Denial-of-Service Präventionsmaßnahmen

Zusammenfassung

Vorbeugende Maßnahmen zur Abwehr von Denial of Service Angriffen sind zur Schadensbegrenzung notwendig. Verdächtige Anfragen können mittels Challenge Response Protocols aussoriert werden, die Authentifizierung kann verlagert, direkte Kommunikation unterbunden, Verbindung begrenzt und Ressourcen limitiert werden. Die methodischen Ansätze dieser Verfahren wird in diesem Paper betrachtet.

I. Einleitung

Online Services stellen einen unabdingbar Teil unseres alltäglichen Lebens dar. Diese reichen von den großen Unternehmen wie Google, Amazon, Apple und Microsoft, deren Services im Web kaum noch wegzudenken sind, bis zu Websites von kleinen Unternehmen, Hochschulen, Netzwerken und Plattformen.

In Hinsicht auf die Wichtigkeit dieser Dienste lässt sich in diesem Sektor auch ein gewisser wirtschaftlicher und politischer Einfluss denken. Folglich kann durch deren Manipulation auch ein großer Schaden angerichtet werden. Cyberkriminalität in Form von Malware, Phishing, Trojanern und anderen sind daher für Unternehmen von Vereine, die online aktiv sind, eine ernst zu nehmende Bedrohung - und laut einer Studie des BKA [5] nahm die Zahl dieser Delikte in den Letzten Jahren zu.

Eine dieser ernstzunehmenden Bedrohungen ist der Denial-of-Service-Angriff.

II. Begriffserklärung

Unter einem Denial-of-Service (DoS) Angriff versteht man Angriffe auf Online-Services, die darauf abzielen die Verfügbarkeit des Services zu unterbrechen, indem Ressourcen wie CPU, Speicher oder Bandbreite überlastet werden. Falls dieser Angriff durch mehrere, mit Malware infizierte Geräte, so genannte Slaves, durchgeführt wird, der Angriffsaufwand also auf mehrere Geräte verteilt wird, so spricht man auch von einem Distributed-Denial-of-Service (DDoS) Angriff. [6]

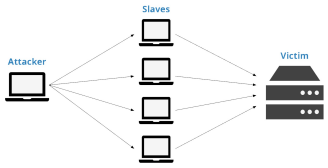

Abbildung 1: Visualisierung eines DDoS Angriffes

Aufgrund der Überlastung kann der Host eingehende Anfragen echter Nutzer nicht mehr ordnungsgemäß bearbeiten und muss schlimmstenfalls das System neu starten. Mit der entstehenden Downtime sind natürlich auch Kosten verbunden.

Eine Studie aus dem 4.Quartal 2017 von [3], welche US-Unternehmen im IT Bereich nach deren Erfahrungen mit DDoS Angriffen befragte, hat ermittelt, dass der durchschnittlich verursachte Schaden bei 40.000$ pro Stunde lag. Um diese Schäden einzugrenzen werden bestimmte Maßnahmen beim Aufbau der System-Infrastruktur ergriffen.

III. Taxonomie

Mögliche Abwehrmaßnahmen gegen DoS-Angriffe lassen sich grob in drei Kategorien unterteilen[1]:

- Prävention
- Feststellung
- Eingrenzung

Die Unterteilung erfolgt dabei abhängig davon, welchen Problempunkt der DoS-Abwehr die zuständige Software Adressiert. Dieses Paper setzt sich mit den präventiven Maßnahmen nach [1, 6] auseinander.

IV. DoS Prävention

Die DoS Prevention versucht den Ausfall des Systems, bzw. dessen Überlastung, zu verhindern oder im schlimmsten Falle einzugrenzen.

IV.1 Challenge Response Protocols

Challenge Response Protocols (CPR) dienen dazu, echte Nutzer von Maschinen/Botnets zu unterscheiden. Der Host führt essenziell einen Turning Test am Client durch, um festzustellen, ob dieser sich "menschlich"verhält. Ein bekannter Vertreter solcher Turning Test ist das grafischen CAPTCHA.[1] Dem Nutzer wird in einem Bild verformte, verzerrte oder teils überlagerte Information gegeben, die er wiedergeben soll. Diese Aufgabe ist für Menschen leicht zu bewältigen, für Maschinen allerdings nicht.

Abhängig davon, ob der Turning-Test erfolgreich bearbeitet werden konnte, wird der Client dann in einer Whitelist oder Blacklist gespeichert. [4]. Clients mit einer validen IP-Adresse haben Zugriff aus den Host-Service, während Anfragen von Clients auf der Blacklist ausgefiltert und ihnen der Zugriff verwehrt wird.

Ein Problem der CPRs jedoch ist, dass sie beim Host Speicher und Rechenkapazität beanspruchen. Auf eine große Anzahl eingehender Anfragen müssen viele dieser Turning Tests generiert und gespeichert werden.

IV.2 Versteckte Server / Ports

Anstatt, dass der Client direkt mit den Service-Host kommunizieret, kann ein Knotenpunkt dazwischen zur Authentifizierung der Anfragen genutzt werden.[2, 1] Im Falle eines DoS Angriffs stehen die gesamten Ressourcen des verwaltenden Knotenpunktes zur Auswertung der eingehenden Anfragen zur Verfügung. Authentifizierte Anfragen werden dann auf den Service-Host oder einem Proxy Server zur weiteren Bearbeitung zur Verfügung.

Des weiteren werden auch dynamische Server oder Ports verwendet um direkte Kommunikation zwischen Client und Service-Host zu erschweren. [2]

Versteckte Server sind jedoch schwer auf größere Netzwerke skalierbar. Zudem wird durch die Einbindung eines oder mehrerer zusätzlicher Knotenpunkte die benötigte Zeit zur Kommunikation zwischen Host und Client erhöht.

IV.3 Zugriffsbeschränkung

Zur Entlastung eines Host-Servers oder eines Authentifizierungspunktes kann die Zugriffsrate von Clients beschränkt oder gar komplett unterbunden werden. Eine generelle Beschränkung aller Clients ist möglich, jedoch nicht wünschenswert, weil dadurch auch Anfragen echter Nutzer beeinflusst werden.

Stattdessen wird auch hierfür eine Blacklist verwendet. Ist ein Client auf dieser Blacklist, so werden alle von ihm versandten Anfragen temporär beschränkt oder ignoriert.

Die Entscheidung, ob ein Nutzer auf der Blacklist landet oder nicht, trifft man basierend auf seinen vorangehenden Web-Zugriffen oder seinem Zugriffsverhalten. Werden beispielsweise eine Großzahl an Paketen mit geringer Größe in kurzer Zeit versandt, so handelt es sich beim Client wahrscheinlich nicht um einen legitimen Nutzer.

Zugriffsbeschränkungen weisen ähnliche Nachteile wie CRPs auf. Jeder Client muss auf Basis seiner Aktivität evaluiert und darauf basierend kategorisiert behandelt werden.[1] Ein Angriff mit einem Botnet, welches Geräte mit vielen verschiedenen IPs für einen Flooding-Angriff nutzt, beansprucht beim verwaltenden System viel Rechenkapazität zur Auswertung jedes einzelnen Clients. Zudem kann ein geplanter Angriff die Zugriffsbeschränkung umgehen, indem man die Anfragen so gestaltet, dass sie als legitim angesehen

werden (z.B. authentische Zugriffsrate und Zugriffsverläufe). Die Anzahl an als legitim anerkannten Anfragen, die dann zum Host bzw. Proxy Server weitergeleitet wird, kann diesen dann überlasten.

IV.4 Ressourcenbeschränkung

Die vorangehenden Präventionsmaßnahmen versuchen unnötiger Auslastung durch einen DoS Angriff vorzubeugen. Im Gegensatz dazu fokussiert sich die Ressourcenbeschränkung darauf, den angerichteten finanziellen Schaden zu begrenzen.

Wie bereits erwähnt richten DoS Angriffe Schäden an, indem sie Ressourcen des Hosts verbrauchen und diesen gegebenenfalls zum Neustart zwingen. Die Ressourcenbeschränkung versucht diesen angerichteten Schaden einzugrenzen, indem, je nach Auslastung des Netzwerkes und Legitimität einer Anfrage, die für einen Nutzer aufgebrachten Ressourcen nach oben beschränkt werden. Dies erfolgt durch analytische Algorithmen, die zu verteilende Ressourcen als Abhängigkeitsfunktion von den verfügbaren Ressourcen, sowie der zu erwartenden Systemleistung darstellt.[6]

Die kontrollierte Beschränkung und Verteilung vorhandener Kapazitäten erhöht zwar somit die Bearbeitungszeit, verhindert jedoch eventuell die komplette Überlastung des Systems. Dies ist besonders in Cloud Computing wichtig, wo für den Kunden Rechenleistung zur Verfügung gestellt wird, demnach jeder Client selbst viel Rechenleistung bzw. Bandbreite beansprucht.

V. Fazit

Vorbeugende Maßnahmen zur Abwehr von DoS-Angriffen ermöglichen es, sich präventiv gegen Überlastung zu schützen. Authentifizierung durch CPRs, Knotenpunkte zur Authentifizierung zwischen Client und Host, sowie das selektive Unterbinden bzw. Beschränken verdächtiger Anfragen helfen, die Auslastung im Angriffsfall zu minimieren. Zur Schadensbegrenzung kann über Ressourcenbeschränkung Nutzern eine Mindestkapazität garantiert werden.

Jedoch weist jede dieser Präventionsmaßnahmen Schwachstellen auf. Zur Regulierung von Anfragen kann unter Umständen selbst große Rechenleistung abverlangt werden, und die Angriffe können angepasst werden, diese Maßnahmen zu umgehen.

Präventionsmaßnahmen allein sind nicht genug um sich vor DoS-Attacken zu schützen, und sind oftmals auch von Feststellungs-Maßnahmen abhängig.

Literatur

[1] DDoS attacks in cloud computing: Issues, taxonomy, and future directions. *Computer Communications*, 107:30–48, 2016.

[2] D. F. W. P. F. L. A. S. Huangxin Wang, Quan Jia. A moving target DDoS defense mechanism. *Computer Communications*, 46:10–21, 2014.

[3] T. Matthews. Incapsula Survey: What DDoS Attacks Really Cost Businesses. https://lp.incapsula.com/rs/incapsulainc/images/eBook2014.

[4] K. K. D. Rashmi V. Deshmukh. Understanding DDoS Attack and Its Effect In Cloud Environment. *Procedia Computer Science*, 49:202–210, 2015.

[5] J. Wagner. BKA-Statistik: Internetkriminalität nimmt in Deutschland zu. http://www.cnet.de/88169943/bka-statistik-internetkriminalitaet-nimmt-in-deutschland-zu/, 2017.

[6] S. Yu. *Distributed Denial of Service Attack and Defence*. Springer, 2013.