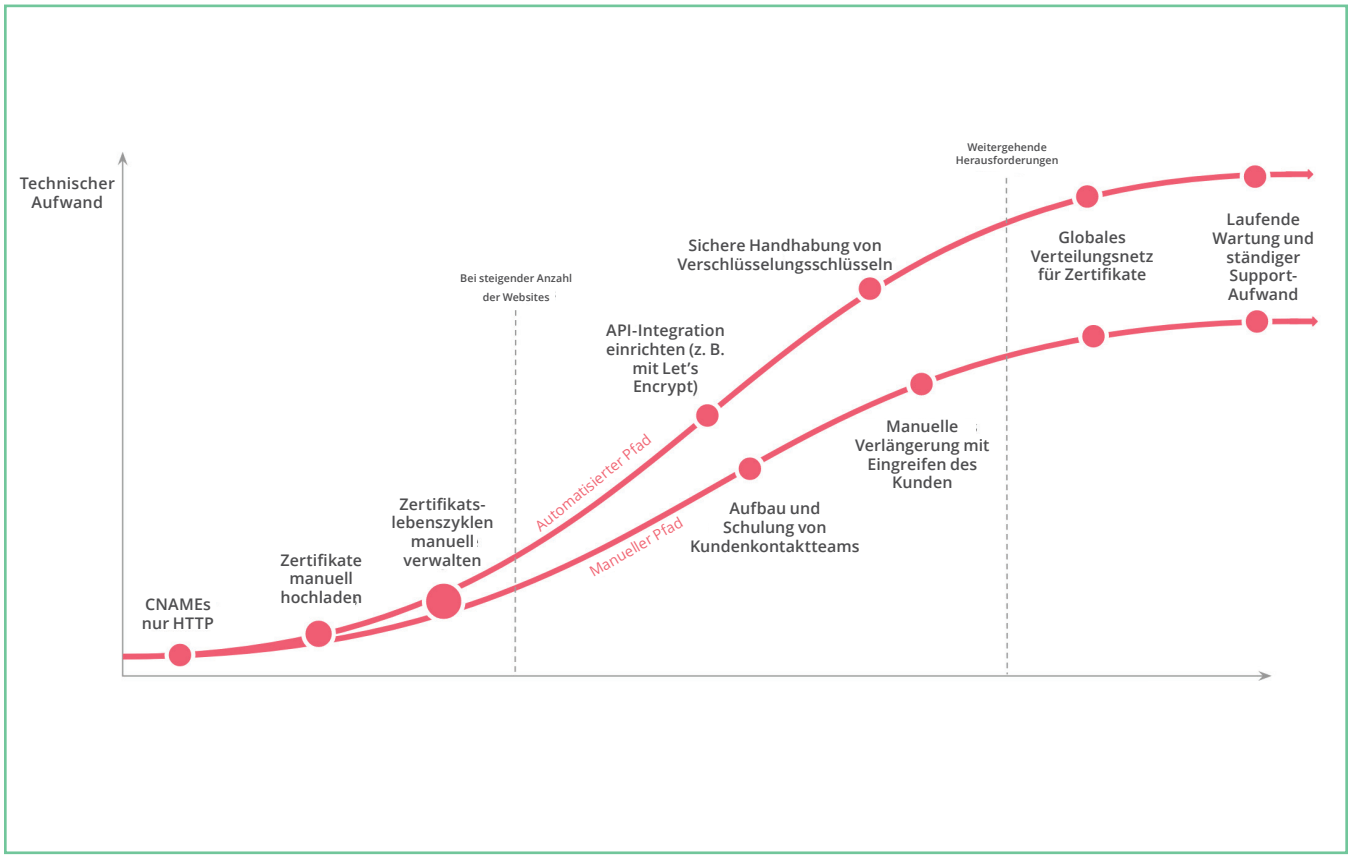


ANSPRUCHSVOLLER INTERNER ANSATZ

SaaS-Anbieter, die verschlüsselte markenbezogene Vanitydomains anbieten möchten, können die SSL-Lebenszyklen entweder manuell verwalten, was zu langen Bereitstellungszeiten und hohem finanziellen Aufwand führt, oder eine komplexe automatisierte interne Lösung entwickeln.

Dabei müssen die technischen Herausforderungen für SaaS-Anbieter bei der Entwicklung einer eigenen Lösung zur Verwaltung der SSL für Kundendomains berücksichtigt werden. Die untenstehende Grafik stellt eine typische Roadmap von SaaS-Anbietern dar, die versucht haben, automatisierte interne SSL-Lösungen zu entwickeln.

Es gibt zwei Pfade, die man bei der Entwicklung einer internen Lösung beschreiten kann. Beide sind jedoch nicht ideal. Beim ersten (oberen) Pfad wird der SSL-Prozess automatisiert. Dies erfordert jedoch einen hohen technischen Aufwand und es sind komplexe Herausforderungen zu bewältigen. Der zweite Pfad erfordert einen adäquaten manuellen Aufwand sowohl seitens des SaaS-Anbieters als auch seitens des Endkunden.



Cloudflare für Sicherheit, Performance und Verfügbarkeit von SaaS-Anwendungen

Cloudflare verbessert das Endbenutzererlebnis für SaaS-Anbieterwebsites, -anwendungen und -APIs durch Reduzierung der Latenz und Optimierung der Performance bei der Inhaltsbereitstellung und weitet diese Vorteile gleichzeitig auf Internetassets von Endkunden aus.

Global verfügbare Präsenz

Im Mittelpunkt der Lösung von Cloudflare steht ein globales Anycast Content Delivery Network (CDN), das aus 117+5 Rechenzentren besteht, die sich auf 57 Länder verteilen und den Besuchern in allen Regionen die SaaS-Anwendungsinhalte näherbringen. Cloudflare betreibt außerdem 38 % der verwalteten DNS Domains und damit eines der größten autoritativen DNS-Netzwerke der Welt. Mit einer Abfragegeschwindigkeit von im Schnitt nur wenigen Millisekunden ist Cloudflare der Anbieter verwalteter DNS mit der schnellsten globalen Performance.

Anwendungsverfügbarkeit im großen Maßstab

Zusätzlich zur hochverfügbaren DNS-Infrastruktur und dem globalen Anycast™-Netzwerk von Cloudflare reduziert der Cloudflare-Lastenausgleich die Latenz, indem er die Datenverkehrsauslastung ausgewogen über mehrere Server verteilt und den Datenverkehr in die nächstgelegene geografische Region lenkt. Der Lastenausgleich beinhaltet Statusprüfungen mit schnellem Failover, um Besucher schnell von Fehlern wegzuleiten. Außerdem kann der Lastenausgleich über mehrere Cloud-Anbieter oder On-Premise-Infrastrukturlösungen hinweg eingesetzt werden, um die Auswirkungen von Unterbrechungen, die von einem einzigen Anbieter oder Server verursacht werden, zu mindern und gleichzeitig ein Anbieter-Lock-in zu vermeiden.

Schnellere Besuchererlebnisse

Bei der Entwicklung des CDN von Cloudflare wurden erweiterte Optimierungen vorgenommen, darunter die automatische Minimierung von HTML, CSS und JavaScript und die Gzip-Komprimierung, mit der 20 % der Größe von Dateien und Ressourcen eingespart werden können. Ein urheberrechtlich geschütztes Image und mobile Optimierungen sorgen für weitere Verbesserungen Ihrer SaaS-Anwendungsperformance.

10 % des weltweiten Datenverkehrs werden von Cloudflare übermittelt. Dabei werden der tatsächliche Status und die Zuverlässigkeit der Netzwerkpfade in Echtzeit überprüft. Der Argo-Smart-Routing-Algorithmus von Cloudflare verwendet die so gesammelten Informationen zum Routing von Datenverkehr über die schnellsten verfügbaren Pfade und gewährleistet so offene, sichere Verbindungen ohne Latenz durch den Verbindungsaufbau. Mit Argo Smart Routing werden die Internetlatenz durchschnittlich um weitere 35 % und Verbindungsfehler um 27 % gesenkt.

„Cloudflare hat die Servicequalität für Crisp maximiert und die Antwortzeit des Dienstes minimiert. Es ist eine Kommodifizierung, mit der teure Netzwerkinfrastruktur für die Massen verfügbar wird. Wir können nicht darauf verzichten."

crisp™ | **Valérian Saliou**
CTO, Crisp

Schutz von SaaS-Anwendungen und Kundendaten

Die cloudbasierte Sicherheitslösung von Cloudflare schützt die Websites, Anwendungen und APIs von SaaS-Anbietern und bietet gleichzeitig zusätzliche Vorteile bis hin zu den Internetassets der Endkunden.

Das aus über 117 Rechenzentren bestehende Anycast-Netzwerk von Cloudflare mit einem Durchsatz von 10 Tbit/s ist zehnmal größer als der größte DDoS-Angriff, der je aufgezeichnet wurde. So bietet es Schutz vor Angriffen auf die Schichten 3, 4 und 7 des OSI-Modells. In Verbindung mit der Ratenbegrenzung und einer Web Application Firewall (WAF) schwächt die Sicherheitslösung von Cloudflare auch komplexe Angriffe auf die Anwendungsebene ab. Und mit Cloudflare SSL für SaaS können SaaS-Anbieter und Endkunden verschlüsselte Kommunikation erwarten, die verhindert, dass Daten abgefangen oder bösartige Inhalte eingeschleust werden, auch wenn sie weiterhin individuelle Vanitydomains verwenden.

Schutz und Sicherheit für sensible Kundendaten

Da SaaS-Anwendungen immer mehr private und kommerziell sensible Daten enthalten, muss der Schutz vor Brute-Force-Anmeldeversuchen, Datenlecks und Man-in-the-middle-Angriffen unbedingt gewährleistet sein.

Zunächst einmal kann der Schutz vor Angriffen dieser Art mit der Web Application Firewall (WAF) von Cloudflare erreicht werden, die komplexe Angriffe auf die Anwendungsebene abschwächt. Die WAF von Cloudflare bietet auch standardmäßigen Schutz vor den zehn wichtigsten vom OWASP identifizierten Schwachstellen sowie vor anwendungsspezifischen Schwachstellen, die sich gegen häufige Integrationen und Sprachen richten, z. B. PHP, Magento, WordPress, Drupal, Atlassian usw. Mit der WAF von Cloudflare können SaaS-Anbieter ohne Vorbereitung benutzerdefinierte Regelsätze zum Schutz vor neu entdeckten Angriffsvektoren und Schwachstellen erstellen und Regeln in weniger als 30 Sekunden im Netzwerk von Cloudflare weitergeben.

Zusammen mit dem DDoS-Schutz von Cloudflare ermöglicht die Ratenbegrenzung eine engmaschige Kontrolle, um Besucher mit verdächtigen Anforderungsraten zu blockieren. Die Ratenbegrenzung ist so angelegt, dass sie Brute-Force-Anmeldeversuche abwehren kann, mit denen man sich zu Bereichen einer Anwendung oder Website Zugang verschaffen möchte, auf die man keinen Zugriff hat. Mit der Ratenbegrenzung wird die Anzahl der Anforderungen, die von einer bestimmten IP-Adresse aus an einen bestimmten Endpunkt gerichtet werden dürfen, für einen festgelegten Zeitraum begrenzt.

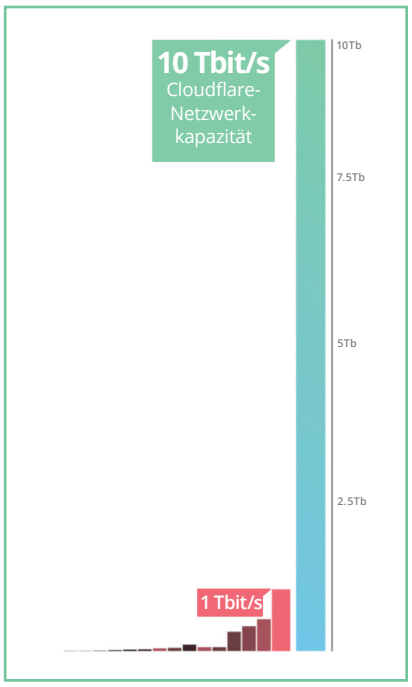
„Die Lösung von Cloudflare funktioniert einfach. Das Cloudflare-Team erfüllte alle unsere Anforderungen und die Anpassungen wurden fast sofort propagiert."

zendesk | **Amanda Kleha GM**
Zendesk Online-Geschäftseinheit

Cloudflare SSL für SaaS ist die effizienteste Möglichkeit, die Verwaltung von SSL-/TLS-Zertifikaten für individuelle Vanitydomains mit CNAME zu automatisieren und den Schutz vor dem Abfangen von Daten durch Man-in-the-Middle-Angriffe oder dem Ausspähen von Datenverkehr wegen ungesicherten Verbindungen sicherzustellen.

Gesicherte Verfügbarkeit durch Blockieren böswilligen Datenverkehrs

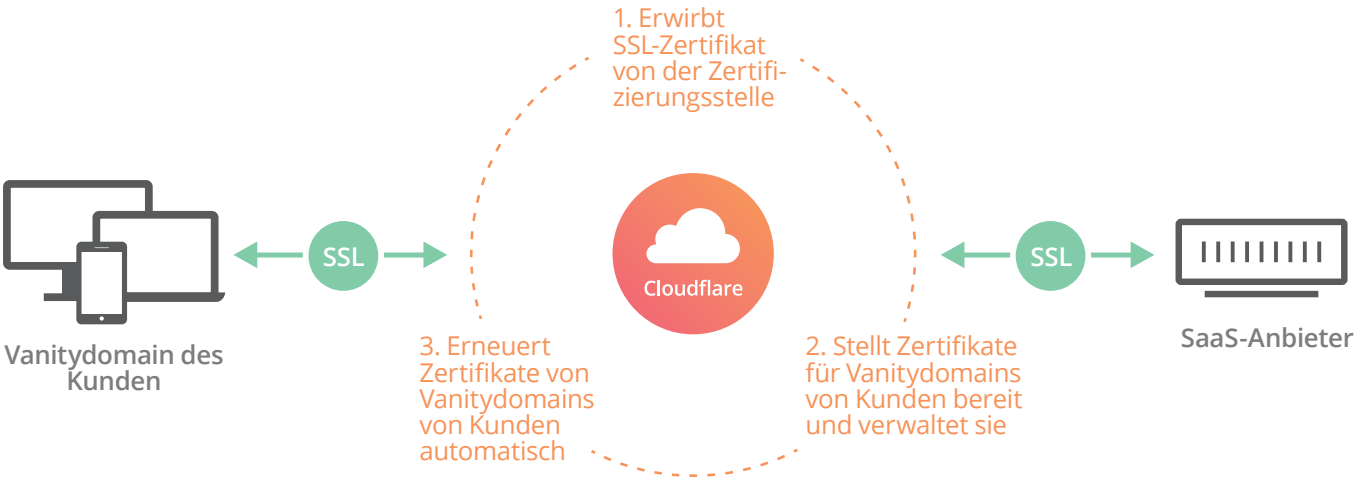
Der Diebstahl oder Verlust sensibler Kundendaten kann katastrophale Auswirkungen haben. Ebenso zerstörerisch kann es jedoch sein, wenn man einem erfolgreichen Angriff zum Opfer fällt, durch den die Verfügbarkeit von Diensten unterbrochen werden soll. Das Rückgrat von Cloudflare ist sein globales Content Delivery Network (CDN) aus über 117 Rechenzentren in 57 Ländern. Der gesamte Netzwerkdurchsatz von Cloudflare beträgt mehr als 10 Tbit/s, das ist etwa das Zehnfache des größten jemals aufgezeichneten DDoS-Angriffs. Jeder versuchte volumetrische DDoS-Angriff auf die Schichten 3, 4 und 7 wird absorbiert und gleichmäßig über das Netzwerk von Cloudflare verteilt. So werden Ausfälle verhindert und die höchste Verfügbarkeit für SaaS-Kunden gewährleistet. Die Ratenbegrenzungslösung von Cloudflare arbeitet mit dem DDoS-Schutz zusammen. So ermöglicht sie eine engmaschige Kontrolle, um Besucher mit verdächtigen Anforderungsraten zu blockieren. Wenn eine bestimmte IP-Adresse bestimmte Schwellenwerte überschreitet, kann sie für einen bestimmten Zeitraum daran gehindert werden, weitere Anforderungen bei einem bestimmten Endpunkt zu stellen.



Eine automatisierte SSL-Lösung für SaaS-Anbieter

SSL für SaaS ermöglicht es SaaS-Anbietern, die Vorteile bei der Sicherheit und Performance des Netzwerks von Cloudflare auf die Endbenutzer auszudehnen, die nun eigene Vanitydomains nutzen können. Die Lösung SSL für SaaS von Cloudflare ermöglicht

es den Kunden, ihre Vanitydomains weiterhin mittels CNAMEs der Subdomain eines SaaS-Anbieters zuzuordnen. So genießen sie die Vorteile einer markenbezogenen URL, während Cloudflare den gesamten SSL-Lebenszyklus für die SaaS-Anbieter und ihre Kunden aktiviert und verwaltet. Durch Aktivieren von SSL für Kundendomains wird das Vertrauen der Besucher gesteigert, die SEO-Suchrankings werden verbessert und das moderne HTTP/2-Protokoll kann genutzt werden. Das führt zu weiteren Geschwindigkeitsverbesserungen.



Markenbezogene Besuchererlebnisse

Kunden von SaaS-Anbietern, die die Möglichkeit haben, ihre eigenen individuellen markenbezogenen Vanitydomains mitzubringen, können dies auch weiterhin tun. Gleichzeitig genießen sie die Vorteile eines vollständig verwalteten SSL-Zertifikats. Individuelle, per CNAME verknüpfte Vanitydomains bieten SaaS-Kunden eine bessere Markendarstellung sowie bessere SEO-Rankings. Gleichzeitig steigern sie das Vertrauen der Besucher der Websites oder Anwendungen.

Sichere, leistungsfähige Kundenassets

Mit SSL für SaaS können spezielle SSL-/TLS-Zertifikate reibungslos zu individuellen Vanitydomains mit CNAME hinzugefügt werden. Die Übertragung von Daten über HTTPS gewährleistet die sichere Übertragung von sensiblen Kundendaten und schützt vor Man-in-the-Middle-Angriffen und Ausspähen des Netzwerks. Wenn SSL aktiviert ist, kann das HTTP/2-Protokoll verwendet werden, das weitere Geschwindigkeitsverbesserungen ermöglicht.

Automatische Verwaltung des Lebenszyklus und schnelle Bereitstellung von SSL

Cloudflare verwaltet den gesamten SSL-Lebenszyklus der mit einem CNAME versehenen Vanitydomains der Kunden eines SaaS-Anbieters, vom Ausstellen/Schutz des Privatschlüssels über die Validierung, Ausstellung und Verlängerung von Domains bis zur Neuausstellung. Die Arbeit mit dem SSL-Lebenszyklus wird dem SaaS-Anbieter und dem Endkunden abgenommen. Während der SSL-Ausstellung überträgt Cloudflare neue Zertifikatsanforderungen und sorgt dafür, dass HTTPS innerhalb von Minuten online ist.

„Als Ingenieur würde ich immer wieder mit Cloudflare arbeiten."

UDACITY

Paul Bauer
Platform Engineer bei Udacity

Kernpunkte

Registrieren Sie sich bei Cloudflare, um die Performance und Sicherheit Ihrer SaaS-Anwendung zu verbessern und gleichzeitig ganz einfach SSL für die mit einem CNAME versehenen Vanitydomains von Endkunden bereitzustellen. Die Registrierung dauert in der Regel weniger als 5 Minuten. Informationen zu den verschiedenen Tarifen von „Kostenlos“ bis „Enterprise“ finden Sie unter www.cloudflare.com/de/plans/. Weitere Informationen über Cloudflare für SaaS-Anbieter finden Sie unter www.cloudflare.com/de/saas/.

1 888 99 FLARE | enterprise@cloudflare.com | www.cloudflare.com/de/