Schutz für Ihre zustandsbehafteten Geräte

DDoS-Angriffe sind so sehr auf dem Vormarsch, dass die Anzahl der beobachteten DDoS-Angriffe zum ersten Mal die Schwelle von zehn Millionen überschritten hat. Das ATLAS Security Engineering and Response Team (ASERT) von NETSCOUT hat im Verlauf des letzten Jahres insgesamt 10.089.687 Angriffe gezählt. Während des Lockdowns durch die Pandemie im Frühling letzten Jahres starteten Cyberkriminelle außerdem 929.000 DDoS-Angriffe allein im Mai. Das ist die höchste Anzahl an Angriffen, die wir jemals in einem Monat gemessen haben. Diese Angriffe richteten sich hauptsächlich gegen kritische zustandsbehaftete Home Office- und Home Schooling-Infrastrukturen wie etwa Firewalls und VPN-Konzentratoren (Virtuelles privates Netzwerk).

Herausforderung

Die Angriffe werden nicht nur immer häufiger, sondern auch immer komplexer. Bei der Worldwide Infrastructure Security Survey (WISR) meldeten 58 % der teilnehmenden Unternehmen Multi-Vektor-Angriffe. Dies entspricht einem Anstieg von 38 % im Jahresvergleich. In der zweiten Jahreshälfte 2020 wurden bei einem Angriff 26 verschiedene Angriffsvektoren eingesetzt. Das ist ein neuer Rekord. Diese komplexen Angriffe nutzen eine dynamische Mischung aus State Exhaustion- und volumetrischen Angriffen sowie Angriffen auf der Anwendungsebene. Die Angreifer führen mehrere Angriffstypen gleichzeitig oder abwechselnd aus, was sehr schwer abzuwehren ist.

Die zunehmenden Netzwerkzugriffe durch Benutzer und Geräte durch den Anstieg der Home Office-Mitarbeiter während der Pandemie tragen ebenfalls zur Gefährdung der Geschäftskontinuität bei. Die Cyberkriminellen wissen, dass Unternehmen mit vielen Remote-Mitarbeitern angreifbarer sind und lassen sich davon zu gezielten Angriffen motivieren, um Server zum Absturz zu bringen und Systeme aller Größen in die Knie zu zwingen. Einige der typischen Ziele für Verbrecher sind zustandsbehaftete Geräte wie Firewalls und VPN-Geräte. Tatsächlich meldeten 83 % der WISR-Teilnehmer DDoS-Angriffe, bei denen Ausfälle durch überlastete Firewalls und/oder VPN-Geräte entstanden, was einer Zunahme um 21 % gegenüber 2019 entspricht.

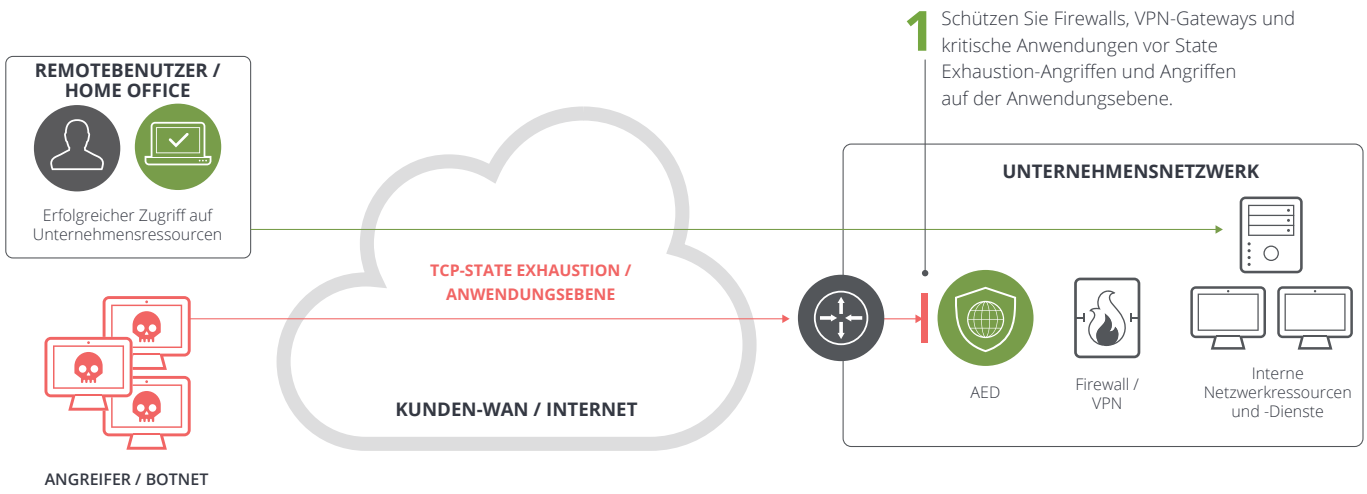
Bedrohung

Firewalls, VPNs und andere Sicherheitsprodukte sind unverzichtbare Elemente einer mehrschichtigen Verteidigungsstrategie, wurden jedoch speziell für Sicherheitsprobleme entwickelt, die sich grundlegend von dedizierten DDoS-Erkennungs- und -Abwehrprodukten unterscheiden. Das Problem besteht darin, dass Firewalls und VPNs üblicherweise zustandsbehaftet sind. Dies bedeutet, dass sie Tabellen verwenden, um Verbindungsdetails wie IP-Adressen, Ports und Zeitstempel zu erfassen. Der Speicherplatz für diese Tabellen ist endlich, und selbst leistungsstarke Geräte, die Millionen von Verbindungen verarbeiten können, können mit Flooding-Angriffen überwältigt werden und sind daher anfällig für DDoS-Angriffe und werden sogar häufig direkt zum Ziel der Angriffe. Da die zustandsbehafteten Geräte bei mehrschichtigen Angriffen oft direkt oder indirekt ins Visier geraten, müssen diese Geräte ebenfalls geschützt werden. Selbst ein Angriff mit geringem Volumen kann die Ressourcen von VPN-Konzentratoren oder Firewalls erschöpfen. Spezielle Angriffsvolumen von wenigen MBit/s können ausreichen, um Netzwerkfirewalls so weit zu überlasten, dass sie keine weiteren Verbindungen mehr annehmen.

Um sich angemessen vor DDoS-Angriffen zu schützen, brauchen Sie eine Lösung, die alle Arten von Angriffen abwehren und Ihre zustandsbehafteten Geräte schützen kann.

Risiko

Die Verfügbarkeit von geschäftskritischen Diensten ist entscheidend, und zwar nicht nur zum Schutz vor Ertragseinbußen. Die Dienstverfügbarkeit stärkt außerdem die Reputation des Unternehmens in der Branche und trägt zu nachhaltigen Geschäftserfolgen bei. Cyber-Resilienz bezeichnet die Fähigkeit einer Entität, ein gewünschtes Ergebnis auch angesichts von widrigen Cyber-Ereignissen zu liefern. Widrige Cyber-Ereignisse sind Ereignisse, die die Verfügbarkeit vernetzter IT-Systeme und der zugehörigen Informationen und Dienste beeinträchtigen.



VPNs

Historisch gesehen wurden VPNs nicht immer eingesetzt, aber in der COVID-19-Pandemie haben sie sich zum Rückgrat vieler Unternehmen entwickelt. Die normalen Kapazitäten werden weit überschritten, und kritische Anwendungen und Ressourcen sind stark ausgelastet. In dieser Situation können auch relativ kleine DDoS-Angriffe mehr denn je ein VPN-Gateway in die Knie zwingen und den Geschäftsbetrieb für Remotebenutzer im Home Office zum Erliegen bringen. Auch nach der Aufhebung von pandemiebedingten Lockdowns und einer Rückkehr zur Normalität werden viele Unternehmen weiterhin zumindest eine Hybrid-Arbeitsumgebung mit Home Office anbieten, und VPN-Gateways müssen auch weiterhin geschützt werden.

Firewalls

Firewalls sorgen für die Einhaltung von Richtlinien und verhindern unbefugte Zugriffe auf Daten. Diese Sicherheitsprodukte schützen zwar die Integrität und Vertraulichkeit von Netzwerken sehr effektiv, bieten jedoch praktisch keinen Schutz vor einem der Hauptprobleme bei DDoS-Angriffen: der Verfügbarkeit. Eine Firewall der nächsten Generation (Next-Generation Firewall, NGFW) ist eine Cybersicherheitslösung, die Netzwerke mit Fähigkeiten schützt, die weit über die Funktionen herkömmlicher Firewalls hinausgehen. Während herkömmliche Firewalls Negativlisten verwenden, um verdächtigen Datenverkehr zu erkennen und Netzwerkzugriffe zu blockieren, bieten NGFWs zusätzliche Funktionen wie Einbruchsschutz und Deep-Packet-Inspection. Dennoch bieten momentan selbst NGFWs keinen angemessenen Schutz und werden oft selbst zum Ziel von Angriffen.

Abwehr

Arbor Edge Defense® (AED) ist eine lokale, immer aktive, zustandslose, DDoS-spezifische Abwehrlösung. AED kann Angriffe mit bis zu 40 Gbit/s abwehren und ist dank des zustandslosen Designs nicht anfällig für State Exhaustion-Angriffe, die sich gegen zustandsbehaftete Geräte wie VPN-Gateways, Firewalls oder Lastenausgleichsmodule richten. AED wird am Rand des Netzwerks zwischen dem Internet und den zustandsbehafteten Geräten in Ihrem Netzwerk eingesetzt und schützt Ihre Geräte vor den gegen sie gerichteten Angriffen. Wenn ein großer volumetrischer Angriff versucht, den Internetanschluss zu überlasten, routet die Cloud-Signaling-Funktion von AED den Datenverkehr automatisch zu einem cloudbasierten DDoS-Schutz wie NETSCOUT Arbor Cloud oder einer Lösung Ihres ISPs.

Normalerweise kann AED die DDoS-Bedrohungen und die Gefahren für Ihre zustandsbehafteten Geräte abwehren und dafür sorgen, dass die geschäftskritischen Anwendungen und Dienste Ihres Unternehmens durchgängig verfügbar bleiben.

Zusammenfassung

Die Häufigkeit und Komplexität von DDoS-Angriffen nimmt eindeutig zu, wenn man die Anzahl und die Vielfalt der Vektoren bei den einzelnen Angriffen betrachtet. Durch die Pandemie bedingt arbeiten zahlreiche Mitarbeiter von Zuhause, und Angreifer nutzen die durch VPN-Geräte und Firewalls entstandene zusätzliche Angriffsoberfläche. Tatsächlich haben die Ausfälle, bei deinen diese zustandsbehafteten Geräte das Ziel von Angriffen wurden, zugenommen, obwohl diese Geräte überall zum Sicherheitsstack gehören und bei jeder Netzwerkschutzstrategie berücksichtigt werden. Es ist nur eine Frage der Zeit, bis durch diese Zunahme an Angriffen die Verfügbarkeit Ihrer Dienste für Ihre Endbenutzer oder Kunden beeinträchtigt wird, was sich wiederum auf Ihre Erträge auswirkt. Die Best Practice für den DDoS-Schutz ist ein Hybrid-Ansatz mit einer cloudbasierten und lokalen zustandslosen In-Line-DDoS-Schutzlösung wie AED, um Ihre zustandsbehafteten Geräte vor weiteren Angriffen zu schützen.

NETSCOUT

Unternehmenszentrale
NETSCOUT Systems, Inc.
Westford, MA 01886-4105
Telefon: +1 978-614-4000
www.netscout.com

Vertriebsinformationen
USA gebührenfrei: 800-309-4804
(Internationale Nummern siehe unten)

Produktsupport
USA gebührenfrei: 888-357-7667
(Internationale Nummern siehe unten)

NETSCOUT bietet Vertrieb, Support und Dienste in mehr als 32 Ländern an. Globale Adressen und internationale Telefonnummern finden Sie auf der NETSCOUT-Website unter: www.netscout.com/company/contact-us

SECUC_015_DE-2102 10/2021