WHITEPAPER

Die rasante Evolution und wachsende Bedrohung durch DDoS-Angriffe

Da alle Angriffe immer gezielter, ausgeklügelter und häufiger werden, muss jedes Unternehmen wachsam bleiben.

Kein Unternehmen ist mehr vor DDoS-Angriffen (Distributed Denial of Service) sicher. Cyberkriminelle, die sich auf Erpressung, Hacktivismus oder Rache konzentrieren, können mit großen und ausgeklügelten Angriffen problemlos jedes Unternehmen angreifen. Aus diesem Grund benötigt jedes digitale Unternehmen einen ganzheitlichen Schutz vor DDoS-Angriffen.

Einer der frühesten Angriffe im Internet

Am 22. Juli 1999 überforderten 114 kompromittierte Computer einen einzelnen Computer der University of Minnesota mit überflüssigen Datenpaketen und legten ihn zwei Tage lang lahm.

Dies war laut MIT Technology Review der erste jemals dokumentierte DDoS-Angriff.

In den folgenden Wochen und Monaten gingen wichtige Akteure – von CNN bis Amazon – offline, als Hacktivisten und andere Cyberkriminelle feststellten, wie einfach diese Angriffe waren. Es brauchte nur ein paar Zeilen Code.

DDoS wurde zu einer Bedrohung für jedes Unternehmen mit einer Online-Präsenz.

Diese Angriffe werden immer größer und raffinierter

Die DDoS-Abwehrmaßnahmen sind seit 1999 weit vorangeschritten. Aber die Angreifer auch. Die DDoS-Bedrohungsakteure von heute verfügen über Dutzende von Angriffsvektoren und kostengünstigen Angreifer-Toolkits sowie unzählige anfällige Geräte im Internet, mit denen sie ihre Kampagnen verstärken können. 2016 legten Angreifer einen großen Teil des Internets mit kompromittierten DVRs von Sicherheitskameras lahm.

Seitdem sind viele Millionen ungeschützter IoT-Geräte online gegangen. Durch die 5G-Revolution werden es mindestens noch einmal so viele werden. Stellen Sie sich nur die Stärke und den Umfang der Angriffe vor, die durch die exponentiellen Verbesserungen von 5G bei Geschwindigkeit, Kapazität und Latenzzeit möglich werden.

Außerdem wächst die Anzahl der ungeschützten und nicht verwalteten Server im Internet, die Kriminelle für Verstärkungs- und Reflection-Angriffe kidnappen können, immer weiter. Viele dieser Server – und die Kriminellen kennen deren IP-Adressen – können Fake-Anfragen um einen Faktor von mehr als 50.000 multiplizieren.

Das ist DDoS-Abwehr und -Schutz bei Notfällen rund um die Uhr.

Akamai-Kunden, die von einem DDoS-Angriff bedroht sind, sollten sich an das Akamai Security Operations Command Center (SOCC) wenden.

Wenn Sie kein Akamai-Kunde sind, aber Notfallschutz benötigen, füllen Sie das Formular auf unserer **DDoS-Hotline-Seite** aus, oder rufen Sie die Nummer **+1-877-425-2624** an, um sofort Hilfe zu erhalten.

Keine Branche ist immun gegen DDoS-Angriffe

Heute wehrt Akamai jedes Jahr Tausende von DDoS-Angriffen ab.

In einigen Fällen sind die Motive offensichtlich. Ein Gamer kann DDoS-Angriffe nutzen, um Netzwerke zu verlangsamen und sich einen Wettbewerbsvorteil gegenüber anderen Spielern zu verschaffen. Hochschulstudenten haben bereits gezielte DDoS-Angriffe durchgeführt, um die Kunden eines Internetproviders zu frustrieren und das Geschäft eines Mitbewerbers zu fördern.

Manchmal sind die Motive jedoch komplexer oder schwerer fassbar. Wir haben erlebt, dass Kriminelle DDoS-Angriffe auf eine Unternehmensabteilung nutzen, um die Vorfallsreaktionsteams von einem anderen weniger offensichtlichen Angriff auf eine andere Abteilung abzulenken.

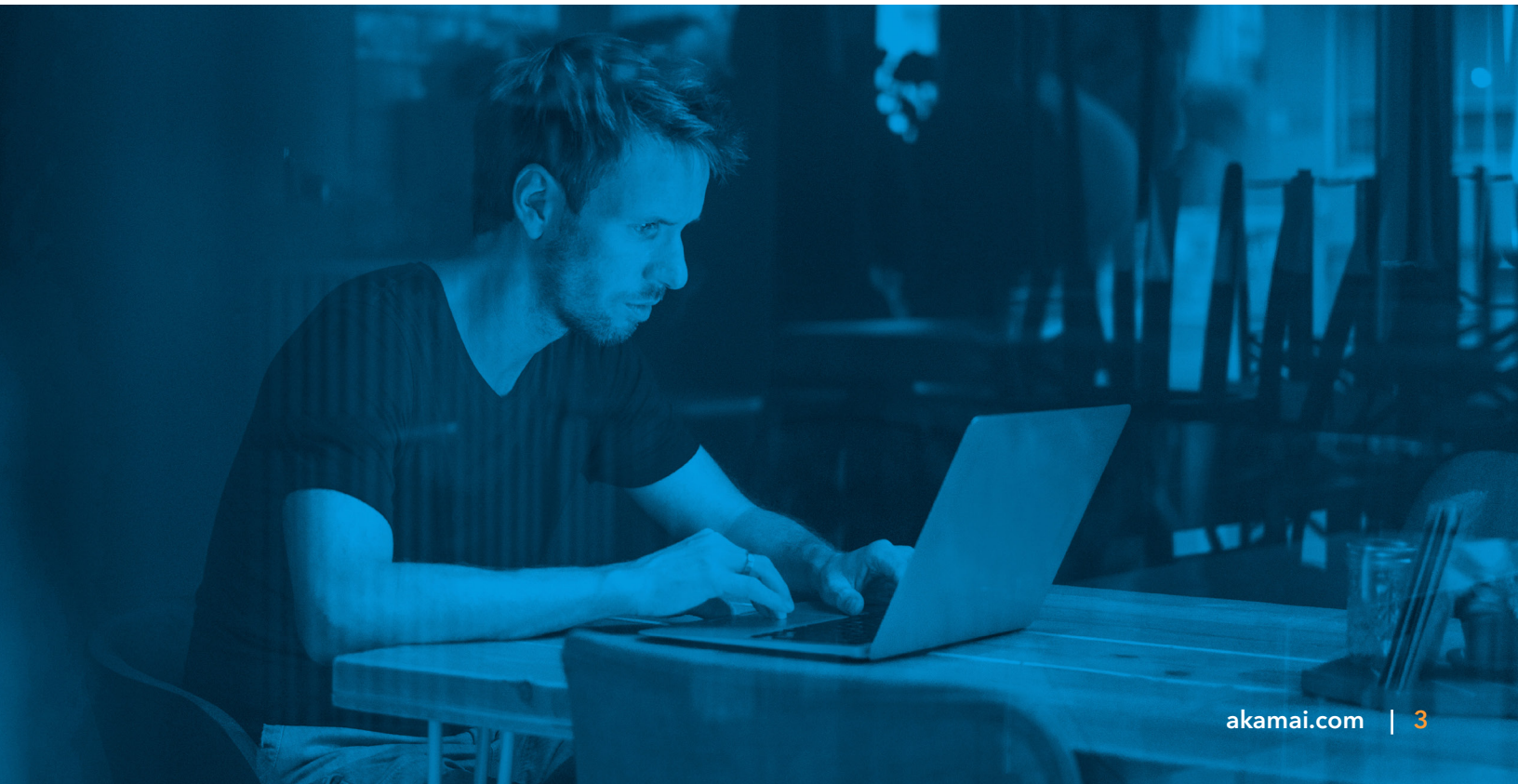
Für böswillige Akteure, die nicht über die entsprechenden Fähigkeiten verfügen, gibt es im Darknet „DDoS for Hire"-Unternehmen. Die Preise beginnen bei 5 $ für einen fünfminütigen Angriff und steigen für 24 Stunden auf 400 $ an. Wenn jemand ein Hühnchen mit einem Unternehmen zu rupfen hat, kann er mit 200 oder 300 $ Schäden in Millionenhöhe verursachen.

Im Jahr 2020 gab es größere und raffiniertere Angriffe

Im ersten Halbjahr 2020 stoppte Akamai massive Angriffe mit 1,44 Terabit pro Sekunde (Tbit/s) und 809 Millionen Paketen pro Sekunde (Mpps), dem größten jemals beobachteten Mpps-Angriff.

Obwohl diese Angriffe in weniger als einer Sekunde entschärft wurden, spiegeln sie einen Trend zu mehr Angriffen mit 100 Gbit/s oder mehr wider. Viele davon nutzen einzigartige und komplexe Kombinationen aus mehreren Vektoren. Es geht darum, Abwehrmechanismen zu überfordern oder zu umgehen und Ressourcen zur Reaktion auf Vorfälle zu blockieren.

Auch Angriffe, die nicht nur automatisierte Reaktionen, sondern zumindest einen gewissen Grad an Eingriffen durch den Menschen erfordern, sind auf dem Vormarsch.



Start der größten DDoS-Erpressungskampagne der Geschichte

Im August 2020 gab das Akamai Security Intelligence Research Team eine Warnung heraus, die darauf hinwies, dass Unternehmen in verschiedenen Branchen DDoS-Erpressungs-E-Mails erhalten haben. Die Angreifer drohten damit, den Betrieb lahmzulegen, und deuteten an, dass die Unternehmen mit enormen Ausfallzeiten und schweren finanziellen Verlusten rechnen müssten, wenn sie nicht ein Lösegeld in Bitcoin zahlen würden.

Nur wenige Wochen später berichtete das FBI, dass Tausende von Unternehmen weltweit ähnliche Erpressungs-E-Mails erhalten hätten. Die Angreifer schwärmten aus und bedrohten Unternehmen in einer Branche, wechselten dann zu einer anderen und danach zu einer weiteren. Die gut organisierten Angreifer kehren häufig zurück, um frühere Ziele erneut zu bedrohen.

Je besser Ihre Abwehrmechanismen sind, desto unwahrscheinlicher ist es, dass Sie angegriffen werden

Cyberkriminelle sind wie alle anderen Kriminellen. Sie sehen sich den Laden an und suchen nach einer Schwachstelle. Für DDoS bedeutet dies, dass die DNS, Webanwendungen und die dem Internet zugewandten Rechenzentren des Opfers untersucht werden.

Wenn dabei verwundbare Ressourcen, Websites oder Dienste erkannt werden, können Cyberkriminelle eindringen. Wenn sie starke Verteidigungsmaßnahmen feststellen, ziehen sie oft weiter.

Tatsächlich wurde die große Mehrheit der neuen Prolexic-Kunden, die vor der Weiterleitung auf die Plattform angegriffen wurden, nicht mehr angegriffen, nachdem Prolexic-Abwehrmechanismen eingerichtet wurden. Für Cyberkriminelle sind die von Prolexic verteidigten Ziele möglicherweise nicht die Zeit wert, vor allem wenn es anderswo einfachere Beute gibt.

So funktioniert eine ganzheitliche DDoS-Abwehr

Akamai gewährleistet durch ein transparentes Netz von dedizierten Edge-, verteilten DNS- und Cloud-Scrubbing-Lösungen ein gestaffeltes DDoS-Sicherheitskonzept mit einer Netzwerkgesamtkapazität von über 175 Tbit/s. Diese speziellen Clouds wurden entwickelt, um die DDoS-Sicherheit zu stärken und gleichzeitig die Angriffsflächen zu reduzieren. Dieser End-to-End-DDoS-Schutz ist so konzipiert, dass er die Qualität der Abwehr verbessert, Fehlalarme reduziert und gleichzeitig die Widerstandsfähigkeit gegen die größten und komplexesten Angriffe steigert.

Darüber hinaus kann die Lösung gezielt auf die spezifischen Anforderungen Ihrer Webanwendungen oder internetbasierten Services abgestimmt werden.

Edge-Schutz

Akamai hat seine global verteilte Intelligent Edge Platform als Reverse-Proxy konzipiert, der nur Traffic über die Ports 80 und 443 akzeptiert. Alle DDoS-Angriffe auf Netzwerkebene werden mit einem Null-Sekunden-SLA sofort an der Edge abgewehrt.

Bei Ereignissen auf der Anwendungsebene, einschließlich solcher, die über APIs ausgelöst werden, absorbiert der Kona Site Defender die Angriffe und gewährt gleichzeitig legitimen Nutzern den Zugang.

DNS-Schutz

Der autoritative DNS-Dienst von Akamai, Edge DNS, filtert auch Traffic an der Edge. Akamai Edge DNS ist im Gegensatz zu anderen DNS-Lösungen speziell für Verfügbarkeit und Ausfallsicherheit bei DDoS-Angriffen ausgelegt. Edge DNS bietet durch Redundanzen auf mehreren Ebenen, darunter Nameserver, Points of Presence, Netzwerke und sogar segmentierte IP-Anycast-Clouds, eine überragende Performance.

Schutz durch Cloud-Scrubbing

Prolexic schützt ganze Rechenzentren und hybride Infrastrukturen vor DDoS-Angriffen über alle Ports und Protokolle hinweg, mit 20 globalen Scrubbing-Zentren und 8,2 Tbit/s dedizierter DDoS-Abwehr. Diese Kapazität ist so konzipiert, dass internetfähige Assets verfügbar bleiben – ein Eckpfeiler jedes Informationssicherheitsprogramms.

Prolexic ist ein vollständig verwalteter Service und unterstützt sowohl positive als auch negative Sicherheitsmodelle. Der Service kombiniert automatisierte Abwehrmaßnahmen mit der Eindämmung durch Experten aus dem globalen SOCC-Netzwerk von Akamai. Prolexic bietet zudem ein **branchenführendes** SLA für die Abwehr in null Sekunden über proaktive defensive Kontrollen an.

Wie Prolexic einen rekordverdächtigen Angriff stoppte

Der Angriff vom Juni 2020 mit 809 Mpps war der größte Angriff an Paketen pro Sekunde (PPS), der jemals im Internet beobachtet wurde. Im Gegensatz zu den häufigeren Bits-pro-Sekunde-Angriffen, die versuchen, die eingehende Internet-Pipeline zu überlasten, zielen PPS-Angriffe darauf ab, die Netzwerkauslastung im Rechenzentrum oder in der Cloud auszuschöpfen.

Dieser gewaltige Angriff beinhaltete eine enorme Anzahl von Quell-IP-Adressen. Mehr als 96 % davon waren zuvor noch nie bei Angriffen beobachtet worden. Der Angriff stieg in nur zwei Minuten von 418 Gbit/s auf 809 Mpps an.

Glücklicherweise war das Zielunternehmen ein Prolexic-Kunde, der durch ein Null-Sekunden-SLA geschützt wurde. Das Akamai SOCC hat mit diesem Kunden zusammengearbeitet, um die Basisprofile des Traffic in ruhigen Zeiten zu verstehen und Kontrollen und Sicherheitsrichtlinien einzurichten, um DDoS-Angriffe sofort zu blockieren.

Fragen Sie noch heute nach einem nutzerspezifischen Briefing

Besuchen Sie dafür **akamai.com/ddos-briefing**