LINK11

DDOS-REPORT

1. Halbjahr 2022

Inhalt

Einleitung und Zusammenfassung

Im Auge des Sturms

Anzahl der DDoS-Angriffe geht zurück, gleichzeitig werden sie schneller und gefährlicher

Seit mehr als zwei Jahren beeinflusst die Corona-Pandemie das gesellschaftliche Leben und die Wirtschaft. In vielen Bereichen des Lebens wurde dadurch die **digitale Transformation** beschleunigt. Laut des SZ-Digitalbarometers sind über 90 % der Menschen ab 14 Jahren in Deutschland online und 94 % der Berufstätigen nutzen das Internet.[1] Es wurden vor allem hybride Arbeitsmodelle, Migration in die Cloud und Verbesserungen unternehmenseigener IT-Services sowie Web-Services, die den beruflichen Alltag sicherstellen, vorangetrieben.

Auch wenn eine im Juni 2022 veröffentlichte Bitkom-Studie zum Ergebnis kommt, dass der russische Angriffskrieg auf die Ukraine, die Unterbrechung von Lieferketten, steigende Energiekosten und eine beschleunigte Inflation die **Digitalisierung** in Deutschland verlangsamen[2], gehören die damit verbundenen **Cybergefahren** beständig zu den **gravierendsten Folgen.** Immer häufiger kommt es zu kostenintensiven und schädlichen Cybervorfällen, die verstärkt staatliche Einrichtungen, kritische Dienste und Infrastrukturen betreffen.

Das **Versagen der Cyber-Security** gehört dem „Global Risks Report 2022“ des Weltwirtschaftsforums[3] zufolge weltweit zu den **Top-10-Risiken** innerhalb der kommenden fünf Jahre. Umso verständlicher ist es, dass knapp zwei Drittel (62 %) der von der Managementberatung Horváth befragten Top Manager Cyber-Security als eine der wichtigsten Managementherausforderungen betrachten.[4] Laut Hiscox Cyber Readiness Report 2022 war fast die Hälfte (48 %) der befragten Unternehmen weltweit im Jahr 2021 von mindestens einer Cyber-Attacke betroffen.[5]

Die **Bedrohungslage** im Cyberraum **verschärft sich** weiter. PwC zufolge sind Cyberattacken global betrachtet der am häufigsten auftretende Fall von Wirtschaftskriminalität.[6] Zum einen liegt das an dem stets größer werdenden Einfluss von **Cyberkriminellen**, die immer **professioneller** und international **vernetzt** arbeiten, und zum anderen werden immer mehr **innovative Werkzeuge** und **ausgeklügelte Methoden** zu relativ geringen Kosten verfügbar.

Trotz dieser Bedrohungslage erleben wir aktuell besonders im Hinblick auf das Thema DDoS eine **paradoxe Situation:** Im vergangenen Jahr registrierte das Link11 Security Operations Center (LSOC) eine rekordverdächtige Anzahl an DDoS-Angriffen und gleichzeitig gab es kaum mediale Aufmerksamkeit für diese sehr angespannte Gefahrenlage. Seit Beginn des Ukraine-Krieges und der damit verbundenen Cyberoperationen hat die mediale Aufmerksamkeit für DDoS-Angriffe deutlich zugenommen, während die harten Fakten – die Zahlen – ein anderes Bild zeichnen.

Erstmals verzeichnete das LSOC einen **temporären Rückgang** der DDoS-Attacken im Netzwerk. Im Betrachtungszeitraum ist die Gesamtzahl der Angriffe um mehr als drei Viertel (80 %) zurückgegangen, verglichen mit dem Vorjahreszeitraum des DDoS-Rekordjahres 2021. Bereits im Jahr 2020 und insbesondere in der ersten Jahreshälfte 2021 waren mehrere Wellen von **DDoS-Erpressungen** (RDDoS – Ransom Distributed Denial of Serivce) durch Armada Collective, Fancy Bear, Lazarus-Group oder Fancy Lazarus eine **große Triebkraft**. Nach diesen Höhepunkten der Erpresseraktivitäten gab es bisher deutlich weniger Ransom-DDoS-Attacken. Zudem wurden in letzter Zeit mehrere illegale **Darknet-Marktplätze**, darunter auch der weltweit größte Darknet-Umschlagplatz „Hydra-Market“, **abgeschaltet** und damit die Sammelstellen krimineller Energien trockengelegt.[7]

Es sind zwar **weniger Attacken**, gleichzeitig sind sie **gefährlicher.** Denn wie das LSOC in den vergangenen Jahren beobachten konnte, verändert sich die **DNA der Angriffe** kontinuierlich. Anstatt wahllos in der Hoffnung auf Erfolg die Unternehmen zu überfallen, werden Unternehmen inzwischen sehr gezielt mit **hochentwickelten DDoS-Attacken** angegriffen. Zudem sind die im Betrachtungszeitraum verzeichneten Angriffe deutlich kürzer, intensiver und anspruchsvoller.

Einleitung und Zusammenfassung

Erstmals wurde bei den im Link11-Netzwerk registrierten DDoS-Attacken analysiert, wie viele Sekunden nach der Übertragung der ersten Bytes vergehen müssen, bis der Traffic seinen Maximalwert erreicht. Im ersten Halbjahr 2022 wurde eine **kritische Nutzlast** im Durchschnitt bereits 55 Sekunden nach Einsetzen der DDoS-Attacke erreicht. Im Vergleich dazu erzielten die Angriffe im Jahr 2021 erst nach durchschnittlich 184 Sekunden ihren Höhepunkt. Anstatt wie in den bisher hauptsächlich beobachteten Fällen kontinuierlich anzusteigen, erreichen diese **„Turboangriffe“** sehr schnell ihren Höhepunkt. Das bedeutet, dass der Angriff die Netzwerksysteme bereits lahmlegen kann, noch bevor die Abwehrmaßnahmen ihre volle Wirkung entfalten können.

Der Trend zu DDoS-Angriffen mit einer **hohen Bandbreite** ist ungebrochen. Die durchschnittlichen maximalen Angriffsbandbreiten sind gegenüber dem Vorjahreszeitraum von 266 Gbps im ersten Halbjahr 2021 auf 325 Gbps im ersten Halbjahr 2022 weiter gestiegen. Die größte Attacke wurde bei 574 Gbps gestoppt. Die Zunahme der **Intensität** spiegelt sich auch in der Zunahme des Volumens hinsichtlich der Menge an übertragenen Paketen wider. Während im Betrachtungszeitraum die durchschnittliche Anzahl der Paketrate bei 1,5 Millionen Pakete pro Sekunde lag, war die Paketrate im ersten Halbjahr 2021 deutlich geringer. Im Angriffsfall wurden nur 277.000 Pakete

Wirft man einen Blick auf die Korrelation zwischen Dauer und Intensität der DDoS-Angriffe, ist aktuell eine deutliche Veränderung erkennbar: Die Angriffe sind **kürzer** und gleichzeitig **intensiver**. Je konzentrierter, gezielter und anspruchsvoller Angriffe durchgeführt werden, desto mehr sind Präzision und Geschwindigkeit bei der Erkennung und Abwehr von Angriffen erforderlich. Das bedeutet, dass im Umgang mit DDoS-Angriffen Zeit ein immer wesentlicherer Faktor wird.

DDoS in den Nachrichten
1. Quartal 2022

Januar 2022
Mehrfacher Ausfall des Solana-Netzwerks – Kryptowährung erleidet Kursverluste

Das Solana-Netzwerk fällt mehrfach aufgrund von DDoS-Attacken aus. Als Folge fällt der Kurs der Kryptowährung. Grund hierfür könnte die Verwendung der neuartigen Blockchain-Technologie sein.[8]

Januar 2022
Kein Internet in Andorra: Angriff auf Minecraft-Spieler legt Internet lahm

Durch DDoS-Angriffe auf den Internet Service Provider (ISP) in Andorra während eines Twitch-Gaming-Turniers wurden mehrere Minecraft-Spieler aus einem Turnier geworfen und das Internet im ganzen Land lahmgelegt.[9]

Februar 2022
DDoS-Angriffswelle auf die Ukraine

Vor dem russischen Einmarsch in die Ukraine kam es zu mehreren DDoS-Attacken auf staatliche Institutionen wie das Verteidigungsministerium und staatliche Banken.[10]

Februar 2022
Webseiten der russischen Regierung mit DDoS-Angriffen attackiert

Nach Ankündigungen des Hacker-Kollektivs Anonymous kam es bei Webseiten der russischen Regierung und staatlicher Medien wiederholt zu Ausfällen aufgrund von DDoS-Attacken.[11]

Februar 2022
Ausfall der Website der Moskauer Börse

Die Website der Moskauer Börse war am Montag, 28. Februar 2022 nicht erreichbar. Die Börse blieb an diesem Tag geschlossen.[12]

März 2022
Angriff auf nationalen ukrainischen Internet-Provider

Das Internet in der Ukraine fällt nach einem Angriff auf Ukrtelecom, dem nationalen Internetprovider, 15 Stunden lang aus.[13]

DDoS in den Nachrichten

2. Quartal 2022

April 2022
Angriff auf die Website des finnischen Verteidigungsministeriums

Während der Rede des ukrainischen Präsidenten Zelensky wurde die Website des finnischen Verteidigungsministeriums durch einen DDoS-Angriff lahmgelegt. Daneben war auch das Außenministerium betroffen.[14]

April 2022
Online-Portal der hessischen Polizei nach DDoS-Angriffen offline

Aufgrund von DDoS-Attacken hat die hessische Polizei ihr Online-Portal vorübergehend aus dem Netz genommen.[16]

Mai 2022
Angriff auf Eurovision Songcontest und die darauffolgenden Attacken gegen italienische Behörden

Nach der pro-russischen Attacke auf den Eurovision Songcontest, der erfolgreich von der italienischen Polizei abgewehrt wurde, gab es Angriffe auf italienische Behörden.[18]

Juni 2022
Staatliche und private Websites in Litauen gehackt

Litauische staatliche und private Websites wurden von russischen Hackern angegriffen. Der Angriff sei eine Vergeltung für die Entscheidung von Vilnius, den Transit einiger Waren in die russische Exklave Kaliningrad zu stoppen.[21]

Juni 2022
Norwegen Ziel eines Cyberangriffs

Eine Reihe von privaten und öffentlichen Einrichtungen in Norwegen waren Opfer eines sogenannten DDoS-Angriffs. Hinter den Angriffen scheint eine kriminelle pro-russische Gruppe zu stecken, so die norwegischen Sicherheitsbehörden.[22]

April 2022
Russische Hackergruppe „KillNet“ greift rumänische Regierungsseiten an

Mehrere öffentliche, von staatlichen Stellen verwaltete Webseiten in Rumänien waren von einer Reihe von DDoS-Angriffen betroffen. Dazu gehörten u. a. die offizielle Website der rumänischen Regierung und die des rumänischen Verteidigungsministeriums.[15]

Mai 2022
DDoS-Attacken „größeren Ausmaßes“ gegen E-Mail-Dienst Posteo

Der E-Mail-Dienst-Anbieter Posteo hat seit Dienstag mit Distributed-Denial-of-Service-Attacken (DDoS) „größeren Ausmaßes“ zu kämpfen. Im Gegensatz zu früheren Angriffen habe es bisher keine Geldforderungen im Kontext der Angriffe gegeben.[17]

Mai 2022
Hackerangriff auf deutsche Behörden

Mehrere Websites deutscher Behörden und Ministerien waren von DDoS-Attacken betroffen. Dabei handelte es sich wahrscheinlich um einen pro-russischen Hackerangriff.[19]

Juni 2022
Alle Systeme down: Cyberangriff auf italienische Stadt Palermo

In Italiens fünftgrößter Stadt Palermo ist es zu einem Cyberangriff gekommen. Der hatte massive Auswirkungen auf allerhand Dienstleistungen für Einwohner und Touristen.[20]

Juni 2022
DDOS-Angriff auf Kryptowährung-Plattform Tether

Die Anfragen auf die Website der Kryptowährung Tether stiegen durch einen DDoS-Angriff um mehr als 400 % von zweitausend auf acht Millionen alle fünf Minuten.[23]

Entwicklung der Gesamtzahlen im Link11-Netzwerk

Weniger DDoS-Angriffe in der ersten Jahreshälfte

Nach den stets steigenden Angriffszahlen in den vergangenen Jahren und dem Allzeithoch im Jahr 2021 verzeichnete das LSOC erstmals einen temporären Rückgang der DDoS-Attacken im Netzwerk. Die Anzahl der Attacken verringerte sich im ersten Halbjahr 2022 um mehr als drei Viertel (80 %), verglichen mit dem Vorjahreszeitraum. Besonders in der ersten Jahreshälfte 2021 ging eine enorme Anzahl der Angriffe auf mehrere Wellen von DDoS-Erpressungen (RDDoS – Ransom Distributed Denial of Serivce) zurück. Nach diesem Höhepunkt gab es bisher deutlich weniger DDoS-Erpressungen.

Hinzu kommt, dass im April dieses Jahres der weltweit größte illegale Darknet-Marktplatz geschlossen wurde. Bei dieser Operation arbeiteten deutsche Behörden wie das BKA mit dem US-Justizministerium zusammen. Bei der deutsch-amerikanischen Gemeinschaftsaktion wurden die Server des „Hydra-Marktes", einer russischen Website sowie 25 Millionen Dollar in Kryptowährung beschlagnahmt.[24]

Daneben zielten in den beiden Rekordjahren 2020 und 2021 viele Angriffe auf Web-Services, die das Leben, Lernen und Arbeiten unter Pandemie-Bedingungen sicherstellten. Dazu zählten Impfplattformen, Lernportale und IT-Infrastrukturen für das mobile Arbeiten im Home-Office. Außerdem standen Hosting Provider und ISPs, die die Express-Digitalisierung in Wirtschaft und Gesellschaft erst ermöglichten, unter Beschuss.

Aufgrund des Ukraine-Krieges und dem dazu parallel verlaufenden Cyberkrieg könnten viele Akteure auf dem Cybercrime-Spielfeld ihre Kapazitäten auf andere Ziele konzentrieren. Auch im Netzwerk von Link11 ist eine Fluktuation hinsichtlich des Ursprungs der DDoS-Angriffe erkennbar. Relativ betrachtet kommen mehr Angriffe aus Russland und weniger aus den USA und China.
Möglicherweise ist das jedoch nur die Ruhe vor dem Sturm.

Die aktuelle Gemengelage ist sehr dynamisch und unvorhersehbar. Seit Beginn des Ukraine-Krieges sind neben den üblichen Akteuren verstärkt auch staatlich unterstützte Hackergruppen unterwegs. Die pro-russische Hackergruppe „KillNet" beispielsweise hat mehreren Staaten, darunter auch Deutschland, den Cyberkrieg erklärt.[25] Welche Folgen diese Kriegserklärung hat, konnte in Italien, Litauen, Norwegen und Polen bereits beobachtet werden.[26]

Auch wenn sich die Anzahl der Attacken im Vergleich zum Vorjahreszeitraum deutlich reduziert hat, bergen sie weiterhin eine große Gefahr. Ihre DNA verändert sich kontinuierlich. Umso wichtiger ist es, sich intensiv mit einer sinnvollen und effektiven IT-Sicherheitsstrategie auseinanderzusetzen.

Neue Entwicklungen

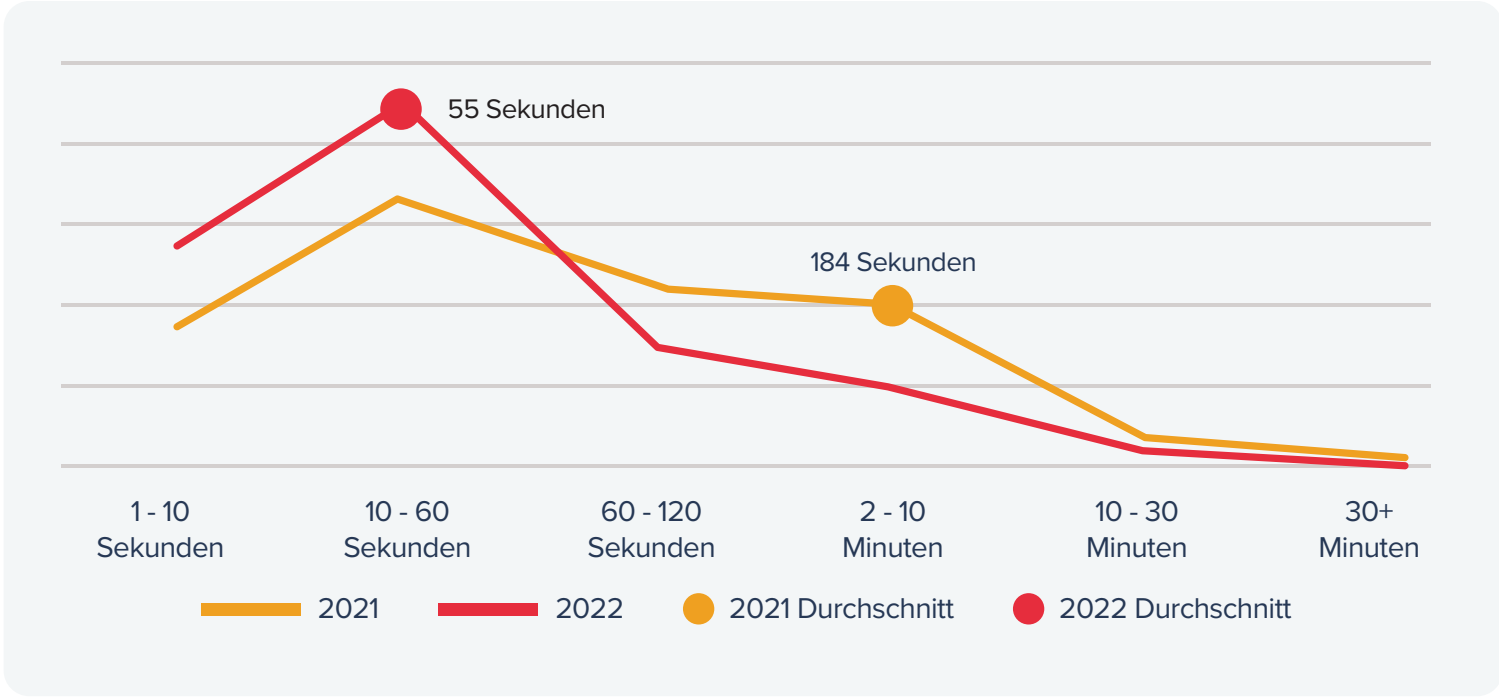
Schneller und intensiver – DDoS-Attacken werden anspruchsvoller

Bei den im Link11-Netzwerk registrierten DDoS-Attacken wurde erstmals analysiert, wie viele Sekunden nach der Übertragung der ersten Bytes vergehen müssen, bis der Traffic seinen Maximalwert erreicht. Diese schnell einsetzenden DDoS-Attacken oder „Turboangriffe“ sind in der Regel von kürzerer Dauer. Gleichzeitig erreichen sie sehr schnell ihren Höhepunkt beziehungsweise eine kritische Nutzlast, anstatt kontinuierlich anzusteigen, wie bisher in den meisten Fällen zu beobachten war.

Das bedeutet, dass der Angriff die Netzwerksysteme bereits lahmlegen kann, noch bevor die Abwehrmaßnahmen ihre volle Wirkung entfalten können.

Aufgrund der erstmaligen Analyse wurde als Vergleichszeitraum das Gesamtjahr 2021 angenommen. Im ersten Halbjahr 2022 ist eine kritische Nutzlast im Durchschnitt 55 Sekunden nach Einsetzen der DDoS-Attacke erreicht worden. Im Vergleich dazu erzielten die Angriffe im Jahr 2021 erst nach durchschnittlich 184 Sekunden ihren Höhepunkt.

Dauer bis zum Höhepunkt einer Attacke | 1. Halbjahr 2022 vs. 2021



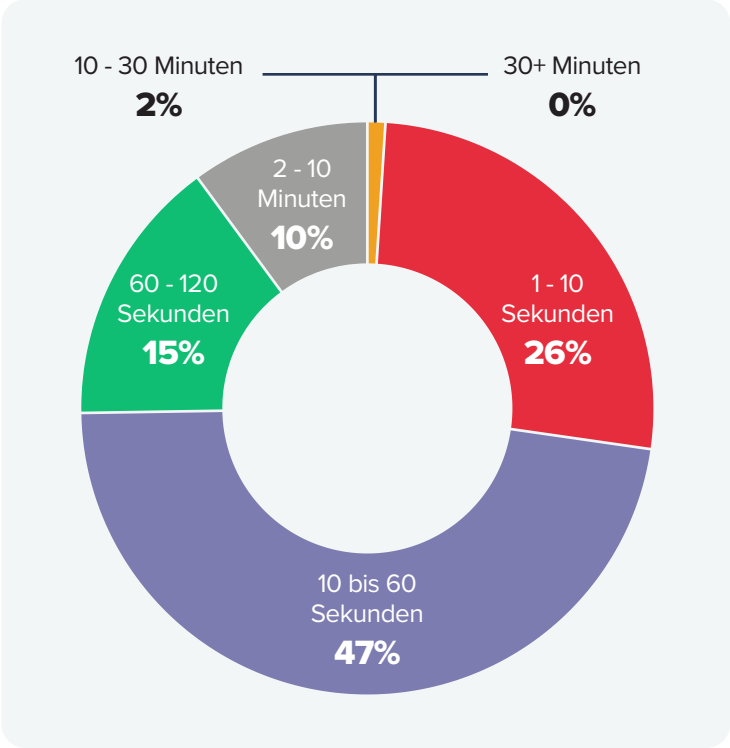
Ein Blick auf die Verteilung der Zeit, die während des DDoS-Angriffes bis zum Erreichen des Höhepunktes vergeht, zeigt für das erste Halbjahr 2022 folgende Ergebnisse: In mehr als einem Viertel der Angriffe (26 %) wurde innerhalb der ersten zehn Sekunden die kritische Nutzlast erreicht. Im vergangenen Jahr lag dieser Anteil bei 17 %. In der ersten Jahreshälfte 2022 machten Angriffe, die in zehn bis 60 Sekunden ihren Maximalwert erzielten, fast die Hälfte aller im Netzwerk registrierten Attacken aus (47 %). Im Vergleich dazu näherten sich ein Drittel der Angriffe (34 %) im Jahr 2021 in der gleichen Zeit ihrem Höhepunkt.

> **Neben langanhaltenden Attacken, die mehr als 12 Stunden dauern, ist auch ein Trend zu schnell einsetzenden Angriffen zu beobachten. Diese Angriffe sind kürzer, erreichen aber sehr schnell eine kritische Nutzlast, bevor die Schutzmaßnahmen ihre volle Wirkung entfalten können.**
>
> **– Jag Bains,** Vice President Solution Engineering, Link11

Neue Entwicklungen

In nur 15 % der Fälle dauerte es zwischen einer und zwei Minuten bei den DDoS-Angriffen im ersten Halbjahr 2022, bis der kritische Maximalwert erreicht wurde. Bei mehr als zwei Minuten lag der Anteil bei rund einem Zehntel der vom LSOC verzeichneten DDoS-Angriffe. Im Vergleich zum Vorjahr zeigen sich hier große Unterschiede. Im Jahr 2021 erreichten knapp ein Viertel der Angriffe (23 %) in ein bis zwei Minuten ihren Höhepunkt und in einem Fünftel der Fälle (21 %) dauerte es mehr als zwei Minuten.

Verteilung der Dauer bis zum Höhepunkt der Attacke



Kurze Angriffszeiten deuten nicht auf die Größe und Schwere eines Angriffs hin. Stattdessen kann eine Attacke schnell ihren Höhepunkt erreichen und dabei kaum eine Störung verursacht haben, während ein anderer Angriff schon kritische Auswirkungen, wie einen vollständigen Ausfall, haben kann, bevor das maximale Angriffspotenzial erzielt wurde.

Doch gerade bei diesen schnell einsetzenden Angriffen ist die Zeit bis zur Schadensbegrenzung, d. h. die Time-to-Mitigate (TTM), entscheidend. Im Link11-Netzwerk sind DDoS-Attacken aufgetreten, die in der Lage waren, die doppelte Nutzlast in nur 70 % der Zeit zu übermitteln. In einem solchen Szenario reicht bereits eine TTM von lediglich einer Minute nicht aus, um einen kompletten Ausfall des Systems zu vermeiden.

Im Angriffsfall kommt es vor allem darauf an, dass keine wertvolle Zeit etwa bei einer manuellen Bewertung von Vorfällen, dem oftmals damit verbundenen reaktiven Schwenk des Datenverkehrs und den Routenänderungen verstreicht. Kommt es zudem noch zu unvorhergesehenen Routing-Problemen oder haben neue Angriffsmethoden das Radar unterlaufen, können solche Verzögerungen in der Abwehr zu großen Schäden führen.

Bei einer effizienten IT-Sicherheitsstrategie geht es darum, den Datenverkehr mit smarten, schnellen und sicheren Methoden in Echtzeit zu analysieren, um die größtmögliche Transparenz über den gesamten Netzverkehr zu erzielen. Die wohl effektivste Methode, um DDoS-Angriffe abzuwehren, besteht aus einer Mischung aus einem Basis-Schutz sowie intelligenter und automatisierter KI-Technologie.

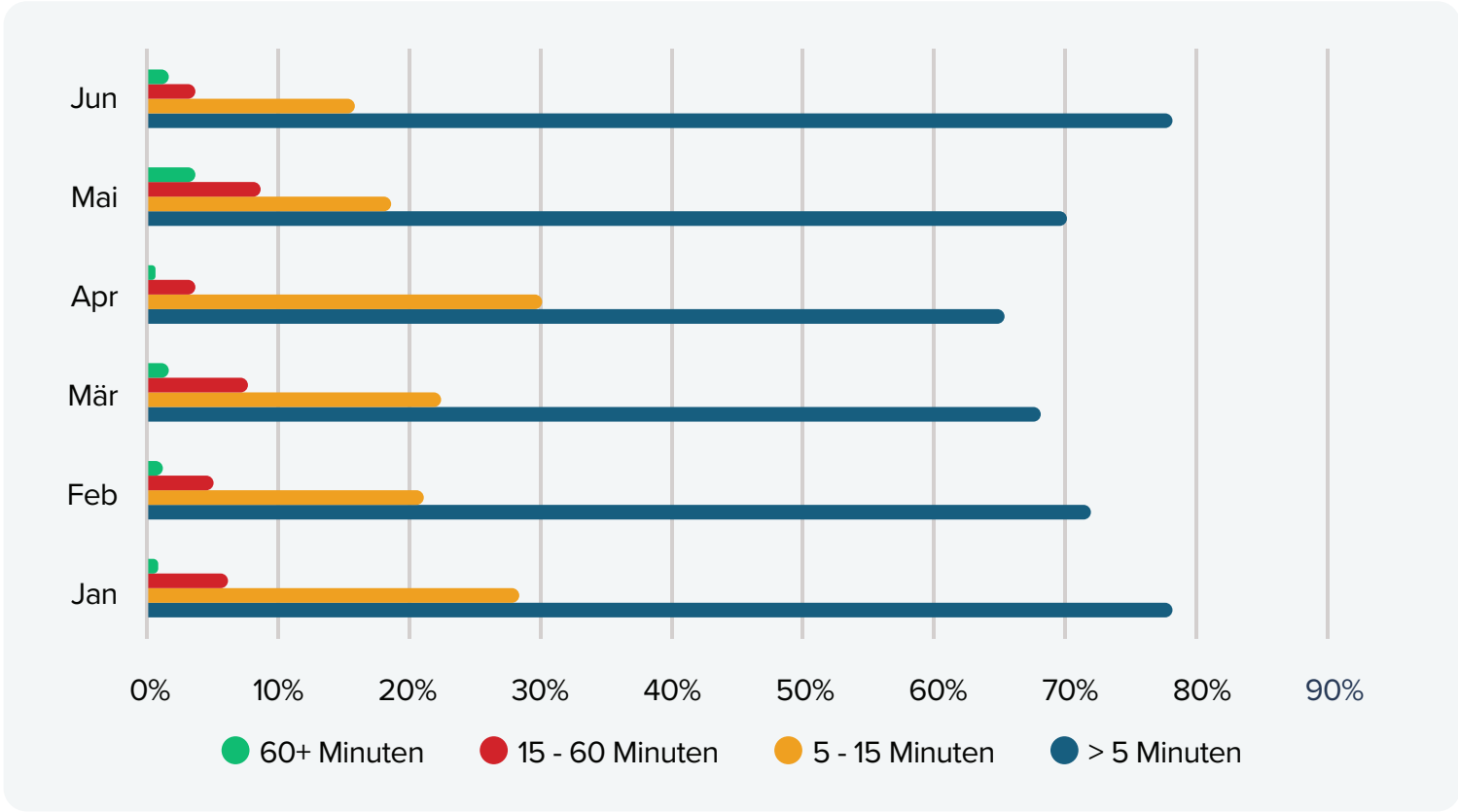
Entwicklung der Angriffsdauer

In der Kürze liegt die Würze

Die Dauer der im ersten Halbjahr 2022 im Link11-Netzwerk registrierten DDoS-Angriffe hat sich im Vergleich zum Vorjahreszeitraum verkürzt. Zwar gab es fast jeden Monat signifikante Ausreißer, doch die Angriffsdauer ist insgesamt zurückgegangen. Ein Blick auf die Grafik oben zeigt deutlich, wie sich die Normalverteilung der Angriffsdauer gegenüber den Ausreißern darstellt. Trotz ihrer kurzen Dauer wurde bei den bisher verzeichneten DDoS-Attacken ein erheblicher Anstieg des Volumens sowohl bei den Paketen als auch bei den Bits pro Sekunde festgestellt.

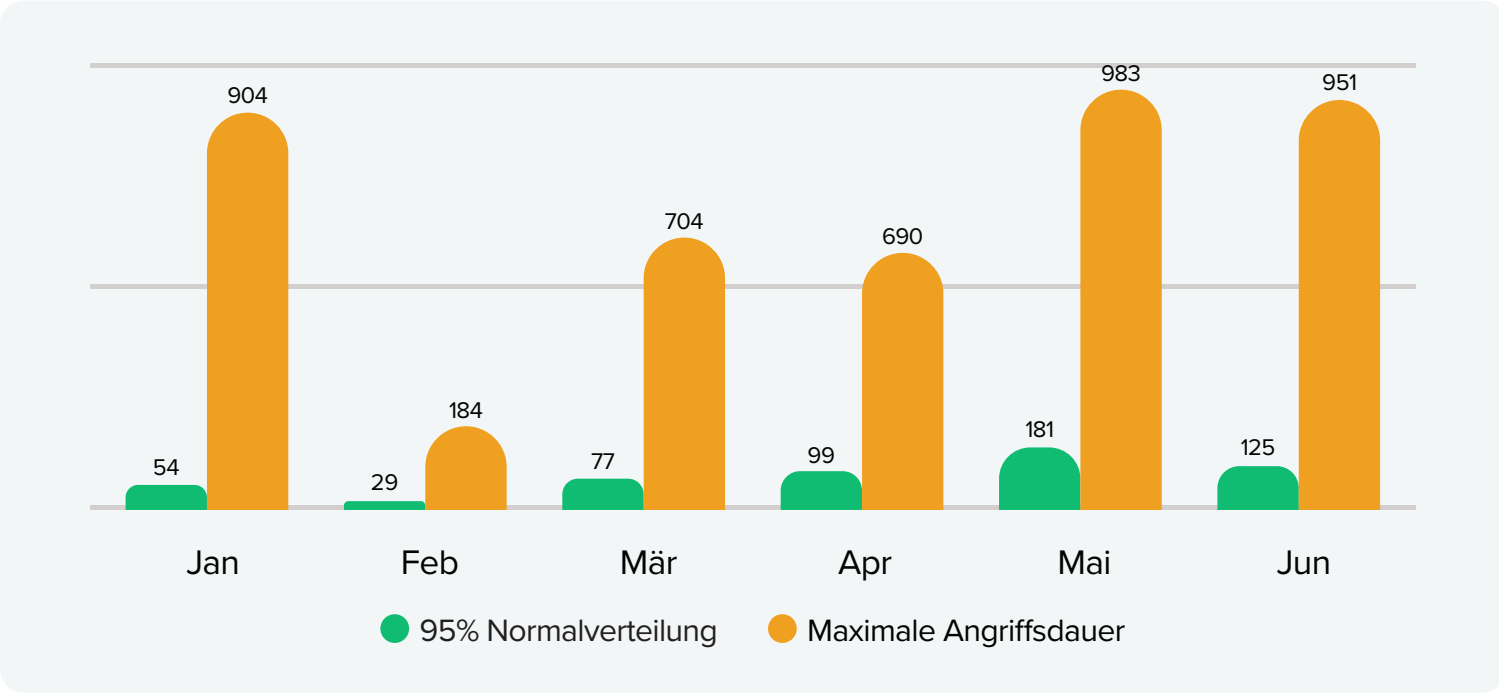
Die weitere Analyse zeigt, dass die Länge der Angriffe zwischen wenigen Minuten und mehreren Stunden schwankte. Der Großteil der Angriffe (70 %) dauerte weniger als 5 Minuten. Knapp ein Viertel aller registrierten Angriffe (22 %) war zwischen 5 und 15 Minuten lang, weitere 6 % bis zu 60 Minuten. Nur rund 2 % der Angriffe waren länger als 60 Minuten. Der Höchstwert in der Angriffsdauer betrug 981 Minuten, das entspricht knapp 16,5 Stunden. Im gleichen Zeitraum 2021 hielt der längste Angriff noch 1.440 Minuten an, was genau einem Tag entspricht.

Übersicht Angriffsdauer | 1. Halbjahr 2022



Entwicklung der Angriffsdauer

Normalverteilung und maximale Angriffsdauer in Minuten | 1. Halbjahr 2022



Ob es zu einem kurzen oder langen Angriff kommt, hängt vielfach mit der Angriffstechnik zusammen. Mit kurzen Attacken von wenigen Minuten auf einzelne IP-Adressen klopfen Angreifer die IT-Infrastruktur ihres Ziels auf Schwachstellen ab. Daneben werden kleine und kurze DDoS-Angriffe in hoher Frequenz eingesetzt, um gleichzeitig verlaufende Hacker-Attacken auf Server und Netzwerke zu verschleiern. Im Windschatten eines DDoS-Angriffs können die Hacker jedoch unbemerkt durch die Hintertür in die Netzwerksicherheit eindringen und angreifen.

Zur Abwehr der DDoS-Attacke werden in kürzester Zeit die vorhandenen IT-Ressourcen mobilisiert, um die Systemausfälle und weitere Schäden zu minimieren.

Darüber hinaus gibt es DDoS-Attacken, die kurz sind, weil die Angreifer realisieren, dass sie ihr Ziel nicht erreichen. Prallen die Angriffe an gut geschützten Infrastrukturen ab, ziehen sich die Angreifer meist zurück, um ihre Ressourcen zu schonen. Geht es den Angreifern darum, die attackierten Infrastrukturen dauerhaft zu torpedieren bzw. zu stören, sind meist langanhaltende Angriffe das Mittel der Wahl.

Entwicklung der Angriffsbandbreiten

Intensität der Attacken nimmt weiter zu

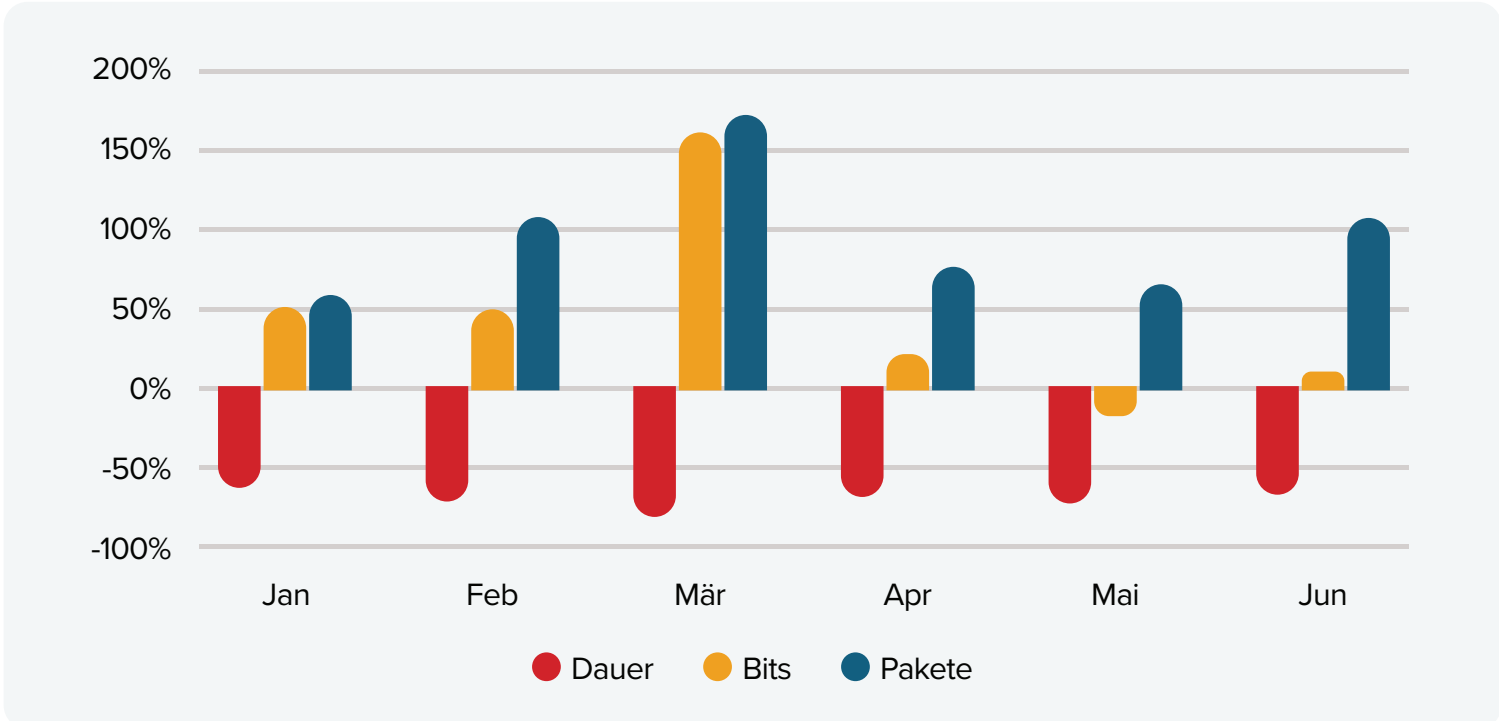
Der bereits im Vorjahreszeitraum erkennbare Trend zu Hochvolumen-Attacken hat sich in den ersten sechs Monaten des Jahres 2022 verstetigt. Die Intensität der DDoS-Angriffe hat im Betrachtungszeitraum gegenüber dem Vergleichszeitraum sogar weiter zugenommen. Die durchschnittlichen maximalen Angriffsbandbreiten sind gegenüber dem Vorjahreszeitraum von 266 Gbps im ersten Halbjahr 2021 auf 325 Gbps im ersten Halbjahr 2022 gestiegen. Der Trend zu DDoS-Angriffen mit einer hohen Bandbreite ist ungebrochen. Die größte Attacke wurde bei 574 Gbps gestoppt.

Die Zunahme der Intensität spiegelt sich jedoch nicht nur in der größer gewordenen durchschnittlichen Bandbreite wider, sondern auch in der Zunahme des Volumens hinsichtlich der Menge an den übertragenen Paketen.

Während im Betrachtungszeitraum die durchschnittliche Anzahl der Paketrate bei 1,5 Millionen Paketen pro Sekunde lag, war die Paketrate im ersten Halbjahr 2021 deutlich geringer. Im Angriffsfall wurden nur 277.000 Pakete pro Sekunde übermittelt.

Wirft man einen Blick auf die Korrelation zwischen Dauer und Intensität der DDoS-Angriffe, ist aktuell eine deutliche Veränderung erkennbar: Die Angriffe sind kürzer und gleichzeitig intensiver. Das bedeutet, dass im Umgang mit DDoS-Angriffen Zeit ein immer wesentlicherer Faktor wird. Dabei ist entscheidend, wie viel Zeit bis zur ersten Reaktion auf den Angriff und dem Start der Schadensbegrenzung der sogenannten Time-to-Mitigate (TTM) vergeht und wie lange es dauert bis der Ursprungszustand wiederhergestellt wurde, die sogenannte Mean-Time-To-Repair (MTTR). Wie Link11 und andere Wettbewerber zu diesem entscheidenden Faktor positioniert sind, finden Sie in der Frost & Sullivan-Studie **„The New Benchmark: Why Fast DDoS Detection Is No Longer Good Enough“.**

Veränderung in Dauer und Intensität der Attacken | 1. Halbjahr 2021 vs. 1. Halbjahr 2022



Entwicklung der Angriffsbandbreiten

Je konzentrierter, gezielter und anspruchsvoller Angriffe durchgeführt werden, desto mehr sind Präzision und Geschwindigkeit bei der Erkennung und Abwehr von Angriffen erforderlich. Denn besonders bei den schnell auftretenden und intensiven Attacken mit großen Bandbreiten sowie hohen Paketraten werden die Schutzlösungen auf die Probe gestellt. Einige der On-Premise-Lösungen sind in der Lage, einfache und unkoordinierte Angriffe abzuwehren. Primär deckt der Schutz vor allem netzwerkartige Angriffe (z. B. ICMP-UDP-Floods) auf Layer 3 oder 4 ab. Gleichzeitig können komplexere und besonders intensive Angriffe die lokalen Geräte überfordern.

Besonders die TTM kann hier von entscheidender Bedeutung sein. Viele moderne On-Premise-Systeme verfügen über eine hybride Cloud-Lösung, die eingreifen und den Datenverkehr umleiten kann, sobald dieser ein bestimmtes Niveau erreicht hat. Unter Laborbedingungen sollte eine solche Umleitung innerhalb von 10 bis 90 Sekunden erfolgen (sie beginnt, sobald der Angriff ein kritisches Niveau erreicht hat). Unter Beschuss eines DDoS-Angriffes herrschen jedoch keine Laborbedingungen.

Mit Blick auf das unmittelbare Einsetzen der Attacken und der **Frost & Sullivan-Ergebnisse,** ist besonders für **Betreiber kritischer Infrastrukturen (KRITIS)** eine schnelle TTM erforderlich. Wenn ein Vor-Ort-Schutz vorgeschrieben ist, muss ein solcher auch vorhanden sein. Mithilfe eines hybriden Systems kann eine möglichst kurze TTM garantiert und regelmäßig überprüft werden.

> **Die Angriffslandschaft hat sich radikal weiterentwickelt: Die Denial-of-Service-Attacke von vor zehn Jahren hat mit den ausgefeilten, hochgradig komplexen und intelligenten DDoS-Angriffen von heute nicht mehr viel zu tun.**
>
> **– Marc Wilczek,** Geschäftsführer, Link11

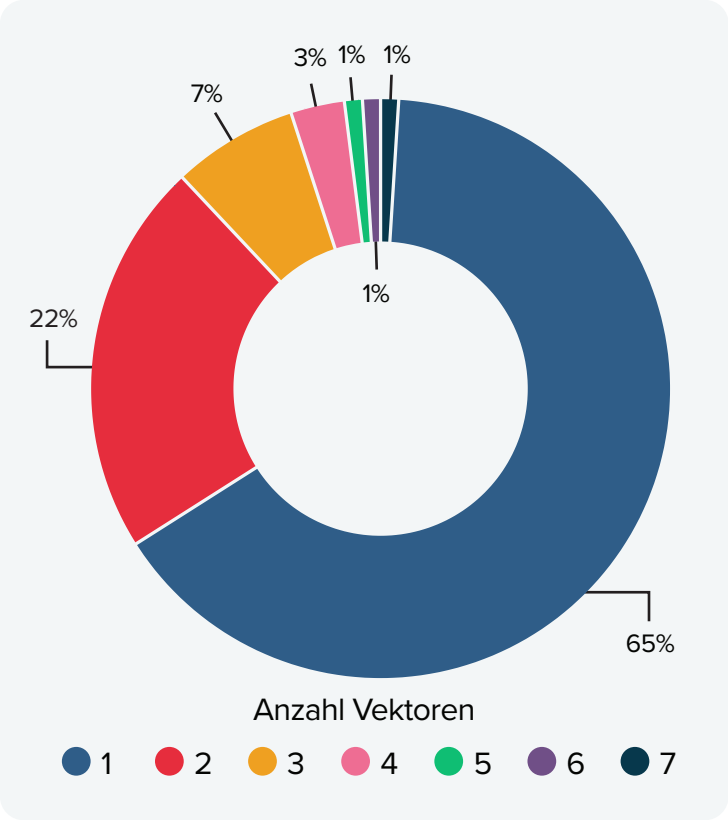
Multivektor-Attacken

Ganz nach dem Motto: Ressourcen sparen

Nachdem in den vergangenen Jahren die Komplexität der DDoS-Attacken stetig zugenommen und 2021 ihren Höchststand erreicht hat, ist der Anteil der Multivektor-Attacken im ersten Halbjahr 2022 im Vergleich zum Vorjahreszeitraum zurückgegangen. Multivektor-Angriffe zielen parallel auf Schwachstellen in Transport-, Applikations- und Protokollebene. Je mehr Schwachstellen und Protokolle Angreifer bei einem Angriff missbrauchen, umso schwieriger sind die Angriffserkennung und -abwehr.

Anstatt solch multidimensionaler Angriffe, bei denen es sich praktisch um mehrere gleichzeitig laufenden Attacken handelt, bevorzugten die Angreifer in den vergangenen sechs Monaten gezielte, konzentrierte und ressourcenschonende Attacken. Im Betrachtungszeitraum waren rund ein Drittel der Attacken (35 %) Multivektor-Attacken, während in den ersten sechs Monaten des vergangenen Jahres bei zwei Dritteln (65 %) der Angriffe mehrere Vektoren genutzt wurden. Die höchste Anzahl an im Link11-Netzwerk beobachteten gleichzeitig eingesetzten Vektoren betrug 11.

Multivektor-Attacken



Hinkt die IT-Sicherheit der Bedrohungslandschaft hinterher, genügt bereits ein einzelner Vektor, der gezielt und konzentriert eingesetzt wird, um großen Schaden anzurichten.

Obwohl im Link11-Netzwerk weniger Multivektor-Angriffe registriert wurden, ist die Gefahrenlage weiterhin angespannt. Mulitvektor-Angriffe sind immer noch eine große Bedrohung. Unterschiedliche Angriffsvektoren können die Abwehrbemühungen erschweren und die TTM insgesamt verlangsamen. Nur mit einer Schutzlösung deren Patch- und Updatezyklen eingehalten werden und die somit auf dem neuesten Stand ist, kann die Unternehmens-IT zuverlässig absichern. Hinkt die IT-Sicherheit der Bedrohungslandschaft hinterher, genügt bereits ein einzelner Vektor, der gezielt und konzentriert eingesetzt wird, um großen Schaden anzurichten.

Reflection-Amplification-Angriffe

Alte Bekannte und eine neue Schwachstelle

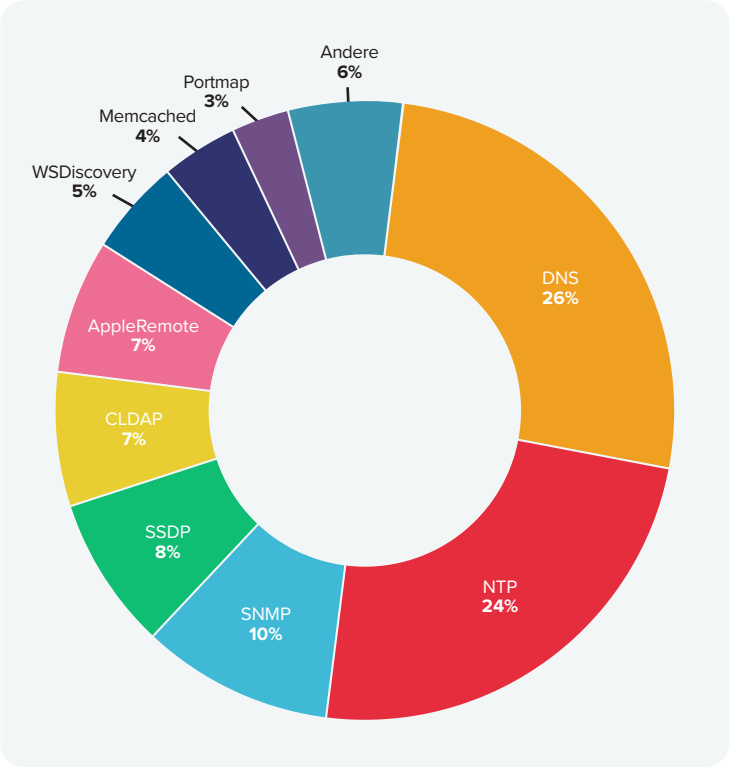
Reflection-Amplification-Angriffe sind eine Klasse von Mulitvektor-Angriffen, die verschiedene falsch konfigurierte offene Server und Services im Internet auf ähnliche Art ausnutzen. Dabei wird das Zielsystem nicht direkt angegriffen, sondern es werden Dienste wie DNS oder NTP missbraucht. Der Angreifer sendet dabei zunächst kleine Mengen von Datenpaketen an die zwischengeschalteten Server, die als Verstärker dienen: Sie spiegeln die Anfragen (reflection) und leiten sie vielfach gesteigert (amplification) an das eigentliche Angriffsziel weiter.

Das LSOC hat im ersten Halbjahr 2022 mehr als ein Dutzend Verstärkertechniken registriert. Darunter waren Angriffstechniken wie DNS oder NTP Reflection Amplification, die schon seit 2013 zum Handwerkszeug von DDoS-Angreifern zählen. Sie zeichnen sich durch hohe Verstärkungsfaktoren aus. Die Steigerung liegt dabei bei 100-facher Verstärkung bei DNS-Attacken und bis zu 200-facher Verstärkung bei NTP-Angriffen. Vektoren wie SSDP und SNMP, die ebenfalls seit einigen Jahren zum Einsatz kommen, spielten ebenfalls eine wichtige Rolle.

Angreifer entdecken ständig neue Schwachstellen wie unzureichend geschützte Internetdienste und offene Dienste. Gleichzeitig wurden im Betrachtungszeitraum für die meisten Angriffe bereits bekannte und altbewährte Vektoren eingesetzt.

> **Die Angriffsmethoden entwickeln sich weiter und die Cyberkriminellen können immer ausgeklügeltere Verstärkungstechniken in ihr Repertoire aufnehmen. Mit cloud-basierten und automatisierten DDoS-Schutzlösungen können Unternehmen damit Schritt halten.**
>
> **– Jag Bains,** Vice President Solution Engineering, Link11

Top 10 Reflection-Amplification-Vektoren 2022



Der Internetdienst, der in den ersten sechs Monaten 2022 am häufigsten für Angriffe ausgenutzt und als Verstärker missbraucht wurde, war DNS (26 %) gefolgt von NTP (24 %), SNPM (10 %) und SSDP (8 %).

Fast jedes Jahr identifizieren DDoS-Angreifer neue Schwachstellen für DDoS-Attacken. Das LSOC warnt, dass kein UDP-Service vor Missbrauch durch DDoS-Angreifer sicher ist. Die Langzeitbeobachtung zeigt, dass Angreifer das Internet permanent nach neuen Ports und Protokollen durchsuchen, über die sich die IT-Infrastrukturen von Unternehmen überlasten lassen. Einer der größten Verstärkungsfaktoren ist mit einer 50.000-fachen Verstärkung Memcached. Es gibt jedoch einen neuen TCP-Middleware-Angriff, der unter bestimmten Umständen das Potenzial hat, dies zu übertreffen. Theoretisch zeigte eine Forschungsarbeit im August 2021, dass mit dieser Verstärkungstechnik Angreifer Middleboxen wie Firewalls über TCP missbrauchen können, um Denial-of-Service-Angriffe zu verstärken. Die Forscher identifizierten zudem Hunderttausende IP-Adressen, die Angriffe mithilfe von Firewalls und Inhaltsfiltern um das Hundertfache verstärken.[27]

Was erwartet uns in nächster Zeit

Zeit wird zum immer entscheidenderen Faktor bei der Abwehr von DDoS-Angriffen

Nahezu überall – am Arbeitsplatz oder zuhause – sind wir mehr denn je von der digitalen Welt abhängig. Gleichzeitig sind einige Unternehmen nur einen einzigen DDoS-Angriff davon entfernt, dass Geschäftsbereiche zum Erliegen kommen oder Produktionsanlagen der Stillstand droht. Denn je nach Angriffsform vergehen nur wenige Sekunden, bis die DDoS-Attacke ihre volle Wirkung entfalten kann.

Ausgehend von den Beobachtungen des LSOC spielt für die Abwehr dieser Angriffe Zeit eine wesentliche Rolle. Im Link11-Netzwerk sind DDoS-Attacken aufgetreten, die in der Lage waren, die doppelte Nutzlast in nur 70 % der Zeit zu übermitteln. Die DDoS-Attacken sind kürzer und gleichzeitig intensiver geworden. Daneben gehen Angreifer gezielter vor und agieren zunächst sehr umsichtig, in dem sie das Netzwerk und dessen Schutz erst einmal testen.

Haben die Angreifer eine dieser anspruchsvollen und gefährlichen DDoS-Attacken gestartet, gibt es nur noch ein sehr enges Zeitfenster, um die potenziellen Schäden zu begrenzen. Denn besonders bei den schnell auftretenden und intensiven Attacken mit großen Bandbreiten sowie hohen Paketraten werden die Schutzlösungen auf die Probe gestellt. In einem solchen Szenario reicht bereits eine Time-to-Mitigate von lediglich einer Minute nicht aus, um einen kompletten Ausfall des Systems zu vermeiden. Stattdessen geht es darum, den Datenverkehr in Echtzeit mit einer cloudbasierten automatisierten KI-Technologie zu analysieren, um die DDoS-Angriffe innerhalb kürzester Zeit abzuwehren.

Neue Angriffstechniken entwickeln sich

Wie im Link11-Netzwerk beobachtet werden konnte, gibt es mehr als ein Dutzend Verstärkungstechniken für DDoS-Angriffe. Neben den vielen altbekannten Angriffstechniken wie DNS oder NTP Reflection Amplification, die schon seit 2013 eingesetzt werden, gibt es einen neuen TCP-Middleware-Angriff, der „Middleboxen“ wie Firewalls missbrauchen kann. Die Angriffe beziehen sich auf das Transmission Control Protokoll (TCP), ein Protokoll, das für die sichere Kommunikation zwischen vernetzten Maschinen im Internet verantwortlich ist.

Bei diesem Angriff werden die Vorteile von Netzwerk-Middleboxen genutzt, die nicht dem TCP-Standard entsprechen. Für ihre Forschungsarbeit haben die Forscher der Universität Maryland das gesamte IPv4-Internet gescannt. Dabei haben sie Hunderttausende IP-Adressen entdeckt, die Verstärkungsfaktoren von mehr als dem Hundertfachen bieten. Laut dem Forschungsteam existieren Netzwerkphänomene, die dazu führen können, dass einige der TCP-basierten Angriffe so effektiv sind, dass sie technisch gesehen einen unendlich großen Verstärkungsfaktor haben. Nachdem der Angreifer eine konstante Anzahl Bytes gesendet hat, erzeugt dieser Reflektor unendlich viel Datenverkehr.[28]

Was bis Anfang März 2022 nur als theoretisch möglich betrachtet wurde, konnte inzwischen auch in der Realität beobachtet werden.[29] Es ist also davon auszugehen, dass in Zukunft diese Angriffsmethode Einzug in das Repertoire der Cyberkriminellen hält und zudem weiterentwickelt wird.

Onlinezugangsgesetz – Herausforderung für Behörden und neue Angriffsfläche für Cyberkriminelle

Bereits 2021 kam es zu mehreren erfolgreichen Cyberangriffen auf öffentliche, deutsche kommunale Verwaltungen. Der schwerwiegendste Cybervorfall im vergangenen Jahr war unter anderem der Angriff auf den Landkreis Anhalt-Bitterfeld, der die öffentlichen Debatten zum Thema IT-Infrastrukturschutz kommunaler Behörden angefacht hat.[30] Im Mai 2022 wurden vermutlich von pro-russischen Hackergruppen mehrere Websites deutscher Behörden und Ministerien mittels DDoS-Angriffe lahmgelegt.

Die Bedrohungslage für Kommunen, öffentliche Einrichtungen und Behörden nimmt zu. Gleichzeitig stehen deutsche Verwaltungen unter dem Druck sämtliche Dienstleistungen zu digitalisieren, denn am 1. Januar 2023 tritt das Onlinezugangsgesetz genauer das „Gesetz zur Verbesserung des Onlinezugangs zu Verwaltungsleistungen“ in Kraft. Das Gesetz verpflichtet Bund, Länder und Kommunen, Verwaltungsleistungen elektronisch anzubieten und wurde bereits 2017 verabschiedet.

In den kommunalen Verwaltungen wird täglich mit sensiblen Daten gearbeitet, Sozialleistungen werden ausgezahlt und es gibt zahlreiche Schnittstellen, deren Verfügbarkeit sichergestellt werden muss. Die jüngsten Angriffe auf Kommunen und deren Verwaltungseinrichtungen zeigen, wie akut hier der Handlungsbedarf ist und wie wichtig der Einsatz präventiver Schutzmaßnahmen ist. Denn müssen erst einmal alle Verwaltungsdienste und Services online angeboten werden, vergrößert sich schlagartig auch die Angriffsfläche für Cyberkriminelle. Umso wichtiger ist es jetzt, präventive Maßnahmen in die Wege zu leiten, die die Cyber-Resilienz deutscher Behörden langfristig steigert. Mit cloudbasierten und automatisierten IT-Sicherheitslösungen müssen zumindest keine zusätzlichen personellen Ressourcen eingesetzt werden. Denn Sicherheit sollte bei der Digitalisierung immer mitgedacht werden.

Quellen

1 https://www.bidt.digital/wp-content/uploads/2022/01/Analysen-Studien-bidt-SZ-Digitalbarometer.pdf

2 https://www.bitkom.org/Presse/Presseinformation/Daempfer-Digitalisierung-Weltlage-bremst-digitale-Transformation-Wirtschaft

3 https://www.weforum.org/reports/global-cybersecurity-outlook-2022

4 https://www.horvath-partners.com/en/media-center/studies/cxo-priorities-2022-managing-overlapping-crises

5 https://www.hiscox.de/pressebereiche/dramatischer-einbruch-bei-cyber-selbsteinschaetzung-deutsche-unternehmen-durch-angespannte-risikolage-stark-verunsichert/

6 https://www.pwc.com/gx/en/services/forensics/economic-crime-survey.html

7 https://www.bka.de/DE/Presse/Listenseite_Pressemitteilungen/2022/Presse2022/220405_PM_IllegalerDarknetMarktplatz.html

8 https://hackernoon.com/has-solana-encountered-another-ddos-attack

9 https://www.golem.de/news/ddos-angriff-auf-minecraft-spieler-legt-internet-in-andorra-lahm-2201-162654.html

10 https://www.zdnet.com/article/ukraine-ministry-of-defense-confirms-ddos-attack-state-banks-loses-connectivity/

11 https://www.spiegel.de/netzwelt/ukraine-krieg-mehrere-webseiten-der-russischen-regierung-lahmgelegt-a-5f944891-a877-4f63-8073-8df-0be3c31b3

12 https://www.forbes.com/sites/thomasbrewster/2022/02/28/moscow-exchange-and-sberbank-websites-knocked-offline-was-ukraines-cyber-army-responsible/?sh=38adc2e677ca

13 https://www.cshub.com/attacks/news/iotw-ukraine-suffers-15-hour-internet-outage

14 https://news.err.ee/1608559405/finnish-defense-and-foreign-ministries-hit-by-cyberattack

15 https://www.bleepingcomputer.com/news/security/russian-hacktivists-launch-ddos-attacks-on-romanian-govt-sites/

16 https://www.faz.net/aktuell/rhein-main/hessische-polizei-nimmt-website-nach-ddos-attacken-vom-netz-17994484.html

17 https://www.heise.de/news/DDoS-Attacken-bei-E-Mail-Dienst-Anbieter-Posteo-7098580.html

18 https://www.inside-it.ch/ddos-attacke-auf-eurovision-song-contest-wurde-abgewehrt-20220516

19 https://www.tagesschau.de/inland/cyberattacke-bundesregierung-ddos-101.html

20 https://t3n.de/news/cyberangriff-palermo-1477797/

21 https://www.reuters.com/technology/lithuania-hit-by-cyber-attack-government-agency-2022-06-27/

22 https://thebarentsobserver.com/en/security/2022/06/pro-russian-hacker-group-says-it-attacked-norway

23 https://cryptoslate.com/tether-confirms-ddos-attack-on-tether-io/

24 https://www.bka.de/DE/Presse/Listenseite_Pressemitteilungen/2022/Presse2022/220405_PM_IllegalerDarknetMarktplatz.html

25 https://www.emcrc.co.uk/post/killnet-declare-war-on-the-uk-and-nine-other-nations

26 https://zero.bs/ddos-as-attackvector-for-state-sponsoredhacktivist-groups-in-times-of-crisis.html#evolution_of_killnet

27 https://www.usenix.org/conference/usenixsecurity21/presentation/bock

28 https://www.usenix.org/conference/usenixsecurity21/presentation/bock

29 https://www.akamai.com/blog/security/tcp-middlebox-reflection

30 https://www.bigs-potsdam.org/app/uploads/2022/04/2022_BIGS-Essenz-Nr.19-WEB.pdf

Kontakt

Link11 GmbH
Lindleystr. 12
60314 Frankfurt

info@link11.com
+49 69 264929777