LINK11

EUROPEAN CYBER REPORT

2025

www.link11.com

Liebe Leserinnen und Leser,

Cyberangriffe sind längst kein abstraktes Risiko mehr – sie dominieren weltweit die Risikoagenda von Unternehmen. Das Allianz Risk Barometer 2025[1] zeigt: Die digitale Transformation eröffnet Chancen, vergrößert aber auch die Angriffsflächen für Cyberkriminelle. DDoS-Attacken, Datendiebstahl und Industriespionage stellen Unternehmen vor große Herausforderungen. Wer seine Sicherheitsstrategie nicht kontinuierlich anpasst, riskiert finanzielle Verluste und langfristige Schäden für Reputation und Geschäftsabläufe.

Die Bitkom-Studie „Wirtschaftsschutz 2024“[2] verdeutlicht die Dringlichkeit: 8 von 10 deutschen Unternehmen (81 %) waren im letzten Jahr von Cyberangriffen betroffen. Der Schaden durch Cybercrime erreichte 178,6 Milliarden Euro und macht mittlerweile zwei Drittel aller kriminell verursachten Verluste aus.

Angesichts der dynamischen Bedrohungslage müssen Unternehmen ihre Sicherheitsinfrastrukturen weiterentwickeln und an die neue Angriffsdynamik anpassen. Neben der verstärkten Integration von KI in die Angriffserkennung und -abwehr spielt der Schutz von Webapplikationen und APIs (WAAP) eine zentrale Rolle. Diese Komponenten gehören mittlerweile zu den bevorzugten Angriffszielen von Cyberkriminellen, da sie häufig sensible Daten verarbeiten und wichtige Geschäftsprozesse unterstützen. Eine ganzheitliche Sicherheitsstrategie sollte daher fortschrittliche WAAP-Lösungen beinhalten, die Bedrohungen wie SQL Injection, Cross-Site-Scripting und API-spezifische Angriffe proaktiv verhindern können. Gleichzeitig sind regelmäßige Updates und eine kontinuierliche Überwachung des Netzwerkstatus unerlässlich, um auf volatile Angriffsmuster reagieren zu können. Ergänzt durch robuste DDoS-Abwehrmechanismen schaffen Unternehmen so eine resiliente Sicherheitsbasis.

Cybersicherheit ist 2025 keine Randnotiz mehr, sondern eine geschäftskritische Priorität. Unternehmen müssen jetzt handeln, um ihre Widerstandsfähigkeit zu stärken und sich gegen die nächste Angriffswelle zu wappnen. Wer Cybersicherheit als strategischen Erfolgsfaktor begreift, fördert Innovation und Wachstum und sichert sich einen Wettbewerbsvorteil.

Ich wünsche Ihnen eine spannende Lektüre!

Herzliche Grüße
Jens-Philipp Jung, CEO, Link11

Inhalt

Executive Summary

Das Jahr 2024 war geprägt von einer beispiellosen Welle an Distributed-Denial-of-Service (DDoS-) Angriffen, die mit Rekordzahlen und zunehmender Komplexität die Cybersicherheitslandschaft dominierten. Die Verbreitung von DDoS-as-a-Service sowie der Einsatz von Künstlicher Intelligenz verstärkten diese Angriffe und stellten Unternehmen vor neue Herausforderungen. Diese Zunahme zeigt nicht nur ein Wachstum in der Häufigkeit von Angriffen, sondern auch eine Veränderung in der Angriffstaktik.

Zentrale Erkenntnisse:

- **Rekordverdächtiger Anstieg:** Die Anzahl der DDoS-Angriffe im Link11-Netzwerk stieg um 137%.
- **Von Gigabit zu Terabit:** Der größte im Link11-Netzwerk gemessene Angriff erreichte mit 1,4 Tbit/s in Europa eine neue Dimension.
- **Neue Angriffstaktiken:** Angreifer setzen vermehrt auf schnelle, gezielte Angriffe mit geringem Ressourceneinsatz, die größere Störungen verursachen.
- **Komplexität und Geschwindigkeit:** Die Angriffe sind schneller und kürzer geworden, zwei Drittel der Angriffe erreichen ihr Maximum innerhalb von 10 bis 60 Sekunden.
- **Multi-Vektor-Angriffe:** Die Kombination verschiedener Angriffspunkte und Protokolle erschwert die Erkennung und erfordert präzisere Abwehrmaßnahmen.
- **Geopolitische Spannungen:** Konflikte und politische Unruhen heizen die Bedrohungslage an, und auch weniger versierte Akteure können dank leistungsfähiger Werkzeuge komplexe Angriffe durchführen.
- **Traditionelle Abwehrmaßnahmen stoßen an ihre Grenzen:** Herkömmliche Schutzmethoden reichen oft nicht aus, um mit der Geschwindigkeit und Komplexität der neuen Angriffe Schritt zu halten.
- **KI als Schlüssel zur Abwehr:** Unternehmen setzen zunehmend auf KI-basierte Systeme, um Angriffe in Echtzeit zu erkennen und zu neutralisieren.
- **Datenschutz und Compliance:** Die Diskussion um den EU-US-Datenschutzrahmen unterstreicht die Bedeutung europäischer CDNs und Geofencing-Technologien für den Schutz sensibler Daten.

2024

So können Unternehmen ihre Abwehr stärken

Angesichts der dynamischen Bedrohungslage müssen Unternehmen ihre Sicherheitsinfrastrukturen weiterentwickeln und an die neue Angriffsdynamik anpassen. Dies bedeutet nicht nur eine stärkere Integration von KI in die Angriffserkennung und -abwehr, sondern auch eine umfassende Überwachung des Netzwerk- und Serverzustands. Eine ganzheitliche Sicherheitsstrategie, die sowohl Netzwerkschutz als auch Schutz für Web-Anwendungen und APIs umfasst, ist heutzutage unerlässlich. Dazu gehört auch eine verstärkte Fokussierung auf die kontinuierliche Anpassung an volatile Angriffsmuster und die Integration von fortschrittlicher DDoS-Abwehrtechnik.

Die DDoS-Angriffe im Jahr 2024 sind schneller, gezielter und komplexer als je zuvor gewesen. Unternehmen müssen ihre Sicherheitsstrategien kontinuierlich modernisieren, KI-basierte Systeme für eine schnelle und präzise Angriffserkennung und -abwehr implementieren und sich auf zunehmend subtile Angriffstechniken vorbereiten. Nur durch eine ganzheitliche, adaptive Sicherheitsarchitektur können Organisationen sicherstellen, dass sie gegen die immer raffinierteren Bedrohungen der Zukunft gewappnet sind.

Entwicklung der Gesamtzahlen im Link11-Netzwerk

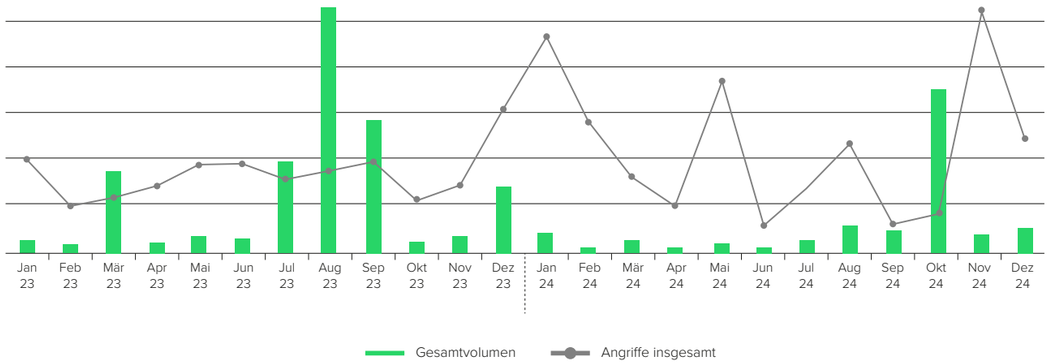
Angreifer erhöhen Schlagzahl

Die Entwicklung der DDoS-Angriffe im Link11-Netzwerk hat für das Jahr 2024 eine alarmierende Dynamik gezeigt. Nachdem bereits im Jahr 2023 ein signifikanter Anstieg der Attacken um über 70 % im Vergleich zum Vorjahr zu verzeichnen war, hat sich diese Entwicklung im Jahr 2024 in noch drastischerer Form fortgesetzt. Die Anzahl der Angriffe stieg im Vergleich zum Vorjahr um 137 %.

Auffällig ist eine strategische Veränderung der Angriffsformen: Während großvolumige Angriffe mit mehr als 100 Gbit/s weiterhin ein ernstzunehmendes Problem darstellen[3], haben vor allem kleinere und häufigere Angriffe deutlich zugenommen. Klassische Brute-Force-Angriffe mit reiner Bandbreitengröße stehen weniger im Vordergrund, stattdessen setzen die Angreifer zunehmend auf raffinierte, zielgerichtete Attacken. Während die Anzahl der Attacken kontinuierlich gestiegen ist, sank das durchschnittliche Datenvolumen pro Angriff. Diese Entwicklung zeigt, dass die Angreifer ihre Methoden optimieren, um Netzwerke schneller und effektiver zu stören – oft mit minimalem Ressourceneinsatz, aber maximaler Wirkung.

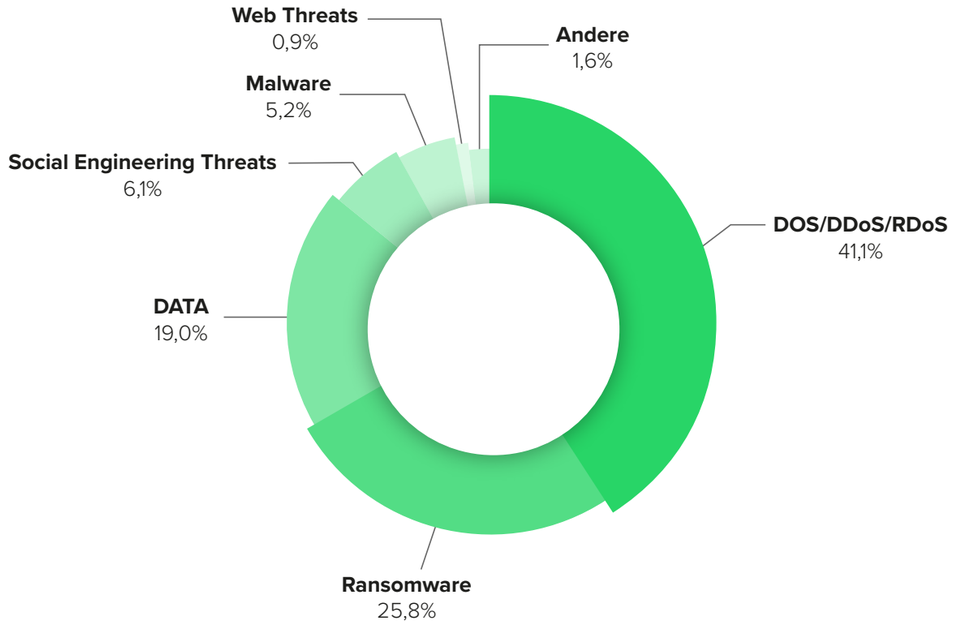
Für Unternehmen und Institutionen stellt dies eine große Herausforderung dar, da herkömmliche DDoS-Abwehrmaßnahmen in erster Linie auf großvolumige Angriffe ausgelegt sind. Die zunehmende Verlagerung hin zu kleineren, technisch ausgefeilteren Attacken erfordert daher einen neuen Ansatz beim Schutz von Netzwerken, insbesondere durch adaptive Erkennungssysteme und proaktive Abwehrmechanismen.

Die Grafik zeigt, dass das Gesamtvolumen zurückgegangen ist.
Gleichzeitig hat die Anzahl der Angriffe allerdings zugenommen.



Ursachen für den Anstieg der DDoS-Angriffe 2024

Der massive Anstieg der DDoS-Angriffe 2024 ist eng mit geopolitischen Konflikten verbunden. Laut ENISA-Bericht[4] sind DDoS-Attacken die häufigste Cyberbedrohung in der EU – fast die Hälfte aller Angriffe zielt darauf ab, Systeme lahmzulegen. Besonders betroffen sind staatliche Einrichtungen, kritische Infrastrukturen und wirtschaftliche Institutionen. Die prorussische Gruppe NoName057(16)bleibt neben Gruppen wie Mr. Hamza[5] der aktivste Akteur. Neben dem Krieg in der Ukraine haben auch der Nahostkonflikt und die Gründung der „Holy League“[6] zu einer Zunahme politisch motivierter Attacken geführt. Die Angreifer nutzen fortschrittliche Werkzeuge wie das „DDoSia-Projekt“, das auch weniger versierten Akteuren effektive Angriffe ermöglicht.



Quelle: ENISA Threat Landscape 2024

„Die zunehmende Komplexität von DDoS-Angriffen erfordert innovative Lösungen. KI-basierte Systeme sind der Schlüssel, um die schnelleren und raffinierteren Angriffe zu erkennen und abzuwehren.“

Jag Bains, VP Solution Engineering, Link11

NoName057(16): Mehr Kapazitäten, raffiniertere Angriffe

NoName057(16) hat seine Angriffskapazitäten 2024 erheblich gesteigert. Durch gezielte Rekrutierung ist ihr Telegram-Kanal auf über 80.000 Mitglieder[7] angewachsen. Ihre global verteilte Serverinfrastruktur und häufig wechselnde IP-Adressen erschweren Gegenmaßnahmen erheblich. Neue Angriffstechniken umgehen klassische DDoS-Schutzmechanismen, was ihre Bedrohung weiter steigert.

Obwohl ihre Tools noch manuelle IP-Wechsel erfordern, zeigt dies den hohen Aufwand, den die Gruppe betreibt.[8] Die Bereitstellung von Angriffswerkzeugen wie „DDoSia“ hat zudem die Beteiligung internationaler Akteure erleichtert, was die politische Dimension der DDoS-Angriffe 2024 verstärkt hat.

Zielprofile der Angriffe

Betroffen sind kritische Infrastrukturen wie Energieversorger, Banken und Behörden, zunehmend aber auch mittelständische Unternehmen. Besonders gefährdet sind E-Commerce-Plattformen, Telekommunikationsanbieter und Cloud-Dienstleister. Medienhäuser, die kritisch über geopolitische Konflikte berichten, geraten ebenfalls verstärkt ins Visier.

Technologische Entwicklung und Abwehrstrategien

Angesichts der steigenden Komplexität der Attacken wird KI-basierte Cyberabwehr unerlässlich. Reine Bandbreitenüberwachung reicht nicht mehr aus – intelligente Systeme müssen verdächtige Aktivitäten in Echtzeit erkennen und blockieren. Ohne Weiterentwicklung der Schutzmaßnahmen droht eine wachsende Gefahr für Wirtschaft und kritische Infrastrukturen.

DDoS-Angriffe werden schneller, kürzer und nutzen multiple Angriffspunkte, was herkömmliche Monitoring-Methoden herausfordert. Gleichzeitig bauen Angreifer systematisch Botnetze aus, um hochvolumige Attacken gezielt einzusetzen. Unternehmen und Institutionen müssen sich auf eine langfristige Bedrohung einstellen.

Link11 hat als Reaktion seine Infrastruktur erheblich erweitert. Zusätzliche Scrubbing-Center und eine optimierte Netzwerkarchitektur erhöhen die Resilienz gegen DDoS-Angriffe. Fortschrittliche KI-gestützte Erkennungssysteme sind entscheidend, um zukünftige Bedrohungen in Echtzeit zu identifizieren und abzuwehren.

Die Holy League – Eine neue Bedrohung

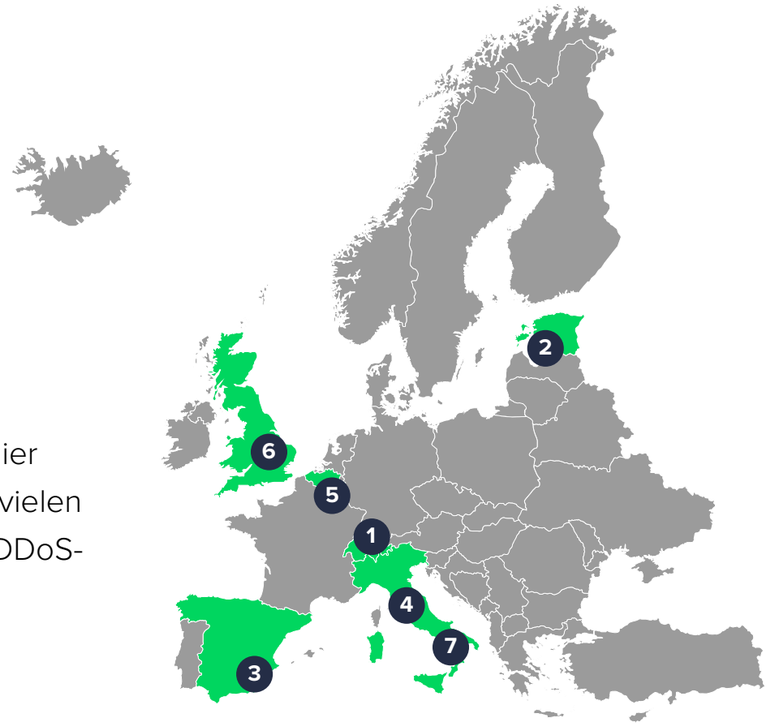
Die Holy League ist eine im Juli 2024 gegründete Allianz aus prorussischen und propalästinensischen Hacktivisten[9], die sich als größte koordinierte Cyberkriminalitätsgruppe gegen den Westen betrachtet. Laut eigenen Angaben umfasst die Holy League mittlerweile über 70 aktive Gruppen.

Ihr erklärtes Ziel ist die Destabilisierung westlicher Länder, insbesondere Europa, Ukraine, Israel sowie der NATO. Ihre Angriffe konzentrieren sich auf DDoS-Attacken, wie etwa auf die französische Regierung[10], Datenlecks und Systemstörungen bei Regierungs- und Wirtschaftsorganisationen.

Die Gruppe nutzt eine Mischung aus religiöser Rhetorik und politischer Propaganda, um Unterstützer zu gewinnen. Sie fordern weitere prorussische Hackergruppen auf, sich ihrem Bündnis anzuschließen. Eine der Kampagnen richtete sich gegen die spanische Infrastruktur, nachdem spanische Behörden drei prorussische Hacktivisten[11] verhaftet hatten. Infolgedessen rief die Holy League zu einer „Vendetta“ gegen Spanien auf.

Klicken Sie sich hier durch einige der vielen NoName057(16) DDoS-Angriffe in 2024.

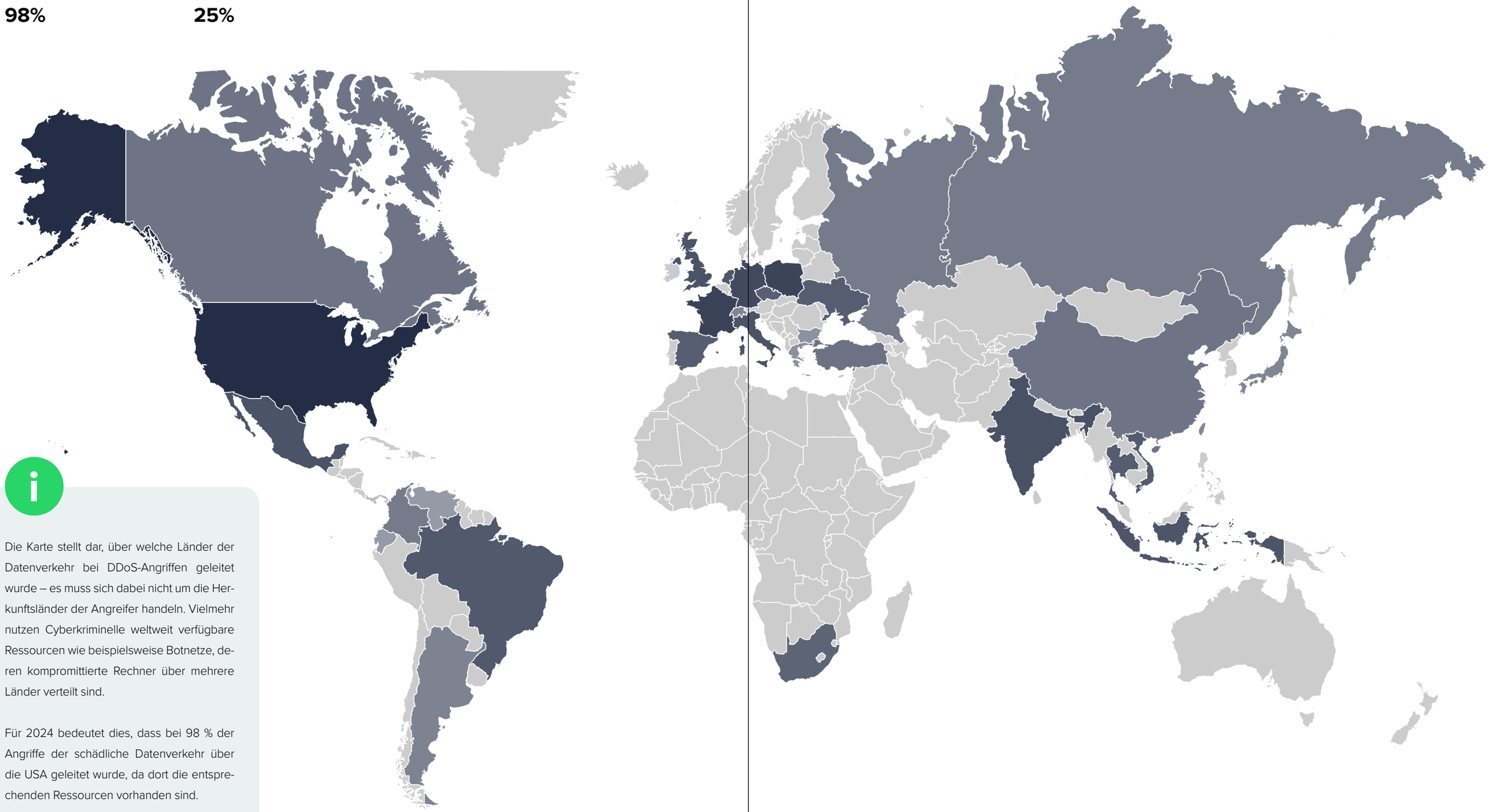
1 =



Herkunft des DDoS-Traffics

Globale Verteilung der Angriffsinfrastruktur 2024

98% 25%



Die Karte stellt dar, über welche Länder der Datenverkehr bei DDoS-Angriffen geleitet wurde – es muss sich dabei nicht um die Herkunftsländer der Angreifer handeln. Vielmehr nutzen Cyberkriminelle weltweit verfügbare Ressourcen wie beispielsweise Botnetze, deren kompromittierte Rechner über mehrere Länder verteilt sind.

Für 2024 bedeutet dies, dass bei 98 % der Angriffe der schädliche Datenverkehr über die USA geleitet wurde, da dort die entsprechenden Ressourcen vorhanden sind.

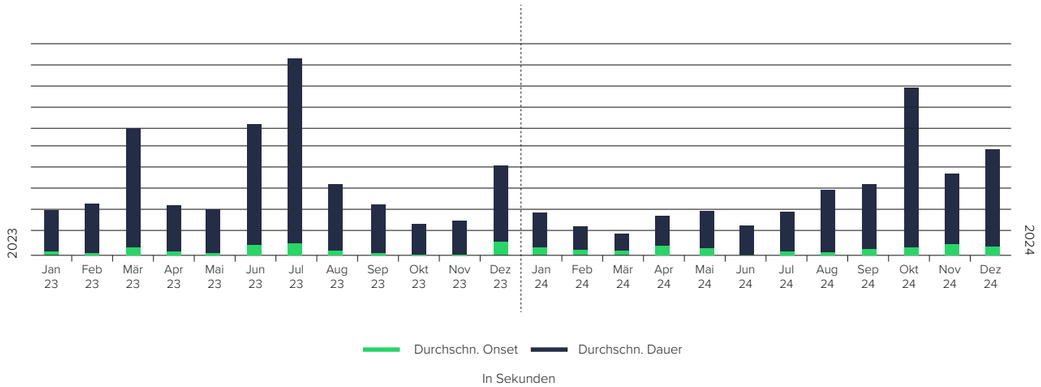
Entwicklung der Angriffsdauer

Neue Taktik: Kürzere, schnellere DDoS-Attacken

Bei den im Link11-Netzwerk registrierten DDoS-Attacken wird seit dem ersten Halbjahr 2022 die Zeitspanne bis zum Erreichen des maximalen Traffics („Onset“) analysiert. Entscheidend ist, wie schnell ein Angriff ein kritisches Volumen erreicht.

2024 benötigten DDoS-Angriffe im Durchschnitt 29 Sekunden, um eine kritische Schwelle zu überschreiten – länger als 2023, als dieser Wert bei 14 Sekunden lag. Gleichzeitig stieg die Anzahl der Attacken mit kurzen Onset-Zeiten deutlich: Zwei Drittel (65 %) der Angriffe erreichten ihr Maximum innerhalb von 10 bis 60 Sekunden, während es 2023 nur 25 % waren.

Die Grafik verdeutlicht, dass sowohl die gesamte Angriffsdauer (dunkelblau) als auch die Zeit bis zum Erreichen des maximalen Volumens (hellblau) im Sommer 2024 deutlich zurückgegangen sind. Dies zeigt, dass DDoS-Attacken nicht nur schneller beginnen, sondern insgesamt kürzer andauern. Angreifer passen ihre Taktiken gezielt an, um mit möglichst kurzen, aber effektiven Angriffen Sicherheitsmaßnahmen zu umgehen.



„Die Zeitfenster für die Abwehr schrumpfen: Zwei Drittel aller DDoS-Attacken 2024 erreichten innerhalb einer Minute ihr Maximum.“

Sean Power, Solution Engineer, Link11

Die Dauer und Geschwindigkeit von DDoS-Angriffen verändern sich:

Schnellere Angriffsstarts

Attacken dauern insgesamt weniger lang, erfordern gleichzeitig eine schnelle Reaktion.

Kürzere Angriffszeiten

Die Onset-Zeit sinkt, Angriffe erreichen innerhalb weniger Sekunden kritische Werte.

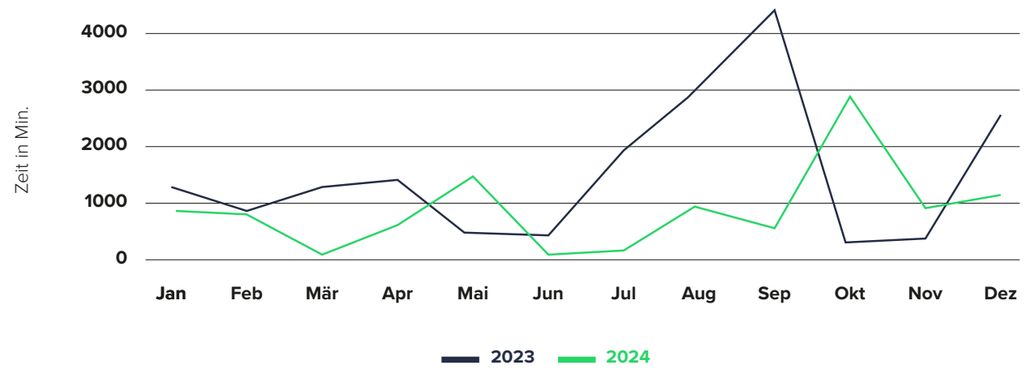
Hohe Frequenz der Attacken

Mehr Angriffe in kurzen Intervallen überfordern herkömmliche Abwehrmechanismen.

Die steigende Geschwindigkeit und Kürze der Attacken stellt IT-Sicherheitslösungen vor neue Herausforderungen. Die traditionelle, auf Volumen basierende Erkennung und Abwehr reicht in diesem Szenario nicht mehr aus. Es bedarf einer neuen Generation von Sicherheitslösungen, die in der Lage sind, schnellere und komplexere Angriffe zu erkennen und abzuwehren.

Von lang andauernden Angriffen zu kürzeren Attacken

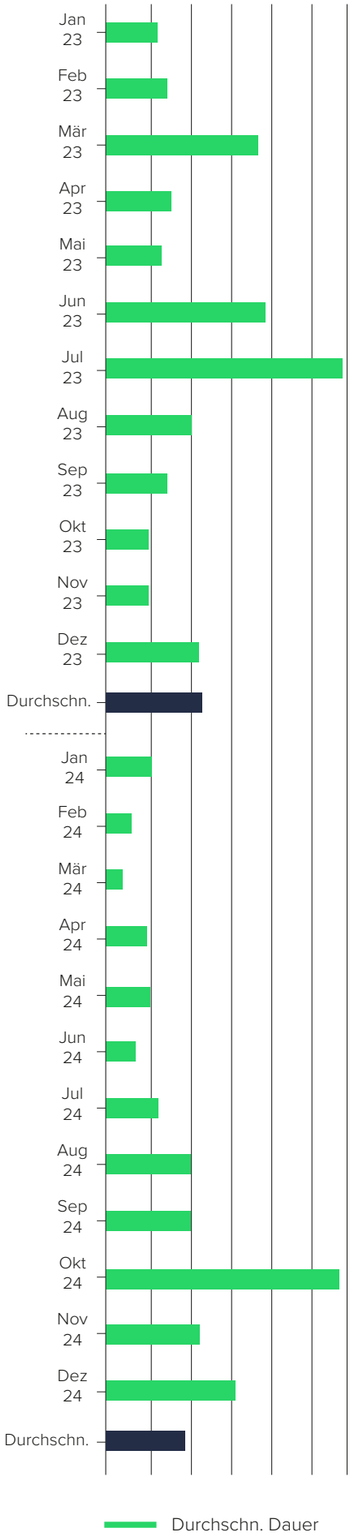
Die Grafik veranschaulicht die Entwicklung der Dauer von DDoS-Attacken im Link11-Netzwerk: Während 2023 noch besonders lang andauernde Angriffe dominierten, zeigt sich 2024 ein deutlicher Trend zu kürzeren, aber häufigeren Angriffen, die neue Anforderungen an Abwehrstrategien stellen. Im Jahr 2023 erreichte die längste registrierte DDoS-Attacke eine Dauer von 4.489 Minuten (74 Stunden und 49 Minuten). Im Vergleich dazu dauerte der längste Angriff im Jahr 2024 2.689 Minuten (44 Stunden und 49 Minuten) – eine deutliche Reduktion um 40 %. Dieser Rückgang spiegelt einen generellen Trend wider: Statt auf lang andauernde Angriffe setzen Cyberkriminelle zunehmend auf kürzere und taktisch optimierte Attacken, die bestehende Abwehrmechanismen gezielt aushebeln sollen.



Es zeigte sich noch ein weiteres auffälliges Muster: Während die durchschnittliche Angriffsdauer im Jahr 2023 im Vergleich zu 2022 noch zugenommen hat, ist im Jahr 2024 ein deutlicher Rückgang zu verzeichnen. Dies zeigt, dass die Angreifer ihre Methoden anpassen – weg von ressourcenintensiven Langzeitangriffen hin zu kurzen, schnellen Störmanövern. Diese neue Strategie überfordert klassische DDoS-Schutzmaßnahmen, die auf große, lang andauernde Angriffe ausgelegt sind.

Die verkürzte Angriffsdauer erfordert eine entsprechend schnelle Reaktionszeit. Besonders entscheidend ist dabei die Time-to-Mitigate (TTM), also die Zeit, die ein Schutzsystem benötigt, um einen Angriff zu erkennen und erfolgreich abzuwehren (siehe dazu unsere Benchmark-Studie: „The New Benchmark: Why Fast DDoS Detection Is No Longer Good Enough"). Hier gewinnen automatisierte, KI-basierte Abwehrmechanismen zunehmend an Bedeutung, um Angriffe in Echtzeit zu analysieren und in Sekundenschnelle Gegenmaßnahmen einzuleiten.

Die Zahlen zeigen: DDoS-Angriffe entwickeln sich weiter – sie sind nicht mehr nur eine Frage der Bandbreite, sondern erfordern eine agile, intelligente und vorausschauende Sicherheitsstrategie. Wer sich ausschließlich auf herkömmliche Schutzmechanismen verlässt, riskiert erhebliche Ausfallzeiten und Sicherheitslücken in der IT-Infrastruktur.



Entwicklung der Angriffsbandbreiten

Von Gigabit zu Terabit

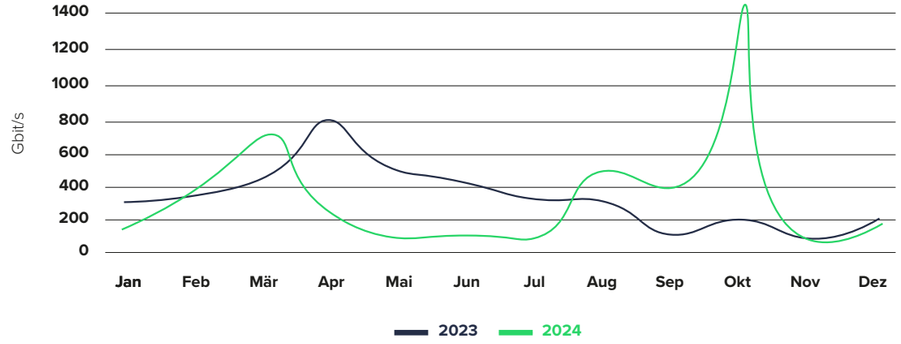
Die DDoS-Landschaft hat sich in den vergangenen Jahren immer wieder verändert. Während das Jahr 2023 von einer Zunahme der Häufigkeit und Intensität von DDoS-Angriffen geprägt war, markiert das Jahr 2024 einen neuen Höhepunkt. Mit einem größten gemessenen Angriff von 795 Gbit/s und einer durchschnittlichen Gesamtbandbreite von 3,0 Gbit/s übertrafen die DDoS-Angriffe 2023 die Werte des Vorjahres deutlich. Die Angreifer erhöhten nicht nur die Bandbreite, sondern auch die Paketrate drastisch.

Das Jahr 2024 übertraf jedoch alle Erwartungen: Mit dem größten in Europa gemessenen Angriff von 1,4 Tbit/s wurde eine neue Dimension erreicht. Diese Steigerung um mehr als das Doppelte verdeutlicht die rasante Entwicklung der Angriffsvektoren. Gleichzeitig zeigt sich aber auch ein differenzierteres Bild der Bedrohungslage. Neben massiven Angriffen mit hoher Bandbreite setzen die Angreifer zunehmend auf verfeinerte Techniken, um ihre Angriffe schwerer erkennbar zu machen.

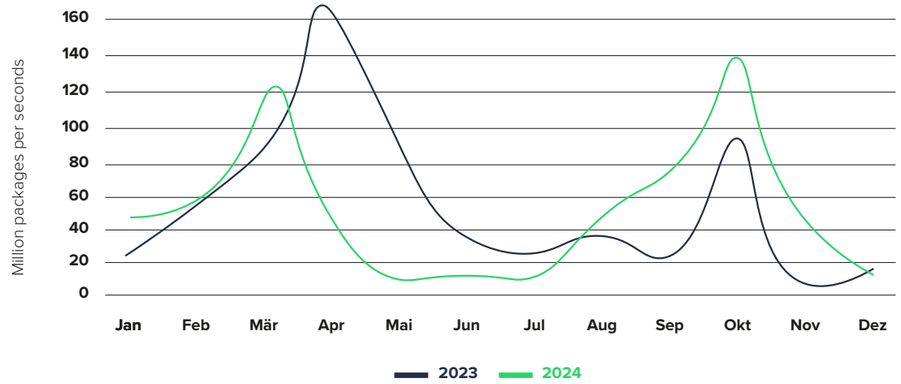
Von Quantität zu Qualität: Subtilere und gezieltere Angriffe

Während die Höchstwerte einzelner Angriffe neue Rekorde erreichen, zeichnet sich gleichzeitig eine strategische Verschiebung ab. Die Angreifer gehen zunehmend subtiler und gezielter vor. Sie nutzen geringere Bandbreiten und Paketraten, was die Erkennung durch herkömmliche Monitoring-Systeme erschwert. Statt massiver Brute-Force-Angriffe sind die Attacken oft besser getarnt und fügen sich nahtlos in den normalen Datenverkehr ein. Diese Entwicklung zeigt, dass DDoS-Bedrohungen nicht nur an Intensität, sondern auch an Raffinesse zunehmen.

Maximale Bandbreite



Maximale Paketraten



Carpet Bombing

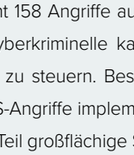
Carpet Bombing ist eine besonders perfide Form von DDoS-Angriffen, die Unternehmen und kritische Infrastrukturen zunehmend vor massive Herausforderungen stellt. Im Gegensatz zu herkömmlichen DDoS-Attacken, die gezielt einzelne Server oder Netzwerkknoten überlasten, setzt Carpet Bombing auf eine breit gestreute Angriffstaktik: Große Mengen schädlichen Datenverkehrs fluten gleichzeitig eine Vielzahl von IP-Adressen innerhalb eines Netzwerks. Dies erschwert die Identifikation des Angriffs und führt dazu, dass selbst modernste Schutzmechanismen oft erst dann Alarm schlagen, wenn die Infrastruktur bereits überlastet ist.

Mehrere Vorfälle in Japan zeigen das erschreckende Ausmaß der Bedrohung: Zwischen Dezember 2023 und Februar 2024 wurden insgesamt 158 Angriffe auf 64 Unternehmen registriert, darunter Banken, Flughäfen und Telekommunikationsanbieter. Cyberkriminelle kaperten weltweit mindestens 300 IoT-Geräte, um koordinierte Angriffe aus dem Verborgenen zu steuern. Besonders tückisch: Viele Unternehmen hatten zwar Schutzmaßnahmen gegen klassische DDoS-Angriffe implementiert, nicht aber gegen die breit gestreuten Carpet-Bombing-Attacken. Die Folge waren zum Teil großflächige Systemausfälle, die zentrale Geschäftsprozesse lahmlegten.[19]

Experten sind sich einig, dass herkömmliche Abwehrmechanismen nicht ausreichen, um dieser eskalierenden Bedrohung zu begegnen. Eine proaktive Sicherheitsstrategie ist in diesem Zusammenhang ein entscheidender Faktor. Angriffe werden frühzeitig erkannt und Gegenmaßnahmen eingeleitet, bevor das System lahmgelegt wird. Dazu gehören fortschrittliche Erkennungssysteme, intelligente Traffic-Filter und adaptive Netzwerk-Schutzmaßnahmen, die über eine reaktive DDoS-Abwehr hinausgehen.

„Unternehmen müssen ihre IT-Sicherheitsstrategien anpassen, um ausgefeilte DDoS-Angriffe wie Carpet Bombing abzuwehren. Entscheidend wird ein mehrschichtiger Schutz mit Echtzeitüberwachung und automatisierter Bedrohungsabwehr sein.“

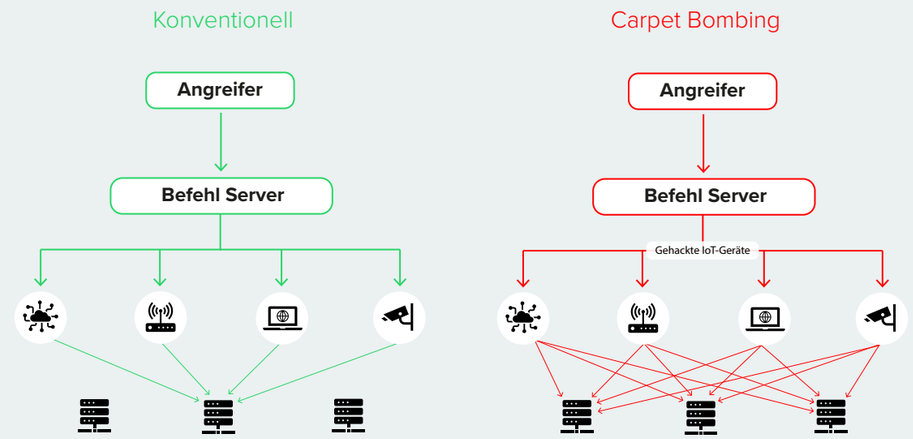
Rolf Gierhard, CRO, Link11



Carpet Bombing - Kontrollierter Massen-DDoS-Angriff

Im Gegensatz zu herkömmlichen DDoS-Attacken, die gezielt einzelne Server oder Netzwerkknoten überlasten, setzt Carpet Bombing auf eine breit gestreute Angriffstaktik: Große Mengen schädlichen Datenverkehrs fluten gleichzeitig eine Vielzahl von IP-Adressen innerhalb eines Netzwerks.

Der Fokus des Botnetzes liegt dabei nicht nur auf einer IP-Adresse, sondern verteilt sich auf 100 bis mehrere 1000 IP-Adressen, um flächendeckend Schaden anzurichten.



UDP Floods und TCP SYN Floods

UDP Floods greifen auf Layer 3 und 4 an, da UDP keine Absenderverifizierung erfordert und keinen Handshake durchführt. Dies ermöglicht eine schnelle Datenübertragung, weshalb UDP oft in latenzkritischen Anwendungen wie Streaming oder Gaming genutzt wird. Angreifer generieren massenhafte Pakete an zufällige UDP-Ports (packet storm), wodurch Firewalls, Router und Switches jedes Paket verarbeiten und validieren müssen. Da diese Systeme nur eine begrenzte Anzahl von Paketen pro Sekunde bewältigen können, führt dies schnell zu einer Überlastung. Durch Reflection-Techniken, die Protokolle wie DNS, NTP, SSDP oder Chargen einbeziehen, können UDP-Attacken zusätzlich verstärkt werden.

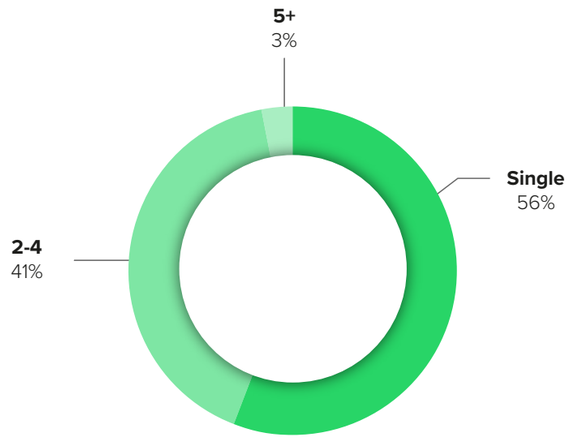
TCP SYN Floods nutzen Schwächen im TCP-Drei-Wege-Handshake aus. Beim Verbindungsaufbau sendet der Client ein SYN-Paket an den Server, der mit SYN/ACK antwortet und eine Bestätigung (ACK) erwartet. Der Server speichert diese halboffenen Verbindungen temporär in den Transmission Control Blocks (TCB). Bleibt die Bestätigung aus, weil die SYN-Anfragen von gefälschten oder nichtexistierenden Absender-IP-Adressen stammen, läuft der TCB-Puffer voll. Der Server kann dann keine neuen Verbindungen mehr annehmen. Angreifer halten den Puffer durch ständige SYN-Anfragen künstlich voll. Maßnahmen wie eine Reduzierung des Puffers sind gegen großflächige SYN-Flood-Angriffe mit Tausenden infizierten Systemen wirkungslos.

Multi-Vektor-Attacken

Präzision statt Masse

Die Bedrohung durch Multi-Vektor-DDoS-Angriffe hat sich im Jahr 2024 weiterentwickelt. Während sich bereits 2023 ein Trend zu gezielteren und ressourcenschonenderen Angriffen abzeichnete, haben Cyberkriminelle ihre Strategien 2024 weiter verfeinert.

Im Jahr 2023 lag der Anteil der Multi-Vektor-Angriffe bei 52 %, während 2024 56 % aller Angriffe auf Single-Vector-Methoden setzen. Dennoch bleibt der Anteil komplexer Multi-Vektor-Attacken hoch: Bei 41 % der Angriffe kamen bis zu vier Vektoren zum Einsatz und bei 3 % sogar mehr als vier. Die höchste beobachtete Vektoranzahl stieg von 11 im Jahr 2023 auf 12 im Jahr 2024.



DNS als dominierender Vektor

Die Analyse der Top-5-Vektoren zeigt eine Verschiebung in der Gewichtung: DNS-Angriffe nehmen nach wie vor den größten Anteil aller Vektoren ein. Es folgen HTTPS-basierte Angriffe, während NTP als Angriffsvektor etwas an Bedeutung verloren hat. Neu in den Top 5 sind SNMP- und Chargen-Angriffe, die bisher keine nennenswerte Rolle spielten. Diese Veränderungen spiegeln die zunehmende Präzision und Anpassungsfähigkeit der Angreifer wider.

SNMP-DDoS-Attacken: Gefährliche Kombination aus Reflection und Amplification

Das Simple Network Management Protocol (SNMP) wird zunehmend für DDoS-Angriffe missbraucht. Dabei nutzen Angreifer offene SNMP-Instanzen, um durch gefälschte Anfragen große Datenmengen auf ihr Ziel umzuleiten. Besonders problematisch ist die Kombination von **Reflection**, bei der Geräte ungewollt Daten an das Opfer senden, und **Amplification**, bei der die Antwortpakete um ein Vielfaches größer sind als die ursprüngliche Anfrage. Das Ergebnis sind Angriffe mit enormen Datenmengen, die Netzwerke überlasten und Dienste lahmlegen.

Kritische Schwachstellen

Unsichere SNMP-Server mit Standard-Community-Strings wie „public“

Fehlende Netzwerkfilterung, die IP-Spoofing ermöglicht

Botnetze, die Angriffe koordinieren und verstärken

Automatisierte Abwehr durch KI und adaptive Schutzmechanismen

2024 zeigt sich: die Angriffe sind zielgerichteter, schwerer zu erkennen und nutzen ein breites Spektrum an Protokollen und Techniken, um Abwehrmaßnahmen zu überwinden. Besonders gefährlich sind sich schrittweise aufbauende Angriffe.

Klassische DDoS-Attacken fielen durch hohe Bandbreiten oder Paketraten auf, moderne Angriffe bleiben hingegen oft unterhalb der Erkennungsschwellen. Herkömmliche Traffic-Monitoring-Systeme stoßen daher an ihre Grenzen.

KI-gestützte Systeme sind unerlässlich, um komplexe Angriffsmuster zu analysieren und rechtzeitig Gegenmaßnahmen einzuleiten. Unternehmen sollten auf eine Kombination aus automatisierter DDoS-Abwehr, umfassendem Monitoring sowie KI-basierter Erkennung setzen. Ganzheitliche Sicherheitslösungen erkennen auch subtile Anomalien im Netzwerkverhalten.

„Trotz ihrer langen Historie entwickelt sich die DDoS-Bedrohungslandschaft stetig weiter – Angreifer suchen kontinuierlich nach neuen Wegen, um ihre Angriffe zu verstärken und zu diversifizieren.“

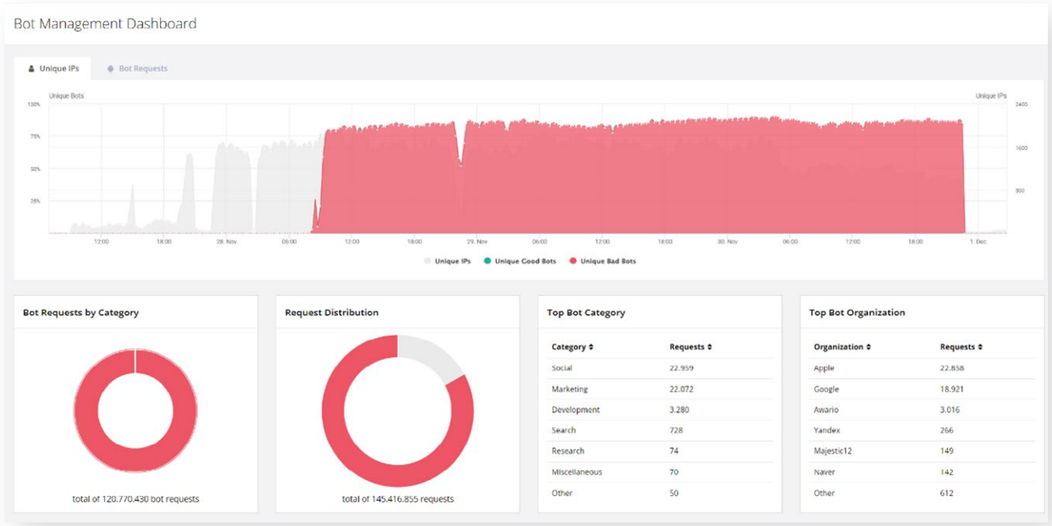
Karsten Desler, CTO, Link11

Um sich vor solchen Angriffen zu schützen, sollten Unternehmen SNMP konsequent absichern, unnötige Instanzen deaktivieren und auf SNMPv3 mit Authentifizierung und Verschlüsselung setzen. Darüber hinaus sind Ingress-Filter gegen IP-Spoofing sowie ein umfassendes Monitoring verdächtiger SNMP-Aktivitäten unerlässlich. Auch ISPs sollten gezielte Filtermaßnahmen implementieren, um verdächtigen SNMP-Verkehr frühzeitig zu blockieren. Nur durch eine Kombination aus sicherer Konfiguration, Traffic-Filterung und proaktiver Erkennung können SNMP-DDoS-Angriffe effektiv abgewehrt werden.

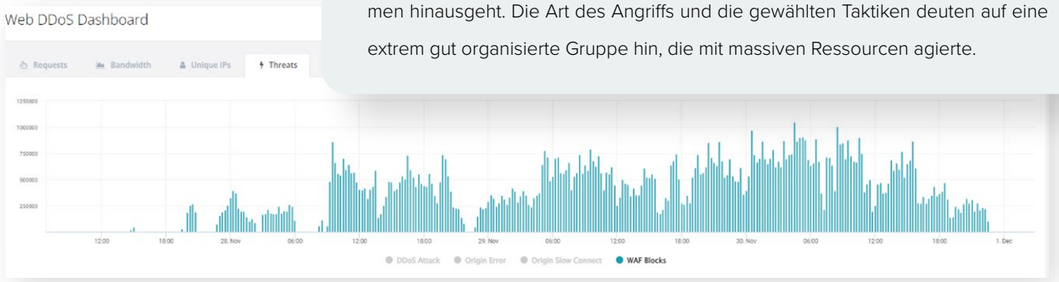
Web Protection

WAAP im Ernstfall: Analyse eines Multi-Vektor-DDoS-Angriffs
Ein kürzlich im Link11-Netzwerk dokumentierter Angriff gibt Aufschluss über die Komplexität und den enormen Aufwand, den Angreifer investieren, um Systeme zu überlasten. Dieser Angriff kombinierte sowohl Layer-3/4- als auch Layer-7-DDoS-Techniken und setzte vor allem in Bezug auf Ressourcenaufwand und Angriffsvektoren neue Maßstäbe.

Der Angriff: Komplexes Zusammenspiel von DDoS-Methoden
Der Angriff erstreckte sich über vier Tage und zeigte ein ausgeklügeltes Zusammenspiel verschiedener Angriffsmethoden. Besonders bemerkenswert war der gleichzeitige Einsatz von Layer-3/4- und Layer-7-Angriffen – eine Kombination, die in der Praxis selten vorkommt. Layer-3/4- Angriffe konzentrieren sich auf die Netzwerkebene und überlasten die Infrastruktur durch massive Datenpakete, während Layer-7-Angriffe auf der Applikationsebene gezielt Webserver und APIs angreifen, indem sie deren Ressourcen beanspruchen und die Antwortzeiten deutlich verlängern.



Bei diesem Angriff erreichten die Angreifer die unglaubliche Zahl von 120 Millionen Requests, was zu mehr als einer Million WAF-Logs (Web Application Firewall Logs) führte – eine Zahl, die weit über das übliche Volumen hinausgeht. Die Art des Angriffs und die gewählten Taktiken deuten auf eine extrem gut organisierte Gruppe hin, die mit massiven Ressourcen agierte.



WAF Verletzungen Top 5
2023 vs. 2024

Im Jahr 2024 hat die Anzahl der Protokollangriffe im Vergleich zu 2023 deutlich zugenommen. Dabei werden gezielt Schwachstellen in Kommunikationsprotokollen ausgenutzt, um Webanwendungen oder Server zu kompromittieren, wobei Angreifer verschiedene Techniken nutzen, um Sicherheitsmechanismen zu umgehen, Daten zu manipulieren oder sich unberechtigten Zugriff zu verschaffen. Die häufigsten Protokollangriffe sind:

- **HTTP-Response-Splitting:** Hierbei wird die HTTP-Antwort eines Servers so manipuliert, dass sie in mehrere einzelne Antworten aufgeteilt wird. Dadurch kann der Angreifer zusätzliche Header oder Inhalte einschleusen, die von zwischengeschalteten Systemen (z. B. Proxies oder Caches) falsch interpretiert werden können. Dies kann zu Cache-Poisoning, Cross-Site Scripting (XSS) oder Session-Fixing-Angriffen führen.

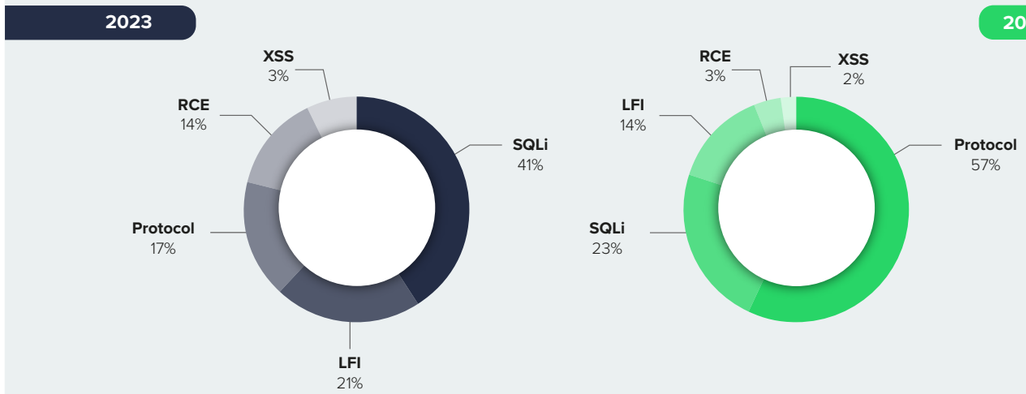
- **HTTP-Smuggling:** Dieser Angriff nutzt Unterschiede in der Interpretation von HTTP-Anfragen durch verschiedene Serverinstanzen (z. B. Load Balancer, Reverse Proxies und Backend-Server) aus. Indem Anfragen so gestaltet werden, dass sie von den Systemen unterschiedlich verarbeitet werden, können Angreifer Sicherheitsmechanismen umgehen, geschützte Bereiche erreichen oder unautorisierten Code einschleusen. HTTP-Smuggling wird häufig eingesetzt, um Firewalls oder Intrusion-Detection-Systeme zu umgehen.

- **HTTP-Header-Injection:** Hierbei werden manipulierte Header in HTTP-Anfragen oder -Antworten eingefügt, um das Verhalten des Servers oder nachgeschalteter Systeme zu verändern. Dadurch können Sicherheitsmaßnahmen umgangen oder Schwachstellen in Webanwendungen ausgenutzt werden. Mögliche Folgen sind unter anderem Cross-Site-Scripting (XSS), Open Redirects oder sogar Remote Code Execution (RCE).

- **HTTP-Parameter-Pollution (HPP):** Bei dieser Angriffstechnik fügen Angreifer mehrere identische oder manipulierte Parameter in eine HTTP-Anfrage ein, um die Verarbeitung auf der Serverseite zu beeinflussen. Dies kann dazu führen, dass Anwendungen falsche Werte verwenden, Sicherheitsprüfungen umgehen oder unerwartetes Verhalten zeigen. HPP kann für Angriffe wie Privilege Escalation, SQL Injection oder Denial-of-Service (DoS) verwendet werden.

Neben diesen spezifischen Angriffstechniken gibt es auch andere Protokollangriffe, die auf Schwachstellen in Transport- oder Anwendungsschichtprotokollen abzielen. Dazu gehören beispielsweise TLS-Downgrade-Angriffe, bei denen Angreifer versuchen, die Verschlüsselung auf eine unsichere Version herabzustufen, oder DNS-Spoofing, bei dem gefälschte DNS-Antworten verwendet werden, um Benutzer auf bösartige Webseiten umzuleiten.

Angesichts der wachsenden Bedrohung durch Protokollangriffe ist es entscheidend, moderne Sicherheitsmechanismen wie Web Application Firewalls (WAFs), strikte Header-Validierung und sichere Serverkonfigurationen zu implementieren, um potenzielle Angriffe frühzeitig zu erkennen und abzuwehren.



Angreifer mit hohen Ressourcen

Eine Besonderheit des Angriffs war die Herkunft der Angriffe. Diese stammten von Unternehmen, die international tätig sind und deren Infrastruktur normalerweise nicht mit DDoS-Angriffen in Verbindung gebracht wird. Darüber hinaus wurde eine große Anzahl von IP-Adressen gleichzeitig blockiert, was darauf hindeutet, dass die Angreifer in der Lage sind, ihre Ressourcen schnell und gezielt zu skalieren.

Ein weiterer auffälliger Aspekt war die Verwendung von bis zu 2.000 eindeutigen IP-Adressen, was eine massive Steigerung gegenüber den üblichen Hunderten von IP-Adressen darstellt. Auch die Tatsache, dass die Angreifer im späteren Verlauf des Angriffs vermehrt veraltete User-Agents wie Windows XP und Browserversionen der letzten fünf Jahre einsetzten, deutet auf den Einsatz automatisierter Botnetze hin, die von kompromittierten Systemen weltweit gesteuert werden.

Kosten und Motivation des Angriffs

Ein Angriff dieser Größenordnung ist mit erheblichen Kosten verbunden. Es ist unwahrscheinlich, dass solch eine Attacke zum Nulltarif durchgeführt wurde. Die von den Angreifern in vier Tagen generierten 145 Millionen Anfragen würden in einer regulären Hosting-Infrastruktur mehrere tausend Euro kosten. Daraus lässt sich schließen, dass es sich um eine hoch organisierte Aktion handelt.

Die mögliche Motivation hinter diesem Angriff könnte politisch motivierter Hacktivismus oder ein Angriff im Auftrag politischer Akteure sein. Ein weiterer plausibler Hintergrund könnte die Nutzung von DDoS-as-a-Service sein – eine Praxis, die im Bereich der DDoS-Angriffe zunehmend an Bedeutung gewinnt. Die hohe Komplexität und der Aufwand des Angriffs sprechen jedoch gegen die einfache Vorstellung eines „Script-Kiddies“ oder eines einzelnen Akteurs.

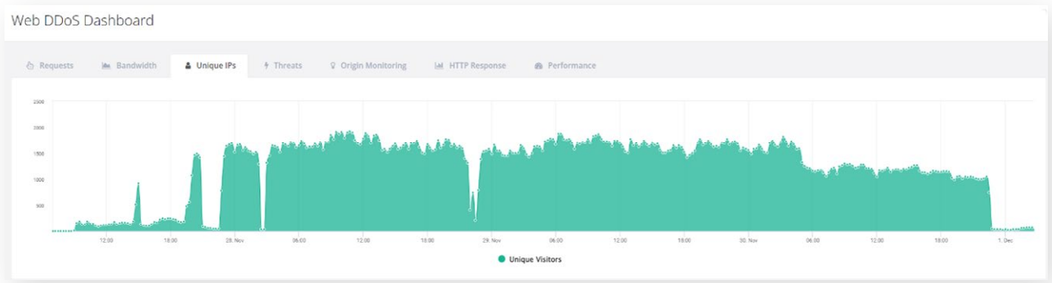
Ungewöhnliche Angriffsmuster

Ein besonders interessantes Detail war das Verhalten der Angreifer: Es schien, als hätten sie alle ihre Methoden getestet, um herauszufinden, welche gegen die Schutzmechanismen der Zielsysteme wirksam sind. Die Angreifer versuchten, alle Werkzeuge und Taktiken aus ihrem Arsenal einzusetzen, von Layer-3/4- bis hin zu Layer-7-Angriffen. Es handelte sich um eine Attacke, bei der das gesamte Spektrum getestet wurde, um zukünftige Angriffe weiter zu optimieren.

Darüber hinaus gab es während des Angriffs ein „On-Off-Szenario“, bei dem die Angriffe in regelmäßigen Abständen pausierten und dann wieder mit voller Kraft fortgesetzt wurden. Dies weist darauf hin, dass die Angreifer mit den Schutzmechanismen der Zielsysteme experimentierten und testeten, wie diese auf unterschiedliche Angriffsmuster reagieren. Zu Beginn der Attacke wurde ein solcher Wechsel der Techniken beobachtet.

Die Rolle von Bot-Management und Web Application Firewalls (WAF)

Als Reaktion auf den Angriff wurden Maßnahmen wie Bot-Management und Web Application Firewalls (WAF) eingesetzt, die eine wichtige Rolle bei der Abwehr der Angriffe spielten. WAF-Systeme, die sich anfangs in einer Lernphase befanden, konnten schließlich den Großteil der Angriffe identifizieren und abwehren. Dies zeigt, wie wichtig es für Unternehmen ist, ihre Sicherheitslösungen regelmäßig anzupassen und zu optimieren, um den sich ständig weiterentwickelnden Bedrohungen durch DDoS-Angriffe standhalten zu können.



„Angriffe wie dieser verdeutlichen, dass effektiver Schutz nur durch einen ganzheitlichen Ansatz möglich ist, der Bot Management, WAF und kontinuierliches Monitoring vereint.“

Ziv Greenberg, VP Product, Link11

Zudem wurde in diesem Fall ein kontinuierlicher Schutzmodus aktiviert, um sicherzustellen, dass der Angriffsschutz nicht vorzeitig deaktiviert wird, was die Effektivität der Abwehr zusätzlich erhöht.

Eine immer komplexere Bedrohung

Dieser Fall zeigt eindrucksvoll, wie sich DDoS-Angriffe zu immer komplexeren und langwierigeren Bedrohungen entwickeln. Die Angreifer verwenden nicht nur traditionelle Methoden, sondern kombinieren verschiedene Angriffstechniken und testen ständig neue Strategien, um bestehende Schutzmechanismen zu überwinden.

Für IT-Experten und Unternehmen, die Web-Applikationen und APIs schützen müssen, ist daher eine ganzheitliche Schutzstrategie entscheidend, die Bot-Management, WAF, Layer-3/4- und Layer-7-Abwehrmechanismen kombiniert. Dieser mehrschichtige Ansatz ist der Schlüssel, um gegen die immer raffinierteren DDoS-Angriffe der Zukunft gewappnet zu sein.

Der Fall zeigt, dass nicht nur die Technik, sondern auch die Motivation und das Ressourcenpotenzial der Angreifer immer stärker in den Fokus rücken müssen. Ein gezieltes und kontinuierliches Monitoring sowie die rasche Anpassung der Schutzmechanismen sind unabdingbar, um der Bedrohung durch hochentwickelte DDoS-Angriffe erfolgreich zu begegnen.

In der heutigen Bedrohungslandschaft sind DDoS-Angriffe nicht nur zahlreicher, sondern auch immer komplexer geworden. Besonders bemerkenswert an diesem Angriff war die gleichzeitige Verwendung von Layer-3/4- und Layer-7-Angriffen – eine Kombination, die bei DDoS-Angriffen selten vorkommt, aber zunehmend als Strategie zur Umgehung von Schutzmechanismen eingesetzt wird.

Layer-3- und -4-Angriffe zielen auf die Netzwerkebene und überlasten die Infrastruktur durch massive Datenmengen und manipulierte Paketströme. Diese Angriffe zielen darauf ab, die Serverkapazität und die Netzwerkbandbreite zu überlasten. Im Gegensatz dazu zielen Layer-7-Angriffe auf die Applikationsebene, wo sie gezielt Webanwendungen und APIs angreifen, um Ressourcen wie CPU und Arbeitsspeicher zu überlasten. Sie sind wesentlich zielgerichteter und benötigen weniger Bandbreite, können aber durch Ausnutzung der spezifischen Schwachstellen von Webanwendungen enormen Schaden anrichten.

Die Kombination dieser beiden Angriffsarten stellt eine große Herausforderung für moderne Web Application and API Protection (WAAP) dar. Während Layer-3- und -4-Angriffe die Infrastruktur in den frühen Phasen des Angriffs überlasten, greifen Layer-7-Angriffe gezielt die Anwendungen selbst an, was eine differenzierte Verteidigungsstrategie erfordert.

In diesem Fall testeten die Angreifer beide Angriffsebenen parallel, um herauszufinden, welche Schutzmechanismen wie Web Application Firewalls (WAF) und Bot-Management-Systeme am besten zu umgehen sind. Dieses strategische Vorgehen zeigt, wie wichtig eine ganzheitliche WAAP-Strategie ist, die sowohl die Netzwerkschicht als auch die Anwendungsebene umfasst.

Web Performance

EU-US Datenschutzrahmen wackelt – eine Chance für europäische CDNs und Geofencing

Die jüngsten Entwicklungen rund um das transatlantische Datenabkommen, offiziell bekannt als EU-US Data Privacy Framework (DPF) haben erhebliche Auswirkungen auf den Austausch personenbezogener Daten zwischen der EU und den USA. Seit dem Amtsantritt von Donald Trump am 20. Januar 2025 gibt es ernsthafte Bedenken über die Zukunft des Abkommens.[20]

Hauptprobleme sind die Schwächung des „Privacy and Civil Liberties Oversight Board“ (PCLOB), die Überprüfung aller nationalen Sicherheitsentscheidungen der Vorgängerregierung und die drohende Rechtsunsicherheit für europäische Unternehmen, die US-Cloud-Dienste nutzen. Sollte das DPF scheitern, könnten sich tausende Unternehmen in einer rechtlichen Grauzone wiederfinden und gezwungen sein, nach alternativen Lösungen zu suchen.

In diesem Zusammenhang gewinnen europäische Content Delivery Networks (CDNs) und Geofencing-Technologien an Bedeutung. Diese Mechanismen ermöglichen eine gezielte Kontrolle des Datenflusses innerhalb sicherer Rechtsräume und helfen Unternehmen, die Einhaltung der Datenschutz-Grundverordnung (DSGVO) sicherzustellen. Geofencing kann verhindern, dass personenbezogene Daten in Länder mit unzureichendem Datenschutz gelangen, während europäische CDNs eine DSGVO-konforme Alternative zu US-Anbietern darstellen.

Geoblocking: Effiziente Zugangskontrolle zur Abwehr von Bedrohungen

Mit Geoblocking können Unternehmen den Zugriff auf ihre IT-Infrastruktur selektiv steuern, indem sie den Traffic aus bestimmten Ländern oder Regionen blockieren. Dies ist insbesondere zur Abwehr von Cyberangriffen wie DDoS-Attacken sinnvoll, die häufig aus bestimmten geografischen Regionen stammen. So kann beispielsweise ein plötzlicher Anstieg von bösartigem Datenverkehr aus einem bestimmten Land durch die gezielte Sperrung dieses Herkunftslandes effektiv entschärft werden.

In der Praxis wird Geoblocking bevorzugt an der Edge implementiert, da das CDN als erste Verteidigungslinie fungiert. Moderne Anbieter integrieren DDoS-Mitigation direkt in ihr Netzwerk, um Angriffe frühzeitig zu neutralisieren.

Darüber hinaus spielt Geoblocking eine zentrale Rolle bei der Zugangskontrolle zu digitalen Inhalten. Streaming-Dienste und Mediatheken setzen Geoblocking ein, um sicherzustellen, dass Inhalte nur in bestimmten Ländern abgerufen werden können. Ohne Geoblocking könnte ein Nutzer in einem gesperrten Land weiterhin auf gecachte Inhalte zugreifen, was zu rechtlichen und lizenzrechtlichen Problemen führen kann.

Geofencing: Datenschutz, Compliance und gezielte Kontrolle

Geofencing erweitert die Funktionen von Geoblocking, indem es nicht nur den Zugang regelt, sondern auch kontrolliert, wo Daten verarbeitet oder gespeichert werden. Dies ist insbesondere für die DSGVO-Compliance relevant, da personenbezogene Daten nicht unkontrolliert in Drittstaaten übermittelt werden dürfen.

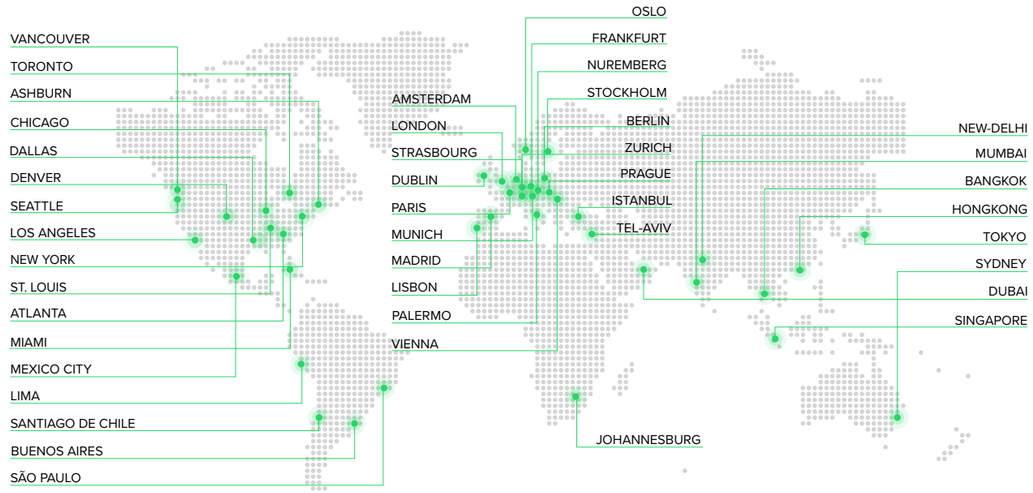
Ein konkretes Beispiel für die Bedeutung einer datenschutzkonformen Datenverarbeitung ist der Einsatz von Sicherheitsdiensten wie Captchas. Anbieter wie Google speichern und verarbeiten Nutzerdaten häufig in den USA, was datenschutzrechtliche Risiken birgt. Während Geofencing nicht direkt mit Captchas in Verbindung steht, kann es Unternehmen dennoch ermöglichen, den Zugriff auf alternative, DSGVO-konforme Captcha-Dienste innerhalb der EU gezielt zu kontrollieren und sicherzustellen, dass Nutzerdaten in datenschutzkonformen Regionen verarbeitet werden.

Technisch wird Geofencing durch spezielle CDN-Technologien ermöglicht, die den Datenverkehr gezielt steuern und Nutzeranfragen an Server in bestimmten geografischen Regionen weiterleiten. So kann sichergestellt werden, dass beispielsweise europäische Nutzer ausschließlich mit Servern innerhalb der EU interagieren. Dies trägt nicht nur zur Einhaltung von Datenschutzbestimmungen bei, sondern kann auch die Netzwerkleistung optimieren.

Geofencing und flexible CDN-Steuerung

Viele internationale CDN-Anbieter setzen auf Technologien wie

Link11 Hyperscale Cloud



13 Scrubbing Centers **43** Edge POPs **107** Cloud POPs

Anycast, die eine IP-Adresse mit mehreren Serverstandorten verknüpfen, um Performance und Redundanz zu maximieren. Dies kann jedoch die genaue Steuerung des Datenverkehrs erschweren.

Europäische Anbieter wie Link11 bieten gezieltere Steuerungsmöglichkeiten und setzen dabei auf speziell optimierte Mechanismen. So kann der Traffic konsequent innerhalb Europas gehalten oder bestimmte Regionen ausgeschlossen werden, was für Unternehmen mit hohen Datenschutzanforderungen eine flexible Lösung darstellt.

Andere Anbieter verwenden alternative Technologien, die möglicherweise weniger flexibel sind, wenn es darum geht, den Datenfluss strikt an Datenschutz- und Compliance-Anforderungen anzupassen.

Kapazität vs. Compliance: Die Rolle spezialisierter europäischer CDNs

Ein häufiges Argument globaler CDN-Anbieter ist ihre riesige Infrastruktur mit einer hohen Anzahl von Points-of-Presence (PoPs). Entscheidend ist jedoch nicht nur die absolute Anzahl der Server, sondern deren strategische Platzierung in den relevanten Märkten. Für europäische Unternehmen kann eine gezielt optimierte regionale Infrastruktur oft vorteilhafter sein als ein weltweit verteiltes Netzwerk.

So betreibt Link11 weltweit zahlreiche CDN-Knoten mit besonderem Fokus auf eine leistungsfähige und engmaschige Infrastruktur in Europa. Diese gezielte Standortwahl gewährleistet eine optimale Performance in den entscheidenden Märkten und bietet Unternehmen eine zuverlässige Alternative zu global verteilten Netzwerken, die in strategisch wichtigen Regionen möglicherweise weniger gut ausgebaut sind.

Sicherheit, Compliance und Performance im Einklang

Im Spannungsfeld zwischen IT-Sicherheit, regulatorischer Compliance und Performance bieten Geoblocking und Geofencing einen entscheidenden Mehrwert. Während globale CDN-Anbieter häufig nach maximaler Performance streben, setzen europäische Anbieter verstärkt auf Datenschutzkonformität und gezielte Steuerung des Datenverkehrs.

Unternehmen, die sich auf DSGVO-Compliance verlassen müssen, sollten daher prüfen, ob ein europäischer CDN-Anbieter wie Link11 nicht die bessere Alternative darstellt. Die Wahl der richtigen IT-Sicherheitsstrategie hängt nicht nur von der technischen Machbarkeit ab, sondern muss auch regulatorische und geschäftliche Anforderungen berücksichtigen. Geoblocking und Geofencing sind in diesem Zusammenhang unverzichtbare Instrumente einer ganzheitlichen IT-Sicherheitsstrategie.

DNS-Sicherheit: Die oft unterschätzte Achillesferse von IT-Infrastrukturen

Die Lektion von Mastercard: Ein DNS-Fehler mit weitreichenden Folgen

Im Januar 2025 sorgte eine sicherheitskritische DNS-Fehlkonfiguration bei Mastercard für Schlagzeilen.[21] Fünf Jahre lang war ein einfacher, aber folgenschwerer Tippfehler in der DNS-Konfiguration des Unternehmens unbemerkt geblieben. Eine der fünf von Mastercard verwendeten DNS-Adressen war falsch geschrieben und verwies auf eine nicht registrierte Domain. Ein Sicherheitsforscher sicherte sich diese für nur 300 US-Dollar und stellte fest, dass sie bereits Millionen von DNS-Anfragen verarbeitete. Wäre diese Schwachstelle von Cyberkriminellen ausgenutzt worden, hätte dies massive Folgen haben können – von der Umleitung des Internetverkehrs bis hin zum Diebstahl von Zugangsdaten.

Der Vorfall zeigt eindrücklich, dass auch vermeintlich triviale Komponenten wie das Domain Name System (DNS) für die IT-Sicherheit entscheidend sind. Das DNS ist das „Telefonbuch des Internets", das Domainnamen in IP-Adressen auflöst. Ein einziger Fehler oder eine Sicherheitslücke kann ausreichen, um den gesamten Datenverkehr eines Unternehmens zu kompromittieren.

Warum DNS-Sicherheit wichtig ist

Obwohl das DNS eine der kritischsten Komponenten des Internets ist, wurde es ursprünglich ohne integrierte Sicherheitsmechanismen entwickelt. Heute sind DNS-basierte Angriffe ein lukratives Ziel für Cyberkriminelle, da viele Unternehmen diesem Bereich zu wenig Aufmerksamkeit schenken. Die Bedrohungsszenarien sind vielfältig:

- **DNS-Spoofing und Cache Poisoning:** Angreifer manipulieren DNS-Antworten und leiten Nutzer so auf gefälschte Webseiten, um deren Daten abzugreifen.
- **DDoS-Attacken auf DNS-Server:** Durch massenhafte Anfragen werden DNS-Server überlastet und lahmgelegt, sodass Internetdienste nicht mehr erreichbar sind.
  DNS-Hijacking: Cyberkriminelle übernehmen die Kontrolle über DNS-Einstellungen, um Datenverkehr umzuleiten oder E-Mail-Kommunikation abzufangen.
- **Datenexfiltration durch DNS-Tunneling:** Malware nutzt DNS-Anfragen, um unbemerkt Daten aus Netzwerken zu schleusen.

Strategien zur Verbesserung der Sicherheit des DNS

Angesichts dieser Bedrohungen ist eine robuste DNS-Sicherheitsstrategie unerlässlich. Eine sichere DNS-Infrastruktur umfasst verschiedene Maßnahmen, um Angriffe abzuwehren und eine hohe Verfügbarkeit zu gewährleisten.

Wichtige Maßnahmen zur Erhöhung der DNS-Sicherheit:

- **Globale Anycast-Infrastruktur:** Weltweit verteilte Server ermöglichen eine schnelle und zuverlässige DNS-Auflösung.
- **Schutz vor DoS/DDoS-Angriffen:** Moderne DNS-Filter und Monitoring-Mechanismen helfen, verdächtige Aktivitäten frühzeitig zu erkennen und abzuwehren.
- **DNSSEC-Implementierung:** Der Einsatz von DNS Security Extensions (DNSSEC) stellt sicher, dass DNS-Antworten authentifiziert und nicht manipuliert werden können.
  Einfache Verwaltung und Automatisierung: Moderne Management-Plattformen und APIs ermöglichen eine sichere und effiziente Konfiguration.
- **Redundanz und Ausfallsicherheit:** Mehrere Serverstandorte sorgen dafür, dass DNS-Dienste auch bei Ausfällen zuverlässig funktionieren.

DNS-Sicherheit ist kein Luxus, sondern eine Notwendigkeit

Der Mastercard-Vorfall zeigt, dass auch milliardenschwere Unternehmen grundlegende Sicherheitsaspekte wie die Integrität des DNS vernachlässigen können. Die richtige Absicherung dieser kritischen Infrastruktur ist entscheidend, um Cyberangriffe zu verhindern und Geschäftsprozesse zu schützen. Link11 Secure DNS ist eine robuste, skalierbare und sichere Lösung, die Unternehmen den Schutz und die Performance bietet, um ihre digitale Präsenz zu sichern.

Denn im Internet gilt: Ohne DNS geht nichts - und ohne sicheres DNS ist alles gefährdet.

„Das DNS ist die Achillesferse des Internets – ein einzelner Konfigurationsfehler kann ausreichen, um den gesamten Datenverkehr eines Unternehmens zu kompromittieren."

Lukas Frank, Product Manager, Link11

2024

Das Jahr 2024 war geprägt von einer beispiellosen Welle von DDoS-Angriffen, die mit Rekordzahlen und zunehmender Komplexität die Cybersicherheitslandschaft dominierten. Die Verbreitung von DDoS-as-a-Service und der Einsatz von künstlicher Intelligenz verstärkten diese Angriffe und stellten Unternehmen vor neue Herausforderungen. Gleichzeitig führte der anhaltende Fachkräftemangel zu einer verstärkten Automatisierung sicherheitskritischer Prozesse. Ein weiterer Fokus liegt auf der Absicherung von APIs, die zunehmend ins Visier von Cyberkriminellen geraten.

2025

Für 2025 zeichnet sich eine weitere Professionalisierung der Angreifer ab, die verstärkt auf KI-gestützte und automatisierte Angriffstechniken setzen. Volumetrische Angriffe in Rekordhöhe werden weiterhin für Schlagzeilen sorgen, gleichzeitig gewinnen Turboangriffe an Bedeutung – unauffällige, aber hochwirksame Angriffe, die traditionelle Abwehrmechanismen umgehen. Unternehmen müssen ihre IT-Sicherheitsstrategien ständig weiterentwickeln, um mit diesen Bedrohungen Schritt halten zu können. Der Schlüssel liegt in KI-gestützten Sicherheitssystemen, Observability und einer ganzheitlichen Cyberresilienz, um sich gegen immer raffiniertere Angriffe zu wappnen.

Ihr Ansprechpartner

Michael Scheffler
Vice President Sales

+49 69 58004926-306
m.scheffler@link11.com

Nachweise

[1] https://commercial.allianz.com/news-and-insights/reports/allianz-risk-barometer/de.html

[2] https://www.bitkom.org/Bitkom/Publikationen/Studie-Wirtschaftsschutz

[3] https://www.bitkom.org/Bitkom/Publikationen/Studie-Wirtschaftsschutz

[4] https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024

[5] https://www.spiegel.de/panorama/justiz/cyberattacke-auf-bundesbehoerden-bnd-internetseite-lahmgelegt-a-ba0b8f18-e20f-4cee-8a68-b84d7d327920 / https://www.it-journal.de/218414-hacker-legten-internetseite-des-bundes-nachrichtendienstes-lahm.html

[6] https://cybernews.com/cybercrime/holy-league-hacker-alliance-attack-nato/

[7] https://www.dcso.de/hacker-gruppe-will-kein-geld-sondern-propaganda/

[8] https://blog.sekoia.io/noname05716-ddosia-project-2024-updates-and-behavioural-shifts/

[9] https://cybernews.com/cybercrime/holy-league-hacker-alliance-attack-nato/

[10] https://thecyberexpress.com/holy-league-hacktivists-uniting-against-france/

[11] https://cybernews.com/news/noname-pro-russian-hackers-arrested-in-spain-group-vows-retaliation/

[12] https://www.seco.admin.ch/seco/en/home/seco/nsb-news.msg-id-99736.html

[13] https://news.err.ee/1609278921/ria-estonia-s-state-institutions-hit-by-largest-cyberattack-to-date

[14] https://thecyberexpress.com/tram-barcelona-cyberattack-noname/

[15] https://www.spf.org/iina/en/articles/osawa_04.html

[16] https://www.brusselstimes.com/belgium/1258228/pro-russia-cyberattack-targets-several-belgian-government-websites

[17] https://www.infosecurity-magazine.com/news/uk-council-sites-recover-russian/

[18] https://www.reuters.com/technology/cybersecurity/cyber-attack-italys-foreign-ministry-airports-claimed-by-pro-russian-hacker-2024-12-28/

[19] https://japannews.yomiuri.co.jp/politics/defense-security/20250204-236952/

[20] https://borncity.com/win/2025/02/02/will-the-eu-us-data-transfer-agreement-be-axed-by-donald-trump/

[21] https://krebsonsecurity.com/2025/01/mastercard-dns-error-went-unnoticed-for-years/ / https://www.golem.de/sonstiges/zustimmung/auswahl.html?from=https%3A%2F%2Fwww.golem.de%2Fnews%2Fmastercard-tippfehler-in-dns-eintrag-bleibt-jahrelang-unentdeckt-2501-192683.html

Hauptsitz

Link11
Lindleystr. 12
60314 Frankfurt