WHITEPAPER

DNS-Entwicklung – Verfügbarkeit und Ausfallsicherheit bei DDoS-Angriffen

Einführung

Edge DNS bietet Unternehmen einen autoritativen DNS-Dienst, über den sie Endnutzer mit ihren Websites und anderen Anwendungen verbinden können. Bei aller Aufmerksamkeit, die dem Thema Performance gewidmet wird, übersehen Unternehmen oft, wie wichtig auch die Faktoren der Verfügbarkeit und Ausfallsicherheit von DNS sind. Das gilt insbesondere, wenn DDoS-Angriffe Dienstausfälle und Verbindungsprobleme hervorzurufen versuchen. Akamai hat Edge DNS so entwickelt, dass es auch bei den größten DDoS-Angriffen verfügbar bleibt. Kunden profitieren von umfangreicher globaler Skalierung, einer segmentierten IP-Anycast-Architektur und verschiedenen DDoS-Kontrollen, einschließlich der Möglichkeit, bei Bedarf andere Akamai-Services zu nutzen. Edge DNS wird als verwalteter DNS-Dienst angeboten und bietet eine optimale Kombination aus Performance und Verfügbarkeit, sodass Unternehmen immer mit ihren Endnutzern in Verbindung bleiben können.

Hinweis zu Statistiken

Akamai hatte Edge DNS ursprünglich entwickelt, um autoritative DNS-Dienste zur Unterstützung seiner globalen CDN-Lösungen (Content Delivery Network) bereitzustellen. Im Laufe der Jahre konnte Akamai umfassende Kenntnisse darüber erwerben, wie sich die Skalierung und Verfügbarkeit einer derart umfangreichen DNS-Infrastruktur am besten sicherstellen lässt. Die allgemeinen Statistiken auf der rechten Seite geben einen Überblick über den Umfang der Plattform. Statistiken allein bieten jedoch keine zuverlässige Aussage über Verfügbarkeit und Ausfallsicherheit und sollten zusammen mit der Plattformarchitektur, spezifischen Funktionen zur DDoS-Abwehr und der Gesamtkapazität, die Akamai zum Schutz der Plattform vor Angriffen zur Verfügung steht, beurteilt werden.

Plattformstatistiken

- Tausende von Nameservern
- Über 1.000 Points of Presence
- Über 140 Städte
- Über 40 Länder

Beachten Sie, dass Akamai aus Sicherheitsgründen keine genauen Angaben zur Anzahl der Nameserver oder zu Menge, Standorten oder Größen der Points of Presence macht. Dies dient dem Schutz von Akamai und unserer Kunden vor Angreifern, die diese Informationen bei der Planung von Angriffen verwenden könnten.

Architektur

Wie Sie den Statistiken oben entnehmen können, hat Edge DNS einen größeren Umfang als die meisten autoritativen DNS-Dienste von Mitbewerbern auf dem Markt. Generelle Statistiken über die Anzahl der Server und Points of Presence oder die Gesamtkapazität des Netzwerks reichen jedoch nicht aus, um die Verfügbarkeit und Ausfallsicherheit einer globalen Plattform zu verstehen. Im Gegensatz zu anderen DNS-Lösungen, die sich bisher ausschließlich auf Performance konzentriert haben, hat Akamai Edge DNS speziell für Verfügbarkeit und Ausfallsicherheit bei DDoS-Angriffen entwickelt. Daneben wurde die Performance berücksichtigt. Die Lösung umfasst Redundanzen auf mehreren Ebenen einschließlich Nameservern, Points of Presence, Netzwerken und sogar segmentierten IP-Anycast-Clouds.

IP Anycast

Edge DNS besteht aus Tausenden von Nameservern, die an mehr als 1.000 Points of Presence bereitgestellt werden. Die Reaktion auf DNS-Abfragen erfolgt unter Verwendung eines IP-Anycast-Modells. IP Anycast leitet Abfragen von Endnutzern für die Auflösung zum nächstgelegenen Point of Presence weiter. IP Anycast bietet nicht nur eine schnellere Performance, sondern auch mehrere grundlegende Vorteile bezüglich Verfügbarkeit und Ausfallsicherheit. Daher wird IP Anycast von den meisten autoritativen DNS-Diensten genutzt:

- **Verfügbarkeit** – Mit IP Anycast können Nameserver an verschiedenen Netzwerkstandorten auf Abfragen an eine einzige IP-Adresse reagieren. Durch die Nutzung von IP Anycast bietet Edge DNS Unternehmen nicht nur eine DNS-Auflösung in mehreren Rechenzentren, sondern verbessert auch die Verfügbarkeit dank globaler Lastenverteilung. Darüber hinaus können einzelne physische Server oder ganze Points of Presence offline geschaltet werden, ohne dass die Fähigkeit zur Namensauflösung einer gesamten Domain beeinträchtigt wird.

- **Skalierbarkeit** – Die Infrastruktur von Edge DNS bietet Unternehmen umfangreiche Rechenressourcen, auf die sie sich bei der Reaktion auf große Mengen von DNS-Anfragen immer verlassen können. Edge DNS hat auch Zugriff auf eine beträchtliche zusätzliche Netzwerkkapazität an vielen seiner Points of Presence, da die Kapazität oft mit anderen Akamai-Diensten geteilt wird. Dies ermöglicht Edge DNS, wesentlich wirksamer auf DNS Floods und andere Arten von DDoS-Angriffen zu reagieren als ein eigenständiger DNS-Dienst.

- **Verteilung** – IP Anycast bietet nicht nur einen größeren Umfang, sondern auch eine Verteilung des Traffics auf mehrere Points of Presence und verschiedene Netzwerkstandorte. Durch sorgfältige Berücksichtigung der geografischen Standorte und Netzwerkbereitstellungen für diese Points of Presence können die Auswirkungen kleinerer Angriffe auf bestimmte Regionen oder Netzwerke eingedämmt und die Verfügbarkeit für Clientsysteme in anderen Bereichen aufrechterhalten werden.

Nicht nur Akamai verwendet IP Anycast. Da die Endnutzer-DNS-Abfragen von mehreren Nameservern aufgelöst werden können, verbessert IP Anycast die Verfügbarkeit dieser Namensauflösung für alle DNS-Dienste. Doch selbst mit IP Anycast wird die Ausfallsicherheit durch die Gesamtgröße der Plattform beschränkt, und große DDoS-Angriffe können eine cloudbasierte Plattform überfordern. Darüber hinaus haben bei einer weniger vielfältigen Architektur selbst kleinere Angriffe das Potenzial, DNS-Dienste in bestimmten geografischen Regionen zu unterbrechen, sodass sie für eine große Anzahl von Endnutzern nicht verfügbar sind und Nutzer auch auf Websites, über die sie eine Verbindung herstellen, nur eingeschränkt zugreifen können.

Edge DNS-Clouds

Um die Ausfallsicherheit bei Angriffen weiter zu verbessern, segmentiert Edge DNS die zugehörigen Nameserver und Points of Presence in mehrere IP-Anycast-Clouds. Eine Edge DNS-Cloud besteht aus dedizierten Nameservern und Points of Presence und bietet die erforderliche Netzwerkkapazität und Konnektivität. Alle Clouds funktionieren unabhängig voneinander, und Edge DNS kann in Bezug auf Verfügbarkeit, Umfang und Verteilung mehreren eigenständigen DNS-Anbietern entsprechen.

Die IP-Anycast-Clouds von Edge DNS repräsentieren eine Vielzahl von Architekturen. Die Clouds sind nicht identisch, doch alle sind weitgehend auf zwei wichtige Aspekte ausgerichtet: Performance und Verfügbarkeit.

- **Performance** – Eine Performance-Cloud kann weltweit mehr als 100 Points of Presence umfassen, die jeweils aus einer Gruppe von Nameservern bestehen. Wie in Abbildung 1 dargestellt, stellt eine Performance-Cloud kleine Cluster von Nameservern an vielen Standorten in der Nähe von Endnutzern und lokalen Internetdienstanbietern (ISPs) bereit, um schnellere Abfragezeiten und eine bessere reine Performance zu bieten. Der Nachteil ist, dass kleine Points of Presence naturgemäß weniger widerstandsfähig gegen DDoS-Angriffe sind, da sie über weniger Rechenressourcen und Netzwerkkapazität verfügen.
- **Verfügbarkeit** – Edge DNS umfasst viele Verfügbarkeits-Clouds. Wie in Abbildung 1 dargestellt, haben Verfügbarkeits-Clouds weniger Points of Presence, enthalten aber mindestens eine Ankerregion, die Hunderte von Nameservern in einem zentralen Rechenzentrum mit einer hohen dedizierten Netzwerkkapazität und Konnektivität über mehrere Netzwerke umfassen kann. Dank der Ankerregion wird die Verfügbarkeits-Cloud so groß, dass sie auf hohe DNS-Anfragevolumen und andere Spitzen im Netzwerktraffic reagieren kann. Verfügbarkeits-Clouds ergänzen Ankerregionen durch eine geringe Anzahl kleinerer Points of Presence und sorgen so für eine akzeptable Performance für Nutzer auf der ganzen Welt.

Abbildung 1: Edge DNS kombiniert mehrere DNS-Clouds mit verschiedenen Architekturen und bietet damit eine optimale Kombination aus Performance, Verfügbarkeit und Ausfallsicherheit bei DDoS-Angriffen.

Segmentierte Architektur

Edge DNS bietet im Vergleich zu anderen Anbietern, die autoritative DNS-Dienste in einer einzigen IP-Anycast-Cloud betreiben, eine grundlegend bessere Verfügbarkeit. Von den Vorteilen von IP Anycast profitieren alle Anbieter, denn es stellt die allgemeine Verfügbarkeit des Dienstes bei kleineren Angriffen sicher, die nur bestimmte geografische Regionen und nicht die gesamte Plattform betreffen. Doch selbst lokalisierte Ausfälle wirken sich auf Endnutzer in den betroffenen Regionen sowie auf Unternehmen aus, die über diesen Dienst die Verbindung mit diesen Nutzern herstellen. Auch können größere DDoS-Attacken mit Traffic, der durch Angriffe auf weltweite Systeme generiert wird, zu einem Ausfall der gesamten Plattform führen.

Aber dank zahlreicher und vielfältiger IP-Anycast-Clouds kann Edge DNS auch bei Verlust einer oder mehrerer Clouds weiter funktionieren. Dies bietet im Vergleich zu einer Architektur mit einer einzigen Cloud ein höheres Maß an Verfügbarkeit und Ausfallsicherheit bei DDoS-Angriffen. Darüber hinaus hat der Betrieb mehrerer IP-Anycast-Clouds den Vorteil, dass der Traffic in Unterabschnitte

der gesamten Plattform segmentiert wird. So werden die Auswirkungen selbst von massiven DDoS-Angriffen direkt abgeschwächt. Beispiel: Ein Angriff auf eine einzige IP-Anycast-Cloud von Edge DNS richtet sich gegen die physischen Nameserver und Points of Presence, die dieser bestimmten Cloud zugrundeliegen. Die segmentierte Architektur isoliert die anderen IP-Anycast-Clouds vor den Auswirkungen, sodass Edge DNS die Plattformverfügbarkeit in allen Regionen aufrechterhalten kann, selbst wenn einzelne Clouds oder Kunden Opfer eines DDoS-Angriffs werden.

Abbildung 2: Jeder Kunde von Edge DNS erhält Nameserver in einer einzigartigen Kombination aus Performance-Clouds und Verfügbarkeits-Clouds. Dies minimiert die Kollateralschäden bei Angriffen auf andere Kunden.

Neben der höheren Ausfallsicherheit der gesamten Plattform minimiert die segmentierte Architektur von Edge DNS auch das Risiko von Kollateralschäden für einzelne Kunden, wenn von anderen Kunden genutzte Nameserver angegriffen werden. Edge DNS weist jedem Kunden mehrere Edge DNS-Clouds zu, und zwar in einer einzigartigen Kombination aus Performance-Clouds und Verfügbarkeits-Clouds, die mit keinem anderen Kunden gemeinsam genutzt wird. Wie in Abbildung 2 gezeigt, wird durch diese Verteilung die Überschneidung der Nameserver und IP-Anycast-Clouds zwischen Kunden minimiert. Außerdem ist so sichergestellt, dass jeder Kunde über Nameserver verfügt, die auch dann verfügbar sind, wenn sich ein großer DDoS-Angriff speziell gegen die einem anderen Kunden zugewiesenen IP-Anycast-Clouds richtet.

Verwalten von Kundendelegierungen

Häufig erfolgen mehrere DDoS-Angriffe auf ein einzelnes Unternehmen über einen langen Zeitraum, und Akamai konnte bereits längere und andauernde Angriffe über mehrere Monate oder sogar Jahre beobachten. In dieser Situation bietet die segmentierte Architektur von Edge DNS Akamai mehr Flexibilität, damit Kunden, die nicht angegriffen werden, weiterhin möglichst wenig Auswirkungen erfahren. Wie in Abbildung 3 dargestellt, kann Akamai die Clouds eines einzelnen Kunden neu zuweisen und damit die Folgen von Angriffen bei Bedarf weiter einschränken.

Abbildung 3: Durch die Delegierung von Nameservern kann Akamai die Auswirkungen eines Angriffs weiter minimieren (im Vergleich zu Abbildung 2 oben), z. B. indem ein angegriffener Kunde aus einer bestimmten Cloud entfernt wird. So lassen sich Überschneidungen für Kunden, die nicht von dem Angriff betroffen sind, minimieren.

Akamai kann beispielsweise folgende Maßnahmen ergreifen:

- **Einen angegriffenen Kunden aus einer bestimmten Cloud entfernen** – Jeder Kunde, der Edge DNS nutzt, teilt IP-Anycast-Clouds mit anderen Kunden. Daher kann ein Angriff, der sich gegen alle Edge DNS-Clouds eines Kunden richtet, die Verfügbarkeit von Clouds beeinträchtigen, die auch anderen Kunden zugewiesen sind. Unter normalen Umständen wechseln rekursive Resolver automatisch zu leistungsfähigeren Clouds, aber bei dauerhaften Angriffen kann Akamai die IP-Anycast-Clouds des angegriffenen Kunden neu zuweisen und so die Verfügbarkeit für andere Kunden wiederherstellen, die nicht von dem Angriff betroffen sind.

- **Minimierung von Überschneidungen mit Kunden, die nicht von Angriffen betroffen sind** – In Ausnahmefällen nutzen mehrere Kunden mehr Edge DNS-Clouds gemeinsam als üblich. In diesem Fall ist es möglich, dass ein massiver Angriff auf einen einzelnen Kunden trotz der allgemeinen Verfügbarkeit des Dienstes messbare Auswirkungen auf die Performance für die anderen Kunden hat. Bei Bedarf kann Akamai die Clouds für die Kunden, die nicht von Angriffen betroffen sind, neu zuweisen, um die Überschneidung mit dem angegriffenen Kunden zu reduzieren oder zu beseitigen und die Performance für die Endnutzer wiederherzustellen.

Bereitstellung einer Vielzahl von Servern

In jeder Anycast-Cloud stellt Akamai physische Nameserver an verschiedenen Standorten bereit, um die allgemeine Ausfallsicherheit der entsprechenden Cloud zu erhöhen. Die unterschiedlichen Cloud-Standorte von Edge DNS bieten eine zusätzliche Ebene zur Segmentierung des Traffics zwischen den einzelnen Netzwerken, die Verfügbarkeit unter verschiedenen Umständen maximiert. Beispiele:

- **In Rechenzentren mit mehreren Netzwerken** – Für die Ausfallsicherheit bei DDoS-Angriffen kann die Vielfalt der Netzwerkkonnektivität ebenso wichtig sein wie die Kapazität. Große DDoS-Angriffe können Upstream-ISPs und andere Netzwerke vor dem Erreichen eines Rechenzentrums überlasten und zu Netzwerkengpässen und Serviceausfällen führen, auch wenn das Rechenzentrum selbst nicht betroffen ist. Um die Verfügbarkeit zu erhalten auch bei Angriffen weiterhin auf DNS-Abfragen von Endnutzern reagieren zu können, stellt Edge DNS-Nameserver in großen Rechenzentren bereit, die nicht nur eine hohe Kapazität, sondern auch Konnektivität über mehrere Netzwerke hinweg bieten.

- **ISP-Isolierung** – In vielen Fällen stellt Edge DNS Cluster von Nameservern direkt in den Netzwerken bestimmter ISPs bereit. Diese Nameserver übertragen ihre IP-Anycast-Daten häufig nur innerhalb dieser Netzwerke und lösen DNS-Abfragen nur für Endnutzer der jeweiligen ISPs auf. Mit dieser Praktik wird die Anzahl der Endnutzer eingeschränkt, die ein bestimmter Cluster von Nameservern bedienen kann. Und wenn eine IP-Anycast-Cloud Ziel eines externen Angriffs auf den entsprechenden ISP wird, bleibt die Verfügbarkeit für diese Nutzer erhalten. Ein Angreifer müsste über Systeme im Netzwerk dieses bestimmten ISP verfügen, um diese Nameserver zu sehen, und selbst dann reicht die verfügbare Kapazität oft aus, um die betroffene Cloud zu schützen.

- **Netzwerkvielfalt** – Kunden werden absichtlich verschiedenen Clouds zugewiesen. Einige umfassen Serverstandorte, die nur von bestimmten ISPs genutzt werden. Andere verfügen über eine größere Vielfalt an verbundenen Geräten. Diese Architektur stellt sicher, dass die rekursiven Nameserver eines bestimmten Kunden immer eine Verbindung zu einer verfügbaren Edge DNS-Cloud herstellen können.

- **Rechenzentren, die von weiteren Akamai-Diensten genutzt werden** – Akamai betreibt neben autoritativem DNS zahlreiche weitere Dienste und kann Edge DNS-Nameserver in Rechenzentren bereitstellen, die mehrere Dienste unterstützen. Wie im Folgenden näher erläutert, erhält Edge DNS bei der Reaktion auf große DDoS-Angriffe eine höhere Netzwerkkapazität, sowohl bei der dedizierten Netzwerkkapazität, als auch bei Public Peer-Vereinbarungen, die Akamai bereits für andere Dienste eigegangen ist.

DDoS-Kontrollen

Neben dem architektonischen Design umfasst Edge DNS mehrere Kontrollen, die die Auswirkungen von DDoS-Angriffen (sogenannten „DNS Floods") mindern. Bei DDoS-Angriffen wird eine große Menge an Traffic gesendet, der die Netzwerkverbindungen überlastet. Bei einer DNS Flood wird hingegen eine große Anzahl legitimer DNS-Abfragen generiert, um Rechen- und Speicherressourcen auf physischen Nameservern zu belegen und zu verhindern, dass sie auf Abfragen von tatsächlichen Endnutzern reagieren. Akamai schützt die Edge DNS-Plattform auf unterschiedliche Weise vor DNS Floods:

- **Skalierbarkeit** – Der autoritative DNS-Dienst von Akamai ist um ein Vielfaches umfangreicher als bei den DNS-Lösungen anderer Anbieter. Edge DNS nutzt Tausende von Nameservern, die an mehr als 1.000 Points of Presence weltweit bereitgestellt werden. IP Anycast bietet selbst zwar keine DDoS-Kontrolle, verteilt den Traffic des Angriffs jedoch auf verschiedene geografische Standorte und Netzwerke und stellt Edge DNS genügend physische Nameserver mit ausreichenden Rechen- und Speicherressourcen zur Verfügung. Damit wird der gewaltige Anstieg an DNS-Anfragen bewältigt.

- **Ratenbegrenzung** – Edge DNS bietet Funktionen zur Ratenbegrenzung und kann Anfragen von einzelnen IP-Adressen automatisch zurückweisen, wenn das Anfragenvolumen einen festgelegten Schwellenwert überschreitet. Die Ratenbegrenzung verhindert, dass ein großer Anstieg bei DNS-Anfragen Rechen- und Speicherressourcen auf physischen Nameservern belegt. Außerdem kann sie bei Angriffen nützlich sein, bei denen zwar eine hohe Anzahl von Anfragen generiert, aber eine relativ geringe Bandbreite belegt wird. Beachten Sie, dass die Funktionen zur Ratenbegrenzung von Edge DNS nicht vom Kunden konfiguriert werden können, sondern durch Algorithmen eingesetzt werden, die nur für die Edge DNS-Plattform gelten.

- **DNS-Whitelists** – Akamai stehen umfassende Einblicke in das Verhalten von rekursiven Resolvern zur Verfügung, die für ca. 95 % der legitimen DNS-Abfragen im Internet verantwortlich sind. Bei hoher Belastung kann Edge DNS ein positives Sicherheitsmodell verwenden und DNS-Anfragen auf eine Liste bekannter DNS Resolver beschränken.

Kapazität

DDoS-Kontrollen können zwar nützlich sein, um die Auswirkungen von DNS Floods zu mindern, doch bei anderen Arten von DDoS-Angriffen auf Netzwerkebene ist das hohe Trafficvolumen nur mithilfe einer ausreichend großen Netzwerkkapazität zu bewältigen. Das Risiko von volumetrischen Angriffen hat sich in den letzten Jahren drastisch erhöht, wobei die größten bekannten Angriffe mittlerweile eine Spitzenbandbreite von mehr als 1 Tbit/s überschreiten.

Akamai legt die Kapazität der Edge DNS-Plattform nicht offen, denn potenzielle Angreifer dürfen kein quantifizierbares Ziel kennen. Doch Akamai investiert kontinuierlich in jeden Aspekt des Plattformumfangs, um die Infrastruktur von Edge DNS zu erweitern und mit den Anforderungen neuer Kunden und dem Anstieg des Traffics im Internet Schritt zu halten. Als Cloud-Dienstanbieter kann Akamai Server schnell anderen Zwecken zuweisen und DNS-Kapazität in neuen Regionen bereitstellen. Akamai verfügt über eine beträchtliche verfügbare Kapazität, mit der sich hohes Trafficaufkommen bewältigen lässt, wobei der normale Traffic auf der Edge DNS-Plattform weniger als 1 % der Gesamtkapazität in Anspruch nimmt. Bei Bedarf kann Edge DNS auch Ressourcen von anderen Akamai-Plattformen nutzen, um DDoS-Angriffe abzuwehren.

Nutzung anderer Akamai-Plattformen

Die herkömmliche Methode zur Schätzung der Widerstandfähigkeit gegen einen DDoS-Angriff mit hoher Bandbreite anhand der Netzwerkkapazität funktioniert bei Edge DNS nicht, insbesondere, weil Edge DNS Ressourcen von anderen Akamai-Plattformen nutzen kann. Akamai ist mehr als ein DNS-Unternehmen und betreibt neben Edge DNS zahlreiche weitere Dienste. Unter den von Akamai betriebenen Diensten ist das autoritative DNS für den Betrieb anderer Dienste von entscheidender Bedeutung, weist hinsichtlich des gesamten Traffics jedoch ein geringes Volumen auf. Dies bietet mehrere Möglichkeiten, um die für Edge DNS verfügbare Kapazität bei Bedarf zu erweitern:

- **Kapazitätenübertragung aus dem CDN** – In vielen Fällen stellt Edge DNS Nameserver an denselben Points of Presence bereit, an denen sich auch Server befinden, die andere Akamai-Dienste im CDN von Akamai ausführen. Diese Points of Presence sind oft wesentlich umfangreicher, da sie Dienste unterstützen, die eine sehr viel größere Bandbreite nutzen. Dadurch kann Akamai bei Bedarf Kapazitäten aus dem CDN borgen. Dabei werden andere Dienste auf andere Points of Presence von Akamai verteilt und die gemeinsam genutzte Netzwerkkapazität ausschließlich für Edge DNS verfügbar gemacht, sodass große DDoS-Angriffe abgewehrt werden können.

- **Bereitstellung einer dedizierten Abwehrkapazität** – Neben dem autoritativem DNS und dem CDN betreibt Akamai einen separaten DDoS-Schutzdienst mit dedizierten Kapazitäten und Funktionen zur Abwehr von Angriffen. Zur Abwehr großer DDoS-Angriffe kann Akamai einzelne Nameserver-Delegierungen über seine Prolexic Scrubbing-Center zuweisen und damit diese dedizierte Kapazität und die DDoS-Abwehr-Tools nutzen. Dadurch werden die DDoS-Abwehrfunktionen der Prolexic Plattform, die Edge DNS vorgeschaltet ist, wirksam bereitgestellt. Auf diese Weise bleiben die Ressourcen von Edge DNS für die Bearbeitung legitimer Abfragen von Endnutzern verfügbar.

Mehrere DNS-Anbieter

Edge DNS bietet einen autoritativen DNS-Dienst, der um ein Vielfaches größer ist als der DNS-Dienst vieler Mitbewerber. Er umfasst eine widerstandsfähige Architektur mit zahlreichen segmentierten IP-Anycast-Clouds und bietet die Möglichkeit, zusätzliche Kapazität und die Funktionen anderer Akamai-Dienste zum Schutz vor DDoS-Angriffen zu nutzen. Mit diesen Vorteile von Edge DNS gewährleisten wir die nötige Verfügbarkeit und Ausfallsicherheit, auf die Sie sich bei Akamai als einzigem autoritativem DNS-Anbieter Ihres Unternehmens verlassen können. Einige Unternehmen entscheiden sich jedoch möglicherweise für die Implementierung von Edge DNS neben ihrer bereits vorhandenen Lösung. Mit einer anbieterübergreifenden Implementierung können Unternehmen ihre bestehenden Verfahren zur DNS-Verwaltung beibehalten und gleichzeitig ihre primäre DNS-Lösung durch die zusätzliche Verfügbarkeit und Redundanz von Edge DNS ergänzen.

Implementierungsoptionen

Edge DNS unterstützt verschiedene Optionen zur Implementierung in Umgebungen mit mehreren Anbietern:

- **Herkömmliches sekundäres DNS** – Unternehmen mit einem vorhandenen DNS-Anbieter können Edge DNS als sekundären Dienst implementieren, um ihre primäre DNS-Lösung zu erweitern. Das Unternehmen verwaltet die DNS-Datensätze weiterhin beim primären Anbieter und verwendet Zonenübertragungen oder Edge DNS-APIs, um Edge DNS automatisch zu aktualisieren. Sowohl die primäre als auch die sekundäre Lösung können Abfragen von Endnutzern verarbeiten und bieten so zusätzliche Verfügbarkeit.

- **Hidden Master** – Akamai empfiehlt diese Implementierungsoption für Unternehmen, die DNS-Datensätze weiterhin mit einer internen DNS-Lösung verwalten möchten. Dank der Hidden-Master-Vereinbarung kann Edge DNS (als einziger sekundärer DNS-Anbieter oder einer von mehreren Anbietern) auf Endnutzerabfragen reagieren, ohne die interne Lösung DDoS-Angriffen auszusetzen. Das Unternehmen verwaltet die DNS-Datensätze weiterhin beim primären Anbieter und verwendet Zonenübertragungen oder Edge DNS-APIs, um Edge DNS automatisch zu aktualisieren.

- **Doppeltes primäres System** – Eine Variante des Hidden-Master-Konzepts. Einige Cloud-Dienstanbieter nutzen die herkömmliche Zonenübertragungsfunktion nicht mehr und verlangen von Kunden, dass sie ihre APIs und andere Anwenderschnittstellen für Zonendatensatzänderungen verwenden. Auch für diese Methode kann Edge DNS genutzt werden, wenn es im Primärmodus konfiguriert ist und die Edge DNS-Clouds autoritativ hinzugefügt werden.

Sekundäre Lösung für Verfügbarkeit

Wenn Edge DNS als sekundäre DNS-Lösung implementiert wird, stellen die Zonenaktualisierungen der primären DNS-Lösung sicher, dass es korrekt auf Endnutzerabfragen reagiert. In der Regel haben die Zonendateien der sekundären DNS-Lösung die Gültigkeitsdauer (Time to Live, TTL), die im Feld mit dem Ablaufzeitpunkt des Eintrags „Start of Authority" (Beginn der Zuständigkeit) festgelegt ist. Ein DDoS-Angriff, der einen Ausfall der primären Lösung verursacht, kann auch dazu führen, dass die sekundäre Lösung nicht mehr auf Abfragen reagiert, wenn der Ausfall die Gültigkeitsdauer überschreitet. Edge DNS schützt vor diesem Szenario, indem (1) die Zonendatei auch nach dem Ablauf der Gültigkeitsdauer beibehalten wird und (2) weiterhin auf DNS-Abfragen reagiert wird, solange die DNS-Registrierung auf Edge DNS verweist. Dadurch wird die zusätzliche Verfügbarkeit der sekundären DNS-Lösung sichergestellt, selbst wenn die primäre Lösung nicht verfügbar ist.

Fazit

Die Spitzenbandbreite des bisher größten bekannten DDoS-Angriffs übersteigt bereits 1 Tbit/s. Bei einem solchen Ausmaß lässt sich die Ausfallsicherheit bei solchen Angriffen nicht mehr akkurat beurteilen, indem man die gesamte Bandbreite berechnet, die für einen cloudbasierten Service zur Verfügung steht. Selbst kleinere Angriffe können zu Ausfällen auf regionaler Ebene führen. Um 100%ige Verfügbarkeit für Kunden sicherzustellen, nutzt Edge DNS einen Ansatz mit mehreren Ebenen, der folgende Komponenten umfasst:

- Eine gewaltige Größe und eine globale Präsenz mit Nameservern und Points of Presence, deren Umfang die Dienste vieler Mitbewerber um ein Vielfaches übersteigt
- Eine widerstandsfähige Architektur mit zahlreichen segmentierten IP-Anycast-Clouds, mit denen sich die Auswirkungen von Angriffen abfangen und Kollateralschäden für andere Kunden sowie die gesamte Plattform verhindern lassen
- Eine verwaltete Reaktion auf DDoS-Angriffe, einschließlich der Möglichkeit, DDoS-Kontrollen bereitzustellen oder Kundendelegierungen nach Bedarf neu zuzuweisen
- Die mögliche Nutzung anderer Akamai-Dienste, wie Akamai CDN und Prolexic-DDoS-Schutz, die mehr Kapazität bereitstellen und sowohl großen als auch kleinen DDoS-Angriffen standhalten

Das autoritative DNS ist ein unternehmenskritischer Dienst, der Endnutzer auf der ganzen Welt mit der Online-Präsenz von Unternehmen verbindet. Als einziger autoritativer DNS-Anbieter oder zusammen mit einer vorhandenen DNS-Lösung bietet Edge DNS Unternehmen die Verfügbarkeit, die sie benötigen, um den globalen Zugriff auf ihre Website und andere internetbasierte Anwendungen sicherzustellen.