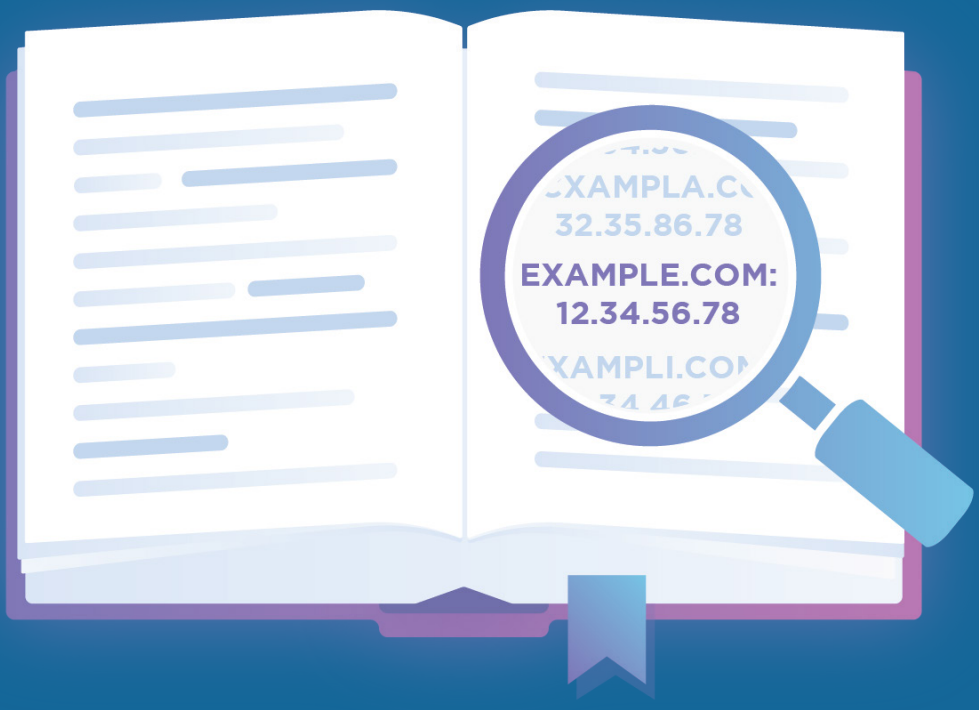
CLOUDFLARE®

DNS optimal einsetzen für eine verlässliche digitale Präsenz



+49 89 2620 4574 | enterprise@cloudflare.com | www.cloudflare.com/de-de/

I. Kurzfassung

Ihre Website ist nur so schnell wie Ihr DNS, unabhängig davon, wie die Website aufgebaut ist und wo sie gehostet wird.

Bei richtiger Verwendung und Implementierung kann das DNS die Sicherheit, Performance und Zuverlässigkeit einer Internetwebsite erheblich verbessern. Die DNS-Infrastruktur ist jedoch in hohem Maße anfällig für ein breites Spektrum von immer häufiger auftretenden Cyberangriffen, die die Performance beeinträchtigen oder DNS-Server zum Ausfall bringen. Diese Angriffe und die steigenden Erwartungen der Benutzer an die Performance und Verfügbarkeit von Websites bergen das Risiko, dass das DNS zum Single Point of Failure wird.

Robuste Sicherheit, Performance und Zuverlässigkeit einer Website erfordern eine integrierte DNS-Sicherheit und eine redundante DNS-Infrastruktur, die für Performance optimiert ist.

II. DNS-Sicherheit: Eine Schwachstelle in der Cybersicherheit von Unternehmen

Die heute verwendete DNS-Infrastruktur wurde in den 1980er Jahren entwickelt, als der Internetzugang auf Regierungsbehörden, Wissenschaftler und das Militär beschränkt war. Den Architekten des Systems ging es in erster Linie um Zuverlässigkeit und Funktionalität, nicht um Sicherheit.[1]

Infolgedessen sind DNS-Server in der heutigen Welt für viele verschiedene Angriffsarten anfällig, darunter Spoofing, Malware, DNS-Tunneling und DoS/DDoS-Angriffe. Diese Angriffe kommen immer häufiger vor and und werden immer kostspieliger. Der Global DNS Threat Report 2019 von IDC zeigt Folgendes auf:

- 82 % der Organisationen waren in den letzten zwei Jahren Opfer eines DNS-Angriffs
- Im Vergleich zum Vorjahr wurden bei allen Arten von Angriffen, von volumetrischen bis hin zu signalarmen Angriffen, signifikante Zunahmen gemeldet
- Die durchschnittlichen Kosten pro Angriff überstiegen im Jahr 2019 1 Million Dollar, 49 % mehr als im Jahr zuvor[2]

DNS-Angriffe werden häufig in Verbindung mit anderen Cyberangriffen eingesetzt und dienen oft dazu, das Sicherheitspersonal abzulenken. Verizon schätzt, dass DNS-Angriffe an etwa einem Drittel der Datenschutzverletzungen beteiligt sind.[3]

DNS für Sicherheit optimieren

Da die DNS-Bedrohungslandschaft so vielfältig ist, erfordert die wirksame Bekämpfung von DNS-Angriffen eine integrative Sicherheitsstrategie, die Folgendes umfasst:

- **Die Aktivierung von DNSSEC**, einer Reihe von Sicherheitsprotokollen, die DNS-Einträge mit kryptografischen Signaturen überprüfen. Indem sichergestellt wird, dass die Signatur einer Website mit dem Eintrag übereinstimmt, können DNS-Resolver den Ursprung der Daten, die vom DNS-Server gesendet werden, authentifizieren und so Spoofing verhindern.

- **Die Implementierung einer mehrschichtigen DDoS-Abwehr**, einschließlich Maßnahmen zur Filterung des Traffics wie Rate Limiting, White-/Blacklisting von IP-Adressen und Tracking von Verbindungen, um böswillige Anfragen zu blockieren und gleichzeitig legitimen Traffic zuzulassen. Die Bekämpfung von DDoS-Angriffen erhöht nicht nur die Sicherheit, sondern verbessert auch Zuverlässigkeit und Performance, da sie verhindert, dass böswilliger Traffic die DNS-Server überlastet.

- **Der Einsatz von DNS-Firewalls** (auch bekannt als DNS-Filterung und DNS-Blockierung), um den Zugriff von bekannten böswilligen Domains zu blockieren.

- **Die Aktivierung von DNS-Protokollierung**. Zusätzlich zur Warnung vor Hackern, die versuchen, Ihre DNS-Server zu manipulieren, bietet die DNS-Protokollierung Einblick in Probleme mit DNS-Abfragen oder -Updates.

- **Die Erzwingung von HTTPS**. Die Anforderung an Browser, Websites immer über HTTPS zu laden, verhindert Domain-Spoofing, indem jede Site mit einem SSL/TLS-Zertifikat authentifiziert wird.

- **Die Aktualisierung der DNS-Server**. Updates enthalten häufig wichtige Sicherheits-Patches.

III. DNS-Performance: Langsame DNS-Lookups bedeuten hohe Latenz

Wenn Benutzer auf ein Web-Asset zugreifen, fragen ihre Geräte einen DNS-Resolver ab, der den Domainnamen des Assets seiner IP-Adresse zuordnet und dann die korrekte IP-Adresse an das Gerät zurücksendet. Jedes Mal, wenn ein Benutzer auf eine neue Seite in seinem Browser zugreift, muss er mindestens einen DNS-Lookup durchführen; viele Seiten laden Assets von mehr als einer Domain, was mehrere Lookups erfordert. Dieser Prozess wird als DNS-Auflösung bezeichnet, und die Zeit, die zur Auflösung jeder angeforderten Domäne benötigt wird, summiert sich schnell. Aus diesem Grund ist die Optimierung der DNS-Auflösungsgeschwindigkeit entscheidend, um eine niedrige Latenz zu erreichen.

Nicht alle DNS-Anbieter sind für eine hohe Auflösungsgeschwindigkeit optimiert. Ein langsamer DNS-Provider könnte über 120 Millisekunden benötigen, um DNS-Abfragen zu aufzulösen.[4] Die schnellsten DNS-Provider lösen Abfragen in weniger als 20 Millisekunden auf: Cloudflare DNS beispielsweise benötigt im Durchschnitt weniger als 12 Millisekunden.[5]

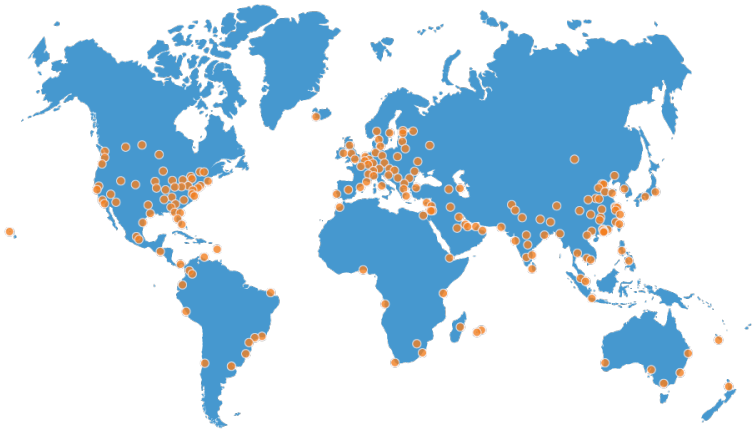
- Die Webbenutzer von heute verlangen, dass digitale Assets sofort geladen werden. Selbst kleine Probleme können spürbare Auswirkungen auf das Engagement und die Konversionsraten haben.
- Eine längere Websitelatenz von nur 100 bis 400 Millisekunden hat messbare Auswirkungen auf das Verbraucherverhalten.[6]
- Eine einzige zusätzliche Sekunde Ladezeit kann die Konversionsrate um 7 % senken.[7]
- Ungefähr die Hälfte der Mobilnutzer erwartet, dass Apps in zwei Sekunden oder weniger reagieren.[8]
- Google verwendet die Seitengeschwindigkeit als Ranking-Faktor für Desktop- und mobile Suchen.[9]

DNS für Performance optimieren

Hier sind einige Schritte, die Sie unternehmen können, um auf einem Markt, auf dem jede Millisekunde zählt, eine hohe Performance zu gewährleisten.

- **Verwendung von globalem geolokalisiertem Routing**. Pro 160 Kilometer geografischer Entfernung zwischen Endnutzern und digitalen Ressourcen wächst die Latenzzeit um etwa 0,82 Millisekunden.[10] Daher ist es wichtig, die Besucher zu einer DNS-Infrastruktur zu lenken, die sich in ihrem Teil der Welt befindet.
- **Bestimmung einer optimalen Time To Live (TTL)**. TTLs steuern indirekt das DNS-Resolver-Caching. Niedrige TTLs können die Performance verschlechtern, können aber die DNS-basierte Lastvertei lung unterstützen. Hohe TTLs verbessern die Performance, führen aber möglicherweise dazu, dass Benutzer zu einem zwischengespeicherten Server geleitet werden, der inzwischen ausgefallen ist. Da so viele Faktoren beteiligt sind, gibt es keinen universell optimalen TTL-Wert.
- **Verwendung von Anycast.** Suchen Sie nach einem DNS-Provider, der Anycast verwendet. Anycast ermöglicht es, dass mehrere global verteilte DNS-Nameserver dieselbe IP-Adresse anbieten. Dies verbessert die DNS-Auflösungsgeschwindigkeit und bietet außerdem einen nahtlosen DNS-Failover-Schutz.

Verschieben Sie Ihr DNS an den Netzwerkrand



11 ms
Durchschnittliche Geschwindigkeit für DNS-Lookup

<5 Sekunden
für weltweite DNS-Propagation

IV. DNS-Zuverlässigkeit: Redundanz verhindert Ausfallzeiten

Wenn Latenzprobleme nicht gelöst werden, führen sie im schlimmsten Fall dazu, dass Ihre Website ganz ausfällt. Die Kosten für Ausfallzeiten sind hoch und nehmen ständig zu. Im Jahr 2010 betrugen die durchschnittlichen Kosten für den Ausfall eines Rechenzentrums 5.617 USD pro Minute; bis zum Jahr 2016 war dieser Wert auf 8.851 USD gestiegen.[11]

Da die DNS-Zuverlässigkeit einen direkten und tiefgreifenden Einfluss auf den Erfolg eines Unternehmens hat, sollte das Ziel für jedes Unternehmen auf jeden Fall 100 % Verfügbarkeit sein. Das mag zwar überaus hoch klingen, aber es ist erreichbar, wenn das Unternehmen einen mehrgleisigen, auf Redundanz ausgerichteten Ansatz verfolgt.

DNS für Zuverlässigkeit optimieren

Performance und Zuverlässigkeit sind wie Kopf und Hals; sie sind eng miteinander verbunden und können ohne einander nicht existieren. Alle Maßnahmen, die Sie zur Verbesserung der Zuverlässigkeit ergreifen, werden auch die Performance steigern. Beispielsweise verringert die Verwendung von zwei DNS-Providern die Seitenladedauer, da die Nameserver standardmäßig den schnellsten DNS-Provider verwenden.

- **Duale (primärer/sekundärer) DNS-Provider**. Bei einer DNS-Einrichtung mit nur einem Provider erhalten alle Benutzer Antworten von dem Nameserver-Satz dieses Providers, wodurch Websites anfällig für Provider-Ausfälle bleiben. Durch das Hinzufügen eines zweiten DNS-Providers verdoppelt sich die Anzahl der Nameserver-Sätze, die für diese Domains verfügbar sind. Wenn der autoritative Provider nicht verfügbar ist, wird der Abfrage-Traffic automatisch an den Backup-Nameserver-Satz weitergeleitet.
- **Cloud-basiertes DNS**. Nur wenige Organisationen verfügen über die internen Ressourcen und Fachkenntnisse, um ihre eigenen DNS-Server zu verwalten. Die Auslagerung an einen Cloud-basierten DNS-Provider ermöglicht es Ihnen, Performance, Zuverlässigkeit und Sicherheit zu verbessern, Kosten zu minimieren und hauseigenes IT-Personal für die Arbeit an internen Projekten freizustellen.
- **Nameserver-Segmentierung**. Einige DNS-Provider gruppieren viele oder sogar alle ihre Kunden in demselben Nameserver-Eintrag. Wenn ein Kunde einen DDoS-Angriff erleidet, sind alle seine „Nachbarn“ stark betroffen. Stellen Sie sicher, dass Ihr DNS-Provider sein Netzwerk so segmentiert, dass nur eine kleine Anzahl von Kunden Nameserver-Einträge gemeinsam nutzen.
- **Ein sehr großes, globales Netzwerk von DNS-Knoten**. Das DNS-Netz Ihres Providers sollte eine große Anzahl global verteilter DNS-Knoten umfassen, sodass bei Ausfall eines Knotens der Traffic an jeden der verbleibenden Knoten weitergeleitet werden kann. Ein globales Netzwerk ermöglicht auch geografisch bedingtes Routing, was die Performance verbessert.
- **Globale und lokale Lastverteilung**. Abgesehen davon, dass einzelne Server nicht überlastet werden, leitet ein Load Balancer den Traffic auf die verbleibenden Server um, wenn ein Server ausfällt.

V. Schlussfolgerung

Auf dem schnelllebigen digitalen Markt von heute können ein paar Millisekunden Ladezeit über die Nutzererfahrung und die Konversionsrate entscheiden. Performance und Zuverlässigkeit von Websites hängen von der Geschwindigkeit der DNS-Auflösung ab, aber DNS-Server sind extrem anfällig für eine Vielzahl von Cyberangriffen. Die Gewährleistung einer sicheren, leistungsstarken DNS-Infrastruktur mit 100 % Verfügbarkeit erfordert einen integrierten Ansatz für Sicherheit, Zuverlässigkeit und Performance.

VI. Wie Cloudflare helfen kann

Cloudflares bietet einen autoritativen DNS-Service für Unternehmen, der viele dieser Best Practices widerspiegelt und die schnellste-Reaktionszeit, unerreichte Redundanz und erweiterte Sicherheit mit integrierter DDoS-Abwehr und DNSSEC bietet. Um mehr zu erfahren und mit einem Mitglied unseres Teams zu sprechen, besuchen Sie www.cloudflare.com/dns/.

Endnoten

1. ICANN, „DNSSEC – What Is It and Why Is It Important?“, https://www.icann.org/resources/pages/dnssec-what-is-it-why-important-2019-03-05-en. Letzter Zugriff am 27. Januar 2020.
2. IDC, „2019 Global DNS Threat Report“, https://www.efficientip.com/resources/idc-dns-threat-report-2019/. Letzter Zugriff am 26. Januar 2020.
3. Global Cyber Alliance, „The Economic Value of DNS Security“, https://www.globalcyberalliance.org/wp-content/uploads/Economic-Value-of-DNS-Security-GCA-2019.pdf. Letzter Zugriff am 27. Januar 2020.
4. Mann, Bill, „The Best DNS Servers for Speed and Privacy in 2019“, Blokt, https://blokt.com/guides/best-dns-servers. Letzter Zugriff am 27. Januar 2020.
5. „DNS Performance Analytics and Comparison“, DNSPerf, https://www.dnsperf.com/. Letzter Zugriff am 23. Juli 2019.
6. Brutlag, Jake, „Speed Matters“, Google AI Blog, https://ai.googleblog.com/2009/06/speed-matters.html. Letzter Zugriff am 27. Januar 2020.
7. Rodman, Tedd, „Marketing & Web Performance: How Site Speed Impacts Metrics“, Yotta, https://www.yottaa.com/marketing-web-performance-101-how-site-speed-impacts-your-metrics. Letzter Zugriff am 27. Januar 2020.
8. Dimensional Research, „Failing to Meet Mobile App User Expectations: A Mobile App User Survey“, https://techbeacon.com/sites/default/files/gated_asset/mobile-app-user-survey-failing-meet-user-expectations.pdf. Letzter Zugriff am 27. Januar 2020.
9. „Using page speed in mobile search ranking“, Google Webmaster Central Blog, https://webmasters.googleblog.com/2018/01/using-page-speed-in-mobile-search.html. Letzter Zugriff am 27. Januar 2020.
10. Sherman, Fraser, „Network Latency Milliseconds Per Mile“, Techwalla, https://www.techwalla.com/articles/network-latency-milliseconds-per-mile/ Letzter Zugriff am 27. Januar 2020.
11. Priceonomics Data Studio, „Quantifying the Staggering Cost of IT Outages“, https://priceonomics.com/quantifying-the-staggering-cost-of-it-outages/. Letzter Zugriff am 27. Januar 2020.