LINK11

EUROPEAN CYBER REPORT

2025 Mid Year

www.link11.com

Liebe Leserinnen und Leser,

DDoS-Angriffe sind schon lange kein Randphänomen mehr, sondern haben sich zu einer zentralen Bedrohung für Unternehmen, öffentliche Institutionen und ganze Infrastrukturen entwickelt. Die im Link11 European Cyber Report dokumentierten Zahlen und Beispiele verdeutlichen die Dimension: Angriffe im Terabit-Bereich, Paketraten im dreistelligen Millionenbereich und zunehmend raffinierte Layer-7-Strategien, die sich kaum noch vom regulären Traffic unterscheiden.

Unsere Aufgabe als Sicherheitsanbieter besteht nicht nur darin, auf diese Entwicklungen zu reagieren, sondern ihnen einen Schritt voraus zu sein. Moderne Angreifer setzen auf Präzision, Täuschung und ökonomische Effizienz – wir setzen auf Automatisierung, künstliche Intelligenz und Erfahrung. Nur so können wir sicherstellen, dass digitale Geschäftsprozesse und kritische Dienste verfügbar bleiben, auch wenn die Angriffe weiter eskalieren.

Der European Cyber Report soll Orientierung bieten und gleichzeitig den Blick schärfen: für die Dynamik einer Bedrohung, die sich nicht mehr allein in Zahlen messen lässt, sondern in ihrer Fähigkeit, das Vertrauen in und die Stabilität von digitalen Systemen infrage zu stellen.

Mit Link11 an ihrer Seite können Unternehmen ihre digitale Widerstandskraft stärken und kritische Systeme nachhaltig schützen.

Ich wünsche Ihnen eine spannende Lektüre!

Herzliche Grüße
Jens-Philipp Jung, CEO, Link11

Inhalt

Executive Summary

Die Bedrohungslage durch Distributed-Denial-of-Service-Angriffe (DDoS) hat sich im ersten Halbjahr 2025 dramatisch verschärft. Im Link11-Netzwerk wurden 225 % mehr Attacken registriert als im Vorjahreszeitraum. Dabei zeigte sich nicht nur eine massive Zunahme der Quantität, sondern auch eine qualitative Weiterentwicklung der Angriffsmethoden.

„Die Dimensionen sind echt erschreckend. Im ersten Halbjahr 2025 wurden 438 Terabyte DDoS-Traffic bewegt. Das entspricht mehr als sieben Jahre ununterbrochenem Netflix-Streaming in 4K. Solche Vergleiche zeigen die Bedrohung besser als jede Statistik.“

Jens-Philipp Jung, CEO, Link11

Wichtigste Erkenntnisse

Starker Anstieg großvolumiger „ISP-Killer-Angriffe“

Die Backbone-Attacken nahmen um

143 %

zu und bedrohen die Infrastrukturen von Providern und Rechenzentren.

Angriffsdauer auf Rekordniveau

Die längste dokumentierte Attacke dauerte über

acht Tage,

oft in koordinierter Langzeitkampagne mit wechselnden Angriffsmethoden.

Explosives Datenvolumen

Das kumulierte Angriffsvolumen stieg von 110 TB auf

438 TB

– genug für sieben Jahre Netflix-Streaming in 4K.

Rekordwerte bei Bandbreite und Paketraten

Maximalwerte von

1,2 Tbit/s

und **207 Mio. Pakete pro Sekunde** überlasten selbst leistungsfähige Systeme.

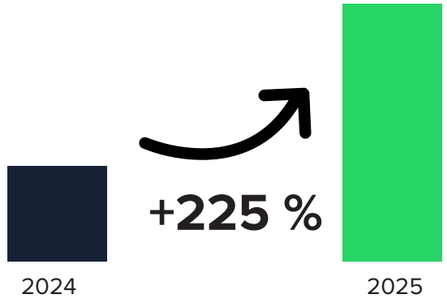
Neben diesen technischen Dimensionen nahmen politisch motivierte Angriffe weiter zu. Gruppen wie NoName057(16) griffen gezielt kritische Infrastrukturen in Europa an – häufig im zeitlichen Zusammenhang mit geopolitischen Ereignissen. Die Ergebnisse des „IBM X-Force 2025 Threat Intelligence Index”[1] bestätigen diese Entwicklung: Im Jahr 2024 richteten sich 70 % aller untersuchten Angriffe gegen kritische Infrastrukturen. Neben DDoS-Attacken bleibt die Ausnutzung von Schwachstellen ein zentrales Risiko, das durch veraltete Technologien und langsame Patch-Zyklen verstärkt wird. Diese Kombination erleichtert es Angreifern, bekannte Exploits und Botnetze aus dem Dark Web zu nutzen.

Doch die Gefährdungslage geht weit über technische Faktoren hinaus. Laut dem „Global Digital Trust Insights 2025“[2] von PwC verfügen lediglich 2 % der Unternehmen über eine unternehmensweite Cyber-Resilienz, obwohl die durchschnittlichen Kosten eines Datenvorfalls bei über 3,3 Millionen US-Dollar liegen. Zwar stufen zwei Drittel der Technologieverantwortlichen Cybersicherheit als zentrales Risiko ein, doch die operative Vorbereitung bleibt oft unzureichend.

Die Akteure agieren zunehmend arbeitsteilig, nutzen künstliche Intelligenz und bieten im Rahmen von „Crime-as-a-Service“-Modellen Cyberangriffe an. In seinem „Global Cybersecurity Outlook 2025“[3] hebt das World Economic Forum (WEF) die steigende Komplexität und Automatisierung solcher Angriffsplattformen als zentralen Treiber hervor. Die Bedrohungslandschaft ist damit so professionell, vernetzt und dynamisch wie nie zuvor. Dies erfordert von Unternehmen und Institutionen einen konsequenten Ausbau ihrer Abwehr- und Resilienzstrategien.

Massive Zunahme der DDoS-Angriffe

Bereits im Jahr 2024 hat sich die DDoS-Bedrohungslage deutlich verschärft. Diese Entwicklung setzte sich im ersten Halbjahr 2025 fort. Im Vergleich zum ersten Halbjahr 2024 stieg die Anzahl der im Link11-Netzwerk registrierten Angriffe um 225 %.



Der Anstieg von DDoS-Angriffen im ersten Halbjahr 2025 resultiert aus mehreren Faktoren. Globale Spannungen führen zu einer Zunahme politisch motivierter Angriffe im Zusammenhang mit internationalen Konflikten oder Wahlen. Der „Global Risks Report 2025"[4] des World Economic Forums stuft geopolitisch motivierte Angriffe, bewaffnete Konflikte und politische Instabilität als unmittelbar bedrohlich ein. Er hebt außerdem hervor, dass Cyberangriffe, die oft durch geopolitische Konflikte getrieben werden, zu den bedeutendsten kurz- und mittelfristigen Risiken zählen.

Eine große Rolle spielt darüber hinaus auch die technologische Weiterentwicklung, insbesondere im Bereich KI. Botnetze werden immer effizienter gemanagt und modular eingesetzt. Mithilfe von KI werden Angriffstechniken verbessert oder Angriffe besser getarnt.

Angreifer setzen Machine Learning und KI ein, um Schwachstellen schneller zu erkennen und auszunutzen. Außerdem können die kompromittierten Geräte und Botnetze automatisiert und zielgenau gesteuert werden. Zudem nimmt weltweit die Anzahl ungeschützter und verwundbarer IoT-Geräte zu. IoT- und Smart-Home-Geräte werden so zu einem riesigen Reservoir für Botnetze. Zwar gab es internationale Ermittlungserfolge, bei denen sogenannte DDoS-Stresser-Services[5] ausgeschaltet wurden, doch es gibt nach wie vor genügend „DDoS-as-a-Service"-Plattformen.

Daneben werden auch die DDoS-Angriffstechniken selbst immer weiterentwickelt. Insgesamt wird deutlich, dass die Professionalisierung und Kommerzialisierung der Cybercrime-Szene weiter zunehmen. Diese Entwicklung wird durch verschiedene Faktoren verstärkt, die DDoS zu einer ernstzunehmenden aktuellen Bedrohung für Wirtschaft, Verwaltung und Gesellschaft machen.

Diese Zunahme wurde maßgeblich von zwei gegenläufigen Trends getrieben:

1

Mehr große Angriffe
mit höheren
Spitzenwerten
(Peak-Bandbreite)

2

Anstieg kleinerer
DDoS-Attacken
im Vergleich zum
Vorjahreszeitraum.

Politischer Hacktivismus in Deutschland

Das erste Halbjahr 2025 war geprägt von einer Vielzahl politisch motivierter Angriffe auf deutsche Ziele. Vor allem die prorussische Gruppe NoName057(16) führte wiederholte, teils mehrwöchige Angriffswellen durch. Aber auch andere Akteure wie Mr. Hamza, Dark Storm oder Keymous wurden zunehmend aktiver.

Häufig erfolgte die Auswahl der Ziele in direktem Zusammenhang mit geopolitischen Ereignissen. Dadurch rückten kritische Sektoren wie die Energieversorgung, die Industrie, das Finanzwesen, kommunale Dienste sowie Regierungs- und Behördensysteme verstärkt in den Fokus. Trotz einzelner Maßnahmen gegen die Angriffsinfrastruktur wie z.B. die Abschaltung von DDoS-Stresser-Services hat sich die Angriffsdynamik kaum abgeschwächt.

Daneben zeigt sich eine deutliche Professionalisierung. Die Kampagnen kombinierten eine breite Zielvielfalt mit regelmäßigen Schwerpunktwechseln. Zudem wiederholten sich viele Attacken gegen bereits bekannte Ziele, was auf persistente Angriffslisten und unzureichende Härtung auf Seiten der betroffenen Organisationen hindeutet.

Das Timing war oft strategisch gewählt. Die Angriffe starteten häufig außerhalb der Kernbetriebszeiten. Einerseits um unmittelbare Auswirkungen zu begrenzen und andererseits den Aufwand für Incident Response und Monitoring zu erhöhen. Erfolgsquoten von 40 bis 50 Prozent zeigen, dass zahlreiche Systeme noch immer verwundbar sind.

Dabei dienten politische Ereignisse und internationale Entscheidungen als Auslöser, wodurch sich die Angriffsdynamik in Teilen vorhersagen ließ. Im Fokus standen die Sektoren Energie, Industrie, Finanzwesen und kommunale Dienste sowie klassische Regierungs- und Behördensysteme.

Es wurde auch klar, dass die Kapazitäten der Angreifer zugenommen haben. Inzwischen werden von unterschiedlichen DDoS-Schutzprovidern Angriffe mit Spitzenwerten im Terabit-Bereich dokumentiert. Zudem verteilt sich die Aktivität zunehmend auf mehrere Gruppen, die unterschiedliche Taktiken und Tools einsetzen.

Neben einer breiteren Monitoring-Strategie sollten Unternehmen deshalb eine zuverlässige und effiziente DDoS-Mitigation auch im Terabit-Bereich implementieren. Die wiederholten Attacken auf dieselben Ziele unterstreichen zudem die Notwendigkeit, nach Vorfällen schnell und konsequent Sicherheitslücken zu schließen.

Hohe Frequenz und Zielvielfalt:
Mehrere groß angelegte Wellen von Januar bis Mai mit teils über 100 angegriffenen Domains pro Kampagne. Kombination von bekannten und neu identifizierten Schwachpunkten.

Taktische Anpassungsfähigkeit:
Schwerpunktwechsel (z. B. von Behörden zu ÖPNV oder Finanzinstituten) erschweren die Verteidigungsplanung. Wiederholte Attacken auf Ziele, die schon kompromittiert wurden, belegen den Einsatz persistenter Angriffslisten.

Geopolitische Trigger:
Politische Ereignisse, darunter die Münchner Sicherheitskonferenz im Februar und die deutsche Ankündigung weiterer Iris-T-Lieferungen an die Ukraine im April, lösten die Angriffe aus.

Steigende Angriffsleistung:
Mehrere Provider berichten von Spitzenwerten im Terabit-Bereich.

Fragmentierung der Angreiferlandschaft:
Die Dominanz von NoName057(16) hat nachgelassen. Es gab mehrere Gruppen mit unterschiedlichen Tools und Vorgehensweisen, was die Abwehr komplexer macht.

Wenn Internet Service Provider ins Wanken geraten

Neben besonders großvolumigen DDoS-Attacken im Terabit-Bereich haben auch Angriffe auf die Infrastruktur im Link11-Netzwerk zugenommen. Solche **Infrastruktur- oder Backbone-Angriffe** verfolgen ein ehrgeiziges Ziel: Sie setzen darauf, die Internet-Uplink-Kapazität eines gesamten Internet Service Providers (ISP) oder Rechenzentrums zu überlasten. Bei einer Backbone-Anbindung von 100 Gbit/s benötigt ein solcher Angriff rund 85 Gbit/s, um den Link nahezu vollständig auszulasten.

Entsprechend groß sind die Datenströme und die Auswirkungen: Anders als bei gezielten **Website-Attacken** können ganze Kundennetze oder Dienste gleichzeitig betroffen sein. In der Regel handelt es sich um hochvolumige, verteilte DDoS-Kampagnen.

Die Anzahl dieser Angriffe hat im Vergleich zum ersten Halbjahr 2024 deutlich zugenommen. Mehr als doppelt so viele DDoS-Attacken (143 %) hatten eine kritische Größe, um Backbone-Anbindungen lahmzulegen. Dieser Trend ist kritisch, da die Schäden großflächiger ausfallen und sowohl für Anbieter als auch für deren Kunden deutlich kostspieliger sind.

Trotz der allgemeinen Zunahme von DDoS-Angriffen ist die Häufigkeit gezielter Website-Angriffe weitgehend konstant geblieben. Im Gegensatz zu Angriffen, die die Dienste eines ISPs lahmlegen, zielen sie darauf ab, eine einzelne Website oder einen einzelnen Server offline zu nehmen.

Technisch genügt dabei oft schon ein moderater Datenstrom: So kann ein Angriff von rund 850 Mbit/s einen Server mit einer Anbindung von 1 Gbit/s nahezu vollständig auslasten. Die Auslastung beträgt dann 85 %, was zu einer massiven Verlangsamung oder sogar einem kompletten Ausfall des Dienstes führt.

Charakteristisch für diese Angriffe sind die vergleichsweise kleinen Datenströme im Gegensatz zu Backbone-Angriffen. Sie werden häufig gezielt gegen bestimmte Unternehmen oder Online-Dienste eingesetzt und führen unmittelbar dazu, dass der betroffene Service für Nutzer nicht erreichbar ist.

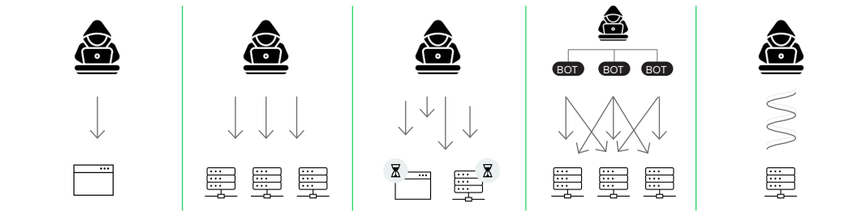
Eine weitere Kategorie, die zunehmend an Bedeutung gewinnt, sind die sogenannten **„Nuisance Attacks“**. Dabei handelt es sich um eine Form von DDoS-Angriffen, deren Ziel nicht die vollständige Abschaltung eines Dienstes, sondern die gezielte Störung von Performance und Verfügbarkeit ist. Typischerweise bewegen sich diese Angriffe im niedrigen Bandbreitenbereich – oft unter 1 Gbit/s – und bleiben damit unterhalb vieler automatischer Abwehrschwellen.

Dennoch verursachen sie spürbare Effekte wie erhöhte Latenzzeiten, Paketverluste oder instabile Verbindungen. Angreifer setzen sie aus unterschiedlichen Motiven ein: Als kostengünstige Schikane, um den Betrieb zu erschweren und Ausfallkosten zu verursachen oder als Ablenkung während anderer Angriffe oder um die Verteidigungsmechanismen eines Ziels zu erkunden. Die Verbreitung solcher Attacken wird durch leicht zugängliche „DDoS-for-Hire“-Dienste begünstigt. Dies hat in den vergangenen Monaten zu einer signifikanten Zunahme dieser Störattacken geführt.

Diese Übergriffe fallen weder in die Kategorie „Website-Killer“ noch in die Kategorie „ISP-Killer“. Sie haben jedoch das Potenzial, gezielt Kosten zu erzeugen und die Performance von Diensten zu beeinträchtigen. Sie verdeutlichen, dass Angreifer ihre Methoden diversifizieren, um unterschiedliche Ziele zu erreichen – von der unmittelbaren Lahmlegung einzelner Dienste bis zu subtilen wirtschaftlichen Störungen.

Zusammenfassend lässt sich sagen: Während Website-Killer-Angriffe weiterhin eine konstante Bedrohung darstellen, ist der signifikante Anstieg der ISP-Killer-Angriffe ein ernstzunehmender Trend. Er belastet die Infrastruktur von Providern stärker und stellt Sicherheitsverantwortliche vor neue Herausforderungen.

Vielfältige Angriffstypen: Vom Website-Killer zum Jo-Jo-Angriff



Kriterium	Website-Killer	ISP-Killer	Nuisance Attack	Carpet-Bombing	Jo-Jo-Angriff
Primäres Ziel	Einzelne Website oder einzelner Server	Uplink-Kapazität eines gesamten ISPs oder Rechenzentrums	Performance-Störung ohne vollständigen Ausfall	Breite Störung ganzer Subnetze oder IP-Bereiche	Cloud-Infrastruktur mit Auto-Scaling-Funktion
Technische Schwelle	85 % Auslastung, d.h. ca. 850 Mbit/s (bei 1 Gbit/s Anbindung)	85 % Auslastung, d.h ca. 85 Gbit/s (bei 100 Gbit/s Backbone)	Ab 50 Mbit/s bis 1 Gbit/s, unter Abwehrschwellen	Abhängig vom Zielnetz, oft mittlere bis hohe Gesamtvolumina	Bereits mittlere Lastspitzen reichen, wenn Auto-Scaling ausgelöst wird
Angriffsvolumen	Mittel	Sehr hoch	Niedrig	Mittel bis hoch (verteilt)	Variabel, oft in Wellen mit wechselnder Intensität
Typische Wirkung	Zielseite nicht erreichbar	Großflächiger Ausfall vieler Dienste/Kunden	Spürbare Latenz, Paketverlust, Zusatzkosten	Überlastung von Firewalls, Routern und Upstream-Links	Instabilität durch permanentes Hoch- und Runterskalieren, Kostenexplosion
Merkmale	Gezielter Angriff, relativ geringer Datenstrom	Hochvolumige, verteilte Kampagnen	Häufige Mini-Angriffe, oft automatisiert	Verteilter Traffic auf viele Ziele, schwerer zu filtern	Wechsel zwischen Traffic-Bursts und Ruhephasen, nutzt Cloud-Auto-Scaling aus

Jo-Jo-DDoS-Angriff

Definition:
Jo-Jo-DDoS-Angriffe[6] sind eine neue Form von Layer-7-Angriffen, die die Auto-Scaling-Funktionen von Cloud-Infrastrukturen gezielt ausnutzen. Im Gegensatz zu klassischen DDoS-Attacken geht es nicht nur darum, Systeme mit Traffic zu überfluten, sondern vielmehr, sie durch wiederholte Schwankungen zwischen Lastspitzen und Ruhephasen in einen instabilen und kostenintensiven Zustand zu versetzen.

Funktionsweise:
Die Angreifer erzeugen zunächst einen plötzlichen Anstieg von Anfragen, wodurch die Cloud-Infrastruktur gezwungen wird, zusätzliche Ressourcen wie Rechenleistung oder Bandbreite bereitzustellen. Sobald diese Ressourcen aktiv sind, wird der Traffic abrupt reduziert, sodass die Kapazitäten wieder zurückgefahren werden. Kurz darauf beginnt die nächste Angriffswelle, was einen permanenten Zyklus des Hoch- und Runterskalierens auslöst, den namensgebenden „Jo-Jo-Effekt“.

Auswirkungen:
Für die betroffenen Unternehmen bedeutet dies nicht nur deutlich höhere Cloud-Kosten, sondern auch spürbare Leistungseinbußen und eine potenzielle Instabilität der bereitgestellten Dienste. Durch die wiederholten „Lastwechsel“ entstehen Latenzen und Unterbrechungen. Zudem kommt es zu einem unnötigen Verschleiß der Ressourcen, wodurch die Verfügbarkeit geschäftskritischer Anwendungen gefährdet werden kann.

Prävention:
Um Jo-Jo-Angriffe abzuwehren, sind gezielte Schutzmaßnahmen erforderlich. Dazu zählen unter anderem Rate Limiting und Throttling, um künstliche Lastspitzen abzufangen, adaptive Auto-Scaling-Strategien mit Cooldown-Phasen, die ein ständiges Hoch- und Runterfahren vermeiden, sowie KI-gestützte Anomalieerkennung, die ungewöhnliche Traffic-Muster frühzeitig identifiziert. Auch intelligente Load-Balancing-Verfahren und ein engmaschiges Kostenmonitoring können dabei helfen, die Risiken zu reduzieren.

1

Infektionsphase

Zunächst wird Malware verbreitet, um verschiedene Geräte wie Computer, IoT-Geräte und Server zu infizieren.

2

Angriffsinitiierung

Die infizierten Geräte bilden ein Botnetz, das das Ziel mit massivem Datenverkehr überflutet.

3

Skalierung

Um mit dem Angriff fertigzuwerden, werden zusätzliche Cloud-Ressourcen bereitgestellt.

4

Wiederholung des Angriffs

Die Angriffe erfolgen in Wellen, wodurch die Ressourcen wiederholt stark belastet werden.

5

Auswirkungen und Wiederherstellung

Der Angriff führt zu finanziellen Belastungen, Betriebsunterbrechungen, Reputationsschäden und erfordert umfassende Wiederherstellungsmaßnahmen.

Mehr Volumen, mehr Pakete, längere Dauer – von Blitzangriffen zu Dauerfeuer

Neben der reinen Anzahl der Attacken haben sich auch die Angriffsmuster verändert: Während das erste Halbjahr 2024 noch von „Turboangriffen“ geprägt war, dominierten im ersten Halbjahr 2025 bereits länger andauernde Kampagnen mit komplexeren Vektorwechseln und einer koordinierteren Vorgehensweise. Die Verdreifachung der Angriffszahlen ging mit einem deutlichen Wachstum des Angriffsvolumens einher.

So lag das summierte Angriffsvolumen in Terabyte (TB) in den ersten Monaten des Jahres 2025 bei rund **438 TB**, im Vergleichszeitraum des Jahres 2024 hingegen bei 110 TB.

4K-Streaming
438 TB entsprechen **mehr als sieben Jahren ununterbrochenem Netflix-Streaming** in 4K-Auflösung. Selbst wenn man Tag und Nacht streamt, würde man in dieser Zeit Tausende Serien und Filme sehen, ohne auch nur einmal das Puffern zu erleben.

Hörbücher
Genug Daten für **mehr als 1.700 Jahre ununterbrochene Hörbuchwiedergabe**. Damit könnte man die gesamte Weltliteratur hören und hätte immer noch genügend Speicher für einige Nachschlagewerke übrig.

MP3-Songs
In dieses Datenvolumen passen rund **93 Millionen Songs**. Das reicht aus, **um über 500 Jahre lang rund um die Uhr Musik zu hören**, ohne einen Titel zweimal zu spielen.

64-GB-Geräte
Das entspricht dem Speicher von **6.800 voll belegten Smartphones mit jeweils 64 GB**. Diese füllen eine ganze Lagerhalle, und jedes einzelne Handy ist bis zum Rand mit Daten gefüllt.

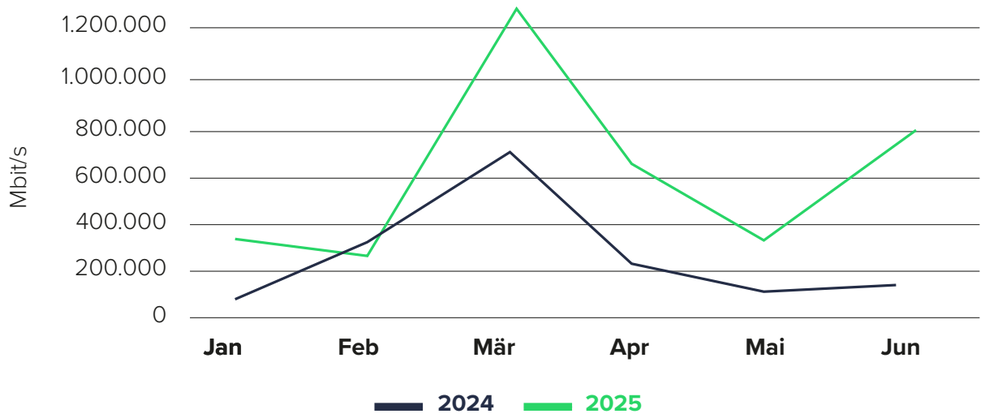
„Wir sehen nicht mehr nur rohe Gewalt in Form von Bandbreite, sondern hochpräzise Layer-7-Angriffe. 20.000 täuschend echte Requests pro Minute können gefährlicher sein als 200 Millionen Pakete pro Sekunde, wenn sie unsichtbar im legitimen Traffic untergehen.“

Jag Bains, VP Solution Engineering, Link11

DDoS im XXL-Format

Die Größenverteilung der im Link11-Netzwerk abgewehrten Angriffe zeigt ein differenziertes Bild: Während die Bandbreiten-Spitzenwerte deutlich zugenommen haben und mehr großvolumige Angriffe registriert wurden, ist die durchschnittliche Bandbreite insgesamt gesunken. Die Vielzahl kleinerer Attacken zieht den Mittelwert nach unten. Im ersten Halbjahr 2025 hat sich der Trend, dass sowohl die Anzahl als auch die Spitzenlasten kontinuierlich gestiegen sind, weiter verfestigt. Die größte DDoS-Attacke zwischen Januar und Juli 2025 erreichte eine maximale Bandbreite von über 1,2 Tbit/s. Der größte Angriff im ersten Halbjahr 2024 war mit 694 Gbit/s im Vergleich dazu „nur“ halb so groß.

Maximale Bandbreite in Mbit/s



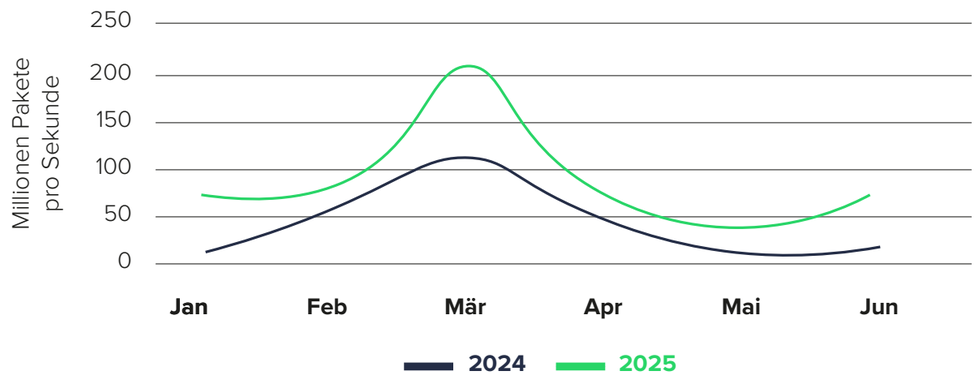
Parallel zur Zunahme der maximalen Bandbreite ist im ersten Halbjahr 2025 auch die maximale Anzahl übertragener Pakete pro Sekunde gestiegen. Der höchste Wert lag bei 207.090.400 Paketen pro Sekunde.

Ein DDoS-Angriffsvolumen von 207 Millionen Paketen pro Sekunde ist sehr hoch und überfordert selbst leistungsstarke Unternehmensserver oder Firewalls. Solche Werte führen zu massiver Netzwerküberlastung, Paketverlusten und potenziellen Totalausfällen von Diensten. Sie treten typischerweise nur bei groß angelegten Botnet-Attacken oder ISP-Level-Kampagnen auf. Um solche Werte zu erzeugen, greifen Angreifer in der Regel auf große Botnetze zurück, die gleichzeitig viele kleine Pakete senden (z. B. SYN-Floods, UDP-Floods).

„207 Millionen Pakete pro Sekunde sind nicht nur ein hoher Wert, sondern können auch Firewalls, Server und ganze Netze binnen Sekunden lahmlegen. Im Angriffsfall ist Geschwindigkeit entscheidend.“

Karsten Desler, CTO, Link11

Maximale Anzahl Pakete pro Sekunde



Marathon statt Sprint

Anders als bei den Turboangriffen, die wir im Link11-Netzwerk in den ersten Monaten des Jahres 2024 beobachtet haben, setzten die Angreifer im ersten Halbjahr 2025 verstärkt auf längere und koordinierte Kampagnen. Diese langandauernden Angriffe sind eher in der Lage, Verteidigungssysteme zu überlasten und nachhaltigen Schaden zu verursachen.

Der längste dokumentierte Angriff in der ersten Jahreshälfte 2025 dauerte 12.388 Minuten, also rund acht Tage und 14 Stunden. Im Vorjahreszeitraum dauerte die längste DDoS-Attacke dagegen nur 1.523 Minuten, also etwa einen Tag und eine Stunde.

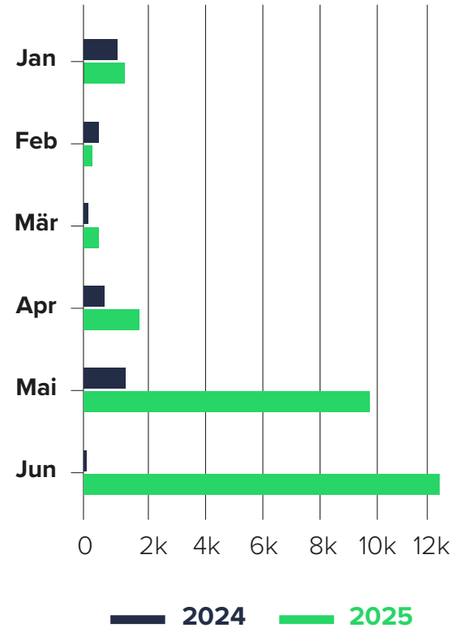
Die Grafik veranschaulicht die Variation der Angriffsdauer während der einzelnen Monate sowie die unterschiedlichen Niveaus. Der größte Unterschied zeigt sich in den Zahlen für den Juni. Während der längste Angriff im Juni 2025 gemessen wurde, lag die maximale Angriffsdauer im Juni 2024 bei nur 73 Minuten.

Der Anstieg der Angriffsdauer ist auch ein Hinweis auf die variierenden Taktiken der Angreifer. Die Verlängerung der Angriffe wird durch mehrere Faktoren begünstigt: komplexere Vektorwechsel, der Einsatz automatisierter Botnetze und KI-gestützter Tools, verschlüsselte Angriffsvektoren sowie die zeitliche Abstimmung auf geopolitische Ereignisse.

Auch politisch motivierte Gruppen wie NoName057(16) führten vermehrt koordinierte, langanhaltende DDoS-Kampagnen durch, die gezielt Regierungsstellen, den öffentlichen Sektor sowie Finanz- und Gesundheitsinstitutionen attackierten.

Insgesamt zeigen die Zahlen, dass Sicherheitsverantwortliche nicht nur die Skalierbarkeit, sondern auch die Ausdauer ihrer Abwehrsysteme erhöhen müssen, um der steigenden Anzahl, Komplexität und Dauer der Angriffe wirksam zu begegnen.

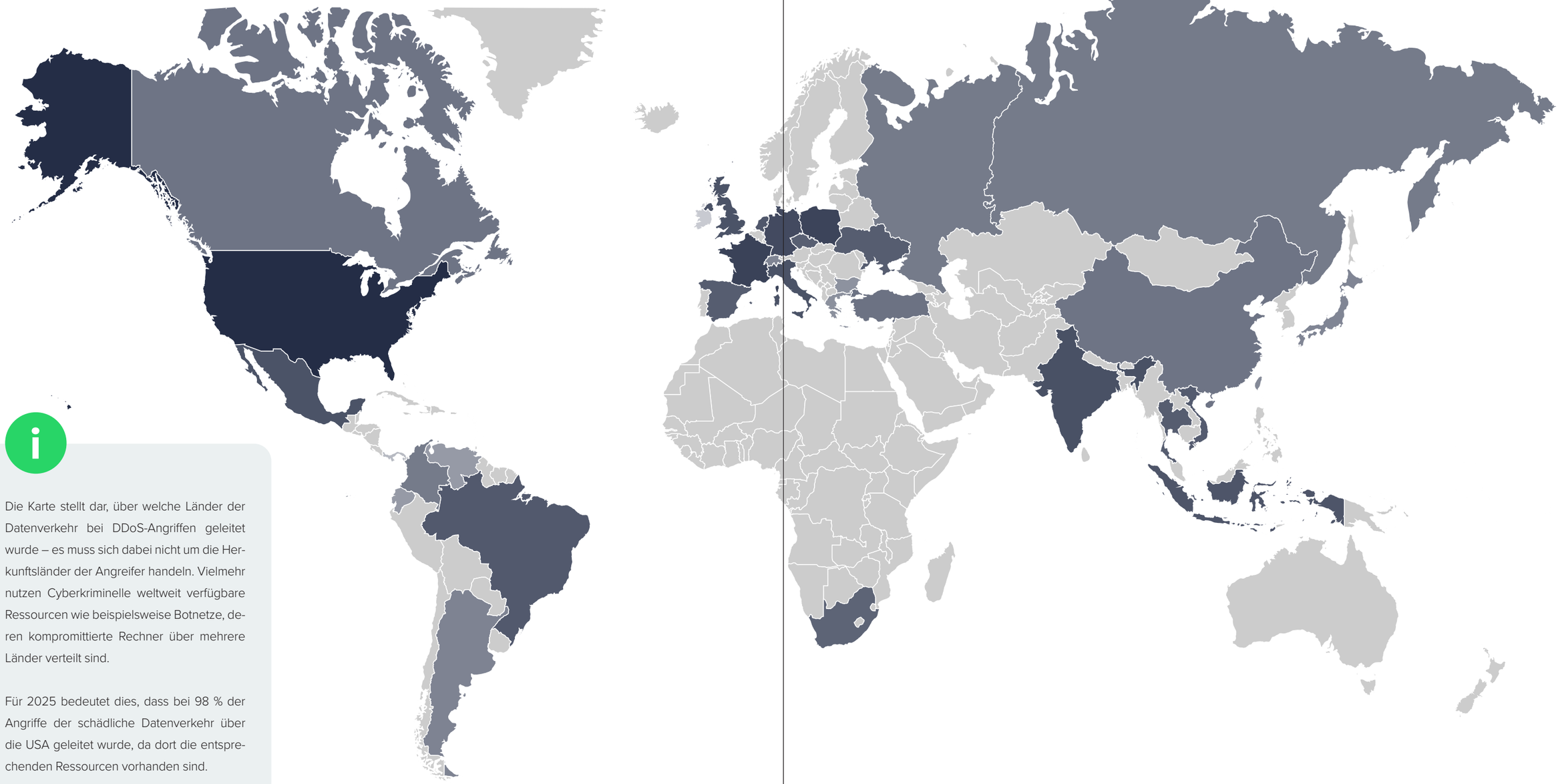
Dauer der längsten DDoS-Attacke pro Monat in Minuten



Herkunft des DDoS-Traffics

Globale Verteilung der Angriffsinfrastruktur 2025

98 % **31 %**



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 2025 bedeutet dies, dass bei 98 % der Angriffe der schädliche Datenverkehr über die USA geleitet wurde, da dort die entsprechenden Ressourcen vorhanden sind.

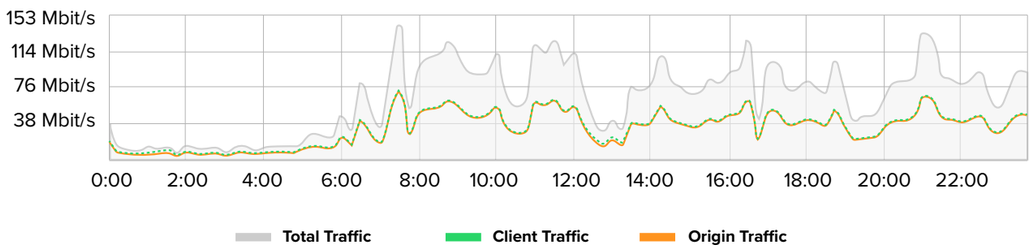
Web Protection

Die Web-DDoS-Angriffe im ersten Halbjahr 2025 im Link11-Netzwerk zeichneten sich durch eine hohe Intensität und eine klare Fokussierung auf Webapplikationen und APIs aus. Sie zielten auf kritische Webservices und Schnittstellen ab, insbesondere auf diejenigen von E-Commerce-, Gaming-, Finanz- und Medienunternehmen. APIs sind zunehmend das Hauptziel, da sie Geschäftsprozesse und sensible Daten steuern. Dadurch sind digitalisierte Geschäftsmodelle so bedroht wie nie zuvor – Schutzkonzepte müssen dringend die neuen Dimensionen und Angriffstaktiken berücksichtigen.

Präzision statt roher Gewalt

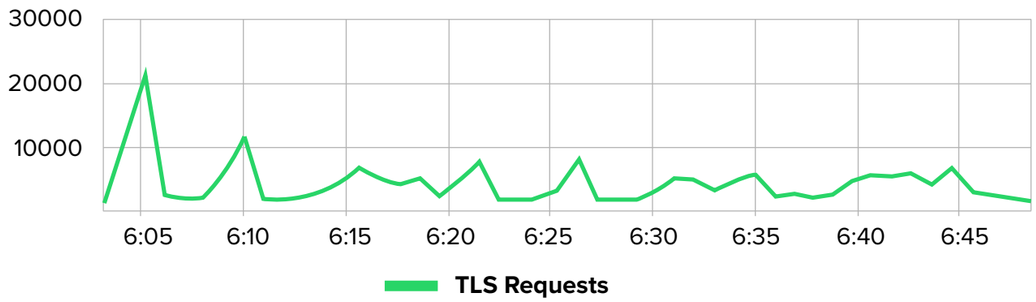
Ende April 2025 kam es im Zuge geopolitischer Spannungen in Deutschland zu einer Reihe unter anderem durch die prorussische Hackergruppe NoName057(16) zu einer Reihe gezielter Cyberangriffe. Binnen weniger Tage waren Websites von Landesbanken, Industrieunternehmen und Stadtverwaltungen wie berlin.de oder stuttgart.de stunden- bis tagelang nicht erreichbar. Während viele dieser Attacken auf hohe Datenmengen setzten, stach ein im Link11 abgewehrter Layer-7-DDoS-Angriff durch seine Raffinesse hervor: Er erzeugte keinen massiven Traffic, sondern zielte präzise auf die Anwendungsebene ab. Dazu nutzte er legitime HTTP-Anfragen, die die Backend-Ressourcen beanspruchten.

Maximale Bandbreite



Um ihre Attacken zu verschleiern, nutzten die Angreifer gezielt die Infrastruktur bekannter Hosting-Provider, die auch VPNs und CDNs dienten. Durch Geo-IP-Täuschungen und die Nutzung edge-basierter Knoten schienen die Anfragen aus Deutschland zu kommen, obwohl sie global verteilt waren. Mit etwa 20.000 Requests pro Minute blieb der Angriff für große Systeme unkritisch, er konnte jedoch an sensiblen Stellen wirksam stören. Moderne Schutzlösungen erkannten und blockierten ihn vor allem aufgrund von Unstimmigkeiten in HTTP-Headern, fehlenden Cookies, JavaScript-Challenges und unvollständigen menschlichen Interaktionsmustern.

Requests pro Minute



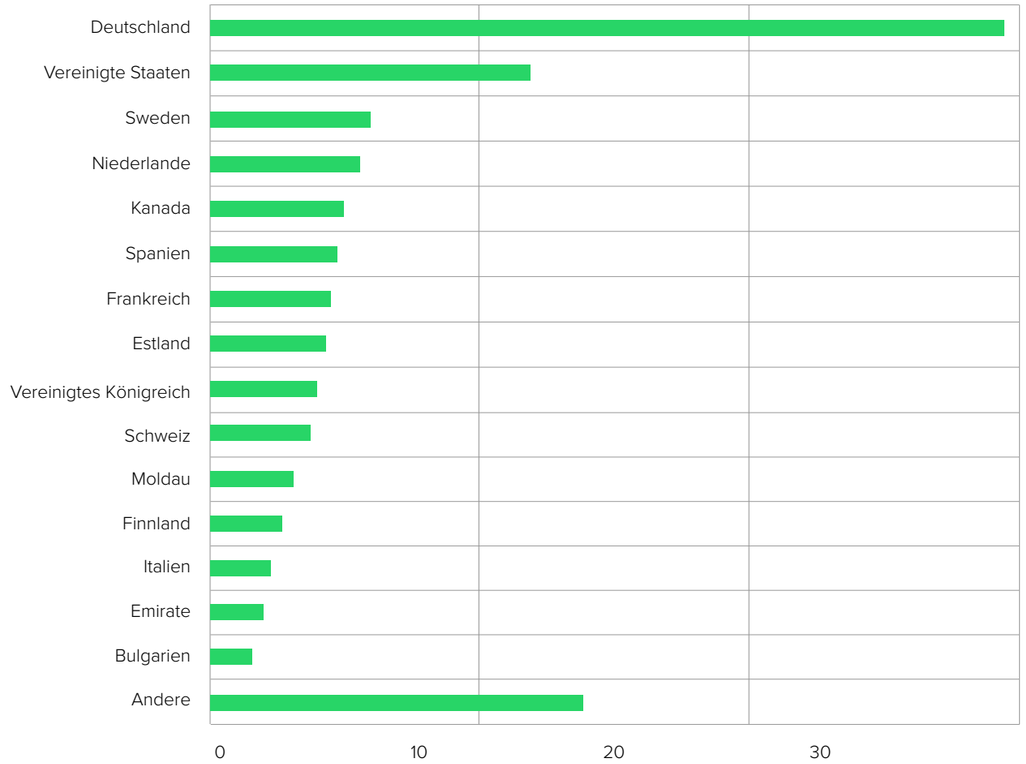
Besonders auffällig war die ökonomische Effizienz: Niedrige Einstiegskosten für VPNs, Testserver oder Mikrojobs ermöglichten es, mit minimalem Aufwand gezielte Störungen durchzuführen. Der Angriff verdeutlichte, dass Layer-7-DDoS-Angriffe nicht auf rohe Gewalt, sondern auf Präzision, Tarnung und Organisation setzen.

Für Unternehmen bedeutet dies, dass klassische volumetrische Schutzmaßnahmen allein nicht ausreichen – intelligente, automatisierte Web-Protection-Lösungen sind unerlässlich, um solche subtilen, aber potenziell wirkungsvollen Attacken abzuwehren.

„Die Angreifer tarnen sich geschickt über VPNs, CDNs und Geo-IP-Verschleierung. Dadurch sieht es plötzlich so aus, als kämen die Anfragen aus der Nachbarschaft, während das System gleichzeitig aus Vietnam, Russland oder den USA bombardiert wird.“

Sean Power, Solution Engineer, Link11

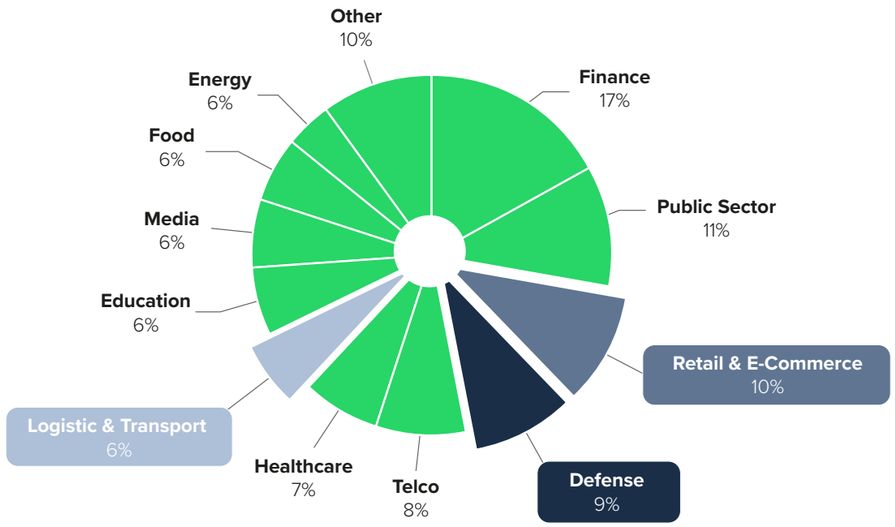
Herkunft des DDoS-Traffics



Neue Zielscheiben im Visier

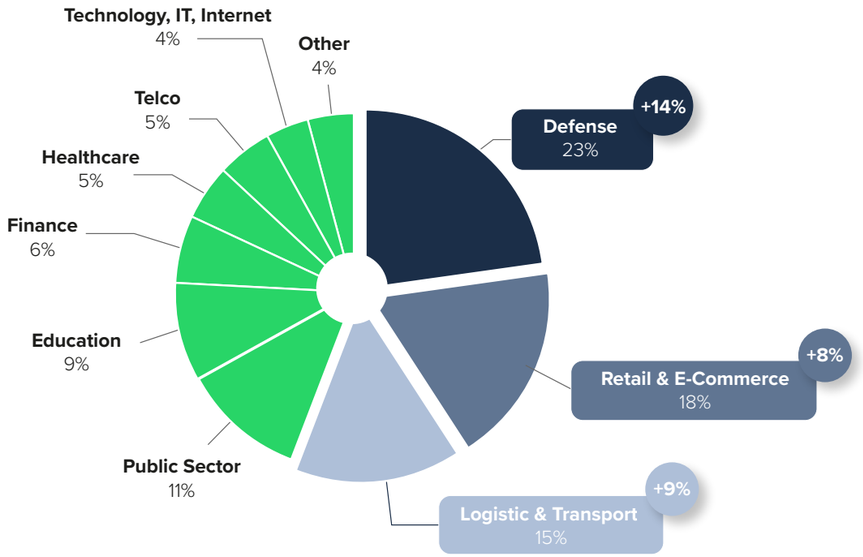
Die Analyse der abgewehrten Cyberangriffe im Bereich Web Application und API Protection (WAAP) zeigt zwischen dem ersten Halbjahr 2024 und dem ersten Halbjahr 2025 einige Verschiebungen innerhalb der betroffenen Sektoren: Finanzwesen, Öffentlicher Sektor sowie Retail, Retail & E-Commerce auf den Spitzenplätzen. Dicht gefolgt vom Verteidigungssektor, der Telekommunikationsbranche und dem Gesundheitswesen.

1. Halbjahr **2024**



Im ersten Halbjahr 2025 haben sich die Angriffsziele verlagert: Vor allem die Angriffe auf den Verteidigungssektor, den Retail- und E-Commerce-Bereich sowie den Logistik- und Transportsektor stiegen an. Die Angreifer suchen zunehmend nach Sektoren, die potenziell großen Einfluss auf Logistik, digitale Dienstleistungen und den kritischen Informationsaustausch haben. Dies könnte auch auf aktuelle geopolitische Ereignisse oder wirtschaftliche Entwicklungen zurückzuführen sein.

1. Halbjahr **2025**



Fazit

Die Analyse der Angriffe im ersten Halbjahr 2025 zeigt deutlich, dass sich die Bedrohungslage im Bereich der DDoS-Attacken weiter verschärft und zugleich diversifiziert hat. Während die Anzahl und Intensität der Angriffe zugenommen haben, ist auch eine Verschiebung der Angriffsarten zu beobachten. Neben den klassischen „Website-Killern" und den hochvolumigen „ISP-Killern" treten zunehmend die raffinierten Layer-7-Angriffe auf. Diese setzen nicht auf rohe Datenmengen, sondern auf Präzision und Verschleierung. Dies macht deutlich, dass Cyberkriminelle ihre Taktiken anpassen und gezielt Schwachstellen in unterschiedlichen Schichten des Netzwerks ausnutzen.

Die geopolitischen Spannungen, insbesondere im Kontext des Ukraine-Kriegs, waren der zentrale Auslöser vieler Angriffswellen. Prorussische Gruppen wie „NoName057(16)" nutzten politische Debatten – etwa die Diskussion um Taurus-Lieferungen – um durch spektakuläre Attacken auf staatliche Institutionen, Banken und Industrieunternehmen Aufmerksamkeit zu erlangen. Neben diesen geopolitisch motivierten Angriffen gehören zudem ökonomisch motivierte „Nuisance Attacks" und hochgradig automatisierte Botnet-Operationen zum aktuellen Angriffsarsenal. Dies ist ein Hinweis auf die zunehmende Professionalisierung und Arbeitsteilung in der Bedrohungslandschaft.

Auffällig sind zudem die enorme Bandbreite und Paketrate mancher Angriffe. Diese reichen von Terabit-Traffic bis hin zu über 200 Millionen Paketen pro Sekunde. Solche Dimensionen verdeutlichen das potenzielle Ausmaß der Auswirkungen auf Unternehmen, Institutionen und ganze Infrastrukturen. Gleichzeitig zeigen präzisere Layer-7-Attacken, dass neben der Größe auch Tarnung und Täuschung ein Risiko darstellen. Unternehmen müssen auf hochkomplexe Angriffe dieser Art vorbereitet sein. Entscheidend sind Notfallpläne, Echtzeit-Monitoring und KI-gestützte Abwehrsysteme, um verdächtigen Traffic frühzeitig zu erkennen und automatisiert zu blockieren. Nur durch schnelle Reaktionsmechanismen und eine kontinuierliche Anpassung der Sicherheitsstrategie lassen sich die Folgen solcher massiven Angriffe begrenzen.

Erfolgreicher DDoS-Schutz erfordert daher mehr als nur ein Management der Bandbreite: Nur durch den Einsatz intelligenter, automatisierter Schutzlösungen, kombiniert mit Notfallplänen und kontinuierlichem Monitoring, können Organisationen den zunehmend hybriden Bedrohungen begegnen.

Ihr Ansprechpartner

Michael Scheffler
Vice President Sales

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

Nachweise

1 X-Force 2025 Threat Intelligence Index | IBM

2 https://www.pwc.com/gx/en/news-room/press-releases/2024/pwc-2025-global-digital-trust-insights.html

3 https://www.weforum.org/publications/global-cybersecurity-outlook-2025/digest/

4 Global Risks Report 2025 | World Economic Forum

5 BKA - Meldungen - Operation „Power OFF": weltweiter Schlag gegen Cybercrime-Infrastruktur und

BKA - Meldungen - Strafverfolgungsbehörden schalten die zwei weltweit größten Cybercrime-Foren mit rund zehn Millionen registrierten Nutzern ab

6 Emerging Threat: Yo-Yo DDoS Attacks Targeting Cloud Environments | Blogs - Cyberware Hub

https://www.flaticon.com/de/kostenloses-icon/hacker_6463383?related_id=6463392&origin=search

Hauptsitz

Link11
Lindleystr. 12
60314 Frankfurt