CLOUDFLARE®

Wie man die infrastrukturellen Voraussetzungen für eine überragende Online-Erfahrung schafft

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

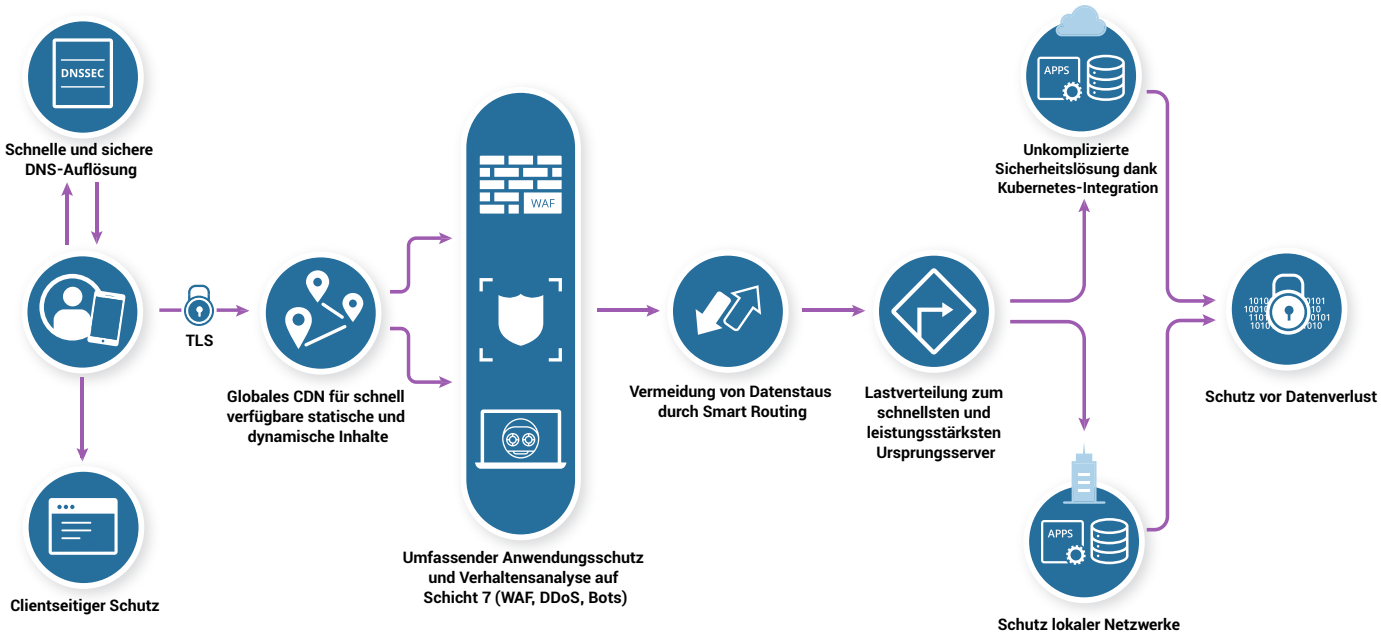
Inhalt

Einführung

Wer Kunden in aller Welt bedient, muss ihnen auch eine überragende Online-Erfahrung bieten. Webbasierte Dienste und Anwendungen werden immer stärker nachgefragt und Unternehmen müssen nicht nur auf die Bedürfnisse ihrer Kunden eingehen, sondern auch für möglichst sichere, schnelle und zuverlässige Websites und Applikationen sorgen.

Diese Entwicklung beschert ihnen einerseits neue Herausforderungen, andererseits aber auch Wachstumschancen – von der Voraussage und Erfüllung digitaler Kundenbedürfnisse über die effektive Abwehr webbasierter Angriffe und die Überwindung von Latenzproblemen bis hin zur Verhinderung von Website-Ausfällen und Aufrechterhaltung von Netzwerkkonnektivität und -Performance.

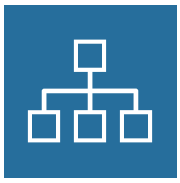
Um eine überragende Online-Erfahrung zu schaffen, ist es nicht mit einem einzelnen Tool oder einem bestimmten Softwarepaket getan. Vielmehr kommt es darauf an, ein ausreichend hohes Sicherheitsniveau zu integrieren – ebenso wie Leistungsmerkmale, die darauf abzielen, die Latenzzeit zu verringern und die Zuverlässigkeit des Netzwerks zu erhöhen. Das folgende Diagramm zeigt diese Elemente im Überblick:



Es folgen fünf wesentliche Schritte zur Erfüllung von Kundenbedürfnissen und Bereitstellung einer sicheren und reibungslosen Nutzererfahrung, auf die kein modernes Unternehmen verzichten kann.

SCHRITT 1

Gewährleistung sicherer, schneller und zuverlässiger Kundenverbindungen



DNS

Obwohl kein gewerblicher Internetauftritt ohne das DNS auskommt, wird es oft übersehen – bis dann etwas nicht mehr funktioniert. Angesichts sich häufender DNS-Angriffe erkennen allerdings immer mehr Firmen, dass ihre allgemeine Sicherheitsstrategie eine Schwachstelle aufweist, weil ihr DNS nicht gegen solche Angriffe gefeit ist. Es bringt nichts, Millionen Euro in den Aufbau und die Absicherung von Websites zu investieren, wenn man auf deren Anwendungen dann nicht zugreifen kann oder die Kunden sie gar nicht erst finden.

Die Herausforderungen

Hohe Latenz: Probleme mit der Web-Performance können auftreten, wenn Internetseiten häufig auf mehr als eine Domain zugreifen, um ihre Inhalte zu laden: Die Auflösung dieser verschiedenen Domains führt zu einem erhöhten Zeitaufwand.

Interne DNS-Infrastruktur: Ein selbst gehostetes DNS verursacht hohe Wartungskosten, erhöht möglicherweise die Latenz für Kunden in aller Welt und ist nicht vollständig vor raffinierten DNS-Angriffen sicher.

DNS-Provider mit kleinem Netzwerk: Bei der Suche nach einer DNS-Lösung machen Unternehmen oft den Fehler, einen Anbieter zu wählen, der nicht über ein großes Netzwerk verfügt und die DNS-Auflösung nicht in allen seinen Rechenzentren durchführt. Darunter leiden unter Umständen Performance und Zuverlässigkeit, insbesondere wenn es darum geht, Kunden in verschiedenen Weltregionen zu erreichen.

Was ein DNS-Provider bieten sollte

Integrierte Sicherheitslösungen: Angesichts des breiten Spektrums an möglichen Bedrohungen wird für eine wirksame Bekämpfung von DNS-Angriffen eine integrierte Sicherheitsstrategie benötigt, die unter anderem DNSSEC, die DDoS-Abwehr und eine DNS-Firewall umfasst. Große Konzerne, die lieber ihre eigene DNS-Infrastruktur unterhalten möchten, können eine DNS-Firewall einrichten lassen und mit einem sekundären DNS kombinieren. Dieses Setup ergänzt die DNS-Infrastruktur vor Ort um eine weitere Sicherheitsebene und trägt dazu bei, eine übergreifende DNS-Redundanz zu gewährleisten.

Schnelle DNS-Auflösung: Unternehmen, die eine cloudbasierte Managed DNS-Lösung in Betracht ziehen, sollten bei der Wahl ihres Providers darauf achten, dass dieser die Performance und Verfügbarkeit durch schnelle DNS-Auflösung sowie mithilfe von geobasiertem oder dynamischem Routing maximieren kann.

Redundanz: Unternehmen, die ihre DNS-Einträge bei einem einzigen Provider hosten, liefern sich damit einem Single Point of Failure aus, was ihre Ausfallrisiken erhöht. Um die Ausfallsicherheit zu maximieren, sollte man nicht nur auf mehrere voneinander unabhängige Managed DNS-Provider zurückgreifen, sondern auch darauf achten, dass diese Anbieter nicht dieselben Nameserver nutzen.

Clientseitige Sicherheit

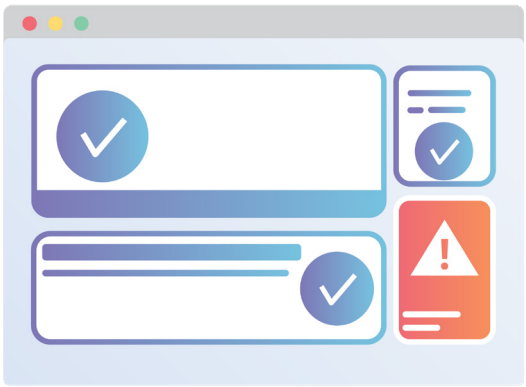
Heute gehen bis zu 70 %[1] des auf Browsern der Nutzer ausgeführten und gerenderten Codes auf externe und nicht überwachte JavaScript-Integrationen zurück. Dadurch entstehen neue und große Einfallstore für clientseitige Angriffe: von Magecart, Cross-Site Scripting (XSS) oder dem Skimming von Kreditkartendaten bis hin zu Website-Verunstaltungen oder noch schwereren Attacken.

Serverseitige Sicherheitstools können clientseitige Bedrohungen gar nicht oder nur begrenzt erkennen und weder Angriffe verhindern noch die genannten Schwachstellen patchen. Kein Unternehmen mit Webpräsenz kann darauf verzichten, einen dedizierten clientseitigen Schutz einzusetzen und zu pflegen, um seine Websites gegen diese gängigen und sich schnell wandelnden Bedrohungen abzusichern.

Clientseitige Angriffe

Cross-Site Scripting (XSS): Von XSS-Angriffen spricht man, wenn ein Angreifer eine seriöse Website ins Visier nimmt und Schadcode anhängt oder einfügt. Häufig besteht das Ziel darin, Anmeldedaten zu stehlen, auf sonstige sensible Informationen zuzugreifen oder Kontrolle über den Browser des Nutzers zu erhalten.

Magecart-Angriffe: Ein Magecart-Angriff ist eine Form des „Skimming“, bei dem Angreifer bösartigen Code in Websites einfügen, um vertrauliche Nutzerdaten (z. B. Kreditkartennummern, Passwörter usw.) aus Online-Zahlungsformularen abzuschöpfen. Für Unternehmen kann es sich als besonders schwierig erweisen, diese Art von Attacke aufzuspüren, weil die Angreifer die Möglichkeit haben, ihren Schadcode in harmlosem Quelltext zu verstecken oder die gestohlenen Daten zu verschlüsseln, um sie unbemerkt auslesen zu können.



Spoofing: Spoofing – die Verschleierung böswilliger Kommunikation durch das Vortäuschen einer vertrauenswürdigen Quelle – ermöglicht es Angreifern, sensible Nutzerdaten zu stehlen, den Datenverkehr für einen DDoS-Angriff umzuleiten oder sich unbefugt Zugriff auf das System oder Netzwerk eines Unternehmens zu verschaffen.

[1] Bermingham, Mark. „Redefining Client-Side Security with the Tala Security Certified Module for NGINX Plus“, NGINX, https://www.nginx.com/blog/redefining-client-side-security-tala-certified-module-nginx-plus/

Was eine clientseitige Sicherheitslösung bieten sollte

Ende-zu-Ende-Sicherheit: Anstatt nur eine bestimmte clientseitige Bedrohung in den Fokus zu nehmen, müssen Firmen sowohl ihre Backend-Infrastruktur als auch ihre Frontend-Prozesse umfassend schützen.

Minimale Auswirkungen auf die Performance: Der Einsatz und die Verwaltung strenger Sicherheitsprotokolle steht bei vielen Unternehmen ganz oben auf der Prioritätenliste; gleichzeitig ist es aber auch immens wichtig, dass Sicherheitsprodukte die Web-Performance nicht beeinträchtigen, da langsame Websites potenzielle Kunden abschrecken sowie zu höheren Absprung- und niedrigeren Konversionsraten führen können.

TLS

Unternehmen, die sensible Informationen speichern und übertragen, müssen Lösungen finden, mit denen sie ihre Daten vor Verlust, Diebstahl und Missbrauch schützen können. Hilfreich sind dabei die TLS-Netzwerkprotokolle (auch „SSL" genannt), die die Kommunikation über öffentliche Netzwerke verschlüsseln und vertrauenswürdige Instanzen authentifizieren. Diese Protokolle dienen dazu, den Schutz von Kundendaten zu gewährleisten und sie vor den Blicken und Manipulationen Dritter abzuschirmen.

Die Herausforderungen

Verwaltung von SSL/TLS-Zertifikaten: Die SSL/TLS-Zertifikate haben den Zweck, die Identitäten vertrauenswürdiger Instanzen zu überprüfen, allerdings können sie von böswilligen Akteuren kompromittiert oder manipuliert werden. Da im Prinzip jeder diese Zertifikate käuflich erwerben kann, haben Angreifer die Möglichkeit, sich mithilfe des Zertifikats als eine vertrauenswürdige Instanz auszugeben, Sicherheitsverfahren zu umgehen und Zugang zu vertraulichen Daten zu erhalten.

Sicherheit auf dem neuesten Stand: Mit jeder neuen Version von SSL/TLS versucht man, bekannte Sicherheitslücken zu patchen und die Abwehr von Angriffen auf Websites zu verbessern. Durch die Verwendung veralteter Versionen dieser Verschlüsselungsprotokolle – zum Beispiel TLS 1.1 oder 1.2 – machen Unternehmen es böswilligen Akteuren unter Umständen unbeabsichtigt leicht, bestehende Sicherheitslücken auszunutzen und Angriffe durchzuführen. Derzeit verwenden nur 22 % der Top-1000-Websites (nach Alexa) die neueste Version von TLS.[2]

[2] Holz, Ralph, Amann, Johanna, Razaghpanah, Abbas und Vallina-Rodriguez, Narseo. „The Era of TLS 1.3: Measuring Deployment and Use with Active and Passive Methods", Universität Sydney, https://arxiv.org/pdf/1907.12762.pdf

Gewährleistung der Einhaltung von Vorschriften und Standards: Viele Unternehmen sind an die Vorschriften der Datenschutz-Grundverordnung (DSGVO) und des California Consumer Privacy Act (CCPA) gebunden. Beide Gesetzeswerke legen Vorgaben zum Schutz von Kundendaten vor Diebstahl und Missbrauch fest. Firmen, die es versäumen, die Übertragung von Kundendaten ordnungsgemäß zu verschlüsseln, übersehen möglicherweise Malware, Datenexfiltration und andere potenzielle Gefahren.

Was eine TLS-Lösung bieten sollte

Einfache Implementierung: Unternehmen, die SSL/TLS-Protokolle manuell konfigurieren müssen, laufen Gefahr, ihre Kunden durch eine versehentliche Fehlkonfiguration am Zugriff auf ihre Websites zu hindern. Sie sollten sich für einen Provider entscheiden, der eine unkomplizierte Implementierung von SSL/TLS sowie einfache Tests und Rollbacks (falls etwas schief gehen sollte) ermöglicht und TLS-Protokolle automatisch aktualisiert, damit die neuesten bekannten Sicherheitslücken gepatcht werden.

Flexibilität: Wenn sich die Sicherheitsbedürfnisse eines Unternehmens verändern, bedarf es möglicherweise eines SSL/TLS-Providers, der verschiedene Arten von Zertifikatskonfigurationen im Angebot hat: von Datensätzen, die von einer Zertifizierungsstelle ausgestellt wurden, bis hin zu selbstsignierten Zertifikaten.

Erfüllung von Compliance-Vorgaben: Mithilfe einer umfassenden SSL/TLS-Entschlüsselung können Unternehmen im verschlüsselten Datenverkehr potenziell verborgene Bedrohungen erkennen. Indem sie diese Risiken schnell ausfindig machen und entschärfen, können sie Kundendaten vor Manipulation und Diebstahl schützen und die Einhaltung der DSGVO, des CCPA und anderer Vorschriften sicherstellen.

SCHRITT 2

Verbesserte Nutzererfahrung durch höhere Geschwindigkeit

Globales CDN

Globalen Unternehmen, die ihre Reichweite mit einer simplen und effektiven Lösung erhöhen möchten, drängen sich CDNs als Alternative zu Investitionen in Remote Hosting-Einrichtungen geradezu auf. Mithilfe von CDNs können sie einen großen und weit verteilten Kundenkreis ansprechen, ohne dafür eine umfangreiche globale Infrastruktur aufbauen zu müssen, deren Verwaltung und Wartung sich als kostspielig und heikel erweisen kann.

Die Herausforderungen

Mehr Sicherheit oder mehr Performance? Einerseits sollte sich ein CDN bei Netzwerkproblemen als robust erweisen und sensible Daten vor Diebstahl und Verlust schützen, andererseits kann aber die Integration von Sicherheitsfunktionen zu Leistungseinbußen führen, weil die Latenz zunimmt.

Fehlende Echtzeit-Analytics: Echtzeit-Analytics sind unter Umständen nur schwer oder mit erheblicher Verzögerung erhältlich, und in diesen Fällen kann sich ein Unternehmen kein klares Bild von der Performance seiner Web-Präsenzen machen.

Monolithische Architektur: Herkömmliche CDNs weisen eine monolithische Architektur auf, sodass es nicht selten zu Verzögerungen kommt, wenn Konfigurationsänderungen im gesamten Netzwerk eingepflegt werden müssen.
Bei den Entwicklern, die Richtlinienänderungen möglichst schnell implementieren und iterieren müssen, führen diese Verzögerungen mitunter zu Frustrationen.

Was ein CDN-Provider bieten sollte

Mehr Performance: Bei der Bewertung eines CDN sollte ein Unternehmen zunächst durch Tests ermitteln, ob in seinen verschiedenen Schlüsselmärkten eine vergleichbare Performance erreicht wird. Jeder CDN-Provider schneidet hier anders ab und manche Anbieter werden ihre besten Resultate in Regionen liefern, die für das Unternehmen weniger wichtig sind. Im Anschluss an diese ersten Tests sollten die Unternehmen dann prüfen, ob etwaige Leistungseinbußen angesichts von Verbesserungen in anderen Regionen hinnehmbar oder zu vernachlässigen sind.

Echtzeit-Analytics: Analytics und Daten zu Nutzung und Nutzererfahrung hinsichtlich der betreffenden Web-Domains in aller Welt sollten sich einfach und mit einer möglichst geringen Verzögerung erfassen lassen.

Entwicklerfreundliche Lösung: Entwickler und Engineering-Teams haben bei der Entscheidung über die Rolle, die ein CDN beim Aufbau ihrer digitalen Infrastruktur spielen soll, ein Wort mitzureden. Unternehmen sollten sich nach einem Provider umsehen, der eine nahtlose API-Integration anbietet und bei kundenspezifischen Konfigurationen ohne extern zugekaufte professionelle Services auskommt.

Schnelleres Routing

Unternehmen, die Kunden in aller Welt bedienen, müssen auf die Performance ihrer Webanwendungen achten. Eine Reihe von Faktoren kann die Latenz nach oben treiben, zum Beispiel schwerfällige Sicherheitsprotokolle oder auch suboptimale Netzwerkbedingungen für globale Nutzer.

Smart Routing kann zur Entschärfung dieser Probleme beitragen, indem es bei der Wahl der Netzwerkpfade Überlastung und Zuverlässigkeit berücksichtigt. Es läuft ergänzend zum BGP und testet die verfügbaren Pfade, um zu ermitteln, welcher eine bessere Performance erlaubt. Paketverluste und die damit in der Regel einhergehenden Verzögerungen und Netzwerkunterbrechungen können durch die Umgehung unzuverlässiger Netzwerkverbindungen ebenfalls vermieden werden.

Die Herausforderungen

Netzwerküberlastung: Netzwerküberlastungen können auf ein bestimmtes geographisches Gebiet mit unzureichender Infrastruktur beschränkt sein oder das gesamte Netz eines ISP betreffen. Sie verschärfen sich, wenn an nationalen Feiertagen, bei globalen Katastrophen oder aufgrund anderer Ereignisse, die einen hohen Traffic mit sich bringen, mehr Nutzer auf die Kommunikationsangebote und Dienste des Internets zugreifen.

Höhere Netzwerklatenz: Eine höhere Netzwerklatenz wirkt sich direkt auf die Ladegeschwindigkeit und Performance einer Website aus, sodass möglicherweise die Nutzererfahrung beeinträchtigt wird, die Konversionsrate sinkt und Umsatzeinbußen entstehen.

Kostspielige Lösungen: Große Service Provider haben private Standleitungen und MPLS-Netze (Multiprotocol Label Switching) im Angebot, mit denen für die Geschäftskommunikation exklusive Zugriffspfade zur Verfügung stehen. Das Anmieten solcher Privatleitungen bietet zwar einige Vorteile, aber häufig bringt ihre Implementierung eine Kostenexplosion mit sich, die die Rentabilität beeinträchtigen und das Budget für andere geschäftskritische Dienste schmälern kann.

Wie man die richtigen Tools zur Festlegung optimaler Netzwerkpfade auswählt

Steigerung der Performance von digitalen Inhalten: Mit dem richtigen Provider sollte ein Unternehmen in der Lage sein, Online-Traffic über die schnellsten verfügbaren Verbindungen bereitzustellen, damit Inhalte schneller verfügbar sind und sich die Endnutzererfahrung verbessert.

In Echtzeit verfügbare Kennzahlen und Analytics: Unternehmen sollten Kennzahlen und Analytics in Echtzeit zur Verfügung stehen, damit sie potenzielle Routing-Probleme untersuchen können. Mithilfe dieser Daten können Überlastungen vermieden, Pfade optimiert, Verbesserungen der globalen Performance gemessen und die Verfügbarkeit erhöht werden – und zwar unabhängig von Nutzerstandort, Gerät oder aktuellen Netzwerkbedingungen.

Tools für die Netzwerküberwachung: Um die Latenz zu senken und Netzwerküberlastungen zu umgehen, können Tools zur Netzwerküberwachung implementiert werden, die potenzielle Überlastungspunkte ausfindig machen und bei der Priorisierung des Datenverkehrs helfen. So wird gewährleistet, dass besonders kritische Workloads ihre Ziele erreichen und nie eine einzelne Anwendung die gesamte Bandbreite für sich beansprucht.

Optimierung für Mobilgeräte

Man erwartet heute, dass sich Webseiten in weniger als drei Sekunden aufbauen – und zwar nicht nur am Desktop-Computer, sondern auch auf Mobilgeräten. Für jeden, der im Online-Geschäft erfolgreich sein will, sind Optimierungen für den mobilen Zugriff deshalb ein Muss. Unternehmen, die nicht in der Lage sind, diese Erwartungen mit einer schnellen und nahtlosen mobilen Nutzererfahrung zu erfüllen, werden ihre Kunden verlieren.

Die Herausforderungen

Mangelhafte Bildoptimierung: Wenn Bildgröße und -format nicht auf die kleineren Bildschirme der Mobilgeräte abgestimmt werden, leidet möglicherweise die Nutzererfahrung: Webseiten werden verzerrt dargestellt und lassen sich nur schwer navigieren. Und je größer die Bilddatei ist, desto länger dauert der Download. Deshalb führt datenintensives Bildmaterial häufig zu einer Verlängerung der Seitenladedauer, die völlig unnötig ist, weil die Größe oder Auflösung der mobilen Bildschirme hochauflösenden Bildern gar nicht gerecht werden können.

Erhöhte Bandbreitennutzung: Große Dateien nehmen mehr Bandbreite in Anspruch und treiben damit auch die Datengebühren der Hosting-Provider nach oben. Unternehmen ohne geeignete Bildoptimierungslösung für ihre mobilen Internetauftritte setzen sich möglicherweise zahlreichen Geschäftsrisiken aus, von steigenden Bandbreitenkosten bis hin zu sinkendem Kundeninteresse sowie niedrigeren Konversionsraten und Einnahmen.

Umständliche interne Entwicklungsprozesse: Webentwickler erhalten häufig den Auftrag, die Optimierung von Inhalten für Mobilgeräte zu unterstützen. Hierfür müssen gegebenenfalls manuelle Prozesse zur Replikation von Bildmaterial für verschiedene Gerätetypen geschaffen werden. Doch ideal ist diese Lösung nicht, denn sie lässt nur wieder ein weiteres System oder Verfahren entstehen, das dann verwaltet und gepflegt werden muss. Die Alternative – die Implementierung einer speziellen Lösung eines Drittanbieters für die Bildoptimierung – kostet oft viel Geld und beeinträchtigt womöglich die Rentabilität der Web-Features.

Was eine Optimierungslösung für Mobilgeräte bieten sollte

CDN-Integration: Eine Optimierungslösung für Mobilgeräte sollte sich nahtlos in bestehende CDN-Dienste einfügen, sodass die Vorteile des Cache voll ausgenutzt werden können und die Abhängigkeit von diesen Diensten für redundante Bilddateien reduziert wird. Eine gute CDN-Lösung trägt zur Verbesserung der mobilen Performance bei, indem sie die Anforderungen der Mobilgeräte erkennt, die Bilddateien durch „Virtualisierung“ verkleinert und sie möglichst nahe am Mobilnutzer zwischenspeichert.

Interne oder externe Wartungsdienste: Bei der Auswahl von Optimierungslösungen für Mobilgeräte sollte man die auf lange Sicht anfallenden Wartungsanforderungen und Updates sorgfältig prüfen und dem Aufwand bei innerbetrieblich erstellten und verwalteten Lösungen gegenüberstellen. Relevant ist auch die Frage, ob diese Optimierungslösungen so erweitert werden können, dass sie Speicherorte von Drittanbietern außerhalb der eigenen Domains unterstützen.

SCHRITT 3

Anhebung des infrastrukturellen Sicherheitsniveaus

Web Application Firewall

Selbst Unternehmen, die sich aktiv um eine Absicherung ihrer Infrastruktur und Daten bemühen, tun sich mitunter sehr schwer damit, ihre Sicherheitsbemühungen operativ umzusetzen. Das gilt umso mehr in einer Welt, in der jede Sicherheitslücke eine Angriffsmöglichkeit darstellt.

Mit einer Web Application Firewall (WAF) können sich Unternehmen vor Zero-Day-Angriffen schützen und ihre Anwendungen gegen gängige Bedrohungen wie Cross-Site Request Forgery (CSRF), Cross-Site Scripting (XSS) und SQL Injection-Attacken abschirmen. Eine WAF bietet Unternehmen zudem die Möglichkeit, eine detaillierte Kontrolle ihrer Sicherheitsrichtlinien zu pflegen, indem sie Regeln aufstellen, mit denen Sicherheitslücken ihrer Anwendungen geschlossen werden und eine Verteidigung gegen neue Bedrohungen aufgebaut wird.

Die Herausforderungen

Hoher Ressourceneinsatz für Implementierung und Verwaltung: Für eine gut gepflegte Präsenz im Cyberspace und den Schutz von geschäftskritischen Anwendungen ist es ganz entscheidend, die Infrastruktur stets mit Patches auf den neuesten Stand zu bringen. Doch angesichts der schieren Menge an Patches und der Häufigkeit, mit der die zahlreichen Anbieter immer wieder neue Korrekturen ausliefern, gelingt dies selbst den größten Sicherheitsteams in der Regel nur für Teile der Infrastruktur. WAF-Lösungen mildern dieses Problem, allerdings ist der Zeit- und Ressourcenaufwand für die Implementierung und Verwaltung dieser Firewalls oft hoch: Bei vielen modernen WAFs können diese Prozesse nicht ohne ein Team von hochqualifizierten Sicherheitsexperten durchgeführt werden.

Mangelnde Flexibilität: Als separates Gerät ausgeführte Hardware-WAFs stellen bei der heutigen Bedrohungslage eine extrem veraltete Sicherheitslösung dar. Da sich Anwendungen und Daten meist in einer hybriden Umgebung befinden – also sowohl innerhalb der Infrastruktur vor Ort als auch in der Cloud –, hat sich die cloudbasierte WAF zu einer wichtigen Komponente der mehrschichtigen Verteidigungsstrategie eines jeden Unternehmens entwickelt. Im Gegensatz zu den Hardwarelösungen können cloudbasierte WAFs auf Sicherheitslücken basierende Angriffe unabhängig vom Hosting-Standort der Anwendung und Infrastruktur abwehren.

Agilität: In einer Welt, in der sich Sicherheitsteams zum Schutz ihrer Inhalte und Daten einen ständigen Wettlauf mit Angreifern liefern, ist Agilität ein entscheidender Faktor. Hardwarebasierten WAFs fehlt ein agiler Mechanismus, mit dem Regeln erstellt und schnell auf die gesamte Infrastruktur übertragen werden können. Die Zeit zwischen der Bekanntgabe einer Sicherheitslücke und der Bereitstellung eines Patchs, der vor Exploits schützen soll, ist entscheidend.

Was eine WAF-Lösung bieten sollte

Benutzerfreundlichkeit: Benutzerfreundlichkeit ist ein zentrales Kriterium, wenn es um die Entscheidung für eine bestimmte WAF, ihre Implementierung und Verwaltung geht. Der Implementierungsprozess einer WAF sollte nicht erst nach Wochen oder gar Monaten abgeschlossen sein und die Verwaltung der Lösung sollte auch ohne Heerscharen von Fachleuten möglich sein. Außerdem sollten Unternehmen eventuell einen WAF-Provider in Erwägung ziehen, der eine nahtlose API-Integration bieten kann.

Echtzeitinformationen über Bedrohungen: Ein wesentliches Defizit hardwarebasierter WAFs besteht darin, dass sie in Bezug auf Bedrohungen und Angriffe keinen Echtzeitkontext liefern. Zwar lässt sich die Bereitstellung von Bedrohungsanalysen gegebenenfalls in eine hardwarebasierte WAF integrieren, aber dadurch entsteht lediglich eine reaktive und keine proaktive Lösung. Angesichts einer alles andere als statischen Bedrohungslage können Firmen nicht darauf verzichten, über herrschende Gefahren in Echtzeit informiert zu werden, damit sie stets über die neuesten Bedrohungen im Bilde sind. WAFs sollten Echtzeitkontext für diverse globale Bedrohungen mitbringen, wobei man nicht nur auf die Größe des Datensatzes zur Bedrohungsanalyse achten sollte, sondern auch auf die Datenvielfalt.

Umfassende Abdeckung: Angreifer versuchen zwar häufig, die OWASP Top 10 und andere bekannte Schwachstellen auszunutzen, doch zunehmend interessieren sie sich auch für Zero-Day- und andere kritische Sicherheitslücken. Zu einer umfassenden WAF-Lösung gehören deshalb auch verwaltete Regelsätze, die regelmäßig aktualisiert werden, um Attacken, die auf diese Schwachstellen abzielen, automatisch zu vereiteln.

Bot-Abwehr

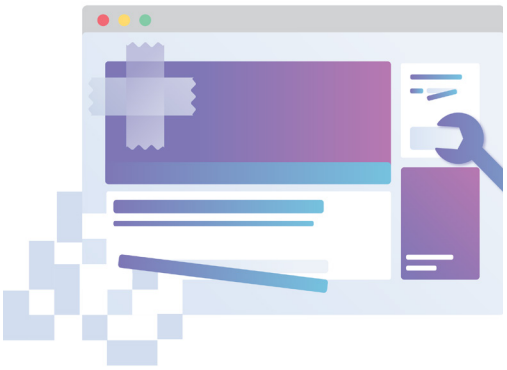
Bösartige Bots können in webbasierten Firmen großen Schaden anrichten: Neben der Gefährdung sensibler Datenbestände und der Störung der allgemeinen Kundenerfahrung können sie auch die Betriebskosten eines Unternehmens unmittelbar nach oben treiben. Außerdem wird es angesichts immer raffinierterer Bot-Angriffe schwieriger, echte Nutzeraktivitäten vom automatisierten Treiben der Bots zu unterscheiden. Für Unternehmen ergeben sich daraus Risiken bisher unbekannten Ausmaßes. Websites laufen Gefahr, kompromittiert zu werden, wenn sie ins Visier bösartiger Bot-Aktivitäten geraten. Überlastete Webserver, verfälschte Analysen, blockierte Webseiten, gestohlene Nutzerdaten, Spam-Versand, Schädigung der Markenintegrität, Beeinträchtigung der Kundenbindung und Umsatzeinbußen sind die möglichen Folgen.

Allerdings gibt es auch nützliche Bots. Um diese von schädlichen Bot-Aktivitäten unterscheiden zu können und zu verhindern, dass bösartiges Verhalten die Nutzererfahrung beeinträchtigt, können Unternehmen eine Bot-Management-Lösung implementieren.

Die Herausforderungen

Hohe Infrastrukturkosten: Online-Traffic ist für ein Unternehmen immer auch mit handfesten Kosten verbunden, da es den Inhalt hosten, die Server bereitstellen und für Speicherkapazitäten und Rechenleistung bezahlen muss. Leider steigen diese Ausgaben, wenn Websites von bösartigen Bots ins Visier genommen werden. Gutartige Bots sind für Unternehmen unverzichtbar, weil sie die SEO, den Kundensupport und andere nützliche Aufgaben übernehmen – doch wenn ein solches Programm Böses im Schilde führt, kommt es regelmäßig zu übermäßigen Bandbreitenkosten, weil es Inhalte ausliest und Dienste stört.

Schlechte Nutzererfahrung: Die Auswirkungen bösartiger Bots auf ein Unternehmen bekommen Kunden deutlich zu spüren. Unter Umständen können sie sich nicht mehr einloggen, vielleicht werden ihnen sogar betrügerische Transaktionen zur Last gelegt oder sie können einfach nicht mehr auf die Website des Unternehmens zugreifen. Wenn Server durch die Aktivitäten eines Bots überlastet werden, können sie seriösen Nutzern keine kurzen Ladezeiten mehr bieten. Dies führt zu mehr abgebrochenen Online-Einkäufen, höheren Absprung- und sinkenden Konversionsraten; die Interaktion mit den Kunden und ihre Bindung an das Unternehmen gehen zurück und Einnahmen brechen weg.



Verzerrte Analysen: Bösartige Bots bewirken nicht nur, dass die Nutzererfahrung leidet und die Infrastrukturkosten durch die Decke gehen, sondern sie verzerren auch Analysen und zeichnen so ein falsches Bild von der Online-Performance eines Unternehmens. Der von einem solchen Bot verursachte Datenverkehr ist in der Regel von geringer Qualität und kann die aggregierten Analysedaten eines Unternehmens beeinträchtigen (z. B. durch eine künstlich nach oben getriebene Zahl der Seitenaufrufe). Dadurch bleiben dem Unternehmen wertvolle Einblicke in die Muster des Datenverkehrs und die neuesten Performance-Kennzahlen verwehrt.

Was eine Bot-Abwehrlösung bieten sollte

Korrekte Erkennung: Bevor Unternehmen bösartige Bots bekämpfen können, müssen sie in der Lage sein, Bot-Aktivität auf ihren Websites richtig zu identifizieren. Einige der besten Erkennungsverfahren kombinieren Informationen zu Bedrohungen mit Verhaltensanalysen, Fingerprinting und maschinellem Lernen. Mit diesem Ansatz können sie Unternehmen beim Aufspüren bösartiger Umtriebe unterstützen, ohne dabei die Aktivitäten seriöser Besucher ihrer Website zu stören oder die Nutzererfahrung zu beeinträchtigen.

Nahtlose Integration: Selbst die umfassendste Bot-Abwehrstrategie ist nutzlos, wenn sie eine langwierige und komplizierte Konfiguration erfordert. Bot-Abwehrlösungen sollten sich einfach und schnell in jeden Technologie-Stack, jede Sicherheitsstrategie (auch in die Abwehr von DDoS-Angriffen) und jedes CDN integrieren lassen, damit Kunden von dem optimierten Schutz vor Angriffen profitieren können, ohne dass es zu messbaren Beeinträchtigungen der Nutzererfahrung kommt.

Verschiedene Abwehrverfahren: Da die Methoden bösartiger Bots von Jahr zu Jahr vielschichtiger und raffinierter werden, müssen Firmen auch ihre Abwehrstrategien entsprechend anpassen, um zu gewährleisten, dass diese Aktivitäten weiterhin umgehend erkannt und vereitelt werden können. Eine Taktik allein reicht nicht aus, um alle Verhaltensformen bösartiger Bots zu bekämpfen. Vielmehr ist es unerlässlich, eine breite Palette an Erkennungs- und Abwehrmethoden zu implementieren, einschließlich einer oder mehrerer der folgenden: Blockade des gesamten Bot-Traffics, Whitelisting gutartiger Bots, Hürden für mögliche Bots in Form von CAPTCHAs, tägliche Protokollierung des gesamten Website-Traffics, Implementierung zusätzlicher Authentifizierungen für alle Nutzer und Umleitung von Bots zu alternativen Inhalten.

Abwehr von DDoS-Angriffen

DDoS-Angriffe verursachen durch die Inanspruchnahme der gesamten zwischen den Zielgeräten und dem Internet verfügbaren Bandbreite erhebliche Dienstunterbrechungen und wirken sich spürbar negativ auf das Geschäft aus, da Kunden nicht auf die Online-Ressourcen des betroffenen Unternehmens zugreifen können.

Zum Schutz von Webservern kann mithilfe eines Reverse Proxys verhindert werden, dass Angreifer IP-Adressen von Servern in Erfahrung bringen und ins Visier nehmen können. Bei komplexeren Layer-7-DDoS-Angriffen kann eine Web Application Firewall (WAF) als Reverse Proxy fungieren und den attackierten Server vor bestimmten Arten schädlichen Datenverkehrs schützen.

Manche Unternehmen bauen oder nutzen eigene Reverse Proxys, aber dafür sind umfangreiche Software- und Engineering-Ressourcen sowie beträchtliche Investitionen in physische Hardware erforderlich. Ein einfacherer und kostengünstigerer Ansatz, von den Vorteilen eines Reverse Proxys zu profitieren, besteht darin, ein CDN zu nutzen, das Global Server Load Balancing bietet. Mit dieser Lösung können Firmen DDoS-Angriffe näher an der Quelle und ohne Beeinträchtigung der Performance abwehren.

Natürlich genügt es nicht, nur die Webserver vor DDoS-Angriffen zu schützen. Große Unternehmen verfügen häufig über eine lokale Netzwerkinfrastruktur, die in öffentlichen oder privaten Rechenzentren gehostet wird und ebenfalls von diesen Bedrohungen abgeschirmt werden muss.

Veraltete Ansätze zur DDoS-Abwehr

Scrubbing: Scrubbing erfordert die Umleitung des Netzwerk-Traffics zu zentralen Scrubbing-Servern, die schädliche Anteile des Datenstroms herausfiltern sollen (engl. to scrub: auswaschen). Allerdings kann dieser Umweg über ein geografisch weit entferntes Scrubbing-Zentrum eine beträchtliche Latenz verursachen, die für die meisten Anwendungen oft nicht vertretbar ist.

Lokale Hardware: Bei einem anderen Ansatz zur Abwehr von DDoS kommt lokale Hardware zum Einsatz, die den Netzwerk-Traffic scannt und bösartige Anfragen herausfiltert. Auch bei dieser Lösung kommt es allerdings zu Netzwerklatenz und einer Beeinträchtigung der Performance, denn die Kapazitäten dieses Umwegs, den der Datenstrom über die für den Scan-Vorgang zuständige Hardware nimmt, sind begrenzt. Häufig verfügen lokale Anti-DDoS-Geräte standardmäßig über eine Bandbreitenbegrenzung, die sowohl von der Netzwerkkapazität des Unternehmens als auch von der Kapazität der Hardware abhängig ist.

Was ein Provider einer DDoS-Abwehrlösung bieten sollte

Schnelle Reaktionszeit und hoher Datendurchsatz: Es empfiehlt sich, die Kapazitäten zu bemessen, die einem Unternehmen für eine DDoS-Abwehr ohne Beeinträchtigung der Website-Funktionalität zur Verfügung stehen. Die traditionelle Vorgehensweise zur Neutralisierung der von DDoS-Angriffen verursachten Datenverkehrsspitzen bestand darin, viel Geld in lokale Serverfarmen zu investieren, die volumetrischen Angriffen trotzdem nicht lange standhalten konnten. Ein effektiverer Ansatz ist eine cloudbasierte Abwehrlösung, die unbegrenzte Kapazitäten zum Schutz vor DDoS-Angriffen bietet und ihre Dienste auch am Netzwerkrand bereitstellen kann.

Ständige Abwehrbereitschaft oder Schutz auf Abruf? Bei auf Abruf eingesetzten Abwehrlösungen muss der Datenverkehr immer dann, wenn ein potenzieller DDoS-Angriff erkannt wurde, zu einem Abwehrservice in der Cloud umgeleitet werden. Für den DDoS-Schutz fallen nur dann Kosten an, wenn er auch wirklich benötigt wird. Allerdings kann etwas Zeit vergehen, bis ein DDoS-Angriff blockiert wird, weil die Datenverkehrsspitzen bestimmte Schwellenwerte erreichen müssen, bevor die Analyse beginnt und jemand den Abwehrservice manuell aktiviert.

Im Gegensatz dazu wird bei einer durchgängig aktiven Lösung der gesamte Website-Datenverkehr ohne Unterbrechung geroutet und gefiltert, sodass die Server des Nutzers stets nur gereinigter Traffic erreicht. Dieser Ansatz ist zwar teurer als die auf Abruf eingesetzten Dienste, er bietet jedoch auch einen automatischen und kontinuierlichen Schutz sowie kürzere Reaktionszeiten. Für Unternehmen, die ständig mit Angriffen zu kämpfen haben, kann sich die Entscheidung für eine durchgängig aktive Abwehrlösung durchaus lohnen.

Integrierte Sicherheit und Performance: DDoS-Angriffe verursachen lange Ladezeiten und Ausfälle, die nicht nur die Performance beeinträchtigen, sondern auch die Fähigkeit des betroffenen Unternehmens zu nachhaltigem Wachstum einschränken. Um Sicherheit mit Performance zu kombinieren, sollten Firmen integrierte Lösungen in Betracht ziehen, die ihnen eine solide Verteidigung gegen DDoS-Angriffe bieten, ohne sich negativ auf die Website-Performance oder das Nutzererlebnis auszuwirken.

SCHRITT 4

Gewährleistung hochverfügbarer Anwendungen durch den Aufbau einer stabilen Infrastruktur

Lastverteilung

Die Maximierung von Serverressourcen und -effizienz kann einen schwierigen Balanceakt darstellen. Überlastete oder geografisch zu weit von den Endnutzern entfernte Server können sich nachteilig auf das Geschäft auswirken, da erhöhte Latenz und Serverausfälle möglicherweise zu Umsatzeinbußen führen, das Vertrauen der Kunden zerstören und das Ansehen der Marke beschädigen.

Cloudbasierte Load Balancer bewältigen Datenverkehrsspitzen, indem sie Anfragen auf mehrere Server verteilen. Die Entscheidung über die Lastverteilung erfolgt am Netzwerkrand, damit sie näher am Nutzer getroffen wird. Dadurch können Unternehmen die Reaktionszeit verbessern, ihre Infrastruktur effektiv optimieren und gleichzeitig das Risiko eines Serverausfalls minimieren. Selbst wenn ein einzelner Server komplett ausfällt, kann der Load Balancer den Traffic umleiten und auf die verbleibenden Server verteilen. So wird gewährleistet, dass Kunden niemals eine signifikante Latenz oder einen Ausfall der Website erleben müssen. Mit dem Load Balancer lassen sich auch aktive Health Checks durchführen, die es Unternehmen ermöglichen, leistungsschwache Server zu identifizieren und vorbeugende Maßnahmen zu ergreifen, bevor es tatsächlich zu einem Ausfall kommt.

Die Herausforderungen

Ausfall und Latenz von Anwendungen: Schon kleine Verzögerungen können sich spürbar auf Kundentreue und Konversionsraten auswirken. Der Nutzer nimmt schon eine Latenz von rund 30 Millisekunden wahr und 100 bis 400 Millisekunden können bereits das Verbraucherverhalten beeinträchtigen.[3] Unternehmen, die es versäumen, eine funktionierende Lastverteilungslösung zu implementieren, müssen mit sinkenden Konversionsraten und Umsatzeinbußen rechnen, weil Probleme mit der Performance ihrer Web-Präsenzen vorprogrammiert sind.

Hohe Kosten und begrenzte Flexibilität: Hardwarelösungen für die Lastverteilung sind teuer und kompliziert, außerdem können sie naturgemäß nicht mit dem Unternehmen wachsen. Beim Erwerb dieser Geräte müssen stattdessen Prognosen hinsichtlich des zukünftigen Umfangs des Website-Datenverkehrs angestellt werden. Nicht selten bedeutet das, dass Firmen entweder für ungenutzte Kapazitäten zahlen, oder dass sie mit suboptimalen Ladezeiten und einer dürftigen Web-Performance auskommen müssen, bis sie die Zahl der eingesetzten Geräte endlich erhöhen können.

Komplexe Steuerung des Datenverkehrs: Um die Performance und Zuverlässigkeit ihrer Internetauftritte zu maximieren, müssen Unternehmen den regionalen Traffic steuern, den Zustand der Ursprungsserver überwachen und die Muster ermitteln, nach denen ihr Datenverkehr verläuft. Denn wenn ihnen diese Erkenntnisse fehlen, sind sie möglicherweise nicht in der Lage zu erkennen, wenn eine Lastverteilungslösung aufgrund eines Defekts versehentlich Datenverkehr zu einem problematischen Server routet, sodass die Nutzer unter Umständen mit erheblichen Verzögerungen und Ausfällen konfrontiert werden.

[3] Brutlag, Jake. „Speed Matters“, Google AI Blog, https://ai.googleblog.com/2009/06/speed-matters.html

Was ein Load Balancer bieten sollte

Anbieterunabhängige Lösung: Ein Load Balancer mit Multi Cloud- und Hybrid Cloud-Unterstützung kann Unternehmen dabei helfen, ihre Auftragnehmer auch weiterhin frei wählen zu können und komplexe Konfigurationen zu vermeiden. Dabei muss eine eigenständige cloudbasierte Lösung vorhandene Lastverteilungsdienste nicht ersetzen, sondern kann auf die eigenen Load Balancers der Cloud-Anbieter oder auch auf traditionelle Hardware abgestimmt werden, um maximale Flexibilität zu erreichen und Fehlkonfigurationen möglichst zu verhindern. Im Wesentlichen sollte sie es Unternehmen erlauben, den Datenverkehr dynamisch über deren Infrastruktur zu verteilen – unabhängig davon, ob die Ursprungsserver lokal oder in Multi Cloud- bzw. Hybrid Cloud-Umgebungen gehostet werden.

Aktive Health Checks und detaillierte Analytics: Ein wesentliches Kriterium bei der Entscheidung für eine Lastverteilungslösung ist die Transparenz – zum einen, damit Unternehmen gewährleisten können, dass sich ihre Server und Anwendungen in einem einwandfreien Zustand befinden, zum anderen aber auch zur frühzeitigen Identifizierung potenzieller Latenzen oder Ausfälle. Detaillierte Analytics der Traffic-Muster und des Zustands der Ursprungsserver sollten Firmen in die Lage versetzen, leistungsschwache Server zu erkennen und ihre Infrastruktur in Bezug auf Verfügbarkeit und Betriebszeit zu optimieren.

CDN-Integration: Eine optimal konfigurierte Lastverteilungslösung arbeitet Hand in Hand mit einem CDN, um eine möglichst geringe Latenz und Bandbreitenbelastung zu gewährleisten. Durch die Zwischenspeicherung statischer Inhalte am Netzwerkrand ist ein CDN in der Lage, dem Endnutzer Inhalte vom nächstgelegenen Server zu liefern. Dies führt zu einer umfassenden Verbesserung der Web-Performance und reduziert die Gesamtzahl der an den Ursprungsserver gesendeten Anfragen.

SCHRITT 5

Identifizierung verdächtigen Verhaltens und Absicherung von Websites am Netzwerkrand

Data Loss Prevention (DLP)

Mit Aufkommen des Cloud Computing haben sich Datenschutzverletzungen zu einer der größten Bedrohungen für moderne Unternehmen entwickelt. Sie entstehen häufig durch gezielte Angriffe, interne Systemfehler oder auch einfach nur durch menschliches Versagen. Mögliche Folgen sind die Offenlegung sensibler Kundeninformationen, die Verletzung von Datenschutzbestimmungen oder auch Einbußen in Millionenhöhe durch Bußgelder oder entgangene Einnahmen.

Allerdings gibt es eine Reihe von Strategien und Produkten, mit denen Unternehmen die Cybersicherheit erhöhen und potenzielle Datenlecks oder die Preisgabe vertraulicher Informationen verhindern können. Lösungen für Data Loss Prevention (DLP) unterstützen außerdem die Einhaltung der DSGVO, des CCPA und anderer Datenschutzvorschriften und schützen vor der unzulässigen Verwendung von Nutzerdaten.

Die Herausforderungen

Komplexe Installation: Ältere DLP-Lösungen sind zwar durchaus solide konzipiert, aber oft auch sehr komplex, und ihre Einrichtung kann viel Zeit kosten. Unternehmen müssen ihre DLP-Richtlinien auf bestimmte Nutzergruppen und geschäftliche Anwendungsfälle zuschneiden – nicht selten ein mühsamer Prozess, der umfangreiche externe Unterstützung und Admin-Leistungen erfordert. Da die DLP-Regeln die Nutzer daran hindern, Daten über genau definierte Grenzen hinweg zu übertragen, schränken sie zudem unter Umständen auch die Produktivität und Zusammenarbeit der Mitarbeiter ein, indem sie den Zugriff auf erforderliche Daten versehentlich blockieren.

Unzureichender Datenschutz: DLP-Richtlinien müssen sowohl gesetzlich geschützte Daten (sensible Daten, die unter Verschluss bleiben sollten) als auch unreglementierte Datenbestände (öffentlich bekannte Informationen, die auch vertrauliche Daten enthalten können) abdecken. Viele ältere DLP-Produkte schützen allerdings keine IP-Daten, die von der Datenschutzgesetzgebung nicht umfasst sind. Dies kann einem Unternehmen im Falle eines Datenlecks erhebliche Verluste bescheren.

Eingeschränkte Transparenz: Um einen Rundumschutz vertraulicher Daten zu gewährleisten, interne Bedrohungen abzuwehren und stets die vor Ort gültigen Datenschutzbestimmungen einzuhalten, sind Firmen darauf angewiesen zu erfahren, wie auf ihre Daten zugegriffen wird und wie sie übertragen werden. Wenn sich Unternehmen zu sehr auf bestehende oder erwartete Bedrohungen konzentrieren, kann das ihre adäquate Vorbereitung auf unerwartete Angriffe beeinträchtigen.

Was eine DLP-Lösung bieten sollte

Unkomplizierte Bereitstellung und Verwaltung: Hardwarebasierte DLP-Systeme einzurichten ist eine komplizierte Angelegenheit, ihre Verwaltung ist umständlich und zum Schutz vor immer neuen Bedrohungen müssen ständig neue Updates aufgespielt werden. Cloudbasierte Lösungen können zu einer Senkung der Bereitstellungskosten beitragen, während gleichzeitig weiterhin flexibel auf Datenrisiken reagiert werden kann. Außerdem geben sie Unternehmen einen besseren Einblick in deren Datennutzung und -verwaltung.

Flexibilität: Unternehmen sollten sich für eine DLP-Lösung entscheiden, die flexibel genug ist, um unterschiedlichen Nutzergruppen und Anwendungsfällen gerecht zu werden. Darüber hinaus muss sie sich problemlos installieren, verwalten und warten lassen. Anstatt sich auf hardwarebasierte und veraltete DLP-Lösungen zu verlassen, empfiehlt es sich, cloudbasierte Alternativen in Betracht zu ziehen: Sie bieten neben höherer Flexibilität auch eine bessere Kontrolle der Richtlinien und Abwehrmethoden, mit denen vertrauliche Unternehmens- und Kundendaten geschützt werden.

Schutz oder Prävention? Ältere DLP-Systeme konzentrieren sich in erster Linie darauf, Datenverluste zu verhindern. Sie sind jedoch nicht in der Lage, vertrauliche Unternehmensdaten vor jeder externen und internen Bedrohung zu schützen. Mit den Lösungen der neuen Generation hingegen können Unternehmen nicht nur diese Gefahren abwehren, sondern sich auch schneller und effizienter von Datenlecks erholen.

Edge-Programmierbarkeit

Dank Edge Computing können Unternehmen die Anwendungsentwicklung an den Netzwerkrand verlagern. Dadurch finden die Rechenvorgänge so nah wie möglich am Endnutzer statt, sodass möglichst wenig Latenz auftritt, Serverressourcen geschont werden und die Bandbreitennutzung minimiert wird. Mit einer Serverless-Architektur können Firmen die Konfiguration und Verwaltung der Infrastruktur auslagern. Ihre Entwickler können sich dann auf die Programmierung und Bereitstellung von Anwendungen konzentrieren, bestehende Lösungen können endlich individuell konfiguriert werden und es entstehen neue Möglichkeiten, die Anwendungsentwicklung und -sicherheit zu optimieren.

Die Herausforderungen

Latenz und Kaltstarts: Da beim Serverless Computing Funktionen nach Bedarf ausgeführt werden, kann deren Aktivierung mehrere Sekunden dauern. Weil diese „Kaltstarts" zu unerwünschter Latenz führen können, müssen Unternehmen vorbeugende Maßnahmen treffen, etwa in Form von Alternativlösungen zur Minimierung der Dauer und Häufigkeit dieser Verzögerungen. Nur so können sie gewährleisten, dass die Nutzer keinen messbaren Rückgang der Web-Performance feststellen.

Fehlender globaler Maßstab: Geht es um Online-Geschäft mit einem breit verteilten Nutzerkreis, muss die Bereitstellung der Anwendungen in globalem Maßstab erfolgen. Durch die Verlagerung von Anwendungen an den Netzwerkrand können Unternehmen die Nutzer effizienter erreichen und gleichzeitig die Performance sowie die Bereitstellung der Applikationen verbessern.

Ineffizienter Ressourceneinsatz: Anwendungsentwicklung und kundenspezifische Programmierung sind aufwendige Prozesse, die dedizierte interne Ressourcen, ausreichend Serverkapazität bei einem zentralen Cloud Provider und genügend Zeit für Tests erfordern. Werden sie schlecht umgesetzt, kann sich die Erstellung von Prototypen deutlich verteuern und die Markteinführung neuer Anwendungen, die möglichst schnell erfolgen sollte, verzögert sich.

Was eine Edge Computing-Lösung bieten sollte

Vereinfachte Skalierbarkeit: Edge Computing dient dazu, die Latenz beim Endnutzer möglichst gering zu halten, indem die Inhalte vom Netzwerkrand aus bereitgestellt werden. Für Unternehmen ist es deshalb entscheidend, einen Anbieter zu wählen, der ein globales Netzwerk betreibt. Zum einen können Firmen dann ihre Reichweite erhöhen und dank einer schnelleren Website eine bessere Nutzererfahrung bieten; zum anderen vereinfacht sich durch die Ausführung des Codes am Netzwerkrand auch der Bereitstellungsprozess, sodass Kunden überall auf der Welt und nicht mehr nur in bestimmten Regionen erreicht werden können.

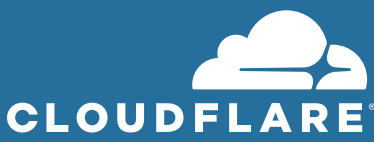
Verbesserte Entwicklungserfahrung: Die Entwicklung und Verbesserung von Anwendungen sollte auf einem schlanken Prozess basieren, der es Entwicklern ermöglicht, Code schnell und einfach zu implementieren – ohne dabei auf technische Betriebsteams angewiesen zu sein.

Geringere Infrastrukturkosten: Wenn Firmen eine Architektur ohne Server betreiben, entfallen die Kosten für ungenutzte Serverkapazitäten oder leerlaufende CPUs. Stattdessen können mehr Anfragebearbeitungen ins Netzwerk verlagert werden und es müssen nur noch die wirklich benötigten Ressourcen bezahlt werden, sodass die Infrastrukturkosten erheblich sinken.

Wie Cloudflare Unternehmen bei der Bereitstellung einer überragenden Online-Erfahrung unterstützt

Wer eine ausgezeichnete Online-Erfahrung bieten möchte, benötigt die richtige Sicherheits- und Performance-Strategie – eine Strategie, die nicht nur eine beschleunigte Bereitstellung von Inhalten ermöglicht, sondern auch die Zuverlässigkeit des Netzwerks gewährleistet und Websites vor Ausfällen, Datendiebstahl, Sicherheitslücken im Netzwerk und kritischen Angriffen schützt.

Cloudflare betreibt ein Netzwerk, das mehr als 200 Städte in über 90 Ländern auf der ganzen Welt umfasst, und stellt auf dieser Grundlage eine skalierbare und integrierte globale Cloud-Plattform bereit. Mit diesem Angebot unterstützt Cloudflare Unternehmen dabei, die Sicherheit, Performance und Zuverlässigkeit ihrer lokalen, cloudbasierten und SaaS-Anwendungen zu gewährleisten. Auf Cloudflare.com erfahren Sie, wie Sie Ihr Online-Geschäft mit Cloudflare schützen und absichern können.



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

REV: 200408