Frühzeitiges Unterbinden von DDoS-Angriffen

In einer Welt, in der die Zahl der vernetzten Geräte ständig wächst, ergeben sich neue Geschäftschancen und Wachstumsmöglichkeiten gerade in solchen Bereichen wie das Internet der Dinge (IoT), Virtualisierung und Online-Handel sowie Unterhaltung.

Gleichzeitig eröffnen sich dadurch aber auch neue Betätigungsfelder für Kriminelle mit immer raffinierteren Cyberangriffen. Durch das Aufkommen von IoT-Geräten handelt es sich dabei oft um verteilte „Denial-of-Service"-Angriffe (DDoS), bei denen der normale Internet-Verkehr durch eine Datenflut unterbrochen wird, und der nützliche Datenverkehr nicht mehr durchdringen kann.

Solche DDoS-Invasionen nehmen unterschiedliche Formen an, wobei der volumetrische Angriff besonders gebräuchlich ist. Bei diesem wird die zur Verfügung stehende Bandbreite dadurch vereinnahmt, dass das Netzwerk mit Datenverkehr überfordert wird, der typischerweise von kompromittierten Geräten stammt, oder dass bestimmte Netzwerkprotokolle genutzt werden. Eine weitere Variante ist der Angriff auf Anwendungsebene, bei dem ein bestimmter Service auf dem Host-Netzwerk, beispielsweise eine Suchmaschine, ins Visier gerät.

Eine Zunahme dieser Bedrohung ist abzusehen: IoT wird mit dem kommenden 5G und dessen Nutzung für Zwecke wie beispielsweise autonomes Fahren an Bedeutung gewinnen, wodurch neue Hotspots für Mobilgeräte entstehen, von denen aus Angriffe gestartet werden können.

DDoS-Trends

In den letzten Jahren haben wir bislang nie dagewesene DDoS-Angriffe im Terabit-Bereich erlebt. Unterstützt wurden diese durch neue Methoden, beispielsweise die Memcached-Technik, wie sie Anfang 2018 zum Einsatz kam, als ein damals spektakulärer 1,7-TB/s-DDoS-Angriff auf einen am Tag davor durchgeführten 1,35-TB/s-Angriff folgte.

2020 kam es zu einem weiteren DDoS-Angriff, der die vorherigen erneut in den Schatten stellte. Amazon Web Services meldete ein 2,3-TB/s-Ereignis, was zu einer über drei Tage andauernden erhöhten Bedrohungslage führte und um 44 % größer war als alle bisher festgestellten volumetrischen Angriffe.

NETSCOUT meldete gleichzeitig, dass es in der zweiten Jahreshälfte von 2019 global einen 16%igen Zuwachs der DDoS-Angriffe gab. Und selbst wenn die Organisation einen signifikanten Rückgang bei der Regelmäßigkeit der Angriffe mit mehr als 200 GB/s feststellen konnte, haben die Täter die Anzahl kleinerer Aktivitäten erhöht, wobei sie ein ständig wachsendes Instrumentarium an neuen oder zunehmend gebräuchlichen Angriffsvektoren einsetzen. NETSCOUT merkte an, dass es 2019 allein sieben derartige Angriffe gab.

COVID-19 hat ebenfalls deutlich gezeigt, wie plötzliche Ereignisse einen potenziellen Einfluss auf das Verhalten der Verbraucher ausüben. Der Informationsdienstleister und Technologieanbieter Neustar wies darauf hin, dass in der ersten Hälfte des Jahres 2020 ein „sprunghafter" Anstieg von DDoS-Aktivitäten mit einer Zunahme an Internet-Datenverkehr einherging, da die Menschen während der Pandemie mehr Zeit zu Hause und online mit Aktivitäten wie Shopping, Gaming und Homeoffice verbrachten. In den ersten sechs Monaten des Jahres 2020 stellte Neustar einen 150%igen Zuwachs im Vergleich zum Vorjahr fest.

Ein neuerer Trend ist die Zunahme von DDoS-Angriffen im Gaming-Bereich, wo es für regelmäßige Anwender mit Kreditkarten einfacher und erschwinglicher geworden ist, auf günstige Services zuzugreifen, mit denen die Verbindungen des Rivalen verlangsamt werden. Mit Hilfe von wenig teuren DDoS-„Bootern" oder „Stressern" können andere Gamer aus dem Spiel gedrängt oder Angriffe gegen bestimmte Ziele wie Finanzdienstleister und reguläre IT- oder Cloud-Dienstleister gefahren werden, die möglicherweise Anwendungen für andere Branchen hosten.

Ebenfalls zu bedenken ist, dass diese Bedrohungen eine Vielzahl von Branchen treffen können, weshalb Unternehmen es sich nicht leisten können, unaufmerksam zu sein.

Ein neuerer Trend ist die Zunahme von **DDoS-Angriffen** im Gaming-Bereich ... Mit Hilfe von wenig teuren **DDoS-„Bootern"** oder **„Stressern"** können andere Gamer aus dem Spiel gedrängt ...

Verteidigungsstrategie

Um sich gegen derartige Bedrohungen zu schützen, können Netzbetreiber und Unternehmen die verschiedensten Vorsorgemaßnahmen ergreifen. Eine wesentliche Maßnahme besteht darin, zunächst diejenigen Assets zu identifizieren, die für den Geschäftsbetrieb besonders kritisch sind, etwa Namens- und Basisserver.

Darüber hinaus sollte man Netzwerkbetriebszentren (Network Operations Center, NOC) mit ins Boot nehmen, um den „normalen" Datenverkehr im Auge zu behalten, damit die Auswirkungen eines Angriffs leicht und schnell identifiziert werden können, noch bevor dieser sich festsetzen und echten Schaden anrichten kann. Viele Unternehmen wissen gar nicht, wie ihre „normalen" Datenverkehrsmuster aussehen, weshalb ungewöhnliche Maße an Aktivität schwer feststellbar sind.

Mit Tools wie NetFlow lassen sich Daten und Informationen zum Netzwerkverkehr für Analysezwecke sammeln, wobei der große Vorteil darin besteht, dass je nach Zahlkräftigkeit gewerbliche und Open-Source-Software zur Verfügung stehen.

Derartige Programme akkumulieren ältere Daten und können in Zukunft feststellen, ob es beim Datenverkehr auffällige Spitzenwerte gibt, die möglicherweise auf einen Angriff hindeuten, wobei mitunter sogar die Herkunft des Angriffs ermittelt wird.

Zudem lohnt es sich, detaillierte Protokolle von Angriffen aufzubewahren, um ähnliche Vorfälle in Zukunft zu unterbinden, etwa durch Erstellung einer Prüfliste und einer Suche nach potenziellen Sicherheitsdiensten, die mit den jeweiligen Störmustern umgehen können.

Auch Angriffssimulationen können dienlich sein, damit Netzwerkbetriebszentren die Bedrohungen bewältigen können und einen speziellen Aktionsplan für diese bereithalten, um kritische Assets schon im Vorfeld identifizieren zu können. Das Network Security Team (NST) des Global IP Network von NTT nimmt gern an derartigen Simulationen teil und fordert die Kunden nachdrücklich auf, das Unternehmen zu diesem Zweck zu kontaktieren.
Ganz generell ist der Aufbau von engen Beziehungen zu den Sicherheitsteams eines Anbieters ein guter Weg zur Stressbewältigung, wann immer ein Angriff passiert.

Eine angemessene Reaktion lässt sich in Zusammenarbeit mit einem Netzwerkanbieter wie NTT deutlich schneller finden.

Die Teams arbeiten dann im Ernstfall effektiv zusammen, um etwaige Bedrohungen einzudämmen, wobei sie je nach Lage auf Verfahren wie Blockieren oder Bereinigen des Datenverkehrs zurückgreifen können. Eine automatisierte Behebung mit Anbietern wie NTT ermöglicht eine schnelle Reaktion in nur 30 Sekunden. Dies ist bei einer zunehmenden Zahl von sehr kurzen Angriffen in Bereichen wie Gaming bedeutsam, wo die Angriffe oft nicht länger als fünf Minuten dauern.

Eine automatisierte Behebung mit Anbietern wie NTT ermöglicht eine schnelle Reaktion in nur **30 Sekunden**.

Prüfung und Zusammenarbeit

Auch wenn der Angriff schon abgewehrt wurde, sollte die Arbeit weitergehen. Dies ist dann der Zeitpunkt für ein „Post-Mortem", wobei analysiert wird, was genau geschehen ist, und welche Fehler und Lücken in der technischen Ausrüstung vorliegen, um dann für den nächsten Angriff gewappnet zu sein.

Auf diese Weise lassen sich bestimmte Faktoren bewerten, beispielsweise ob die Firewalls den unerwünschten Datenverkehr aufhalten konnten, ob es einzelne kompromittierte oder verletzliche Server gab, und ob Upgrades oder eine intelligentere Schadensminderung in Betracht gezogen werden sollten.

Ein Dokumentieren des Angriffstyps kann für das Netzwerkbetriebszentrum nützlich sein, um eine unerwünschte Art von Datenverkehr auch in Zukunft zu erkennen und schnell darauf zu reagieren. Nach dem Angriff ist es eventuell auch möglich, dessen Verursacher ausfindig zu machen und Maßnahmen gegen diesen zu ergreifen.

Zudem ist eine Zusammenarbeit in der Branche entscheidend, um die Auswirkungen von Bedrohungen zu reduzieren: das Global Leaders Forum versammelt regelmäßig Netzbetreiber und mit DDoS befasste Personen, um Ideen und Informationen auszutauschen und ein gegenseitiges Kennenlernen zu fördern, um schnelle Kontaktmöglichkeiten zu eröffnen. Online-Sicherheitsgruppen wie NSP-SEC und Ops-Trust sind weitere Möglichkeiten einer Zusammenarbeit.

NTT arbeitet mit vielen Gruppen und Events zusammen, um Meetings zu arrangieren, bei denen bessere Ansätze gegenüber DDoS-Angriffen gefunden werden können.

DDoS-Schutz mit NTT

Bei der Einführung von neuen Produkten und Dienstleistungen bleibt ein Höchstmaß an Schutz unabdingbar, weshalb NTT genau dort einen proaktiven Ansatz verfolgt. Hierdurch können Bedrohungen schon frühzeitig abgewendet werden, statt auf diese erst im Nachhinein zu reagieren.

Mit eben dieser Perspektive bieten die DDoS Protection Services (DPS) des Global IP Network von NTT intelligente DDoS-Maßnahmen, bei denen schädlicher Datenverkehr bereinigt wird, noch bevor die Internetverbindung des Kunden in Mitleidenschaft gezogen wird. Möglich wird dies durch eine Umleitung des Datenverkehrs auf die unternehmenseigenen Bereinigungszentren, wo sie analysiert und die Angriffsdaten entfernt werden, bevor der Rest dann zum Kundennetzwerk weitergeleitet wird.

Zwischenzeitlich hat NTT unterschiedliche Ebenen von DPS entwickelt, welche die unterschiedlichen Schutzanforderungen der Kunden von Global IP Network abdecken.

Der Service „DPS Max“ richtet sich etwa an Kunden, die einen vollumfänglichen Schutz wünschen, einschließlich Funktionen zur Angriffserkennung und automatischen Behebung. Über die letztgenannte Funktion erhalten die Kunden eine unverzügliche Behebung, indem die Plattform zunächst Angriffe erkennt und automatisch Verteidigungsmaßnahmen ergreift, die von kundendefinierten Schwellenwerten abhängen. Sobald der Angriff vorüber ist, setzt die Plattform den Kunden-Datenverkehr auf die standardisierte Weiterleitung zurück, wie sie vor dem Angriff bestand.

Weitere Stufen des NTT'-Service „DPS Control“, „DPS Core“ und „DPS Detect“. Bei der ersten handelt es sich um einen Einstiegsservice, bei dem Kunden die permanenten Zugriffskontrolllisten (Acess Control Lists, ALC) definieren, um bestimmte Arten von Datenverkehr auf dem Netzwerk zu blockieren. Der ideale Kundentyp für diesen Service ist ein fortgeschrittener Kunde, der sein eigenes Datenverkehrsprofil kennt und Angriffen im Wesentlichen selbst begegnen kann, zugleich aber seine Gefährdung durch bestimmte Bedrohungstypen eindämmen möchte.

Als mittlere Stufe bietet DPS Core weitere Dienstleistungen, indem im Vergleich zum Grundservice weitere Funktionen hinzugefügt werden. Ein Highlight dieses Service sind hochmoderne Technologien, mit denen auf Behebungsanfragen schnell reagiert werden kann. Auf Anfragen über das firmeneigene DPS Portal wird innerhalb von 15 Minuten reagiert, wobei es sich beim Portal um eine exklusive Schnittstelle für DDoS-Schutzservices handelt.

Das DPS Portal bietet den Kunden neben Schnelligkeit aber noch weitere wichtige Vorteile. Zum einen werden in der Support-Struktur von NTT Support-Anfragen eingereicht, zum anderen hilft ein diensthabender Sicherheitstechniker umgehend, dem Kunden. Über das Portal kann der Kunde zudem Konfigurationsänderungen anfordern, beispielsweise das Hinzufügen von Präfixen zwecks besserem Schutz und die Prüfung der Behebungshistorie sowie der Diagramme zu Angriffen.

Eine weitere Servicestufe ist „DPS Detect“. Diese bietet die bereits bei „DPS Core“ enthaltenen Funktionen und ergänzt diese durch solche Dienste wie Erkennungsfähigkeiten, um Kunden vor potenziellen Angriffen zu warnen, und eine kundeninitiierte Behebung auf Knopfdruck.

NTT bietet seinen Global IP Network-Kunden zudem ein selektives Blackholing, um den Datenverkehr im Netzwerk zu blockieren, und Angriffe auf einer geografischen Grundlage einzuschränken. Dies kann gerade dann wirksam sein, wenn großangelegte volumetrische Angriffe an der Ausbreitung gehindert werden sollen.

Die vom Global IP Networkbereitgestellten DDoS Protection Services (DPS) bieten einen intelligenten Umgang mit DDoS-Bedrohungen, bei denen **schädlicher Datenverkehr bereinigt wird,** bevor er die Internetverbindung des Kunden erreicht.

Zusätzliche Absicherung

Eine zusätzliche Schutzebene erhält man durch den Support des Network Security Team von Global IP Network. Abonnenten der DPS-Services erhalten damit direkten Zugang zu Experten, die durchschnittlich seit zehn oder mehr Jahren bei NTT sind und bei der Bewältigung von Angriffen auf einen reichen Erfahrungsschatz zurückgreifen können.

Die DPS-Services von Global IP Network sind für all diejenigen Unternehmen ideal, die einen hohen Grad an Internetkonnektivität benötigen, darunter E-Commerce-Händler, Telekom-Anbieter und Internet-Serviceanbieter, Content-Anbieter wie Video- und Gaming-Unternehmen sowie soziale Netzwerke.

Insgesamt kann man sagen, dass für Anbieter ein Multi-Strategien-Ansatz empfehlenswert ist, da es sich dabei um eine besonders umfassende Strategie im Umgang mit modernen DDoS-Angriffen handelt. Dies umfasst eine Kombination von Filterung am Front-End, um ungenutzte Anwendungen zu blockieren, selektives Blackholing vorzunehmen und eine DDoS-Risikominderung durch intelligente Bereinigung zu erreichen.

Indem man die zuvor empfohlenen Maßnahmen ergreift und eng mit NTT sowie seinen gut etablierten Sicherheitsmechanismen zusammenarbeitet, lassen sich beim gemeinsamen Beheben von DDoS-Problemen gewaltige Fortschritte erzielen.

Together we do great things

Um weitere Informationen oder Feedback zu erhalten,
kontaktieren Sie uns unter: gin@ntt.net

Folgen Sie uns auf Twitter
@GinNTTnet
#globalipnetwork #AS2914

Oder besuchen Sie uns: gin.ntt.net