SOTI

B10 AUSGABE 02

10 YEARS
OF SECURITY INSIGHT

Immer im Einsatz

gegen die zunehmenden DDoS-Bedrohungen in EMEA

Akamai

„State of the Internet“-Sicherheitsbericht

Inhaltsverzeichnis

DDoS wird in EMEA immer häufiger eingesetzt

DDoS-Angriffe (Distributed Denial of Service) nehmen weltweit zu und werden immer raffinierter. Dieser Anstieg ist besonders in Europa, dem Nahen Osten und Afrika (EMEA) zu beobachten, wo Forscher von Akamai eine dramatische Aufwärtsbewegung bei der Wachstumsrate von DDoS-Angriffen beobachten konnten. Tatsächlich steigt die Rate der DDoS-Angriffe in der Region sogar noch schneller an als in anderen Regionen. DDoS-Angriffe betreffen Ziele mit unerwünschtem böswilligem Traffic und behindern den Betrieb von Netzwerken und Websites in EMEA.

Unsere Vermutung ist, dass ein Großteil dieser regionalen Verschiebung auf geopolitische Spannungen zurückzuführen ist – wie Aktivitäten von Nationalstaaten und Hacktivismus als Reaktion auf anhaltende Kriege, einschließlich der Kriege zwischen Russland und der Ukraine und Israel und der Hamas. Und die bevorstehenden hochkarätigen Ereignisse und Wahlen in Europa dürften das Risiko von DDoS-Angriffen noch weiter erhöhen. Doch leider nimmt nicht nur das Ausmaß der EMEA-DDoS-Ereignisse zu – wir haben auch einen Anstieg bei der Anzahl der von Cyberkriminellen eingesetzten DDoS-Angriffsvektoren sowie bei der Dauer dieser Angriffe beobachtet.

In diesem „State of the Internet"-Bericht (SOTI) befassen wir uns mit der Art und Häufigkeit von DDoS-Angriffen in der EMEA-Region und untersuchen einige der wichtigsten Branchen, die von diesen Angriffen betroffen sind, darunter Finanzdienstleistungen, Handel und Gesundheitswesen. Wir betrachten auch die neue EMEA-Gesetzgebung, die den Schutz vor den vermehrten Cybersicherheitsbedrohungen in der Region stärken soll. Und wir stellen Abwehr- und Schutztechniken vor, die gemeinsam die zunehmende Gefahr von DDoS-Bedrohungen in EMEA eindämmen können.

Wichtige Erkenntnisse aus dem Bericht

Akamai-Forscher haben beobachtet, dass die Zahl der DDoS-Angriffe in EMEA seit Anfang 2019 kontinuierlich ansteigt, mit höheren Spitzenwerten.

Mehr als ein Drittel aller DDoS-Angriffe weltweit finden in der EMEA-Region statt.

Die Komplexität und Schwere von DDoS-Angriffen in der EMEA-Region wurde durch geopolitische Motive wie Hacktivismus verändert. Und das kann lebensbedrohliche Folgen haben.

Laut einer Studie von Akamai gehören DNS-DDoS-Angriffstypen zu den häufigsten DDoS-Angriffen. Insbesondere wurde der NXDOMAIN-Vektor (nonexistent domain) beobachtet, der auch als „Pseudo-Random Subdomain"-Vektor bekannt ist. Hierbei werden DNS-Nameserver mit Anfragen für nicht vorhandene Domains überflutet.

Mehr als ein Drittel der DDoS-Ereignisse nutzten mehrere Angriffsvektoren – bis zu zwölf –, um den Erfolg zu steigern.

In der EMEA-Region sind Finanzdienstleistungen die Branche mit der höchsten Anzahl an Layer-3- und Layer-4-Angriffen; bei Layer-7-Angriffen handelt liegt der Handel vorne.

Die Regierungen und Nationen in EMEA haben wollten die Informationssicherheit steigern, indem sie neue gesetzliche Maßnahmen wie NIS2 und DORA erlassen haben, um positiven Einfluss auf IT- und Cybersicherheitsstrategien zu nehmen, einschließlich besserer DDoS-Resilienz und besseren -Schutz.

DDoS damals und heute

DDoS-Angriffe – unabhängig davon, ob sie von Einzelpersonen oder Botnets durchgeführt werden – überfluten Server mit Anfragen und Traffic. Das führt dazu, dass die gehosteten Dienste und Websites für Nutzer und Besucher nicht verfügbar sind.

Seit der Zeit, in der Cyberkriminelle Open-Source-Tools eingesetzt wurden, haben sich DDoS-Angriffe deutlich weiterentwickelt. Für diese Gruppe war die Motivation oft einfach: Vielleicht waren sie mit dem neuesten Update eines Videospiels unzufrieden, wollten sich einen Wettbewerbsvorteil verschaffen oder sahen in den Angriffen eine Art Sport. Im Allgemeinen dominierte in dieser Gruppe weder der Trend, kritische Infrastrukturen oder Krankenhäuser anzugreifen, noch bestand das Ziel darin, Netzwerke ernsthaft zu beschädigen oder Menschenleben zu gefährden.

Doch Hacktivismus hat die Landschaft dramatisch verändert – sowohl in Bezug auf die Identität der Bedrohungsakteure als auch auf ihre Motivation. Während einige Hacktivisten-Angriffe nur begrenzte oder lästige Auswirkungen haben, zielen andere auf die kommerzielle Industrie ab, um erhebliche finanzielle Gewinne zu erzielen. Hierbei können sie tagelange Serviceausfälle verursachen. Angriffe können potenziell lebensbedrohliche Folgen haben, wie es bei einigen Angriffen in Gesundheitszentren zu beobachten ist.

Mit dem Aufkommen von Services wie DDoS-Booter-Dienste ist es in den letzten Jahren einfacher geworden, DDoS-Angriffe durchzuführen. Mit diesen Services kann selbst der unraffinierteste Cyberkriminelle mit nur einem Klick und gegen eine geringe Gebühr – manchmal sogar nur 10 € – einen Angriff starten. Diese einfachen Angriffe führen dann zu einer Fülle von Traffic, der ganze Websites und Netzwerke offline zwingt, Unternehmen sowohl finanziell als auch operativ schadet und Kunden und Nutzern den Zugang zu wichtigen Diensten verwehrt.

Ein Blick durch die geopolitische Linse

DDoS-Angriffe sind ein beliebtes Instrument politisch motivierter Hacktivisten sowie nationalstaatlich geförderter Angreifer. So spielen DDoS-Ereignisse beispielsweise im laufenden Cyberkrieg zwischen ukrainischen und russischen Akteuren eine bedeutende Rolle, da Hacktivisten diese kostengünstigen Angriffe effektiv einsetzen können.

Anfang 2022 begann Akamai, die ukrainische Regierung in ihrem Cyberkrieg zu unterstützen, indem es 20 verschiedene Webressourcen von Regierungsbehörden verteidigte. Dazu gehörte auch die URL president.gov.ua, die am häufigsten angegriffene Website, bei der ein hohes DDoS-Volumen festgestellt wurde – mit Spitzenwerten von einer Million schädlichen Anfragen pro Sekunde.

Hacktivisten wie Anonymous Sudan, NoName057(16) und Killnet machen Schlagzeilen, seit Russland im Februar 2022 in die Ukraine einmarschiert ist. Killnet war die erste dieser Gruppen, die im Oktober 2021 anfing, DDoS-Dienste zur Miete anzubieten. Killnet hat Regierungsbehörden, das Gesundheitswesen, Medienunternehmen und andere angegriffen, die die Gruppe als Verbündete der Ukraine betrachtet.

NoName057(16) wird von vielen Bedrohungsforschern als Unterstützer Russlands angesehen und wurde häufig bei HTTP-basierten (Layer 7) DDoS-Angriffen beobachtet. Anfang 2023 begann die prorussische Gruppe Anonymous Sudan mit DDoS-Angriffen auf Unternehmen in Dänemark, Schweden, den USA und anderen Ländern. Im Juni 2023 wandten sich viele cyberkriminelle Gruppen, darunter ReVIL, Killnet und Anonymous Sudan der kritischen Bankeninfrastruktur zu und nutzten dabei das Chaos, das durch den russisch-ukrainischen Krieg ausgelöst wurde.

In jüngerer Zeit übernahm Anonymous Sudan die Verantwortung für den Angriff die Messaging-App Telegram in Frankreich. Dieser fand im Rahmen der beispiellosen DDoS-Attacke auf das interministerielle Netzwerk des Landes, die zur Störung von mehr als 17.000 IP-Adressen und -Geräten sowie über 300 Domains führte. Es wird angenommen, dass dieser Angriff auf Websites und Dienste der französischen Regierung eine Reaktion auf die Ankündigung des französischen Präsidenten Emmanuel Macron vom 26. Februar 2024 war, möglicherweise französische Truppen in die Ukraine zu entsenden.

Der Konflikt zwischen der Ukraine und Russland ist nicht der einzige Kampf, der zu einem Anstieg von DDoS-Angriffen in der EMEA-Region führt. Der Krieg zwischen Israel und Hamas hat ebenfalls zu verstärkten Angriffen geführt. Anonymous Sudan hat die Verantwortung für DDoS-Angriffe auf den Mossad, den nationalen Geheimdienst Israels, auf die Website und die Facebook-Konten des israelischen Premierministers sowie auf pro-israelische Seiten im Zusammenhang mit der Eskalation des Konflikts im Roten Meer übernommen. NoName057(16) hat als Reaktion auf diesen Konflikt auch israelische Webseiten angegriffen.

Verdreifachung

In der Vergangenheit verschlüsselten Ransomware-Angriffe die Daten ihrer Opfer und machten sie unbrauchbar – es sei denn, sie zahlten ein Lösegeld. Als Nächstes kamen doppelte Erpressungsangriffe: Sie erhöhten den Schaden bei Opfern, indem Kriminelle eine Kopie der Daten ihrer Daten machten, bevor sie das Netzwerk verschlüsselten. Dann drohten sie, die Daten zu veröffentlichen oder zu verkaufen, wenn das Lösegeld nicht gezahlt wurde. Ein dritter Angriffstyp – die dreifache Erpressung – entstand kurz darauf. Bei diesen Angriffen setzen Cyberkriminelle DDoS ein, um zusätzlich zu den beiden anderen Taktiken das Geschäft des Opfers zu behindern. Diese dreifachen Erpressungsangriffe werden oft als Ransom DDoS oder RDDoS bezeichnet.

DDoS ist ein gängiges Element bei Erpressungsangriffen, entweder als Nebelkerze, um Infosicherheitsteams abzulenken, während Hacker versuchen, in die Systeme einzudringen, oder um den Druck auf das Opfer zu erhöhen. Die Verwendung mehrerer Angriffsvektoren steigert die Wahrscheinlichkeit, dass das Opfer das geforderte Lösegeld zahlt. Einer der ersten dokumentierten dreifachen Erpressungsangriffe traf im Oktober 2020 in eine finnischen Psychotherapieklinik namens Vastaamo. Er ereignete sich, als Europa schnell Wege finden wollte, Gesundheitsdaten in der Europäischen Union besser auszutauschen.

Das Gesundheitswesen ist nach wie vor ein Hauptziel für Cyberkriminelle, die dreifache Erpressungsangriffe anwenden. Ein Beispiel ist die Ransomware-Gruppe NoEscape, die letztes Jahr aus der nicht mehr existierenden russischsprachigen Gruppe Avaddon hervorgegangen ist und sich auf Gesundheitsorganisationen konzentriert. Und einige Cybersicherheitsunternehmen bereiten sich bereits darauf vor, dass sich in Zukunft mehr Gruppen auf das Gesundheitswesen konzentrieren werden.

Außerdem soll die in Russland ansässige Ransomware-Gruppe LockBit seit Februar 2024 die weltweit größte und schädlichsten Ransomware-Operation durchgeführt haben, was eine Zerstörung auslöste, die Milliarden von Euro kostete. Europol und Eurojust haben sich zusammengetan, um eine internationale Taskforce namens „Operation Cronos“ zu koordinieren, die LockBit ausschalten soll. Operation Cronos umfasste Festnahmen, Haftbefehle, Anklagen und die Beschlagnahmung von 34 Servern in EMEA, Australien und den USA. LockBit war bekannt dafür, mit neuen Methoden wie RDDoS zu experimentieren, um Opfer dazu zu zwingen, Lösegelder zu zahlen.

Zwar gibt es auch andere bekannte Gruppen, die RDDoS verwenden, wie Darkside, Lazarus, AvosLocker und BlackCat, doch die Auswirkungen von Operation Cronos gegen LockBit sind bedeutend, weil es das erste Mal ist, dass die Cyber-Strafverfolgung einen solchen Effekt erzielt haben. Der Umfang und das Ausmaß dieses Einsatzes umfasste die Zerschlagung und vollständige Kontrolle der Infrastruktur einer großen Ransomware-Gruppe, während diese noch in Betrieb war.

Zurückhacken: Einsatz von DDoS zur Bekämpfung von DDoS

Das Konzept des „Zurückhackens“ mit offensiven Cyberangriffen gegen Cyberkriminelle ist seit Jahren Gegenstand von Diskussionen. Für einige gilt diese Strategie als „ein guter Angriff ist eine gute Verteidigung“ (in dem Sinne, dass sie Unternehmen vor internationalen Bedrohungen schützen kann). Andere sehen darin einen gefährlichen Präzedenzfall, da sie es Cybersicherheitsunternehmen ermöglicht, DDoS-Angriffe auf der ganzen Welt zu starten, wodurch möglicherweise die Beziehungen zwischen Staaten destabilisiert und diplomatische Spannungen verschärft werden. Darüber hinaus werfen rechtliche Unklarheiten in Bezug auf Cyberangriffe wie DDoS höchst komplexe rechtliche Fragen auf.

Wie wir wissen, setzte LockBit DDoS als Teil seiner dreifachen Erpressungsangriffe ein. Ironischerweise wurde der Einsatz dieser Methode teilweise durch einen DDoS-Angriff beeinflusst, den die Gruppe selbst erlebt hatte. Das Cybersicherheitsunternehmen Entrust wurde im Juli 2022 in die Liste der Opfer von LockBit aufgenommen. Als Reaktion darauf startete Entrust einen DDoS-Gegenangriff, der die Darknet-Systeme, die LockBit zur Veröffentlichung gestohlener Daten verwendete, effektiv zunichtemachte.

Gegenangriffe werden auch von einigen Nationalstaaten als Kriegstaktik genutzt. Die Ukraine rekrutiert Freiwillige als Teil einer „IT-Armee“ von Hackern aus der ganzen Welt, die ukrainische Netzwerke durch Hacken verteidigen. Dieses Programm gilt als das erste seiner Art.

Untersuchung der EMEA-DDoS-Daten

Die Ereignisse von DDoS-Angriffen nehmen weltweit zu und das gilt insbesondere für die EMEA-Region. Forscher von Akamai haben regionale DDoS-Daten analysiert und beobachtet, dass die Zahlen der DDoS-Attacken in EMEA stetiger zunehmen als in anderen Regionen, einschließlich Nordamerika, was insgesamt führend ist (Abbildungen 1a und 1b).

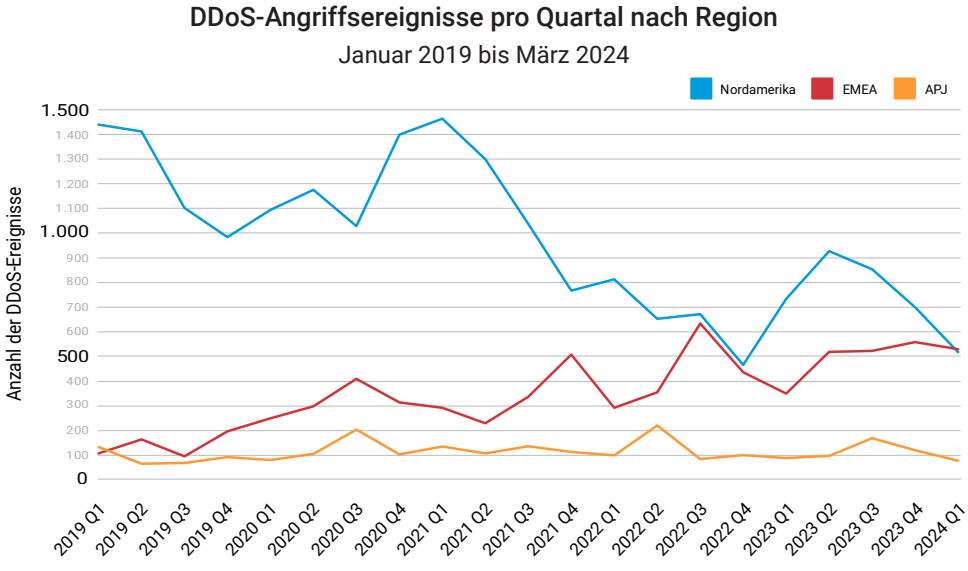

Abb. 1a: Die Anzahl der DDoS-Attacken in EMEA steigt stetiger an als in jeder anderen Region, einschließlich Nordamerika.

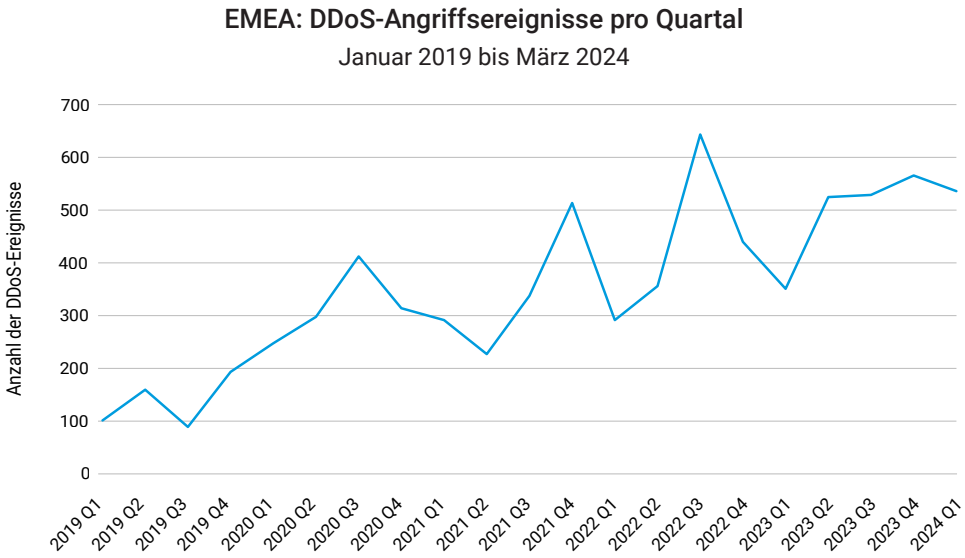

Abb. 1b: Zunahme von DDoS-Angriffen in der EMEA-Region

Innerhalb der EMEA-Region sind das Vereinigte Königreich (26 %), Saudi-Arabien (22,3 %) und Deutschland (9,1 %) führend bei den Ländern mit der höchsten Anzahl von Angriffen. Die Ergebnisse von Akamai zeigen außerdem, dass mehr als ein Drittel aller DDoS-Angriffe weltweit in der EMEA-Region stattfinden (Abbildung 2).

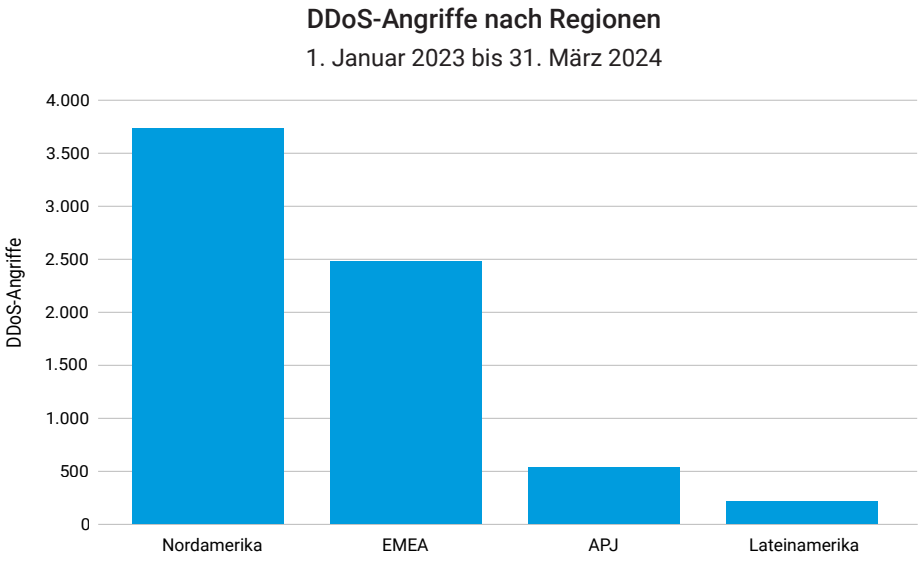

Abb. 2: Die Zahl der EMEA-DDoS-Angriffe stieg von Anfang 2023 bis zum ersten Quartal 2024 auf fast 2.500 – mehr als dreimal so viele wie in den Regionen Asien-Pazifik und Japan (APJ) und Lateinamerika (LATAM) zusammen

In der Finanzdienstleistungsbranche ist EMEA die Region mit dem meisten Traffic von DDoS-Angriffen auf Layer 3 und 4 (Abbildung 3). Wie bereits erwähnt, erklärten russische Hacktivistengruppen ihre Absicht, DDoS-Angriffe auf das europäische Bankensystem zu starten – wir gehen davon aus, dass dieser geopolitische Hacktivismus der Hauptgrund für die Zunahme von DDoS-Angriffen in der Finanzdienstleistungsbranche ist.

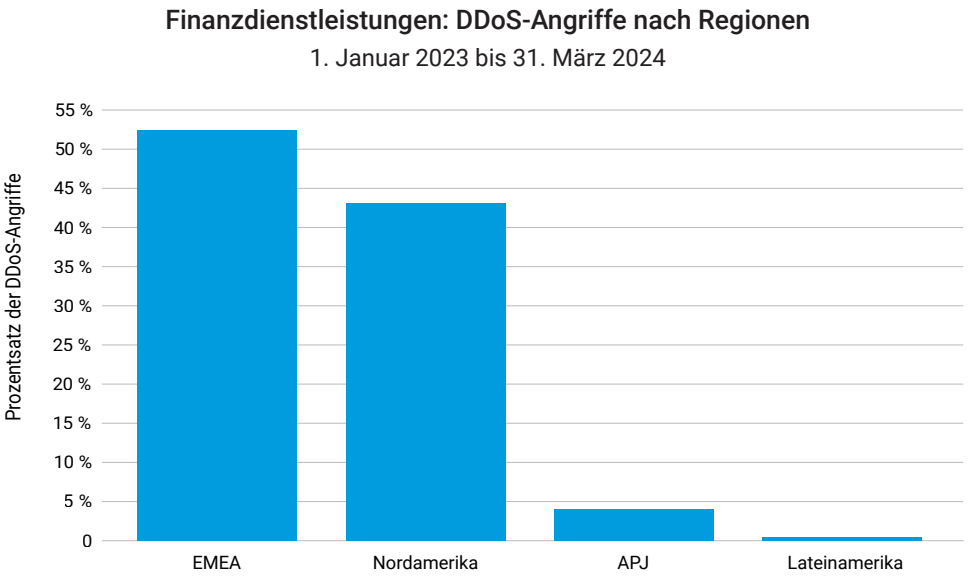

Abb. 3: EMEA verzeichnete 52,5 % des regionalen Traffics von DDoS-Angriffen auf Layer 3 und 4 in der Finanzdienstleistungsbranche.

Neben Layer-3- und Layer-4-Angriffen werden Finanzdienstleistungsanwendungen auch von Layer-7-DDoS-Angriffen heimgesucht. Die Handelsbranche verzeichnet jedoch den größten Anstieg bei Layer-7-DDoS-Angriffen in EMEA: mit fast 30 % aller Angriffe in der Region (Abbildung 4).

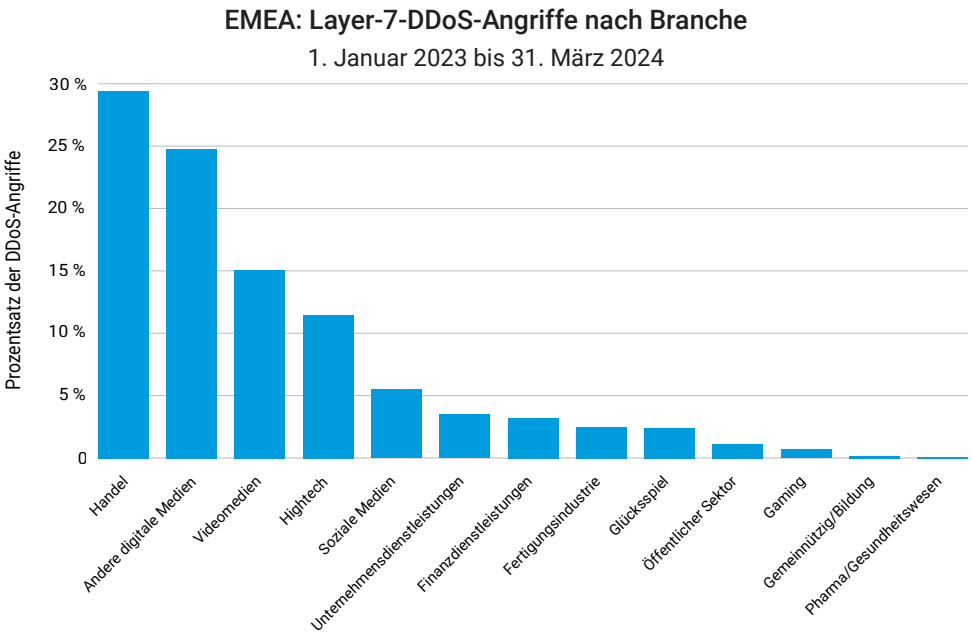

Abb. 4: Die Handelsbranche macht 29,4 % des regionalen Traffics von DDoS-Angriffen auf Layer 7 in EMEA aus.

Es ist möglich, dass DDoS-Angriffe auf Anwendungsebene, wie z. B. HTTP-Flooding, in der Handelsbranche am stärksten verbreitet sind, da Angreifer hierdurch erhebliche Umsatzeinbrüche verursachen können. Diese Art von Angriffen ist für Handelsorganisationen besonders lähmend, da sie dazu führen können, dass ein Onlineshop unzugänglich ist oder ein Reservierungssystem ausfällt, was zu erheblichen Umsatzeinbußen für das betroffene Unternehmen führt. Darüber hinaus können sie als Ablenkungstaktik eingesetzt werden, um die Ressourcen der Vorfallsreaktion auszulasten, damit Angreifer unbehelligt lukrative Kundendaten (wie Kreditkartendaten) aus anderen Bereichen im Netzwerk des Opfers stehlen können.

Doch nicht nur die Anzahl der DDoS-Angriffsereignisse ist gestiegen: Wir haben auch beobachtet, dass die Anzahl der Vektoren, die für die Bereitstellung von DDoS-Angriffen verwendet werden, stark zugenommen hat (Abbildung 5a). Zu diesen Angriffstypen gehören DNS Flood, UDP Fragment und NTP Reflection (Abbildung 5b). Darüber hinaus dauern Angriffe länger an.

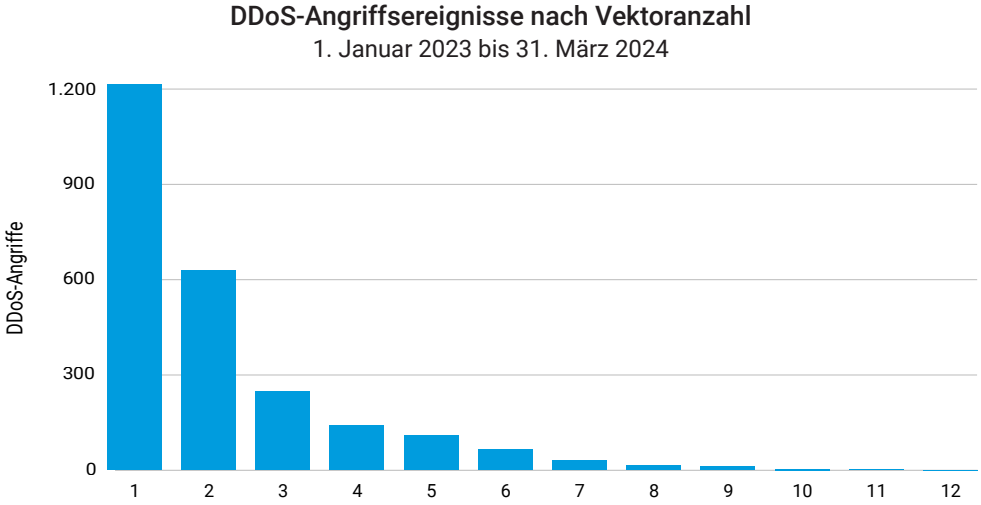

Abb. 5a: Die Anzahl der Vektoren, die für die Bereitstellung von DDoS-Angriffen verwendet werden, hat stark zugenommen.

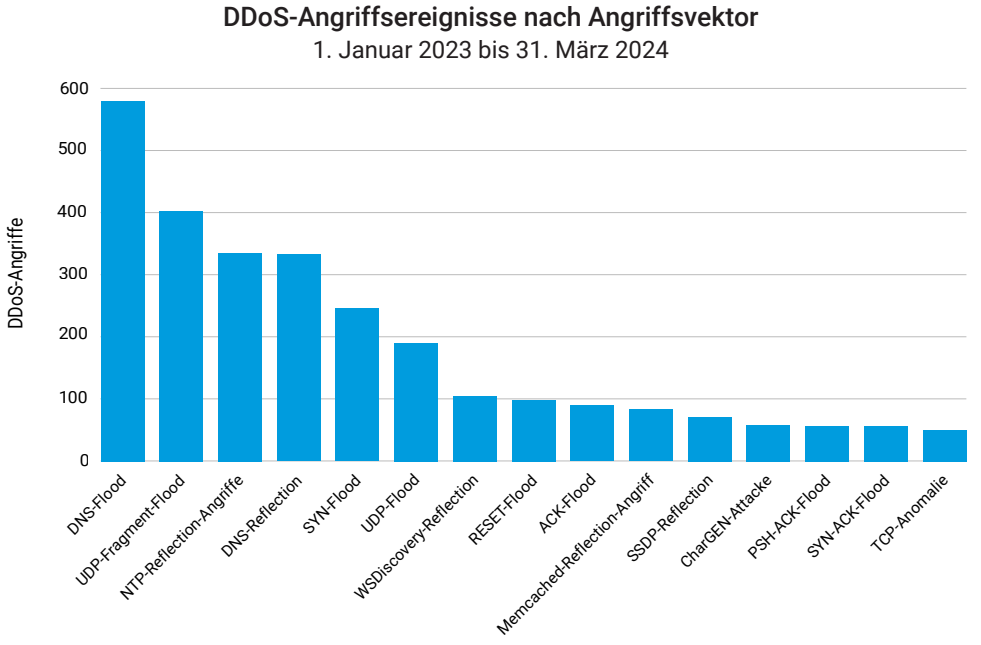

Abb. 5b: Zu den führenden DDoS-Angriffstypen in EMEA gehören DNS Flood, UDP Fragment und NTP Reflection.

Langanhaltende Angriffe beeinträchtigen nicht nur die Produktivität eines Unternehmens, sondern auch seine Fähigkeit, die Kontinuität aufrechtzuerhalten, wenn andere Bedrohungen erkannt werden, die eine Reaktion erfordern. DDoS-Techniken, die länger andauernde Angriffe beinhalten, sowie der Einsatz zusätzlicher DDoS-Angriffsvektoren sind effektive Strategien für Angreifer. Hiermit können sie Ressourcen auslasten und die Netzwerksicherheitsteams des Unternehmens überfordern.

Das neue DDoS-Ziel: DNS

Zu den häufigsten aller DDoS-Angriffstypen gehören diejenigen, die auf das Domain Name System (DNS) abzielen (Abbildung 6). Das DNS ist aufgrund der Folgen, die schädlicher Traffic für diesen wichtigen und grundlegenden Dienst haben kann, ein beliebtes Ziel für DDoS-Angriffe. Ein erfolgreicher DNS-Angriff hat das Potenzial, die Präsenz eines Unternehmens im Internet buchstäblich zu löschen.

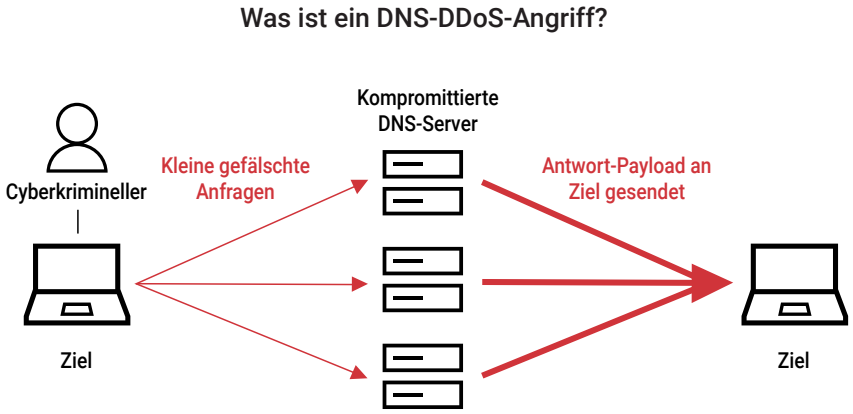

Abb. 6: Bei einem DNS-DDoS-Angriff werden DNS-Server mit gefälschten Anfragen kompromittiert, was zu einer überwältigenden Antwort von Payloads an das Ziel führt.

Insbesondere bei den NXDOMAIN-Angriffen (nonexistent domain), auch Pseudo-Random Subdomain (PRSD) oder „DNS Water Torture“ genannt, wurde beobachtet, dass sie die DNS-Infrastruktur mit Anfragen für nicht vorhandene Domains überfluten. Diese Art von Angriff zielt darauf ab, zu den Ursprungs-Nameservern zu gelangen und eine hohe Belastung der Systeme zu verursachen. Die Verarbeitung einer Anfrage für eine nicht vorhandene Domain ist eine Aufgabe, die viele Verarbeitungszyklen beansprucht und letztendlich die Fähigkeit des Systems erschöpft, zu reagieren. Wir haben viele kurze Angriffe dieser Art erlebt, die in der Regel verwendet werden, um die DNS-Infrastruktur des Opfers zu testen, nur um später mit einem ausgefeilten Angriff in voller Wucht zurückzukehren. Laut Forschungsergebnissen unserer 50 wichtigsten Finanzkunden, die Akamai Edge DNS nutzen, machten Anfragen für nicht vorhandene Domains im März 2024 fast 60 % ihres Internettraffics aus (Abbildung 7).

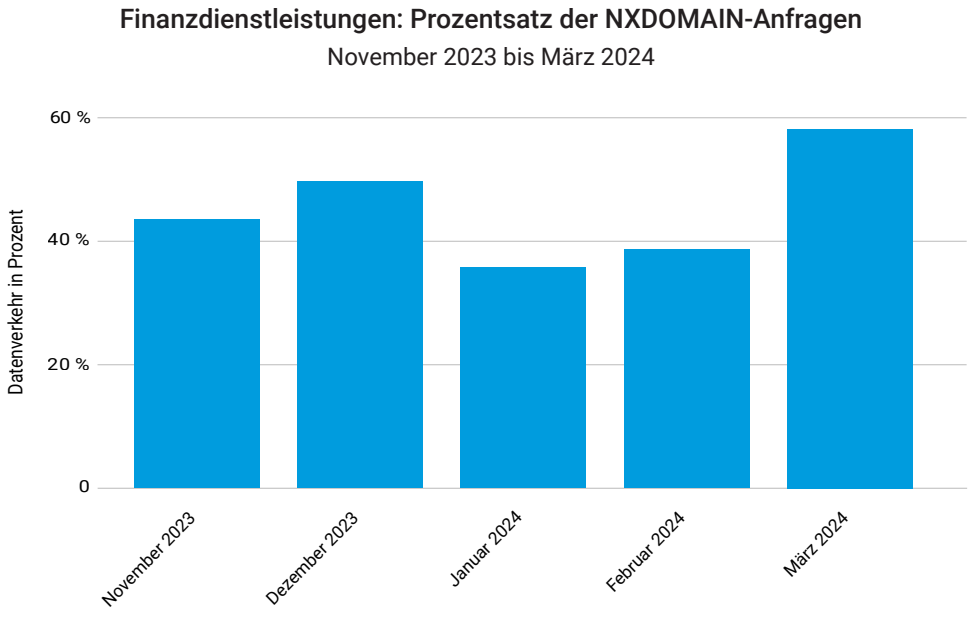

Abb. 7: Seit Ende 2023 erreichten NXDOMAIN-Anfragen im März 2024 mit 58 % einen neuen Höchststand.

DNS-Flood-Angriffe sind eine von zwei Hauptgruppen von DNS-DDoS-Angriffen. Der andere sind DNS-Verstärkungsangriffe, die Reflection-Angriffe beinhalten. Sie umfassen das Spoofing von IP-Adressen, die vom Angreifer erstellt werden, um eine beträchtliche Anzahl von DNS-Anfragen zu senden und so die Ressourcen des Zielgeräts lahmzulegen. Ein weiterer Anreiz für Angreifer, sich für DNS-DDoS zu entscheiden, ist die einfache Ausführung, da der Großteil des Traffics über das User Datagram Protocol (UDP) läuft, das gespoofte IPs ermöglicht.

Bekämpfung der zunehmenden Angriffe durch ein Umdenken bei der Informationssicherheit

Um die Zunahme von Cybersicherheitsbedrohungen (einschließlich DDoS) in der Region zu bekämpfen und zu verhindern, haben die Regierungen und Nationen in EMEA ihre Informationssicherheit überdacht. Die äußerst dynamische Landschaft umfasst die neue Richtlinie für Netzwerk- und Informationssysteme (NIS2) und den Digital Operational Resilience Act (DORA) – neben anderen neuen legislativen Maßnahmen, z. B. die Datenschutz-Grundverordnung (DSGVO), den Cyber Resilience Act (CRA), das Europäische Programm für den Schutz kritischer Infrastrukturen usw.

Für Unternehmen ist es entscheidend, leistungsstarke Sicherheitsmaßnahmen zu implementieren und ihre Anwendungen und Netzwerke routinemäßig zu evaluieren, um Cyberangriffe zu vermeiden und abzuwehren. Das ist besonders wichtig, um sich vor DDoS-Angriffen zu schützen, da hierbei nicht viel Zeit für die Reaktion bleibt. Darüber hinaus zielen DDoS-Angriffe tendenziell auf weniger gut geschützte Opfer ab, die Cyberkriminelle durch präzise Aufklärung und Tests identifizieren. Daher ist es wichtig, dass Unternehmen effiziente Sicherheitsverfahren einführen und über einsatzbereite Pläne für Geschäftskontinuität und Disaster Recovery verfügen. Zusammengenommen können die neuen gesetzlichen Maßnahmen und Richtlinien einige Sicherheitsleitlinien für Unternehmen bieten.

Die NIS2-Richtlinie, die im Dezember 2022 verabschiedet wurde und NIS1 aufhebt und ersetzt, zielt darauf ab, die Umsetzung des bestehenden Cybersicherheits-Frameworks der Europäischen Union zu erweitern, zu stärken und zu harmonisieren, um auf die zunehmende Gefährdung Europas durch Cyberbedrohungen zu reagieren. Die EU-Mitgliedstaaten haben bis zum 17. Oktober 2024 Zeit, die Richtlinie umzusetzen.

Wichtig sind auch Verfahren für die Verwaltung von Anbietern, z. B. von Dritten. DORA konzentriert sich auf die EU-Finanzdienstleistungsregulierung und wird ab dem 17. Januar 2025 gelten. Neben der Förderung der Cyber-Resilienz und der Unterstützung von EU-Finanzdienstleistungsunternehmen bei der Bewältigung von Cybersicherheitsvorfällen bietet DORA auch Leitlinien für Verfahren zur Verwaltung von Drittanbietern. Hierdurch werden Finanzunternehmen unterstützt, indem sichergestellt wird, dass Anbieter von Informations- und Kommunikationstechnologie (IKT), mit denen sie Verträge abschließen, die entsprechenden Informationssicherheitsstandards einhalten. Das sind die Schlüsselkomponenten des Fünf-Säulen-Modells von DORA, das die Cyber-Resilienz von Finanzdienstleistungsunternehmen verbessern soll. Die fünf Säulen sind Risikomanagement, Vorfallsmeldung, Tests der digitalen operativen Resilienz, Risiken von IKT-Drittanbietern sowie der Austausch von Informationen und Erkenntnissen.

Sowohl NIS2 als auch DORA enthalten Leitlinien zu Strategien, die Zero Trust als Methode für Resilienz nutzen. Vertrauen und Verfügbarkeit sind besonders im Online-Universum von entscheidender Bedeutung – ein DDoS-Angriff kann dieses Vertrauen kritisch untergraben. Daher ist es wichtig, dass Unternehmen angemessene Schutzmaßnahmen wie grundlegende Cyberhygiene befolgen. Dieses Konzept beinhaltet die Anwendung von Zero-Trust-Prinzipien, die einen detaillierteren, kontextbezogenen Zugriffskontrollmechanismus vorsehen, der die Identität, den Gerätestatus und das Nutzerverhalten kontinuierlich überprüft, bevor Zugriff auf sensible Ressourcen gewährt wird. Darüber hinaus ist das Konzept der geringstmöglichen Berechtigungen ein wesentlicher Bestandteil der Zero-Trust-Sicherheitspraktiken. Hierbei werden Nutzer segmentiert, die für den Zugriff zugelassen sind. Zero-Trust-Lösungen tragen auch dazu bei, kritische Assets von Unternehmen vor RDDoS zu schützen.

Neben der DDoS-bezogenen Gesetzgebung ist es für Unternehmen auch wichtig, mit anderen bestehenden Gesetzen in der EMEA-Region vertraut zu sein, die auf die Bekämpfung von Cyberbedrohungen abzielen. So zielt das neue CRA der Europäischen Union beispielsweise auf Software- und Hardwareschwachstellen ab, die Angreifer zunehmend nutzen, um Unternehmen zu infiltrieren und Ransomware-Angriffe zu starten. Außerdem wurden mit der DSGVO Verpflichtungen für alle Organisationen eingeführt, die mit personenbezogenen Daten europäischer Unternehmen und Kunden umgehen.

Und außerhalb der Europäischen Union sind andere Länder dabei, ihre eigenen Kontrollen einzuführen und durchzusetzen. Saudi-Arabiens nationale Cybersicherheitsbehörde hat Datenschutzgesetze eingeführt, die der DSGVO ähneln, und der Africa Cybercrime Operations Desk von Interpol hat Programme wie den Africa Cyber Surge eingerichtet.

Fallstudie: Europäische E-Commerce-Organisation erlebt DDoS-Angriffe auf Netzwerkebene

Die Aufrechterhaltung der Verfügbarkeit und Resilienz von Websites ist für jede E-Commerce-Organisation von entscheidender Bedeutung, um den Umsatz zu steigern. Aus diesem Grund hat es für Sicherheitsexperten höchste Priorität, webbasierte Assets und Anwendungen vor DDoS-Angriffen zu schützen, um Ereignisse zu verhindern, die sich auf ihr Unternehmen – und auf Kunden – auswirken. Aber was passiert, wenn die zugrunde liegende Infrastruktur oder die Backend-Systeme, die den Auftragslebenszyklus erst ermöglichen, gestört werden oder vollständig offline gehen? Wenn Kunden zwar Bestellungen aufgeben können, aber diese Bestellungen nicht bearbeitet oder erfüllt werden können, kann der erfolgreiche Betrieb zum Stillstand kommen. Genau das geschah mit einem E-Commerce-Unternehmen in Europa, als ein DDoS-Angriff auf Netzwerkebene erfolgreich Dienste innerhalb des Rechenzentrums anvisierte, die nur unzureichende Kontrollen umfassten.

Viele Angriffskampagnen starten in der Regel an Wochenenden und Feiertagen, wo weniger Sicherheitsmitarbeiter und Ressourcen für die Vorfallsreaktion zur Verfügung stehen, um eine Bedrohung abzuwehren. Im Falle dieser europäischen E-Commerce-Organisation nutzten die DDoS-Angreifer eine Kombination aus SYN- und UDP-Flood-Angriffsvektoren, um das Rechenzentrum des Unternehmens an einem Freitagnachmittag anzugreifen und anfällige Unternehmensressourcen wie das Unternehmens-E-Mail-System in die Knie zu zwingen. So wurde die Übertragung wichtiger Daten an andere Teile des Unternehmens verhindert, einschließlich des Versandlagers.

Infolgedessen war die Logistikinfrastruktur nicht in der Lage, Bestellungen, die von der E-Commerce-Plattform eingegangen waren, zu bearbeiten, obwohl die Logistikinfrastruktur selbst nicht betroffen war. Da das Unternehmen nicht in der Lage war, das anhaltende Ausmaß volumetrischer DDoS-Angriffe abzuwehren, wurde Akamai zur Unterstützung hinzugezogen, um die Rechenzentren des Einzelhändlers mit einer Notfallintegration zu schützen. Innerhalb von 24 Stunden war der Kunde auf der Akamai Prolexic-Plattform und die Konnektivität zu wichtigen Unternehmensservices war wiederhergestellt.

Das Ergebnis: E-Commerce-Unternehmen benötigen einen ganzheitlichen Ansatz zur Abwehr von DDoS-Angriffen, der sowohl Angriffe auf Layer 7 (Anwendungen) als auch Angriffe auf Layer 3 (Netzwerk) und Layer 4 (Transport) abwehrt, um Ausfallzeiten zu vermeiden und die Ausfallsicherheit während des gesamten Auftragszyklus zu gewährleisten.

Schutz und Schadensbegrenzung

Nachdem wir nun die wichtigsten DDoS-Trends und -Gesetze in EMEA besprochen und einige Beispiele für Angriffe genannt haben, wollen wir uns ansehen, was Sie tun können, um Ihr Unternehmen zu schützen. Zusätzlich zur Befolgung der oben genannten gesetzlichen Maßnahmen, einschließlich NIS2, DORA, DSGVO und CRA, und zum Einsatz von Zero-Trust-Lösungen empfehlen die Forscher von Akamai drei umsetzbare Strategien, um die dynamische DDoS-Landschaft zu bekämpfen.

1. **Sorgen Sie für proaktiven DDoS-Schutz Ihrer digitalen Assets.**
   Dies umfasst:
   - Gewährleistung, dass für alle öffentlich verfügbaren IP-Adressen und kritischen Subnetze Sicherheitskontrollen vorhanden sind
   - Bereitstellung von DDoS-Sicherheitskontrollen in einer integrierten Schutzfunktion
   - Gewährleistung, dass Notfallpläne und -teams eingerichtet und auf dem neuesten Stand sind
   - Unterstützung Ihres lokalen DDoS-Schutzes durch eine hybride Schutzplattform, um Angriffe abzuwehren, die On-Premises-Appliances überlasten
   - Einrichtung proaktiver Sicherheitskontrollen über eine Network Cloud Firewall sowie eine Web Application Firewall
   - Implementierung von Ratenbeschränkung
   - Caching von Inhalten in einem CDN
   - Einsatz eines Security Operations Command Center Teams, um den Druck auf kritische interne Ressourcen zu verringern

2. **Schützen Sie Ihre DNS-Infrastruktur:** Fällt das DNS eines Unternehmens aus, so gilt das auch für die Präsenz dieses Unternehmens. Eine herkömmliche DNS-Firewall bietet möglicherweise keinen ausreichenden Schutz, wenn sowohl On-Premises- als auch Cloud-Zonen verwaltet werden. In diesem Fall könnte eine hybride Plattform die optimale Lösung sein. Um ausreichende DDoS-Sicherheit zu erreichen, sollte im Allgemeinen der Traffic vom Internet zu Ihrem Netzwerk überprüft werden. Hierbei sollte Angriffstraffic abgewehrt und gefiltert werden, bevor er Ihre eigentlichen Anwendungen, APIs und Infrastruktur, einschließlich Ihres DNS, erreicht.

3. **Verlassen Sie sich nicht auf Lösungen, die „gut genug" sind:** Es mag einfacher erscheinen, auf Grundlage der Anforderungen und des Budgets nur die Mindestschutzmaßnahmen zu implementieren. Unternehmen stellen jedoch häufig fest, dass diese anfänglichen „Einsparungen" zu einem späteren Verlust führen, weil Angriffe deutlich mehr Kosten und Schäden verursachen, als die Vorteile des ursprünglichen Plans wettmachen könnten. Daher ist es wichtig, dass Sie Ihre Verteidigungsmaßnahmen einem Stresstest unterziehen – sowohl im Hinblick auf Best Practices als auch hinsichtlich Ihrer technischen Lösungen. Diese Tests sollten Vorfalldokumentation, Prozesse, Runbooks und vieles mehr umfassen, um sicherzustellen, dass Ihre Lösungen ein gutes Maß an Cybersicherheit bieten.

Fazit

Die Art und die Auswirkungen von DDoS-Angriffen haben sich erheblich verändert: Sie werden immer schwerwiegender und komplexer.

Die EMEA-Region ist von dieser eskalierenden DDoS-Landschaft besonders betroffen. Regierungen, Finanzdienstleister, Handel und Gesundheitswesen haben allesamt eine erhöhte Anzahl solcher Angriffe erlebt. Dieser regionale Wandel ist zum Teil auf die anhaltenden geopolitischen Spannungen und Konflikte im EMEA-Raum zurückzuführen, die zu einem Anstieg des Hacktivismus und der damit verbundenen DDoS-Aktivitäten geführt haben.

Darüber hinaus dürften die bevorstehenden hochkarätigen Ereignisse und Wahlen in Europa – einschließlich der Wahlen zum Europäischen Parlament, der Wahlen im Vereinigten Königreich und der Olympischen Sommerspiele in Frankreich – das Risiko von DDoS-Angriffen noch weiter erhöhen. Diese Ereignisse, die von erheblicher politischer und wirtschaftlicher Bedeutung sind, könnten Cyberkriminelle als Motivation dienen, die Prozesse durch den Einsatz von DDoS-Taktiken zu stören und zu beeinflussen.

Die Gesetzgeber in EMEA haben ihre Informationssicherheit überdacht und die Sicherheitsmaßnahmen durch neue Richtlinien und Verordnungen verbessert. Im Allgemeinen werden Unternehmen und Organisationen, die diese Vorschriften einhalten und Schutzmaßnahmen ergriffen haben, von Cyberkriminellen weniger wahrscheinlich als leichte Beute angesehen. DDoS-Angreifer zielen in der Regel auf verwundbare Ziele ab, die nicht gut geschützt sind, und Cyberkriminelle betreiben kontinuierlich Aufklärung, um herauszufinden, welche Ziele am einfachsten mit DDoS ausgenutzt werden können. Aufgrund der Vielzahl von DDoS-Angriffsvektoren und der vielen verfügbaren Pfade zwischen Netzwerk-, Transport- und Anwendungsebene ist es entscheidend, eine Kombination verschiedener Lösungen zu verwenden, um vollständigen Schutz vor DDoS zu bieten. Diese Art der Verteidigung ist entscheidend für optimale Erfolgschancen bei der Bekämpfung der zunehmenden DDoS-Bedrohungen in EMEA.

Methodik

DDoS (Layer 3 und 4)

Akamai Prolexic Routed schützt Unternehmen vor DDoS-Angriffen, indem es Attacken und anderen unerwünschten oder schädlichen Traffic in der Cloud stoppt, bevor sie Anwendungen, Rechenzentren und die Cloud- und Hybrid-Internetinfrastruktur (öffentlich oder privat), einschließlich aller Ports und Protokolle, erreichen können. Experten im Security Operations Command Center (SOCC) von Akamai passen proaktive Abwehrkontrollen so an, dass Angriffe sofort erkannt und gestoppt werden. Außerdem führen sie eine Live-Analyse des verbleibenden Datentraffics durch, um bei Bedarf weitere Abwehrmaßnahmen einzusetzen. Diese abgewehrten Angriffe werden organisiert und in Angriffsereignisse gruppiert und alle zugehörigen Daten werden vom SOCC zur Analyse aufgezeichnet.

Sofern nicht anders angegeben, decken die Daten in diesem Bericht den Zeitraum von 15 Monaten vom 1. Januar 2023 bis zum 31. März 2024 ab.

DDoS (Layer 7)

Diese Daten beschreiben Warnungen auf Anwendungsebene über Traffic, der unsere Web Application Firewall (WAF) durchläuft. Die Layer-7-DDoS-Warnungen werden ausgelöst, wenn wir volumetrische Anomalien bei der Anzahl der Anfragen an eine geschützte Website, Anwendung oder API erkennen. Diese Warnungen können sowohl von schädlichen als auch von gutartigen Anfragen ausgelöst werden. In der Regel sind die Anfragen selbst harmlos, aber ihre hohe Anzahl weist auf eine böswillige Absicht hin. Die Warnungen zeigen nicht an, ob ein Angriff erfolgreich war. Obwohl diese Produkte ein hohes Maß an Anpassung ermöglichen, haben wir die in diesem Bericht dargestellten Daten auf eine Weise erfasst, bei der keine nutzerdefinierten Konfigurationen der geschützten Ressourcen berücksichtigt werden.

Die Daten stammen aus einem internen Tool zur Analyse von Sicherheitsereignissen, die in der Akamai Connected Cloud erkannt wurden, einem Netzwerk aus ca. 340.000 Servern an mehr als 4.000 Standorten in fast 1.300 Netzwerken in über 130 Ländern. Diese Daten werden in Petabyte pro Monat gemessen und von unserem Sicherheitsteam verwendet, um Angriffe zu untersuchen, schädliches Verhalten aufzudecken und zusätzliche Informationen in die Lösungen von Akamai einzuspeisen.

Die Daten in diesem Bericht decken den Zeitraum von 15 Monaten vom 1. Januar 2023 bis zum 31. März 2024 ab.

DDoS (NXDOMAIN)

Diese Daten beschreiben den Traffic, den unser Edge-Netzwerk für 50 unserer wichtigsten Finanzdienstleister-Kunden erfasst hat. Die Anfragen an NXDOMAINs werden nachverfolgt und dokumentiert. Diese Anfragen können mit böswilligen oder gutartigen Absichten gestellt werden. Doch im Allgemeinen deutet eine Zunahme von NXDOMAIN-Anfragen innerhalb eines bestimmten Zeitrahmens und/oder einer bestimmten Region auf böswilliges Verhalten hin. Diese Daten werden von unserem Sicherheitsteam verwendet, um Angriffe zu untersuchen, schädliches Verhalten aufzudecken und zusätzliche Informationen in die Lösungen von Akamai einzuspeisen.

Diese Daten betrafen den Zeitraum von 5 Monaten von November 2023 bis März 2024.

Mitwirkende

Redaktion und Text

Lance Rhodes – Editor in Chief
Susan McReynolds – Fallstudien-Autorin
Maria Vlasak – Lektorat

Prüfung und Fachleute

Christian Borggreen
Cheryl Chiodi
Sven Dummer
Jim Gilbert
Mitch Mayne
Richard Meeus
Craig Sparling
Carley Thornell

Datenanalyse

Chelsea Tuttle

Werbematerialien

Annie Brunholzl

Marketing und Veröffentlichung

Georgina Morales Hampe
Emily Spinks

Weitere „State of the Internet“-Sicherheitsberichte

Lesen Sie vorherige Ausgaben und informieren Sie sich über bevorstehende Veröffentlichungen der renommierten „State of the Internet“-Sicherheitsberichte von Akamai. **akamai.com/soti**

Weitere Informationen zur Bedrohungsforschung von Akamai

Halten Sie sich unter diesem Link zu neuesten Threat-Intelligence-Analysen, Sicherheitsberichten und Cybersicherheitsforschung auf dem Laufenden: **akamai.com/security-research**

Greifen Sie auf Daten aus diesem Bericht zu

Sehen Sie sich die hochauflösenden Versionen der Diagramme und Grafiken an, auf die in diesem Bericht verwiesen wird. Diese Bilder können kostenlos verwendet und referenziert werden, vorausgesetzt, Akamai wird ordnungsgemäß als Quelle genannt und das Akamai-Logo wird beibehalten. **akamai.com/sotidata**

Weitere Informationen zu Akamai-Lösungen

Weitere Informationen zu Akamai-Lösungen zum Schutz vor DDoS-Angriffen finden Sie auf unseren Seiten zu **Prolexic-Lösungen** und **Anwendungs- und API-Sicherheit**.

Veröffentlicht: 06/24.