LINK11

# EUROPEAN CYBER REPORT

## 2026 Mid Year

www.link11.com

## Liebe Leserinnen und Leser,

Cybersicherheit ist schon lange kein Nischenthema der IT-Abteilung mehr, sondern eine Frage der Unternehmensführung. Das zeigt auch das aktuelle „Allianz Risk Barometer 2026“: Zum fünften Mal in Folge stehen Cybervorfälle an der Spitze der weltweit wichtigsten Geschäftsrisiken – mit einem deutlichen Abstand zum zweiten Platz seit Beginn der Erhebung. Wer Cyberrisiken heute noch als Randthema behandelt, verkennt die Tatsache, dass sich die Bedrohungslage in den vergangenen Jahren erheblich gewandelt hat.

Ein zentraler Treiber dieses Wandels ist Künstliche Intelligenz. Sie verändert das Spielfeld auf beiden Seiten zugleich: Laut dem „Global Cybersecurity Outlook 2026“ des World Economic Forum erwarten 94 % der weltweit befragten Sicherheitsverantwortlichen, dass KI der wichtigste Einflussfaktor für die Cybersicherheit im laufenden Jahr sein wird.

KI senkt die Einstiegshürde für Angreifer, beschleunigt die Entwicklung neuer Schadsoftware und macht Angriffe präziser steuerbar. Gleichzeitig eröffnet sie Verteidigern neue Möglichkeiten, Bedrohungen schneller zu erkennen und automatisiert zu reagieren. Welche Seite am Ende die Nase vorn hat, entscheidet sich zunehmend an der Geschwindigkeit, mit der Unternehmen diese Technologie selbst nutzen.

Der vorliegende Report ordnet ein, wo diese Entwicklung aktuell steht, was dahintersteckt. Er zeigt, wo sich die Bedrohungslage konkret verschärft hat, welche Ursachen dahinterstecken und welche Schlüsse Unternehmen daraus für ihre eigene Resilienz ziehen können.

Ich wünsche Ihnen eine erkenntnisreiche Lektüre.



Herzliche Grüße
**Jens-Philipp Jung, CEO, Link11**

## Inhalt


Executive Summary 04

Network DDoS Protection 06

Bots, Botnetze und die Praxis moderner WAAP-Abwehr 12

Web Application & API Protection 14

Fazit 19

# Executive Summary

Die Bedrohungslage hat sich branchenübergreifend weiter verschärft. Dem aktuellen „Allianz Risk Barometer 2026“[1] zufolge sind Cybervorfälle erneut das weltweit wichtigste Geschäftsrisiko. Mit 42 % der Nennungen liegt dieses Risiko deutlich vor Platz 2, der von „Künstlicher Intelligenz“ mit 32 % belegt wird.

Auch für Unternehmen in Deutschland hat sich der Handlungsdruck entsprechend erhöht: Laut der PwC „Global Digital Trust Insights 2026”[2] sehen 92 % der deutschen Unternehmen die Notwendigkeit, ihre Cyberstrategie in den kommenden zwölf Monaten grundlegend anzupassen. Nicht zuletzt, weil die finanziellen Folgen zunehmen. Bei mehr als einem Drittel (37 %) der befragten deutschen Unternehmen lagen die Kosten des schwersten Datenvorfalls der vergangenen drei Jahre bei über einer Million US-Dollar – deutlich mehr als im globalen Durchschnitt (27 %).

Innerhalb dieser Bedrohungslage zeigt sich beim Thema DDoS ein eindrückliches Bild: Im ersten Halbjahr 2026 erreichten einzelne Angriffe im Link11-Netzwerk neue Rekordwerte bei Bandbreite, Paketrate und Datenvolumen. Damit hat sich die Wucht der Angriffe noch einmal dramatisch weiterentwickelt. Gleichzeitig ging die reine Anzahl der registrierten Angriffe um 42 % zurück. Dieser scheinbare Widerspruch lässt sich mit zwei parallelen Entwicklungen erklären:

**„Superbotnetze“ und kompromittierte Cloud-Ressourcen treiben die Rekorde**

Haupttreiber sind die IoT-Botnetze Aisuru und sein Nachfolger Kimwolf, ein Netzwerk aus Millionen kompromittierter Router, Kameras und Android-TV-Boxen. Sie sind für Rekordserien verantwortlich. Im Dezember 2025 stellte dieselbe Botnetz-Familie mit 31,4 Tbit/s und 200 Millionen Anfragen pro Sekunde einen neuen Rekord auf: den bislang größten öffentlich bekannten DDoS-Angriff.[3]

Zunehmend kommt eine zweite Angriffsquelle hinzu: gehackte virtuelle Server bei Cloud- und Hosting-Anbietern. Anders als eine private IoT-Kamera mit wenigen Mbit/s Upload-Bandbreite verfügt ein kompromittierter Server im Rechenzentrum über eine Anbindung im Gbit/s-Bereich. Schon einige tausend gehackte Cloud-Instanzen können damit ein Vielfaches der Angriffslast eines IoT-Botnetzes mit Millionen Endgeräten erzeugen.

Für Angreifer ist dies eine besonders effiziente Abkürzung auf dem Weg zu sehr hohen volumetrischen Angriffsstärken, da sie so mit deutlich weniger kompromittierten Systemen auskommen als beim klassischen IoT-Botnetz. Zudem ermöglicht es ihnen den Zugriff auf fremde oder mit gestohlenen Zahlungsdaten angemietete Cloud-Ressourcen.

> *„Ein gängiger Weg dorthin führt über gestohlene Zahlungsdaten: Mit kompromittierten Kreditkartendetails können Cloud-Server gemietet werden. Diese werden dann zwei bis vier Wochen lang genutzt, bevor der Anbieter den Betrug bemerkt und den Zugang sperrt.“*
>
> 
> **Jens-Philipp Jung, CEO, Link11**



**Strafverfolgung dämpft die Massenangriffe**

Der Rückgang der reinen Angriffszahl fällt zeitlich mit internationalem Verfolgungsdruck zusammen. Im Juli 2025 zerschlugen Europol und Eurojust im Rahmen der „Operation Eastwood” einen Großteil der Serverinfrastruktur der prorussischen Gruppe NoName057(16).[4] Diese hatte seit Kriegsbeginn in der Ukraine wiederholt DDoS-Angriffe auf kritische Infrastrukturen in Europa ausgeführt. Dabei wurden mehr als 100 Server beschlagnahmt, mehrere Haftbefehle ausgestellt und Festnahmen in Frankreich und Spanien durchgeführt.

Im März 2026 folgte ein weiterer Schlag: Behörden in den USA, Kanada und Deutschland schalteten die Kontrollserver von vier großen IoT-Botnetzen – Aisuru, Kimwolf, JackSkid und Mossad – ab, die gemeinsam mehr als drei Millionen Geräte kontrolliert hatten. Laut Justizministerium war die Zahl der weltweit von den Botnetz-Betreibern infizierten Geräte bis März 2026 auf über drei Millionen gestiegen, mit Hunderttausenden Geräten allein in den USA.[5]

**Künstliche Intelligenz senkt die Einstiegshürde für neue Botnetze**

Dennoch treibt KI die Verschärfung der Bedrohungslage enorm an. Ein aktuelles Beispiel ist das IoT-Botnetz „TuxBot v3 Evolution“[6]: Der Entwickler hat weite Teile des Codes – C2-Kommunikation, Exploit-Engine und Verschlüsselung – mithilfe eines Large Language Models (LLM) erzeugen lassen und so ein Multi-Architektur-Framework für 17 Prozessorarchitekturen entwickeln können.

Die KI-Herkunft hinterließ jedoch Spuren: unbereinigte Sicherheitshinweise im Code, unkommentierte Modell-Gedankenketten sowie eine fälschlich als „Argon2id” deklarierte, tatsächlich jedoch schwächere Passwort-Hash-Funktion. Dadurch war das Sample nur zu rund 70 % funktionsfähig, doch ließen sich die Fehler mit wenigen Prompts beheben, sodass eine funktionierende Version bereits im Umlauf sein dürfte.

Der Fall zeigt, wie KI den Entwicklungsaufwand und das nötige Fachwissen für neue Botnetze reduziert. Das passt zum aktuellen „Global Cybersecurity Outlook 2026“[7] des World Economic Forums, wonach 94 % der Sicherheitsverantwortlichen KI im Jahr 2026 als zentralen Treiber für Angreifer und Verteidiger sehen.

## Wichtigste Erkenntnisse

1

**Neue Rekordwerte bei Bandbreite und Paketraten:**
Maximalwerte von 2,3 Tbit/s und 322 Mio. Paketen pro Sekunde (H1 2025: 1,2 Tbit/s bzw. 207 Mio. Pakete pro Sekunde) übertreffen selbst die Kapazität leistungsfähiger Systeme deutlich.

2

**Angriffsdauer weiterhin auf hohem Niveau:**
Die längste dokumentierte Attacke im ersten Halbjahr 2026 lag bei rund sechs Tagen (H1 2025: über acht Tage).

3

**Explosives Datenvolumen:**
Das kumulierte Angriffsvolumen stieg von 438 TB auf 705 TB (+61 %) – genug für rund elf Jahre Netflix-Streaming in 4K.

# Network DDoS Protection

**Mehr Wucht, weniger Angriffe**

Auf den ersten Blick wirkt die Zahl wie eine gute Nachricht: Im ersten Halbjahr 2026 gab es im Link11-Netzwerk 42 % weniger DDoS-Angriffe als im Vorjahreszeitraum.

**-42%**




**Abnahme der DDoS-Angriffe im Link11-Netzwerk**

Der Blick hinter die reine Angriffszahl zeichnet jedoch ein anderes Bild: Einzelne Angriffe erreichten neue Rekordwerte bei Bandbreite, Paketrate und Dauer. Gleichzeitig verschob sich die Verteilung zwischen kurzen Blitzangriffen und langanhaltenden Kampagnen. Wer einmal ins Visier gerät, muss zudem mit einer deutlich höheren Wahrscheinlichkeit als im Vorjahr mit weiteren Wellen rechnen. Die Bedrohung hat sich somit nicht abgeschwächt, sondern verschoben – von der Breite in die Tiefe.

Der Rückgang bei der reinen Anzahl lässt sich auf verstärkten internationalen Verfolgungsdruck zurückführen. So nahmen Europol und Eurojust im Juli 2025 gemeinsam mit Behörden aus zwölf Ländern im Rahmen der „Operation Eastwood“ die Infrastruktur von NoName057(16) ins Visier. Diese pro-russische Gruppe war für umfangreiche DDoS-Angriffe gegen die Ukraine und ihre Unterstützerstaaten verantwortlich – genau jene Gruppe, die laut dem letzten Report im Vorjahreshalbjahr für einen Großteil der politisch motivierten Angriffswellen in Deutschland verantwortlich war.

Ganz verschwunden ist die Gruppe damit allerdings nicht: Zum Jahreswechsel 2025/2026 wurde eine neue, konzentrierte Kampagne von NoName057(16) mit über 2.600 Angriffseinträgen registriert. 88 % davon zielten auf deutsche Infrastruktur, und die Angriffe fanden im Zeitraum vom 29. Dezember 2025 bis zum 4. Januar 2026 statt. Der Fokus lag auf kulturellen Einrichtungen, politischen Institutionen und Behörden. Die Gruppe passt sich also an und operiert offenbar in kleineren, gezielteren Wellen als zuvor.

Ergänzend dazu setzten die Ermittlungsbehörden ihre Kampagne gegen DDoS-Stresser- und Booter-Dienste fort. Die jüngste Welle der „Operation PowerOFF” richtete sich im April 2026 gegen die DDoS-Ökosysteme in 21 Ländern. Frühere Wellen hatten bereits Dutzende Booter- und Stresser-Websites abgeschaltet.



## NoName057(16) & DDoSia

NoName057(16) ist eine pro-russische Hacktivisten-Gruppe, die seit März 2022 – kurz nach der Eskalation des Ukraine-Kriegs – aktiv ist. Als Reaktion auf die „IT Army of Ukraine“ entwickelte die Gruppe ein eigenes DDoS-Tool namens DDoSia und positioniert sich ideologisch als Verteidiger russischer Interessen gegen den Westen und die NATO-Staaten.

Das Besondere an DDoSia ist sein Betriebsmodell als „freiwilliges Botnet“: Teilnehmer installieren die Software bewusst und beteiligen sich aktiv an den Angriffen. Die Gruppe motiviert ihre Affiliates über ein gamifiziertes System mit Punkten, Ranglisten und Kryptowährungs-Belohnungen, verbreitet über gut organisierte Telegram-Kanäle mit teilweise über 20.000 Followern.

Das Tool läuft auf Windows, Linux und Android und wurde seit 2022 kontinuierlich weiterentwickelt – von einer einfachen Proof-of-Concept-Version bis zur aktuellen modularen Architektur (V5), die Cloudflare-Bypässe, verschlüsselte C2-Kommunikation und Anti-Analyse-Techniken umfasst.

Angriffe folgen einem klaren geopolitischen Muster: Meist erfolgt die Reaktion binnen 24–72 Stunden nach Ereignissen wie NATO-Beitritten, Sanktionsbeschlüssen oder Waffenlieferungen an die Ukraine. Eine offizielle staatliche Steuerung ist nicht belegt, jedoch duldet Russland die Aktivitäten ohne strafrechtliche Konsequenzen.

### Wichtige Fakten im Überblick:

**Angriffsvektoren**

Vorwiegend TCP-Flood (~53%) und HTTP(S)-Flood (~38%), ergänzt durch UDP-Flood und Slowloris

**Hauptziele**

Behörden, Medien, Finanzsektor, kritische Infrastruktur

**Top-Zielländer**

Ukraine, Litauen, Polen, Estland, Tschechien, Deutschland

**Allianzen**

Kooperation u. a. mit KillNet, CARR, UserSec, Z-Alliance

**Strafverfolgung**

„Operation Eastwood“ (Europol/Eurojust, Juli 2025) führte zu C2-Beschlagnahmungen

Angesichts der andauernden geopolitischen Spannungen ist mit anhaltender und technisch weiter reifender Aktivität zu rechnen.

**Zwischen Rekord und Realität**

Das Angriffsvolumen im Link11-Netzwerk stieg in Summe von 438 TB im ersten Halbjahr 2025 auf rund **705 TB** im ersten Halbjahr 2026. Das entspricht einem Anstieg um 61 %.

### 4K-Streaming

**705 TB** entsprechen **rund elf Jahren ununterbrochenem Netflix-Streaming** in 4K-Auflösung.

### Hörbücher

Genug Daten für **mehr als 2.700 Jahre** ununterbrochene Hörbuchwiedergabe.

### MP3-Songs

In dieses Datenvolumen passen rund **150 Millionen Songs.**

### 64-GB-Geräte

Das entspricht dem Speicher von **11.000 voll belegten Smartphones mit jeweils 64 GB.**

*„Angriffe dauern kürzer, aber das Gesamtvolumen, das wir abwehren mussten, ist so hoch wie nie. Angreifer steuern ihre Botnetze gezielter und kontrollierter, und erzeugen in kürzerer Zeit mehr Traffic.“*



**Karsten Desler, CTO**



**Die größten Angriffe im Vergleich**

Die bislang größte im Link11-Netzwerk registrierte DDoS-Attacke erreichte im ersten Halbjahr 2026 eine maximale Bandbreite von 2,3 Tbit/s. Im ersten Halbjahr 2025 lag der Höchstwert noch bei 1,2 Tbit/s. Der aktuelle Rekord ist somit um rund 85 % größer als der des Vorjahreszeitraums.

Parallel dazu stieg auch die maximale Paketrate deutlich: von 207.090.400 Paketen pro Sekunde im ersten Halbjahr 2025 auf 322.055.800 Pakete pro Sekunde im ersten Halbjahr 2026. Das entspricht einem Anstieg um 56 %.

Ein Angriffsvolumen dieser Größenordnung überfordert selbst leistungsstarke Unternehmensserver oder Firewalls binnen Sekunden. Dies führt zu massiver Netzwerküberlastung, Paketverlusten und potenziellen Totalausfällen von Diensten.

**Bandbreite: Warum der Blickwinkel entscheidet**

Auch die durchschnittliche Bandbreite pro Angriff stieg deutlich, allerdings fiel die Steigerung je nach angewandter Durchschnittsmethode unterschiedlich stark aus. Ein einziger extremer Ausreißer, wie die 2,3-Tbit/s-Attacke, kann einen einfachen Durchschnitt so stark verzerren, dass dieser kaum noch aussagekräftig ist. Wir betrachten deshalb drei Kennzahlen parallel.

**Betrachtete Kennzahlen:**

| | 2025 | | 2026 | % |
|---|---|---|---|---|
| Maximalwert | **1,2** Tbit/s | → | **2,3** Tbit/s | +85% |
| Einfacher Durchschnitt | **4,6** Gbit/s | → | **10,6** Gbit/s | +131% |
| Durchschnitt des mittleren Bereichs | **1,4** Gbit/s | → | **2,3** Gbit/s | +66% |

Der Mittlerer-Bereich-Durchschnitt schließt sowohl die vernachlässigbar kleinen Angriffe am unteren Rand als auch die extremen Ausreißer am oberen Rand aus und bildet damit den „typischen“ Angriff realistischer ab als der einfache Durchschnitt.

Konkret heißt das: Wir schneiden oben und unten jeweils die Extremwerte ab und bilden den Durchschnitt nur aus den mittleren 85 % aller Angriffe. So kann ein einzelner Rekordangriff das Ergebnis nicht mehr verzerren. Die Zahl zeigt, wie groß ein Angriff „normalerweise“ ist, nicht wie groß der spektakulärste Einzelfall war.

Das Bild ist uneinheitlich, aber aufschlussreich: An der Spitze der Verteilung hat sich die Bedrohung dramatisch verschärft, im „typischen“ Fall ist sie dagegen deutlich moderater. Dies belegt, dass wenige extreme Ausreißer für einen Großteil des Anstiegs verantwortlich sind, während sich der „typische“ Angriff langsamer, aber stetig weiterentwickelt.

**Zwei Geschwindigkeiten der Bedrohung**

Der längste dokumentierte Angriff im ersten Halbjahr 2026 dauerte 8.673 Minuten (rund sechs Tage) und wurde im Februar registriert. Er war damit kürzer als der Rekordwert des Vorjahreszeitraums (12.388 Minuten, also rund acht Tage und 14 Stunden), blieb aber weiterhin auf hohem Niveau. Dauer und Wucht der größten Angriffe entwickeln sich zunehmend unabhängig voneinander.

Der „typische" Angriff blieb dabei – anders als der einfache Durchschnitt vermuten lässt – weitgehend stabil: Während der einfache Durchschnitt durch einzelne sehr lange Kampagnen nach oben verzerrt wird (von 25,5 auf 35,3 Minuten, +38 %), zeigt der mittlere Durchschnitt einen moderaten Rückgang von 8,3 auf 7,6 Minuten (−8 %).

**Die eigentliche Verschiebung findet am kurzen Ende statt**

Der Anteil der Angriffe, die zwei Minuten oder weniger dauerten, verdoppelte sich von 16 % im ersten Halbjahr 2025 auf 31 % im ersten Halbjahr 2026. Gleichzeitig sank der Anteil der zwei- bis fünfminütigen Angriffe von 30 % auf 20 %.

Ab einer Dauer von rund zehn Minuten unterscheiden sich die Verteilungen der beiden Halbjahre dagegen kaum noch. Die Verschiebung konzentriert sich somit fast ausschließlich auf die kürzesten Angriffe, die sich weiter in Richtung „Microburst" verkürzen.

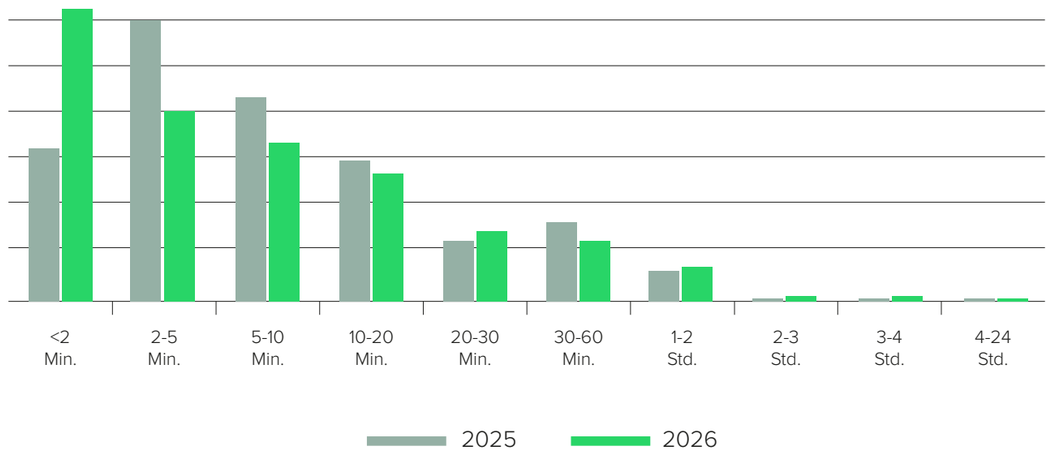
Für diesen Trend zu immer schnelleren Kurzangriffen erscheinen zwei Erklärungen naheliegend:

1. **Payload-first-Taktik:** Angriffe sind zunehmend so ausgelegt, dass sie innerhalb von Sekunden ihre Wirkung entfalten und einen Server ausschalten, bevor Abwehrmaßnahmen greifen können. Anstatt auf eine lange, ressourcenintensive Belastung zu setzen, verlassen sich diese Angriffe darauf, dass automatisiertes Blackholing oder resultierende Serverfehler den Dienst auch nach Ende der eigentlichen Angriffsspitze offline halten – und das ganz ohne den Aufwand einer Dauerattacke.

2. **Frühzeitiger Abbruch:** Angreifer erkennen zunehmend früh, wenn ein Angriff wirkungslos bleibt, und brechen ihn ab, anstatt weitere Ressourcen in einen erfolglosen Versuch zu investieren.

In beiden Fällen deutet das Muster darauf hin, dass Angreifer heute unmittelbare Ergebnisse erwarten und große Traffic-Mengen mit chirurgischer Präzision einsetzen können. Dies steht im Kontrast zu den nach wie vor bestehenden, mehrtägigen Marathon-Kampagnen am oberen Rand der Verteilung. Beide Muster treten also nebeneinander auf, Sprint und Marathon sozusagen gleichzeitig, nicht das eine statt des anderen.

**Vergleich der Angriffsdauer 1. Halbjahr 2025 vs. 2026**






**Wiederkehrende Angriffe: Einmal reicht selten**

Statistisch gesehen hat, wer einmal angegriffen wurde, schlechte Karten, dass es dabei bleibt. In unserer Auswertung betrachten wir, wie viele Tage zwischen Angriffswellen auf denselben Kunden liegen und wie wahrscheinlich es ist, dass ein Angriff Folgeattacken nach sich zieht.

Angriffswellen kommen selten allein. Im ersten Halbjahr 2026 registrierten wir an mehr als der Hälfte aller Angriffstage nicht nur eine, sondern mehrere Angriffswellen am selben Tag – der bereinigte Mittelwert liegt bei 58 % (H1 2025: 49 %). Ein „Angriffstag" ist für die betroffenen Kunden also zunehmend kein einmaliges Ereignis, sondern eher die Regel mit mehreren aufeinanderfolgenden Wellen.

Und danach ist meist nicht Schluss. Die Wahrscheinlichkeit, dass ein Kunde nach einer Attacke für eine bestimmte Zeit verschont bleibt, ist im Jahresvergleich an jedem betrachteten Zeithorizont gesunken.

**Zeitraum ohne erneuten Angriff**

| | H1 **2025** | H1 **2026** |
|---|---|---|
| **1 Tag** | 93% | 89% |
| **7 Tage** | 78% | 71% |
| **30 Tage** | 54% | 44% |
| **60 Tage** | 33% | 24% |
| **90 Tage** | 19% | 12% |

Anders formuliert: Nach Abschluss einer Angriffswelle schafften es im ersten Halbjahr 2026 nur noch 44 % der betroffenen Kunden, 30 Tage lang angriffsfrei zu bleiben – im Vorjahreszeitraum waren es noch 54 %. „Einmal und nie wieder" wird damit seltener – und das nicht nur gefühlt: In jedem der betrachteten Zeithorizonte (1, 7, 30, 60 und 90 Tage) ist die Rückfallquote im Jahr 2026 höher als im Vorjahr. Wer angegriffen wird, muss mit einem Folgeangriff rechnen, und zwar über einen deutlich längeren Zeitraum als bisher.

Wer 2026 einmal getroffen wird, muss mit deutlich höherer Wahrscheinlichkeit auch danach über Wochen mit weiteren Wellen rechnen.

> *„Wir sehen vermehrt Microburst-Angriffe, kurze, harte Schläge, die schnell enden. Früher dauerten die Angriffe drei bis vier Minuten, heute nur noch eine Minute oder weniger. Die Angreifer setzen auf automatisierte Fehlerquellen oder Serverfehler, um die Webseite auch nach dem eigentlichen Angriff offline zu halten."*



**Sean Power, Solution Engineer**

# Bots, Botnetze und die Praxis moderner WAAP-Abwehr

Bots sind fast so alt wie das Internet selbst. Doch was heute unter diesem Begriff läuft, hat mit den harmlosen IRC-Helfern der frühen 1990er Jahre kaum noch etwas gemein. In diesem Kapitel wird die Entwicklung in zwei Schritten beleuchtet. Zunächst wird dargestellt, wie sich Bots und Botnetze über mehr als drei Jahrzehnte von einfachen Chat-Skripten zu KI-gestützten Angriffswerkzeugen entwickelt haben. Im zweiten Teil wird diese Entwicklung anhand von konkreten Fällen aus dem ersten Halbjahr 2026 greifbar gemacht: reale Cyber-Insight-Analysen aus dem Link11 SOC zeigen, wie sich Volumen, Tarnung und Legitimität inzwischen in der Praxis vermischen und was das für eine wirksame WAAP-Strategie bedeutet.

**Von Eggdrop zum Agenten:**
**Die Evolution von Bots und Botnetzen**

Botnetze sind fast so alt wie das Internet selbst, doch ihre Werkzeuge haben sich radikal verändert. Was als IRC-Scherz (Internet Relay Chat, eines der ältesten Chat-Protokolle im Internet) begann, ist heute eine industrialisierte, KI-gestützte Angriffswirtschaft. Ein Blick zurück zeigt, warum starre Abwehrkonzepte dieser Entwicklung, die sich alle paar Jahre neu erfindet, hinterherlaufen.

**1988 – 2000**

**Die Anfänge: Chat-Helfer werden zur Waffe**

Die Geschichte beginnt harmlos. Im Jahr 1993 veröffentlichte Jeff Fisher mit „Eggdrop" einen der ersten IRC-Bots. Diese waren als Verwaltungshelfer für Chatkanäle gedacht.[8] Weil sich Nutzer, die aus Kanälen geworfen wurden, revanchieren wollten, entstanden aus diesen Werkzeugen die sogenannten IRC-Kriege. Sie gelten als Vorläufer heutiger DDoS-Angriffe. 1999 folgten mit „PrettyPark" und „SubSeven" die ersten Malware-Programme, die Passwörter stahlen, Traffic umleiteten und aus der Ferne steuerbar waren.[9] Im Jahr 2000 etablierte sich mit „GTbot" der erste Bot mit gezielter DoS-Funktion.[10] Im selben Jahr entdeckten Forscher mit dem EarthLink Spammer eines der frühesten kommerziellen Botnetze für Massen-Phishing.[11]

**Was ist IRC?**
Internet Relay Chat (IRC) ist ein textbasiertes Chat-Protokoll aus dem Jahr 1988. Nutzer verbinden sich mit einem Server und treten „Channels" bei (z. B. #chat), in denen beliebig viele Teilnehmer in Echtzeit schreiben können.

**Warum das für die Bot-Historie zählt:**
Weil sich IRC-Bots leicht bauen und per Chat-Befehl steuern ließen, wurde das Protokoll ab Mitte der 1990er zum bevorzugten Kanal für Botnetze. Angreifer ließen gekaperte Rechner in einen eigenen Kanal einloggen und steuerten sie zentral, die Blaupause für das Command-and-Control-Prinzip, das bis heute nachwirkt. Auch 2026 taucht IRC noch als Rückfallkanal auf, etwa bei TuxBot v3.

**2002 – 2009**

**Professionalisierung: Malware-Baukästen und Spam-Armeen**

Zwischen 2002 und 2004 etablierten sich mit „Agobot", „SDBot" und „Spybot" regelrechte Baukastensysteme.[12] Da ihr Quellcode offen im Netz kursierte, konnten auch technisch weniger versierte Akteure eigene Varianten erstellen. Dies war ein früher Vorläufer heutiger Malware-as-a-Service-Modelle. Parallel dazu entstanden mit „Sinit" und „Phatbot" die ersten Peer-to-Peer-Botnetze, die ohne zentralen Command-and-Control-Server auskamen und somit schwerer abzuschalten waren.[13] Der bis dahin größte Ausbau der Angriffsfläche gelang 2007 dem Storm-Botnetz, das schätzungsweise bis zu 50 Millionen Rechner infizierte und für Spam, Aktienkursmanipulation und Identitätsdiebstahl genutzt wurde.

**2010 – 2018**

**Der Bruch: Web-Bots, Browser-Emulation und die IoT-Welle**

Mit der Verbreitung webbasierter Dienste verließen Bots die reinen IRC-Kanäle. Angreifer begannen, HTTP, SSL und ICMP als Kommunikationswege zu nutzen. Parallel dazu entstand auf der Webseite eine zweite Bot-Generation: Headless Browser wie PhantomJS konnten komplette Webseiten inklusive JavaScript verarbeiten, ohne eine grafische Oberfläche zu benötigen.[14] Damit ließen sich erstmals Formulare automatisiert ausfüllen und Zugangsdaten im großen Stil durchprobieren. Credential Stuffing wurde zum Massenphänomen.

Den nächsten Bruch markierte im Jahr 2016 das Mirai-Botnetz. Die Schadsoftware durchsuchte das Internet nach IoT-Geräten mit werkseitigen Standardpasswörtern, infizier-

## Zeitstrahl im Überblick

**Die Anfänge**
1988 - 2000

### Chat-Helfer werden zur Waffe

**MEILENSTEINE**
Eggdrop, IRC-Kriege, PrettyPark/ SubSeven, GTbot, EarthLink Spammer

**BEDEUTUNG FÜR DIE BOT-ABWEHR**
Vom Chat-Helfer zur ersten DoS-fähigen Malware

**Professionalisierung**
2002 - 2007

### Malware-Baukästen und Spam-Armeen

**MEILENSTEINE**
Agobot, SDBot, Spybot, P2P-Botnetze (Sinit, Phatbot), Storm-Botnetz

**BEDEUTUNG FÜR DIE BOT-ABWEHR**
Malware-Baukästen demokratisieren den Angriffszugang

**Der Bruch**
2010 - 2016

### Web-Bots, Browser-Emulation und die IoT-Welle

**MEILENSTEINE**
Headless Browser (PhantomJS), Credential Stuffing, Mirai

**BEDEUTUNG FÜR DIE BOT-ABWEHR**
Bots verlassen IRC, IoT wird zur Angriffsfläche

**Tarnung als Prinzip**
2018 - 2023

### Browser-Bots und Residential Proxies

**MEILENSTEINE**
Chrome-basierte Bots, Residential Proxies, Anti-Detect-Browser

**BEDEUTUNG FÜR DIE BOT-ABWEHR**
Tarnung wird wichtiger als reines Volumen

**Die KI-Ära**
2024 - 2025

### Generativ, agentisch, industrialisiert

**MEILENSTEINE**
Generative KI, Bad-Bot-Statistiken (~25 Mio. KI-Bot-Angriffe/Tag), Aisuru/Kimwolf (31,4 Tbit/s)

**BEDEUTUNG FÜR DIE BOT-ABWEHR**
KI demokratisiert Bot-Erstellung, neue Rekord-Botnetze

2026

**MEILENSTEINE**
TuxBot v3 Evolution (LLM-assistiert), Anthropic GTG-1002-Fall

**BEDEUTUNG FÜR DIE BOT-ABWEHR**
KI wird Co-Entwickler – und teilweise autonomer Akteur

te Router, Kameras und Digitalrekorder und erzeugte damit Angriffe von bis dahin unbekannter Größe: Über 600 Gbit/s wurden gegen den Sicherheitsblog von Brian Krebs gerichtet, rund 1 Tbit/s gegen den französischen Hoster OVH und schließlich kam es zu einem mehrstündigen Ausfall beim DNS-Anbieter Dyn, wodurch große Teile des US-amerikanischen Internets betroffen waren.[15] Als der Quellcode wenig später veröffentlicht wurde, entstand daraus eine ganze Familie von Nachahmern, die bis heute aktiv ist.[16]

**2010 – 2023**

**Tarnung als Prinzip: Browser-Bots und Residential Proxies**

In den folgenden Jahren stand ein Wettlauf um Unauffälligkeit im Mittelpunkt. Bots, die auf Basis von Chrome oder Chromium gebaut wurden, konnten Mausbewegungen, Klicks und das Scrollverhalten so realistisch imitieren, dass sie sich kaum noch von echten Nutzern unterscheiden ließen.

Gleichzeitig verlagerten sich die Angriffe zunehmend auf gekaperte Heimrouter und private Internetanschlüsse, sogenannte Residential Proxies. Dadurch kam der Traffic nicht mehr aus verdächtigen Rechenzentren, sondern aus scheinbar gewöhnlichen Haushalten. Sicherheitsanbieter begannen, diese Entwicklung in Generationen einzuteilen: von simplen Skripten über headless Browser bis hin zur vollwertigen Browser-Emulation – jede Stufe war schwerer zu erkennen als die vorherige.

**2024 – heute**

**Die KI-Ära: generativ, agentisch, industrialisiert**

Seit 2024 beschleunigt generative KI diese Entwicklung auf zwei Ebenen gleichzeitig. Erstens sinkt die Einstiegshürde. Bot-as-a-Service-Plattformen und KI-Codegeneratoren ermöglichen es auch technisch unerfahrenen Akteuren, funktionierende Angriffstools zu erstellen. Aktuellen Berichten zufolge sind KI-generierte Bot-Angriffe von rund zwei auf 25 Millionen pro Tag innerhalb eines Jahres angestiegen.[17] Das heißt um ein Zwölffaches. Mittlerweile sollen mehr als die Hälfte aller Web-Anfragen von Bots stammen, davon ist gut ein Drittel schädlich.

Zweitens verändert KI auch die Entwicklung der Schadsoftware selbst. Im Juli 2026 dokumentierte das Threat-Intelligence-Team Unit 42 von Palo Alto Networks mit TuxBot v3 Evolution ein IoT-Botnet-Framework, dessen Autor große Teile des Codes von einem Sprachmodell hatte schreiben lassen, inklusive eines verschlüsselten Command-and-Control-Kanals, eines Domain-Generation-Algorithmus und einer eigenen Exploit-Sprache.

Aufschlussreich sind dabei die Fehler: So hinterließ das Modell unter anderem seine eigenen Gedankengänge als Kommentare im Code und behauptete, eine moderne Argon2id-Verschlüsselung implementiert zu haben; tatsächlich griff es jedoch auf ein deutlich schwächeres Verfahren zurück. KI senkt also die Hürde für die Entwicklung, ersetzt aber nicht die fachliche Kontrolle – ein Muster, das sich in den kommenden Jahren vermutlich wiederholen wird.

Die IoT-Botnetze Aisuru und Kimwolf zeigen auf der Betriebsseite, wohin die Reise geht: Mit einer Kampagne namens „The Night Before Christmas“ erzeugten sie Ende 2025 einen Angriff mit einer Spitzenlast von 31,4 Terabit pro Sekunde und lösten damit den bis dahin größten öffentlich bekannten DDoS-Angriff aus. Dieser wurde über gekaperte Router und zunehmend kompromittierte Android-Fernseher ausgelöst.[18] Im März 2026 zerschlugen das Bundeskriminalamt, US-Behörden und kanadische Ermittler gemeinsam ein Netzwerk aus mehr als drei Millionen gekaperten Geräten, das zu diesem Ökosystem gehörte.[19]

Am weitesten geht bislang ein Fall, der über klassische Botnetze hinausreicht: Im November 2025 gab Anthropic bekannt, dass eine mutmaßlich staatlich gelenkte Gruppe dessen KI-Coding-Werkzeug über einen Zeitraum von mehreren Wochen als weitgehend selbstständigen Angriffsagenten genutzt hatte. Dabei erfolgten Aufklärung, Exploit-Entwicklung und Datenauswertung zu 80 bis 90 Prozent ohne menschliches Eingreifen.[20]

Ob dieser Grad an Autonomie schon die Regel oder noch die Ausnahme ist, wird in der Fachwelt kontrovers diskutiert. Für die Bot-Abwehr verschiebt sich damit die Zielscheibe von reiner Traffic-Erkennung zur Frage, ob hinter einer Anfrage ein Skript, ein Mensch oder ein eigenständig planendes System steckt.

Diese historische Entwicklung vom Chat-Skript zum eigenständig planenden Agenten ist mehr als nur ein Rückblick. Sie erklärt, warum sich die Angriffe, die das Link11 SOC im ersten Halbjahr 2026 tatsächlich beobachtet hat, kaum noch mit dem klassischen Bild eines Botnetzes decken. Die folgenden fünf Fälle zeigen, wie sich das im Alltag konkreter Kunden niederschlägt.



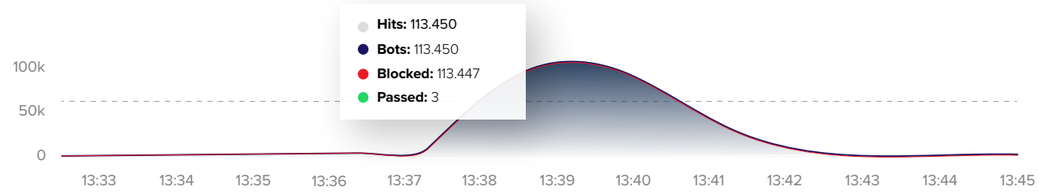
## WAAP in der Praxis: Wenn Traffic nicht mehr ist, was er zu sein scheint

Der klassische DDoS-Angriff – laut, massiv und leicht erkennbar – ist zwar nicht verschwunden, aber er ist nicht mehr der Normalfall. An seine Stelle tritt eine Bedrohungslandschaft, in der das Volumen, die Herkunft und das Ziel eines Angriffs zunehmend entkoppelt sind. Wer nur auf die Bandbreite und bekannte Signaturen achtet, sieht oft nur die halbe Wahrheit.

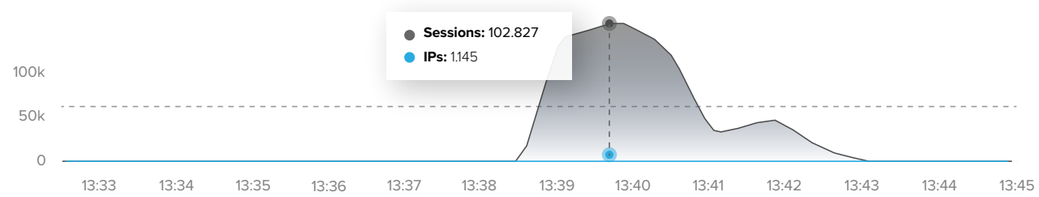
**Kleine Zahlen, reale Wirkung**

Nicht jeder wirksame Angriff erfordert ein Botnetz aus Millionen Geräten. Ein Fall mit rund drei Millionen GET-Requests auf eine einzelne Root-Domain wirkte zunächst harmlos im Vergleich zu Rekordangriffen im zweistelligen Terabit-Bereich. Erst die Kombination aus Geofilterung und Rate Limiting entlarvte das Muster: ein kleines, unauffälliges Botnetz, das gezielt Serverressourcen band, ohne jemals eine Alarmschwelle für „große” Angriffe zu erreichen.

**Passed vs. Blocked**




**Unique Sessions & IPs**



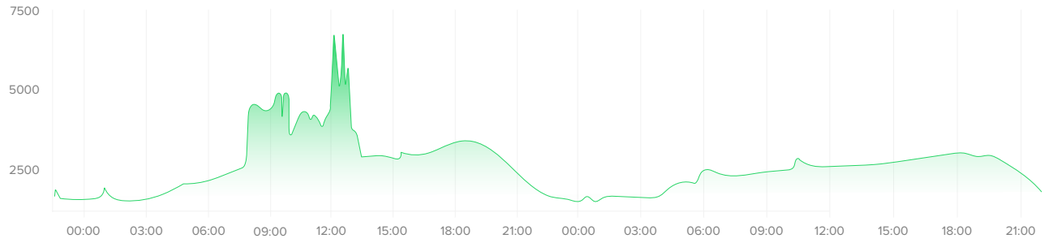

*„Die gefährlichsten Angriffe, mit denen wir es zu tun haben, sind längst nicht mehr die lautesten. Wer nur auf Bandbreite und bekannte Signaturen achtet, übersieht genau die Angriffe, die den größten Schaden anrichten können, denn sie sind so konzipiert, dass sie unauffällig bleiben.“*

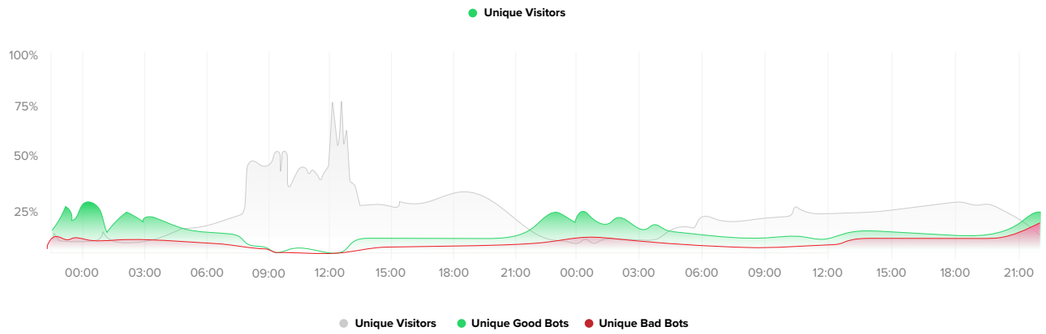


**Jag Bains, VP Solution Engineering**

### Low-and-Slow: Unsichtbar im Rauschen

Noch subtiler agierte ein Angreifer bei einem europäischen E-Commerce-Anbieter: Die Zahl eindeutiger IP-Adressen verdoppelte sich, ohne erkennbaren geschäftlichen Anlass. Bandbreite und Requests pro Sekunde blieben unauffällig, dennoch litten die Response-Zeiten und die Konversionsraten. Verantwortlich dafür waren echte, kompromittierte Endgeräte mit vollwertigen Browsern, die einzeln kaum auffielen, aber in der Masse wirkten – ein klassisches Low-and-Slow-Muster, das sich im statistischen Rauschen normaler Nutzung versteckte. Erst eine Mensch-Maschine-Verifikation zeigte Wirkung, nachdem Geo- und ASN-Filter ins Leere liefen.

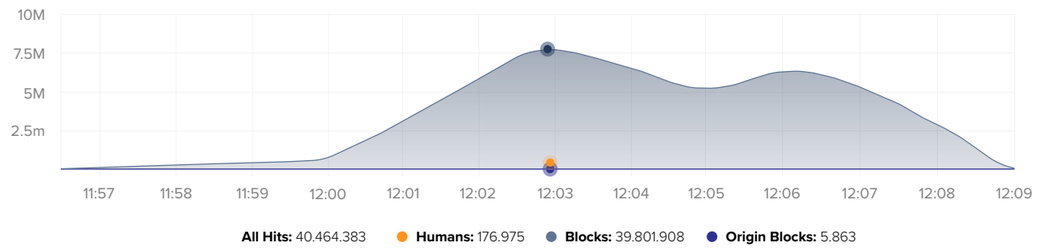



### Lärm als Tarnung

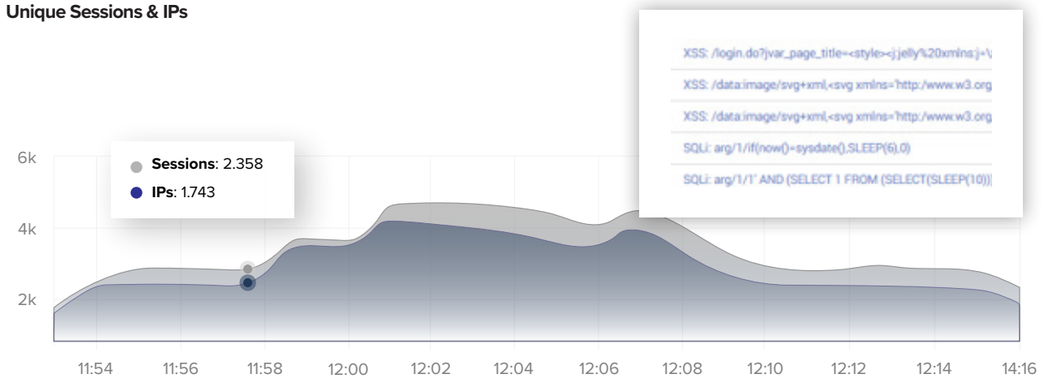
Ein zweites Muster zeigt, dass ein Traffic-Peak nicht zwangsläufig das eigentliche Ziel eines Angriffs darstellt. In einem Fall wurden zwei Domains – darunter eine Buchungsplattform – mit 14 bis 40 Millionen Requests attackiert. Parallel dazu tauchten in der WAF-Analyse gezielte SQL-Injection- und XSS-Signaturen auf. Die Logik hinter solchen „Smokescreen"-Angriffen ist simpel: Der volumetrische Lärm soll Monitoring-Systeme fluten und Logfiles aufblähen, während im Windschatten leise Exploits platziert werden. Im vorliegenden Fall haben sich die Angreifer jedoch selbst verraten, da sie für DDoS-Traffic und Infiltrationsversuche dieselben IP-Adressen genutzt haben. Dadurch wurden beide Vektoren durch dieselbe Sperre blockiert. Ein versierterer Akteur hätte getrennte IP-Pools verwendet und wäre damit deutlich schwerer zu stoppen gewesen.

### Passed vs. Blocked





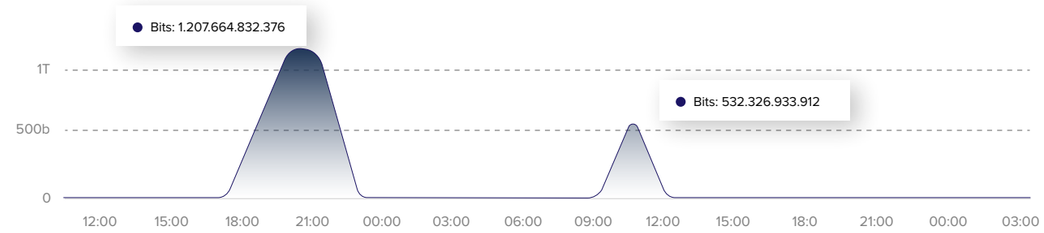

### Unique Sessions & IPs



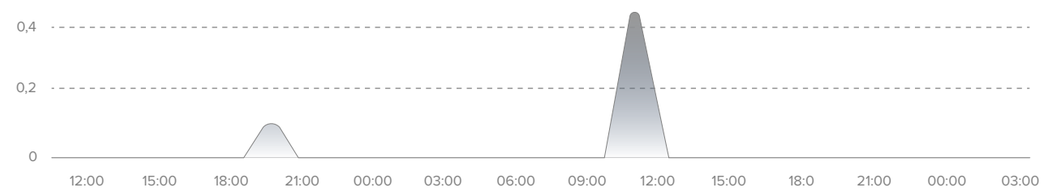

### Request-Rate schlägt Bandbreite

Eine noch komplexere Variante zeigte sich bei einem zweiwelligen Angriff mit über 335 Millionen Requests und mehr als einem Terabit Spitzenlast. Aufschlussreich war die zweite, kleinere Welle: Mit nur der halben Bandbreite der ersten erzeugte sie durch eine höhere Request-Rate pro Sekunde stärkere Latenzeffekte – ein Beleg dafür, dass die CPU-Last durch die Request-Frequenz oft kritischer ist als die reine Bandbreite.

### Gesamtbandbreite (Bits)




### Latenz (Millisekunden)



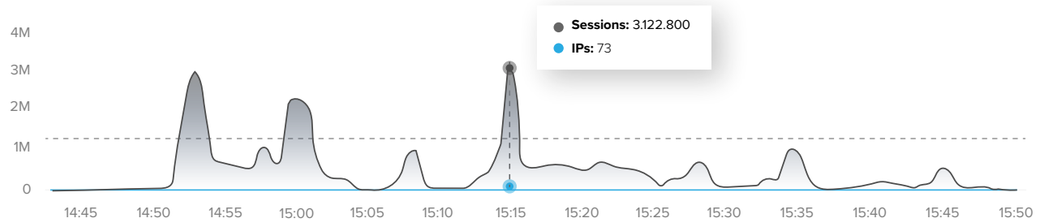
*„Beim zweiwelligen Angriff hatte die zweite Welle nur die halbe Bandbreite der ersten und hat dennoch stärkere Latenzeffekte verursacht – einfach, weil die Request-Rate höher war. Das zeigt: Bandbreite allein sagt oft wenig darüber aus, wie viel Schaden ein Angriff tatsächlich anrichtet.“*



**Sean Power, Solution Engineer**

**Wenn echter Traffic zur Waffe wird**

Am schwersten zu fassen sind Angriffe, die legitime Infrastruktur oder Daten als Deckung nutzen. So stammte bei einem Rüstungsunternehmen der Großteil des Angriffstraffics – über 50 Millionen Requests – nachweislich aus bekannten Cloud- und Hosting-Umgebungen und nicht aus einem diffusen IoT-Botnetz. Nur 73 IP-Adressen erzeugten gemeinsam über drei Millionen parallele Sessions – eine Rechenleistung, die kein Heimrouter aufbringen kann. Der geopolitische Kontext – ein aktiver Konflikt zwischen zwei Staaten – legte eine politische Motivation nahe. Da Cloud-Kapazität günstig, anonym buchbar und technisch vertrauenswürdig ist, verschiebt sich die Bedrohung von der Bandbreite zur Applikationslogik und von kompromittierten Endgeräten zu cloud-nativer Angriffsinfrastruktur.




**Was das für die WAAP-Praxis bedeutet**

In allen Fällen führt dies zu derselben Konsequenz: Weder das Volumen, die Herkunft noch bekannte Signaturen sind heute verlässliche Frühindikatoren. Eine wirksame Abwehr erfordert einerseits endpunktspezifische Baselines, die definieren, wie normaler Traffic auf genau diesem Pfad zu welcher Uhrzeit aussieht. Generische Schwellenwerte reichen für transaktionskritische APIs nicht aus. Andererseits ist eine verhaltensbasierte statt einer rein signaturbasierten Erkennung notwendig, da Replay-Angriffe, Low-and-Slow-Muster und Cloud-native Fluten strukturell „sauber” wirken können.

Die zentrale Lehre des ersten Halbjahres 2026 lautet somit: Ein Traffic-Peak ist nicht automatisch ein Kapazitätsproblem und unauffälliger Traffic ist nicht automatisch harmlos. Resilienz bedeutet somit nicht nur, online zu bleiben, sondern auch, jederzeit erkennen zu können, was tatsächlich hinter dem eigenen Traffic steckt.



# Fazit

Die Analyse der Angriffe im ersten Halbjahr 2026 zeigt deutlich, dass sich die Bedrohungslage im Bereich der DDoS-Attacken weiter verschärft und zugleich diversifiziert hat. So ist die reine Anzahl der Angriffe im Vergleich zum Vorjahreszeitraum zwar um 42 % zurückgegangen, jedoch haben sich Bandbreite und Paketraten der einzelnen Angriffe deutlich erhöht. Die Angreifer konzentrieren sich demnach zunehmend auf weniger, aber deutlich wirkungsvollere Attacken.

**Die fünf wichtigsten Erkenntnisse im Überblick:**

- Weniger, aber deutlich wirkungsvollere Angriffe –
  42 % weniger Angriffe, aber neue Rekorde bei Bandbreite (2,3 Tbit/s) und Paketrate (322 Mio. pps)
- Superbotnetze und Cloud-Ressourcen treiben die Rekorde –
  Aisuru/Kimwolf und gehackte Cloud-Server als effiziente Angriffsquellen
- Zwei Geschwindigkeiten der Bedrohung – Microburst-Angriffe und Marathon-Kampagnen nebeneinander
- Wer einmal getroffen wird, bleibt im Visier – steigende Rückfallquote auf allen Zeithorizonten
- Angriffe werden raffinierter statt nur größer – Layer-7, Tarnung, cloud-native Infrastruktur

Auffällig sind zudem die enorme Bandbreite und Paketrate mancher Angriffe. Diese reichen von Terabit-Traffic bis hin zu über 320 Millionen Paketen pro Sekunde im ersten Halbjahr 2026, was das potenzielle Ausmaß der Auswirkungen auf Unternehmen, Institutionen und ganze Infrastrukturen verdeutlicht. 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 solch massiver Angriffe begrenzen. Erfolgreicher DDoS-Schutz erfordert daher mehr als nur ein Management der Bandbreite, um den zunehmend hybriden Bedrohungen zu begegnen.

## Ihr Ansprechpartner

**Rolf Gierhard**
Chief Revenue Officer

+49 69 58004926-200
r.gierhard@link11.com



# Nachweise


[1] https://commercial.allianz.com/content/dam/onemarketing/commercial/commercial/reports/allianz-risk-barometer-2026.pdf

[2] https://www.pwc.com/us/en/services/consulting/cybersecurity-data-tech-risk/library/global-digital-trust-insights.html

[3] https://www.bleepingcomputer.com/news/security/aisuru-botnet-sets-new-record-with-314-tbps-ddos-attack/

[4] https://www.eurojust.europa.eu/news/hacktivist-group-responsible-cyberattacks-critical-infrastructure-europe-taken-down

[5] https://www.techradar.com/pro/security/europol-announces-takedown-of-major-ddos-for-hire-network

[6] https://unit42.paloaltonetworks.com/tuxbot-v3-evolution-iot-botnet/

[7] https://www.weforum.org/publications/global-cybersecurity-outlook-2026/

[8] https://www.aic.gov.au/publications/tandi/tandi333

[9] https://arxiv.org/pdf/1706.05143

[10] https://abusix.com/blog/bots-and-how-theyve-shaped-the-internet/

[11] https://www.imperva.com/company/press_releases/bots-are-taking-over-the-internet-automated-threats-are-a-growing-risk-for-organizations/

[12] https://www.researchgate.net/publication/241677624_The_evolution_of_malicious_IRC_bots

[13] https://www.usenix.org/legacyurl/peer-peer-botnets-overview-and-case-study

[14] https://www.imperva.com/learn/application-security/what-are-bots/

[15] https://www.cisa.gov/news-events/alerts/2016/10/14/heightened-ddos-threat-posed-mirai-and-other-botnets

[16] https://www.cyber.nj.gov/threat-landscape/malware/botnets/mirai

[17] https://lyrie.ai/research/research/2026-05-02-bad-bot-report-2026-internet-no-longer-human

[18] https://www.cloudflare.com/learning/ddos/glossary/aisuru-kimwolf-botnet/

[19] https://www.bka.de/DE/Presse/Listenseite_Pressemitteilungen/2026/Presse2026/260320_PM_Botnetze.html

[20] https://www.anthropic.com/news/disrupting-AI-espionage


LINK11