AWS – Best Practices für DDoS-Resilienz

Juni 2016

Hinweise

Dieses Dokument wird nur zu Informationszwecken zur Verfügung gestellt. Es stellt das aktuelle Produktangebot und die Praktiken von AWS zum Erstellungsdatum dieses Dokuments dar. Änderungen vorbehalten. Kunden sind für ihre eigene unabhängige Einschätzung der Informationen in diesem Dokument und jedwede Nutzung der AWS-Services verantwortlich. Jeder Service wird „wie besehen“ ohne Gewähr und ohne Garantie jeglicher Art, weder ausdrücklich noch impliziert, bereitgestellt. Dieses Dokument gibt keine Garantien, Gewährleistungen, vertragliche Verpflichtungen, Bedingungen oder Zusicherungen von AWS, seinen Partnern, Zulieferern oder Lizenzgebern. Die Verantwortung und Haftung von AWS gegenüber seinen Kunden werden durch AWS-Vereinbarungen geregelt. Dieses Dokument ist weder ganz noch teilweise Teil der Vereinbarungen von AWS mit seinen Kunden und ändert diese Vereinbarungen auch nicht.

Inhalt

Kurzbeschreibung

Dieses Whitepaper wendet sich an Kunden, die die Resilienz ihrer Anwendungen auf Amazon Web Services (AWS) gegen DDoS-Angriffe (Distributed Denial of Service) steigern möchten. Es enthält eine Übersicht über DDoS-Angriffe, der von AWS bereitgestellten Funktionen, Vermeidungstechniken und einer DDoS-resilienten Referenzarchitektur, die als Anleitung für den Schutz der Anwendungsverfügbarkeit verwendet werden kann.

Einführung

Das Dokument richtet sich an IT-Entscheidungsträger und Sicherheitspersonal, die mit den grundlegenden Konzepten im Bereich Netzwerk, Sicherheit und AWS vertraut sind. Jeder Abschnitt verfügt über Links zur AWS-Dokumentation, in der weitere Details zu den bewährten Methoden oder Funktionen zu finden sind. Außerdem können Sie die AWS re:Invent-Konferenzsitzungen SEC307 – Aufbau einer Architektur mit DDoS-Resilienz[1] und SEC306 – Schutz gegen DDoS-Angriffe[2] ansehen, in denen Sie weitere Informationen erhalten.

DDoS-Angriffe

Bei einem DoS-Angriff (Denial of Service) kann die Verfügbarkeit einer Website oder Anwendung für Endbenutzer eingeschränkt werden. Dazu bedienen sich die Angreifer verschiedener Techniken, die Netzwerk- oder andere Ressourcen belasten und den Zugriff durch rechtmäßige Endbenutzer unterbrechen. Im einfachsten Fall wird ein DoS-Angriff von einem einzelnen Angreifer von einer einzelnen Quelle aus gegen ein Ziel ausgeführt (siehe Abbildung 1).

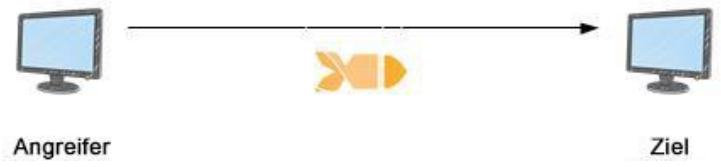

Abbildung 1: Diagramm eines DoS-Angriffs

Bei einem DDoS-Angriff (Distributed Denial of Service) verwendet ein Angreifer mehrere Hosts, die durch mehrere Mithelfer gefährdet oder kontrolliert werden, um einen Angriff gegen ein Ziel durchzuführen. Jeder der Mithelfer oder gefährdeten Hosts nimmt an dem Angriff teil und generiert eine Unmenge an Paketen oder Anforderungen, um das vorgesehene Ziel zu überlasten (siehe Abbildung 2).

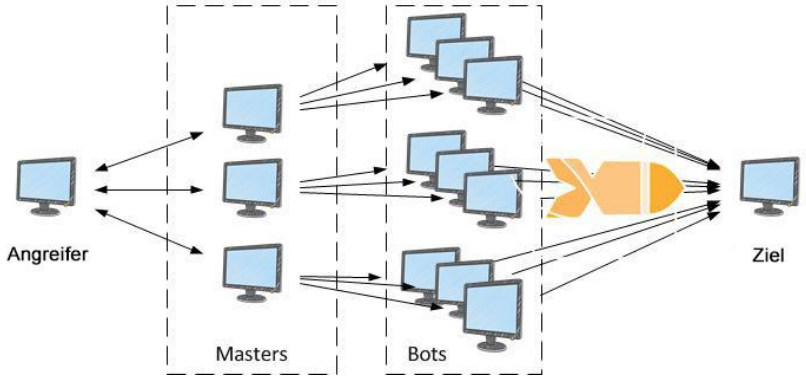

Abbildung 2: Diagramm eines DDoS-Angriffs

DDoS-Angriffe geschehen auf den am meisten verwendeten Ebenen 3, 4, 6 und 7 des OSI-Modells (Open Systems Interconnection), die in Tabelle 1 beschrieben sind. Angriffe auf die Ebenen 3 und 4 entsprechen der Netzwerk- und Transportebene des OSI-Modells: In diesem Dokument werden sie als Angriffe auf die Infrastrukturebene bezeichnet. Angriffe auf die Ebenen 6 und 7 entsprechen der Darstellungs- und Anwendungsebene des OSI-Modells: Sie werden in diesem Dokument als Angriffe auf die Anwendungsebene bezeichnet.

#	Ebene	Einheit	Beschreibung	Vektorbeispiele
7	Anwendung	Daten	Netzwerkverfahren zur Anwendung	HTTP-Floods, DNS-Abfrage-Floods
6	Darstellung	Daten	Darstellung und Verschlüsselung von Daten	SSL-Missbrauch
5	*Sitzung*	*Daten*	*Kommunikation zwischen Hosts*	–
4	Transport	Segmente	Durchgängige Verbindungen und Zuverlässigkeit	SYN-Floods
3	Netzwerk-	Pakete	Festlegung von Pfaden und logische Adresszuweisung	UDP-Reflexionsangriffe
2	*Data Link*	*Frames*	*Physische Adresszuweisung*	–
1	*Physische*	*Bits*	*Medien-, Signal- und binäre Übertragung*	–

Tabelle 1: OSI-Modell (Open Systems Interconnection)

Diese Unterscheidung ist wichtig, da auf diese Ebenen andere Arten von Angriffen ausgerichtet sind und somit andere Techniken für den Aufbau von Resilienz angewendet werden.

Angriffe auf die Infrastrukturebene

Die meisten DDoS-Angriffe – UDP-Reflexionsangriffe (User Datagram Protocol) und SYN-Floods (Synchronize-Floods) – erfolgen auf die Infrastrukturebene. Ein Angreifer kann mit diesen Methoden entweder große Datenverkehrsmengen erzeugen, die die Kapazität eines Netzwerks oder Systems, wie z. B. einen Server, eine Firewall, ein IPS oder einen Load Balancer, überfluten können. Diese Angriffe haben eindeutige Signaturen, anhand derer sie leichter zu erkennen sind. Für eine effektive Vermeidung dieser Angriffe müssen die Netzwerk- oder Systemressourcen die Datenverkehrsmenge übersteigen, die vom Angreifer erzeugt wird.

UDP ist ein zustandsloses Protokoll, mit dem der Angreifer die Quelle einer Anforderung vortäuschen kann, die an einen Server gesendet wurde und eine längere Antwort hervorruft. Der Verstärkungsfaktor – das Verhältnis der Anforderungsgröße zur Antwortgröße – richtet sich nach dem verwendeten Protokoll, beispielsweise DNS (Domain Name System), NTP (Network Time Protocol) oder SSDP (Simple Service Discovery Protocol). Der durchschnittliche Verstärkungsfaktor für DNS kann z. B. in dem Bereich 28-54 liegen. Das bedeutet, dass ein Angreifer eine Anforderungsnutzlast von 64 Byte an einen DNS-Server senden und unerwünschten Datenverkehr von mehr als 3400 Byte generieren kann. Dieses Konzept ist in Abbildung 3 dargestellt.

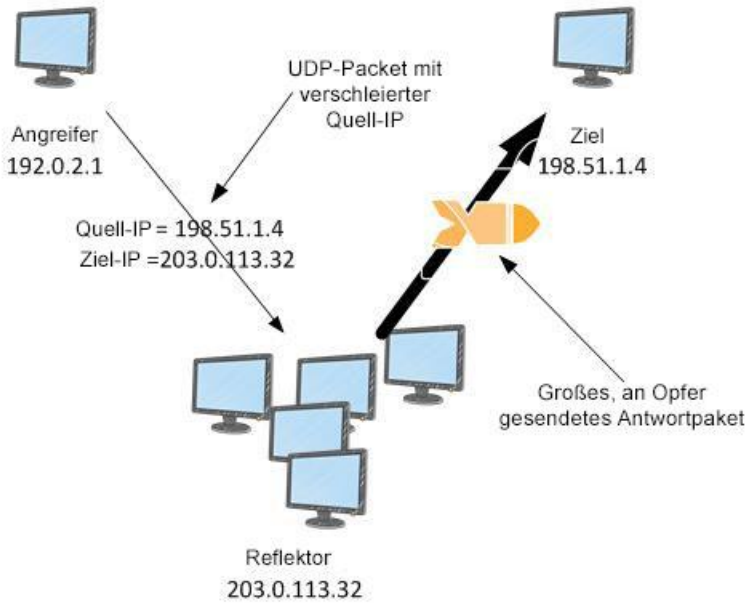

Abbildung 3: UDP-Reflexionsangriff

SYN-Floods können sich im Bereich von mehreren zehn Gbit/s bewegen, doch das Ziel eines solchen Angriffs besteht darin, die verfügbaren Ressourcen eines Systems zu überlasten und damit dafür zu sorgen, dass Verbindungen im halboffenen Zustand bleiben. Wenn ein Endbenutzer eine Verbindung zu einem TCP-Service, wie z. B. einem Webserver, herstellt, sendet der Client ein SYN-Paket (siehe Abbildung 4). Der Server sendet SYN-ACK zurück und der Client sendet ACK zurück, womit ein Three-Way-Handshake abgeschlossen wird.

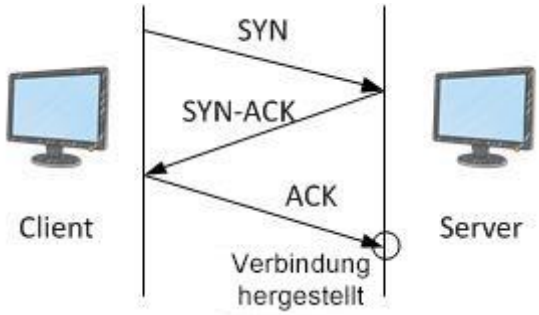

Abbildung 4: 3-Way-Handshake (SYN)

Bei einem SYN-Flood wird der ACK niemals zurückgesendet und der Server muss auf die Antwort warten. Dies kann verhindern, dass neue Benutzer eine Verbindung zum Server aufbauen.

Angriffe auf die Anwendungsebene

Weniger häufig ist ein Angriff auf die Anwendung selbst ausgerichtet. In diesem Fall wird von einem Angriff auf die Ebene 7 oder auf die Anwendungsebene gesprochen. Diese Angriffe unterscheiden sich von Angriffen auf die Infrastrukturebene, da der Angreifer versucht, bestimmte Funktionen einer Anwendung übermäßig auszuführen, damit sie nicht mehr verfügbar sind. In einigen Fällen kann dies durch sehr niedrige Anforderungsmengen erreicht werden, die keine große Menge an Netzwerkdatenverkehr erzeugen. Damit wird der Angriff schwieriger zu erkennen und zu vermeiden. Beispiele für Angriffe auf die Anwendungsebene sind HTTP-Floods, Cache-Busting-Angriffe und XML-RPC-Floods in WordPress.

Bei einem HTTP-Flood sendet der Angreifer HTTP-Anforderungen, die scheinbar von einem echten Benutzer der Webanwendung stammen. Einige HTTP-Floods zielen auf eine bestimmte Ressource ab, während komplexere HTTP-Floods versuchen, menschliches Verhalten nachzuahmen. Damit kann es schwer werden, allgemeine Vermeidungstechniken wie die Einschränkung der Anforderungsrate einzusetzen. Cache-Busting-Angriffe sind HTTP-Floods, bei denen Variationen der Abfragezeichenfolge verwendet werden, um CDN-Caching (Content Delivery Network) zu umgehen, das zu Abrufen vom Ursprungs-Server führt und damit weitere Belastung auf dem Ursprungs-Webserver erzeugt.

Bei einem XML-RPC-Flood in WordPress, der auch WordPress-Pingback-Flood genannt wird, kann ein Angreifer die API-Funktion XML-RPC einer Website missbrauchen, die mit der Content-Management-Software der Marke WordPress gehostet wird, um eine Flut von HTTP-Anforderungen zu erzeugen. Mit der Pingback-Funktion kann eine auf WordPress gehostete Website (Website A) eine andere WordPress-Website (Website B) benachrichtigen, dass Website A einen Link auf Website B erstellt hat. Daraufhin versucht Website B, Website A abzurufen, um das Vorhandensein des Links zu überprüfen. Bei einem Pingback-Flood missbraucht der Angreifer diese Funktion, damit Website B Website A angreift. Diese Art von Angriff hat eine eindeutige Signature, da "WordPress" als "User-Agent" im HTTP-Anforderungsheader vorhanden sein müsste.

Angriffe auf die Anwendungsebene können außerdem auf DNS-Services (Domain Name System) ausgerichtet sein. Bei den meisten Angriffen dieser Art handelt es sich um DNS-Abfrage-Floods, bei denen ein Angreifer viele wohlgeformte DNS-Abfragen nutzt, um die Ressourcen eines DNS-Servers zu überlasten. Solche Angriffe können auch eine Cache-Busting-Komponente enthalten, bei der der Angreifer die Zeichenfolge der Subdomain zufällig festlegt, um den lokalen DNS-Cache eines bestimmten Resolvers zu umgehen. Folglich wird der Resolver bei einem Angriff gegen den autoritativen DNS-Server zwangsläufig verwendet.

Bei Webanwendungen, die über SSL (Secure Sockets Layer) bereitgestellt werden, kann ein Angreifer den SSL-Verhandlungsprozess angreifen. SSL ist rechenintensiv, weshalb ein Angreifer die Verfügbarkeit des Servers beeinträchtigen kann, indem er unlesbare Daten sendet. Bei anderen Variationen dieses Angriffs ist ein Angreifer beteiligt, der das SSL-Handshake durchführt, die Verschlüsselungsmethode jedoch durchgängig erneut verhandelt. Desgleichen kann ein Angreifer Serverressourcen überlasten, indem er viele SSL-Sitzungen öffnet und schließt.

Techniken zur Risikovermeidung

Die AWS-Infrastruktur ist mit DDoS-Resilienz konzipiert und wird von DDoS-Vermeidungssystemen unterstützt, die übermäßigen Datenverkehr automatisch erkennen und filtern können. Zum Schutz der Verfügbarkeit der Anwendung muss eine Architektur implementiert werden, mit der Sie diese Funktionen nutzen können.

Einer der häufigsten Anwendungsfälle für AWS ist eine Webanwendung, die den Benutzern statischen und dynamischen Inhalt über das Internet bereitstellt. In Abbildung 5 ist eine DDoS-resiliente Referenzarchitektur dargestellt, die häufig bei Webanwendungen zum Einsatz kommt.

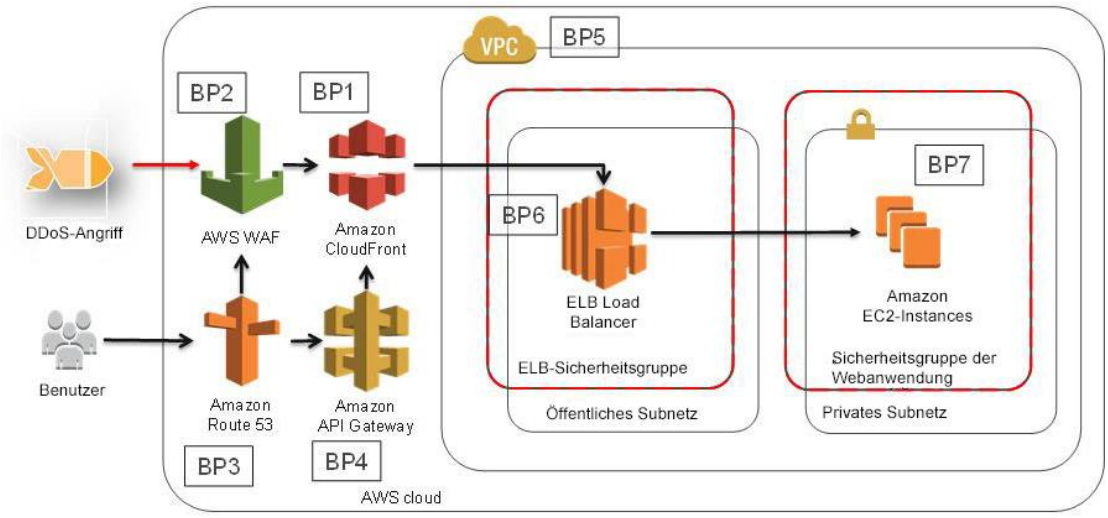

Abbildung 5: Referenzarchitektur mit DDoS-Resilienz

Diese Referenzarchitektur umfasst viele AWS-Services, mit denen Sie die Widerstandsfähigkeit einer Webanwendung gegen DDoS-Angriffe verbessern können. Zur besseren Auffindbarkeit sind die bewährten Methoden in dieser Architektur, die in diesem Dokument erläutert werden, nummeriert. So wird z. B. auf einen Abschnitt, in dem die von Amazon CloudFront erläutert werden, mit einem Indikator für bewährte Methoden (z. B. BP1) verwiesen. Eine Zusammenfassung dieser Services und Funktionen, die bereitgestellt werden können, finden Sie in Tabelle 2.

	AWS-Edge-Standorte			**AWS-Regionen**		
	Amazon CloudFront mit AWS WAF (BP1, BP2)	Amazon API Gateway (BP4)	Amazon Route 53 (BP3)	Elastic Load Balancing (BP6)	Amazon VPC (BP5)	Amazon EC2 mit Auto Scaling (BP7)
Milderung von Angriffen auf die Ebene 3 (z. B. UDP-Reflexion)	✓	✓	✓	✓	✓	
Milderung von Angriffen auf die Ebene 4 (z. B. SYN-Flood)	✓	✓	✓	✓		
Milderung von Angriffen auf die Ebene 6 (z. B. SSL-Flood)	✓	✓	–	✓		
Verringern der Angriffsfläche	✓	✓	✓	✓	✓	
Skalierung zum Abwehren von Datenverkehr auf der Anwendungsebene	✓	✓	✓	✓		✓
Milderung von Angriffen auf die Ebene 7 (Anwendungsebene)	✓	✓	✓			
Geografische Isolierung und Streuung von übermäßigem Datenverkehr und größeren DDoS-Angriffen	✓	✓	✓			

Tabelle 2: Zusammenfassung der bewährten Methoden

Mit Services, die in AWS-Regionen verfügbar sind, wie z. B. Elastic Load Balancing und Amazon Elastic Compute Cloud (EC2) können Sie DDoS-Resilienz aufbauen und für Skalierung sorgen, um unerwartete Datenverkehrsmengen innerhalb einer bestimmten Region zu vermeiden. Mit Services, die in AWS-Edge-Standorten verfügbar sind, wie Amazon CloudFront, AWS WAF, Amazon Route 53 und Amazon API Gateway, können Sie ein globales Netzwerk von Edge-Standorten nutzen, die für größere Fehlertoleranz in der Anwendung und bessere Skalierung für die Verwaltung größerer Datenverkehrsmengen sorgen. In den folgenden Abschnitten werden Vorteile dieser Services beim Aufbau größerer Widerstandsfähigkeit gegen DDoS-Angriffe auf die Infrastruktur- und die Anwendungsebene beschrieben.

Verteidigung der Infrastrukturebene (BP1, BP3, BP6, BP7)

In einer herkömmlichen Rechenzentrumsumgebung können Sie DDoS-Angriffe auf die Infrastrukturebene mit Techniken, wie dem Overprovisioning von Kapazität, der Bereitstellung von DDoS-Vermeidungssystemen oder dem Scrubbing von Datenverkehr mithilfe von DDoS-Vermeidungsservices vermeiden. Mit AWS können Sie die Architektur einer Anwendung so gestalten, dass eine Skalierung möglich ist und größere Datenverkehrsmengen ohne kapitalintensive Investitionen oder unnötige Komplexität abgewehrt werden können. Zu den wichtigen Überlegungen bei der Vermeidung volumetrischer DDoS-Angriffe gehört die Verfügbarkeit von Übertragungskapazität und -diversität sowie der Schutz von AWS-Ressourcen wie Amazon EC2-Instances gegen Datenverkehr eines Angriffs.

Instance-Größe (BP7)

Viele Kunden von AWS nutzen Amazon EC2, um die Rechenkapazität anpassen zu können. Damit wird es bei veränderten Anforderungen schnell möglich, nach oben oder nach unten zu skalieren. Wenn Sie der Anwendung bei Bedarf Instances hinzufügen, können Sie horizontal skalieren. Durch die Nutzung größerer Instances erzeugen Sie eine vertikale Skalierung. Einige Instance-Typen unterstützen Funktionen, wie 10-Gigabit-Netzwerkschnittstellen und Enhanced Networking, mit denen Sie größere Mengen an Datenverkehr bewältigen können.

Mit 10-Gigabit-Netzwerkschnittstellen kann jede einzelne Instance eine größere Datenverkehrsmenge unterstützen. Damit wird die Überlastung von Schnittstellen für jeglichen Datenverkehr vermieden, der an der Amazon EC2-Instance ankommt. Instances, die Enhanced Networking unterstützen, bieten im Vergleich zu herkömmlichen Implementierungen eine höhere E/A-Leistung und eine niedrigere CPU-Auslastung. Damit kann die Instance Datenverkehr mit größeren Paketvolumes besser bewältigen. In AWS sind Sie nicht für die Kosten eingehenden Datenverkehrs verantwortlich.

Weitere Informationen zu Amazon EC2-Instances, die 10-Gigabit-Netzwerkschnittstellen und Enhanced Networking unterstützen, finden Sie unter Amazon EC2-Instance-Typen[3]. Weitere Informationen zur Aktivierung von Enhanced Networking finden Sie unter Aktivieren von Enhanced Networking für Linux-Instances in einer VPC[4].

Auswahl der Region (BP7)

Viele AWS-Services, wie Amazon EC2, sind an zahlreichen Standorten auf der ganzen Welt verfügbar. Diese geografisch getrennten Bereiche werden als AWS-Regionen bezeichnet. Bei der Auswahl der Architektur einer Anwendung können Sie je nach Ihren eigenen Anforderungen eine oder mehrere Regionen auswählen. Dabei spielen allgemeine Überlegungen wie die Leistung, die Kosten und die Datensouveränität eine Rolle. AWS stellt in jeder Region Zugriff auf einen eindeutigen Satz an Internetverbindungen und Peering-Beziehungen bereit, mit denen optimale Latenz und optimaler Durchsatz für die Endbenutzer erzielt werden, die sich an ähnlichen Standorten befinden.

Außerdem ist die Auswahl der Region auch mit Blick auf die DDoS-Resilienz von Bedeutung. Viele Regionen befinden sich näher an großen Internetknoten. Viele DDoS-Angriffe werden international abgesetzt. Daher ist es hilfreich, sich in der Nähe von Internetknoten zu befinden, wo internationale Anbieter und große Peers häufig eine starke Präsenz pflegen. Damit können Sie verhindern, dass Endbenutzer die Anwendung erreichen, wenn größere Datenverkehrsmengen übertragen werden.

Weitere Informationen zur Auswahl der Region finden Sie unter Regionen und Availability Zones[5]. Wenn Sie Fragen zu den Eigenschaften der einzelnen Regionen haben, wenden Sie sich an das Team Ihres AWS-Kontos. Hier erhalten Sie Unterstützung für eine fundierte Entscheidung.

Load Balancing (BP6)

Größere DDoS-Angriffe können die Größe einer einzelnen Amazon EC2-Instance übersteigen. Sie sollten verschiedene Optionen für das Load Balancing von übermäßigen Datenverkehr in Betracht ziehen, um diese Angriffe zu vermeiden. Mit Elastic Load Balancer (ELB) können Sie das Risiko einer Überlast der Anwendung reduzieren, da der Datenverkehr über viele Backend-Instances verteilt wird. ELB kann automatisch skaliert werden, womit Sie große Mengen unerwarteten Datenverkehrs wie Flash Crowds oder DDoS-Angriffe bewältigen können.

ELB akzeptiert nur gültige TCP-Verbindungen. Das bedeutet, dass viele allgemeine DDoS-Angriffe, wie SYN-Floods oder UDP-Reflexionsangriffe, in ELB nicht angenommen und damit nicht an die Anwendung weitergeleitet werden. Wenn ELB einen solchen Angriff erkennt, wird es automatisch skaliert, um den zusätzlichen Datenverkehr abzuwehren. Dennoch entstehen Ihnen keine zusätzlichen Kosten.

Weitere Informationen zur Lastenverteilung und zum Schutz von Amazon EC2-Instances mit ELB finden Sie unter Erste Schritte mit Elastic Load Balancing[6].

Maßgeschneiderte Bereitstellung mit AWS-Edge-Standorten (BP1, BP3)

Durch den Zugriff auf verschiedene hoch skalierte Internetverbindungen erhalten Sie deutlich mehr Möglichkeiten, die Latenz und den Durchsatz für Endbenutzer zu optimieren, DDoS-Angriffe abzuwehren und Fehler zu isolieren. Dabei können Sie gleichzeitig die Auswirkungen auf die Verfügbarkeit so gering wie möglich halten. Mit AWS-Edge-Standorten stehen weitere Ebenen der Netzwerkinfrastruktur bereit, dank derer diese Vorteile mit Amazon CloudFront und Amazon Route 53 auch für Webanwendungen verfügbar sind. Mithilfe dieser Services werden Inhalte bereitgestellt und DNS-Abfragen von Standorten aufgelöst, die sich häufig näher an den Endbenutzern befinden.

Bereitstellung von Webanwendungen am Edge (BP1)

Amazon CloudFront ist ein CDN-Service (Content Delivery Network), der die Bereitstellung Ihrer gesamten Website, einschließlich statischer, dynamischer, gestreamter und interaktiver Inhalte ermöglicht. Mit persistenten TCP-Verbindungen und variabler TTL (Time-to-Live) kann die Bereitstellung von Inhalt beschleunigt werden, selbst wenn er nicht am Edge-Standort in den Cache gestellt werden kann. Damit können Sie Amazon CloudFront zum Schutz Ihrer Webanwendung nutzen, selbst wenn Sie keinen statischen Inhalt bereitstellen. Amazon CloudFront akzeptiert nur wohlgeformte Verbindungen und verhindert damit, dass viele häufig auftretende DDoS-Angriffe wie SYN-Floods und UDP-Reflexionsangriffe den Ursprungs-Server erreichen. DDoS-Angriffe werden in der Nähe der Quelle geografisch isoliert, sodass vermieden wird, dass der Datenverkehr Auswirkungen auf andere Standorte hat. Mit dieser Funktion haben Sie deutlich bessere Möglichkeiten, den Endbenutzern während DDoS-Angriffen weiterhin Datenverkehr bereitzustellen. Mit Amazon CloudFront können Sie einen Ursprungs-Server auf AWS oder an anderer Stelle im Internet schützen.

Weitere Informationen zur Optimierung der Leistung von Webanwendungen mit Amazon CloudFront finden Sie unter Erste Schritte mit CloudFront[7].

Domänennamensauflösung am Edge (BP3)

Amazon Route 53 ist ein hochverfügbarer und skalierbarer DNS-Service (Domain Name System), mit dem Datenverkehr auf eine Webanwendung weitergeleitet werden kann. Er enthält viele erweiterte Funktionen wie Datenverkehrsfluss, latenzbasiertes Routing, Geo DNS, Zustandsprüfungen und Überwachung. Mit diesen Funktionen können Sie steuern, wie der Service auf DNS-Anforderungen reagieren soll, um so die Latenz, den Zustand und andere Aspekte zu optimieren. Sie können mithilfe dieser Funktionen die Leistung Ihrer Webanwendung verbessern und Ausfälle der Website vermeiden.

Amazon Route 53 arbeitet mit Shuffle Sharding und Anycast Striping, damit Endbenutzer auch bei einem DDoS-Angriff auf den DNS-Service auf Ihre Anwendung zugreifen können. Mithilfe von Shuffle Sharding entsprechen alle Namenserver im Delegationssatz einem eindeutigen Satz von Edge-Standorten und Internetpfaden. Dies sorgt für größere Fehlertoleranz und minimiert Überlappungen zwischen Kunden. Wenn ein einzelner Namenserver im Delegationssatz nicht verfügbar ist, können Endbenutzer einen erneuten Versuch starten und eine Antwort von einem anderen Namenserver an einem anderen Edge-Standort erhalten. Mit Anycast Striping wird jede DNS-Anforderung vom bestmöglichen Standort verarbeitet. Damit werden Last verteilt und DNS-Latenz reduziert, sodass Endbenutzer schneller eine Antwort erhalten. Außerdem kann Amazon Route 53 Anomalien in der Quelle und im Volume der DNS-Abfragen erkennen und Anforderungen von Benutzern priorisieren, die als zuverlässig gelten.

Wenn viele Zones über Amazon Route 53 gehostet werden, können Sie einen wiederverwendbaren Delegationssatz erstellen, in dem der gleiche Satz autoritativer Namenserver für die einzelnen Domänen bereitgestellt wird. Damit können Sie die gehosteten Zonen leichter pflegen. Im Fall eines DDoS-Angriffs kann AWS außerdem eine einzelne Vermeidungsstrategie anwenden, die alle gehosteten Zonen abdeckt, in denen der wiederverwendbare Delegationssatz verwendet wird.

Weitere Informationen zur Weiterleitung von Endbenutzern zur Anwendung mit Amazon Route 53 finden Sie unter Erste Schritte mit Amazon Route 53[8]. Weitere Informationen zu wiederverwendbaren Delegationssätzen finden Sie unter Aktionen mit wiederverwendbaren Delegationssätzen[9].

Verteidigung der Anwendungsebene (BP1, BP2, BP6)

Viele Techniken, die in diesem Artikel beschrieben werden, vermeiden die Auswirkungen auf die Verfügbarkeit der Infrastrukturebene bei DDoS-Angriffen wirksam. Wenn Sie Ihre Anwendung gegen Angriffe auf die Anwendungsebene schützen möchten, müssen Sie eine Architektur implementieren, mit der Sie bösartige Anforderungen erkennen und skalieren können, um sie abzuwehren und zu blockieren. Hierbei handelt es sich um einen sehr wichtigen Aspekt, denn netzwerkbasierte Systeme zur Vermeidung von DDoS-Angriffen sind in der Regel unwirksam, wenn es gilt, komplexe Angriffe auf die Anwendungsebene zu verhindern.

Erkennen und Filtern von bösartigen Webanforderungen (BP1, BP2)

Häufig werden Web Application Firewalls (WAFs) verwendet, um Webanwendungen gegen Angriffe zu schützen, die versuchen, eine Schwachstelle in der Anwendung auszunutzen. Dazu gehören z. B. die häufig auftretenden SQL Injections oder Anforderungsfälschung zwischen Websites. Mit WAF können Sie auch DDoS-Angriffe auf die Webanwendungsebene erkennen und vermeiden.

In AWS können Sie Ihre Anwendung mit Amazon CloudFront und AWS WAF gegen solche Angriffe schützen. Mit Amazon CloudFront können Sie statischen Inhalt in den Cache stellen und von AWS-Edge-Standorten aus bereitstellen, mit denen die Last auf dem Ursprungs-Server reduziert wird. Außerdem kann Amazon CloudFront Verbindungen für langsam lesende oder langsame schreibende Angreifer (z. B. Slowloris) schließen. Mit Amazon CloudFront können Sie Geo-Restriction nutzen, um zu verhindern, dass Benutzer an bestimmten geografischen Standorten auf den Inhalt zugreifen. Dies ist hilfreich, wenn Sie Angriffe blockieren möchten, die von geografischen Standorten stammen, an denen Sie nicht erwarten, dass Endbenutzer bearbeitet werden.

Bei anderen Arten von Angriffen, wie HTTP-Floods oder Pingback-Floods in WordPress, können Sie AWS WAF nutzen, um die Angriffe selbst zu vermeiden. Wenn Sie die Quelle der IP-Adresse kennen, die Sie blockieren möchten, können Sie eine Regel mit einer zu blockierenden Aktion erstellen und diese mit einer Web-ACL verknüpfen. Anschließend erstellen Sie eine Übereinstimmungsbedingung der IP-Adresse mit der Web-ACL, um die Quell-IP-Adressen zu blockieren, die an dem Angriff beteiligt sind. Sie können auch eine Regel mit Bedingungen erstellen, mit der nach URI, Abfragezeichenfolge, HTTP-Methode oder Header-Schlüssel blockiert wird. Letzteres ist bei Angriffen hilfreich, die eine eindeutige Signatur haben. So hat z. B. ein WordPress-Pingback-Angriff immer den User-Agent "WordPress".

Oft ist es schwierig, die Signatur eines DDoS-Angriffs zu identifizieren oder die IP-Adressen, die an dem Angriff beteiligt sind, genau zu bestimmten. In manchen Fällen ist es möglich, diese Informationen in den Webserverprotokollen zu finden. Auch können Sie die AWS WAF-Konsole verwenden, um stichprobenartig die Anforderungen anzuzeigen, die Amazon CloudFront an die AWS WAF weitergeleitet hat. Mithilfe von Stichprobenanforderungen können Sie entscheiden, welche Regeln für die Vermeidung eines Angriffs auf die Anwendungsebene erforderlich sein könnten. Wenn Sie viele Anforderungen mit einer zufälligen Anforderungszeichenfolge erkennen, sollten Sie die Weiterleitung von Abfragezeichenfolgen in Amazon CloudFront deaktivieren. Dies kann bei der Vermeidung eines Cache-Busting-Angriffs auf den Ursprungs-Server hilfreich sein.

Einige Angriffe umfassen Webdatenverkehr, der wie normaler Endbenutzer-Datenverkehr aussieht. Mit der AWS Lambda-Funktion können Sie durchsatzbasierte Sperrlisten implementieren und diese Art von Angriff somit vermeiden. Mithilfe dieser durchsatzbasierten Sperrlisten können Sie einen Schwellenwert für die Anzahl der Anforderungen festlegen, die von der Webanwendung bearbeitet werden. Wenn ein Bot oder Crawler diese Begrenzung überschreitet, können Sie alle weiteren Anforderungen mit AWS WAF automatisch blockieren.

Weitere Informationen zur Einschränkung des Zugriffs auf die Amazon CloudFront-Verteilung mit Geo-Restriction finden Sie unter Einschränken der geografischen Verteilung von Inhalt[10].

Weitere Informationen zum Arbeiten mit AWS WAF finden Sie unter Erste Schritte mit AWS WAF[11] und Anzeigen einer Stichprobe von Webanforderungen, die von CloudFront an die AWS WAF weitergeleitet wurden[12].

Weitere Informationen zur Konfiguration von durchsatzbasierten Sperrlisten mit AWS Lambda und AWS WAF finden Sie unter Konfigurieren von durchsatzbasierten Sperrlisten mit AWS WAF und AWS Lambda[13].

Skalierung für die Abwehr (BP6)

Eine weitere Möglichkeit für die Abwehr von Angriffen auf die Anwendungsebene ist die intelligente Skalierung. Sie können ELB für Webanwendungen verwenden, um Datenverkehr auf viele Amazon EC2-Instances zu verteilen, auf denen eine Overprovisioning vorliegt oder die für das Auto Scaling konfiguriert sind, um Spitzen im Datenverkehr unabhängig davon zu bewältigen, ob diese durch einen Flash Crowd- oder einen DDoS-Angriff auf die Anwendungsebene verursacht wurden. Mit Amazon CloudWatch-Alarmen wird das Auto Scaling gestartet. Dabei wird die Größe der Amazon EC2-Flotte als Reaktion auf von Ihnen definierte Ereignisse automatisch skaliert. Damit wird die Verfügbarkeit geschützt, selbst wenn eine unerwartet große Menge an Anforderungen bewältigt werden muss. Mit Amazon CloudFront oder ELB wird die SSL-Verhandlung durch die Verteilung oder den Load Balancer durchgeführt. Damit wird verhindert, dass die Instance durch SSL-basierte Angriffe beeinträchtigt wird.

Weitere Informationen zum Aufruf von Auto Scaling mit Amazon CloudWatch finden Sie unter Überwachen der Auto Scaling-Instances und -Gruppen mit Amazon CloudWatch[14].

Verringern der Angriffsfläche

Ein wichtiger Aspekt, der beim Architecting on AWS beachtet werden muss, ist die Einschränkung der Gelegenheiten, bei denen ein Angreifer Ihre Anwendung angreifen kann. Wenn Sie z. B. nicht erwarten, dass ein Endbenutzer direkt mit bestimmten Ressourcen interagiert, sollten Sie sicherstellen, dass nicht über das Internet auf diese Ressourcen zugegriffen werden kann. Und wenn Sie nicht erwarten, dass Endbenutzer oder externe Anwendungen auf bestimmten Ports oder mit bestimmten Protokollen mit Ihrer Anwendung kommunizieren, sollten Sie sicherstellen, dass kein Datenverkehr akzeptiert wird. Dieses Konzept wird als Verringern der Angriffsfläche bezeichnet. In diesem Abschnitt erläutern wir die bewährten Methoden, mit denen Sie die Angriffsfläche verringern und den Umfang reduzieren können, in dem Ihre Anwendung mit dem Internet verbunden ist. Ressourcen, die nicht mit dem Internet verbunden sind, sind schwerer anzugreifen. Damit reduzieren sich die Möglichkeiten, dass ein Angreifer die Verfügbarkeit Ihrer Anwendung bedroht.

Verschleiern von AWS-Ressourcen (BP1, BP4, BP5)

Die AWS-Ressourcen müssen für viele Anwendungen nicht vollständig mit dem Internet verbunden sein. So müssen z. B. Amazon EC2-Instances hinter einem ELB nicht öffentlich zugänglich sein. In diesem Szenario können Sie entscheiden, ob Endbenutzer auf bestimmten TCP-Ports Zugriff auf ELB haben, und festlegen, dass nur das ELB mit den Amazon EC2-Instances kommuniziert. Zu diesem Zweck werden Sicherheitsgruppen und Netzwerk-ACLs (Netzwerk-Zugriffskontrolllisten, Access Control Lists) innerhalb der Amazon Virtual Private Cloud (VPC) konfiguriert. Mit Amazon VPC können Sie einen logisch isolierten Abschnitt der AWS Cloud bereitstellen, in dem Sie AWS-Ressourcen in einem von Ihnen definierten virtuellen Netzwerk starten können.

Sicherheitsgruppen und Netzwerk-ACLs sind insofern ähnlich, als dass Sie mit beiden den Zugriff auf AWS-Ressourcen in der VPC steuern können. Mit Sicherheitsgruppen können Sie den ein- und ausgehenden Datenverkehr auf Instance-Ebene steuern. Netzwerk-ACLs bieten ähnliche Funktionen, allerdings auf der Ebene des VPC-Subnetzes. Außerdem fallen für die eingehende Datenübertragung keine Kosten für Amazon EC2-Sicherheitsgruppenregeln oder Netzwerk-ACLs an. Damit wird sichergestellt, dass Ihnen für Datenverkehr, der von den Sicherheitsgruppen oder Netzwerk-ACLs zurückgeschickt wird, keine Kosten entstehen.

Sicherheitsgruppen (BP5)

Sie können Sicherheitsgruppen beim Start einer Instance festlegen oder die Instance später mit einer Sicherheitsgruppe verknüpfen. Wenn Sie keine Regel zum *Erlauben* erstellt haben, die den Datenverkehr zulässt, wird der gesamte Datenverkehr vom Internet zu einer Sicherheitsgruppe implizit abgelehnt. Wenn eine Webanwendung z. B. aus einem ELB und vielen Amazon EC2-Instances besteht, können Sie eine Sicherheitsgruppe für das ELB ("ELB-Sicherheitsgruppe") und eine für die Instances ("Sicherheitsgruppe für den Webanwendungsserver") erstellen. Dann können Sie Regeln zum *Erlauben* erstellen, um den Datenverkehr vom Internet zur ELB-Sicherheitsgruppe und von der ELB-Sicherheitsgruppe zur Sicherheitsgruppe des Webanwendungs-servers zuzulassen. Folglich kann der Datenverkehr vom Internet nicht direkt mit den Amazon EC2-Instances kommunizieren und damit wird es für einen Angreifer schwieriger, Informationen über die Anwendung zu erhalten.

Netzwerk-Zugriffskontrolllisten (ACLs) (BP5)

Mit Netzwerk-ACLs können Sie sowohl Regeln zum *Erlauben* als auch zum *Ablehnen* einrichten. Diese sind hilfreich, wenn Sie bestimmte Arten von Datenverkehr zu Ihrer Anwendung explizit ablehnen möchten. So können Sie z. B. IP-Adressen (als CIDR-Bereich), Protokolle und Zielports definieren, die für das gesamte Subnetz abgelehnt werden sollen. Wenn die Anwendung nur für TCP-Datenverkehr verwendet wird, können Sie eine Regel zum *Ablehnen* des gesamten UDP-Datenverkehrs oder umgekehrt erstellen. Dieses Tool ist für die Reaktion auf DDoS-Angriffe hilfreich, da Sie, falls Sie die Quell-IP-Adresse oder eine andere Signatur kennen, eigene Regeln erstellen können, um den Angriff zu vermeiden.

Schutz des Ursprungs-Servers (BP1)

Wenn Sie Amazon CloudFront mit einem Ursprungs-Server verwenden, der sich innerhalb der VPC befindet, sollten Sie die Sicherheitsgruppenregeln automatisch mit einer AWS Lambda-Funktion so aktualisieren, dass nur Datenverkehr von Amazon CloudFront *erlaubt* wird. Damit können Sie die Sicherheit des Ursprungs-Servers verbessern, indem Sie sicherstellen, dass Amazon CloudFront und AWS WAF nicht umgangen werden können.

Weitere Informationen zum Schutz des Ursprungs-Servers durch automatische Aktualisierung der Sicherheitsgruppen finden Sie unter Automatische Aktualisierung der Sicherheitsgruppen für Amazon CloudFront und AWS WAF mit AWS Lambda[15].

Sie sollten auch sicherstellen, dass nur die Amazon CloudFront-Verteilung Anforderungen an den Ursprungs-Server weiterleitet. Mit Edge-to-Origin-Anforderungsheaders können Sie den Wert vorhandener Anforderungsheaders hinzufügen oder überschreiben, wenn Amazon CloudFront Anforderungen an Ihren Ursprungs-Server weiterleitet. Mit dem Header *X-Shared-Secret* können Sie prüfen, ob Anforderungen an Ihren Ursprungs-Server von Amazon CloudFront gesendet wurden.

Weitere Informationen zum Schutz des Ursprungs-Servers mit einem *X-Shared-Secret*-Header finden Sie unter Weiterleiten benutzerdefinierter Header an den Ursprungs-Server[16].

Schutz von API-Endpunkten (BP4)

Wenn eine API öffentlich verfügbar gemacht werden muss, besteht in der Regel das Risiko, dass das API-Frontend zum Ziel eines DDoS-Angriffs wird. Amazon API Gateway ist ein vollständig verwalteter Service, mit dem Sie eine API erstellen können, die als "Eingangstür" für Anwendungen agiert, die auf Amazon EC2, AWS Lambda oder einer beliebigen Webanwendung ausgeführt werden. Mit Amazon API Gateway müssen Sie keine eigenen Server für das API-Frontend ausführen und können andere Komponenten der Anwendung für die Öffentlichkeit verschleiern. Damit können Sie verhindern, dass AWS-Ressourcen zum Ziel eines DDoS-Angriffs werden. Amazon API Gateway ist in Amazon CloudFront integriert – Sie profitieren daher von der zusätzlichen DDoS-Resilienz dieses Service. Außerdem können Sie Ihr Backend vor übermäßigem Datenverkehr schützen. Konfigurieren Sie dazu für alle Methoden in den REST-APIs standardmäßige oder auf Durchsatzraten basierende Einschränkungen.

Weitere Informationen zum Erstellen von APIs mit Amazon API Gateway finden Sie unter Erste Schritte mit Amazon API Gateway[17].

Betriebliche Techniken

Mit den in diesem Artikel beschriebenen Vermeidungstechniken können Sie Architekturen für Anwendungen erstellen, die grundsätzlich resilient gegen DDoS-Angriffe sind. In vielen Fällen ist es sehr hilfreich zu wissen, wann DDoS-Angriffe auf Ihre Anwendung erfolgen, und anhand dieser Daten Maßnahmen zu ergreifen. Zudem sollten Sie weitere Ressourcen aktivieren, um eine Bedrohung zu bewerten, die Architektur Ihrer Anwendung zu überprüfen oder weitere Hilfe anzufordern. In diesem Abschnitt werden die bewährten Methoden für mehr Transparenz bei anormalem Verhalten, für Warnungen und Automatisierung und für die Nutzung von AWS für zusätzlichen Support erläutert.

Sichtbarkeit

Wenn Sie das normale Verhalten Ihrer Anwendung kennen, können Sie im Fall einer Anomalität schneller agieren. Wenn eine wichtige Metrik deutlich vom erwarteten Wert abweicht, deutet dies darauf hin, dass ein Angreifer möglicherweise versucht, die Verfügbarkeit der Anwendung zu beeinflussen. Mit Amazon CloudWatch können Sie Ihre Infrastruktur und Anwendungen in AWS überwachen. Sie können Metriken erfassen und nachverfolgen, Protokolldateien sammeln und überwachen, Alarme festlegen und auf Änderungen in den AWS-

Ressourcen automatisch reagieren. Eine Beschreibung der Amazon CloudWatch-Metriken, die häufig für die Erkennung von und Reaktion auf DDoS-Angriffe verwendet werden, finden Sie in Tabelle 3.

Thema	Metrik	Beschreibung
Auto Scaling	GroupMaxSize	Die maximale Größe der Auto Scaling-Gruppe
Amazon CloudFront	Anforderungen	Die Anzahl der HTTP/S-Anforderungen
Amazon CloudFront	TotalErrorRate	Der Prozentsatz aller Anforderungen mit dem HTTP-Statuscode 4xx oder 5xx
Amazon EC2	CPUUtilization	Der Prozentsatz der zugewiesenen EC2-Recheneinheiten, die gegenwärtig in Gebrauch sind
Amazon EC2	NetworkIn	Die Anzahl der von der Instance auf allen Netzwerkschnittstellen empfangenen Bytes
ELB	SurgeQueueLength	Die Anzahl der Anforderungen, die vom Load Balancer in die Warteschlange gestellt wurden und darauf warten, dass eine Backend-Instance Verbindungen akzeptiert und die Anforderung verarbeitet
ELB	UnHealthyHostCount	Die Anzahl nicht voll funktionsfähiger Instances in jeder Availability Zone
ELB	RequestCount	Die Anzahl der abgeschlossen Anforderungen, die empfangen und an registrierte Instances geroutet wurden
ELB	Latenz	Die verstrichene Zeit in Sekunden bis zum Empfang einer Antwort, nachdem die Anforderung den Load Balancer verlassen hat
ELB	HTTPCode_ELB_4xx HTTPCode_ELB_5xx	Die Anzahl der vom Load Balancer generierten HTTP 4xx- oder 5xx-Fehlercodes
ELB	BackendConnectionErrors	Die Anzahl der Verbindungen, die nicht erfolgreich waren
ELB	SpilloverCount	Die Anzahl der Anforderungen, die abgelehnt wurden, weil die Warteschlange voll war
Amazon Route 53	HealthCheckStatus	Der Status des Zustandsprüfungs-Endpunkts

Tabelle 3: Empfohlene Amazon CloudWatch-Metriken

Bei einer Anwendung, deren Architektur der DDoS-resilienten Referenzarchitektur in Abbildung 5 entspricht, werden allgemeine Angriffe auf die Infrastrukturebene blockiert, bevor Sie die Anwendung erreichen. Folglich werden diese Angriffe nicht in den Amazon CloudWatch-Metriken erfasst.

Ein Angriff auf die Anwendungsebene kann dazu führen, dass einige dieser Metriken ansteigen. Ein HTTP-Flood kann z. B. zu einer Zunahme der Anforderungen sowie der CPU- und Netzwerkauslastung für Amazon CloudFront, ELB und Amazon EC2-Metriken führen. Wenn die Backend-Instances die übermäßigen Anforderungen nicht bewältigen können, werden auch die Werte für TotalErrorRate in Amazon CloudFront und für SurgeQueueLength, UnHealthyHostCount, Latency, BackendConnectionErrors, SpilloverCount oder für HTTPCode in ELB ansteigen. Da die Anwendung nicht in der Lage ist, normale Endbenutzer zu verarbeiten, kann in diesem Fall die Anzahl der HTTP-Anforderungen sinken. Als Abhilfe für diese Bedingung können Sie das Backend Ihrer Anwendung skalieren oder, wie zuvor in diesem Artikel beschrieben, den übermäßigen Datenverkehr mit AWS WAF blockieren.

Weitere Informationen zur Erkennung von DDoS-Angriffen auf die Anwendung mit Amazon CloudWatch finden Sie unter Erste Schritte mit Amazon CloudWatch[18].

Ein weiteres Tool, mit dem Sie für mehr Transparenz beim Datenverkehr zu Ihrer Anwendung sorgen können, ist VPC Flow Logs. In einem herkömmlichen Netzwerk können Sie Netzwerk-Flow-Protokolle verwenden, um Konnektivitäts- und Sicherheitsprobleme zu beheben und sicherzustellen, dass die Netzwerkzugriffsregeln wie gewünscht funktionieren. Mit VPC Flow Logs können Sie Informationen über den IP-Datenverkehr und von Netzwerkschnittstellen in Ihrer VPC erfassen.

Jeder Eintrag im Flow-Protokoll umfasst die Quell- und Ziel-IP-Adressen, die Quell- und Zielports, das Protokoll und die Anzahl der Pakete und Byte, die im Erfassungszeitfenster übertragen wurden. Anhand dieser Informationen können Sie Anomalien im Netzwerkdatenverkehr sowie den jeweiligen Angriffsvektor identifizieren. Die meisten UDP-Reflexionsangriffe haben z. B. bestimmte Quellports (z. B. Quellport 53 für DNS-Reflexion). Dies ist eine eindeutige Signatur, anhand derer Sie den Eintrag im Flow-Protokoll identifizieren können. Als Reaktion können Sie den jeweiligen Quellport auf Instance-Ebene blockieren oder eine Netzwerk-ACL-Regel erstellen, mit der das gesamte Protokoll blockiert wird, falls es nicht erforderlich ist.

Weitere Informationen zum Erkennen von Netzwerkanomalien und DDoS-Angriffsvektoren mit VPC Flow Logs finden Sie unter VPC Flow Logs[19] und VPC Flow Logs – Protokollieren und Anzeigen von Flow im Netzwerkdatenverkehr[20]

Support

Es ist wichtig, einen Plan für DDoS-Angriffe zu erstellen, bevor diese wirklich auftreten. Die in diesem Artikel beschriebenen bewährten Methoden dienen als proaktive Maßnahmen und sollten vor dem Start einer Anwendung implementiert werden, die zum Ziel eines DDoS-Angriffs werden könnte. Das Team für Ihr AWS-Konto kann Ihnen bei Ihrem Anwendungsfall und Ihrer Anwendung helfen und Sie bei bestimmten Fragen oder Herausforderungen unterstützen, die sich ergeben könnten.

In manchen Fällen ist es möglicherweise hilfreich, AWS während eines DDoS-Angriffs um zusätzliche Unterstützung zu bitten. Ihr Fall wird dann schnell beantwortet und an einen Experten weitergeleitet, der Ihnen helfen kann. Wenn Sie den Support auf Business-Ebene abonnieren, können Sie rund um die Uhr per E-Mail, Chat oder Telefon Fragen an die Cloud-Support-Ingenieure stellen.

Wenn Sie aufgabenkritische Workloads auf AWS bearbeiten, sollten Sie den Support auf Enterprise-Ebene in Betracht ziehen. Mit dem Enterprise Support erhalten dringende Fälle höchste Priorität und werden an Senior Cloud Support-Ingenieure weitergeleitet. Außerdem beinhaltet der Support auf Enterprise-Ebene die Unterstützung durch einen Technical Account Manager (TAM), der Ihnen zugeordnet und Ihr technischer Kontaktpunkt ist. Außerdem haben Sie mit dem Support auf Enterprise-Ebene Zugriff auf das Infrastructure Event Management, das bei geplanten Veranstaltungen, Produkteinführungen und Migrationen betriebliche Unterstützung in Echtzeit umfasst.

Weitere Informationen zur Auswahl eines auf Ihre Anforderungen zugeschnittenen Support-Angebots finden Sie unter Vergleich der AWS Support-Angebotes[21].

Fazit

Mit den in diesem Artikel beschriebenen bewährten Methoden können Sie eine DDoS-resiliente Architektur aufbauen, die die Verfügbarkeit Ihrer Anwendung bei zahlreichen allgemeinen Angriffen auf die Infrastruktur- und Anwendungsebene schützen kann. Der Umfang, in dem Sie die Architektur Ihrer Anwendung gemäß den bewährten Methoden aufbauen, bestimmt die Art, den Vektor und die Menge der DDos-Angriffe, die Sie vermeiden können. AWS empfiehlt Ihnen, die bewährten Methoden umzusetzen, damit Sie die Verfügbarkeit Ihrer Anwendung bei allgemeinen DDoS-Angriffen besser schützen können.

Mitwirkende

Dieses Dokument ist unter der Mitarbeit folgender Personen und Organisationen entstanden:

- Andrew Kiggins, AWS-Lösungsarchitekt
- Jeffrey Lyons, AWS DDoS Ops Engineering

Hinweise

[1] https://www.youtube.com/watch?v=OT2y3DzMEmQ

[2] https://www.youtube.com/watch?v=Ys0gG1koqJA

[3] https://aws.amazon.com/ec2/instance-types/

[4] http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/enhanced-networking.html

[5] http://docs.aws.amazon.com/AWSEC2/latest/UserGuide/using-regions-availability-zones.html

[6] http://docs.aws.amazon.com/ElasticLoadBalancing/latest/DeveloperGuide/elb-getting-started.html

[7] http://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/GettingStarted.html

[8] http://docs.aws.amazon.com/Route53/latest/DeveloperGuide/getting-started.html

[9] http://docs.aws.amazon.com/Route53/latest/APIReference/actions-on-reusable-delegation-sets.html

[10] http://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/georestrictions.html

[11] http://docs.aws.amazon.com/waf/latest/developerguide/getting-started.html

[12] http://docs.aws.amazon.com/waf/latest/developerguide/web-acl-testing.html#web-acl-testing-view-sample

[13] https://blogs.aws.amazon.com/security/post/Tx1ZTM4DT0HRH0K/How-to-Configure-Rate-Based-Blacklisting-with-AWS-WAF-and-AWS-Lambda

[14] http://docs.aws.amazon.com/autoscaling/latest/userguide/as-instance-monitoring.html

[15] https://blogs.aws.amazon.com/security/post/Tx1LPI2H6Q6S5KC/How-to-Automatically-Update-Your-Security-Groups-for-Amazon-CloudFront-and-AWS-W

[16] http://docs.aws.amazon.com/AmazonCloudFront/latest/DeveloperGuide/forward-custom-headers.html

[17] https://aws.amazon.com/api-gateway/getting-started/

[18] http://docs.aws.amazon.com/AmazonCloudWatch/latest/DeveloperGuide/GettingStarted.html

[19] http://docs.aws.amazon.com/AmazonVPC/latest/UserGuide/flow-logs.html

[20] https://aws.amazon.com/blogs/aws/vpc-flow-logs-log-and-view-network-traffic-flows/

[21] https://aws.amazon.com/premiumsupport/compare-plans/