LINK11

EUROPEAN CYBER REPORT

2026

www.link11.com

Liebe Leserinnen und Leser,

Digitale Infrastrukturen sind heute das Rückgrat nahezu aller Geschäftsmodelle. Plattformen, Cloud-Services, APIs und datengetriebene Prozesse verbinden Unternehmen, Kunden und Partner. Diese Vernetzung schafft große wirtschaftliche Chancen, aber auch Abhängigkeiten.

Cybersicherheit ist daher längst kein technisches Thema mehr, sondern eine strategische Aufgabe. Internationale Studien belegen: Cyber-Vorfälle zählen zu den größten Geschäftsrisiken. Gleichzeitig werden Angriffe automatisierter, koordinierter und mehr auf operative Wirkung ausgelegt.

Besonders deutlich wird dies bei DDoS-Angriffen: Was früher als einzelne Website-Störungen galt, ist nun ein strukturelles Risiko für die Wertschöpfung. Moderne Angriffskampagnen kombinieren enorme Bandbreiten mit hohen Frequenzen, langen Laufzeiten und immer ausgefeilteren Tarnmechanismen. Zudem verlagern sich viele Angriffe von der Infrastruktur auf Anwendungen, APIs und digitale Prozesse.

Der „European Cyber Report 2026“ analysiert diese Veränderungen auf Basis realer Angriffsdaten aus dem Link11-Netzwerk sowie der internationalen Cyberlandschaft. Ziel ist es, die strukturellen Trends sichtbar zu machen. Denn nur so kann Resilienz geplant werden.

Die zentrale Erkenntnis: Cyberresilienz entsteht nicht erst zum Zeitpunkt des Angriffs. Sie ist das Ergebnis langfristiger Architekturentscheidungen, Verantwortlichkeiten und eines kontinuierlichen Risikobewusstseins.

Die Analysen und Einordnungen dieses Reports sollen Ihnen helfen, Ihre Sicherheitsstrategie zu hinterfragen und weiterzuentwickeln. Digitale Verfügbarkeit ist ein Wettbewerbsfaktor. Sie zu sichern, ist eine gemeinsame Aufgabe von Technologie, Organisation und Führung.

Ich wünsche Ihnen eine erkenntnisreiche Lektüre.



Herzliche Grüße
Jens-Philipp Jung, CEO, Link11

Inhalt

Executive Summary **04**

DDoS im Strukturwandel **06**

30 Jahre DDoS **12**

Web Application & API Protection **14**

Web Performance **21**

Interview mit Lukas Frank **24**

Fazit **26**

Executive Summary

Die neue Ära der Cyberresilienz

In der globalen Risikolandschaft des Jahres 2026 hat sich Cybersicherheit endgültig von einer rein technischen Disziplin zum kritischen Kernfaktor unternehmerischer Steuerung gewandelt. Internationale Analysen wie das „Allianz Risk Barometer 2026“[1] zeigen eindeutig: Mit 42 % der Nennungen stehen Cybervorfälle branchenübergreifend an erster Stelle der weltweiten Geschäftsrisiken. Dass es sich hierbei nicht mehr um abstrakte Gefahren handelt, belegen die „PwC Digital Trust Insights 2026“[2] : Allein in Deutschland verzeichnen bereits 37 % der Unternehmen Schäden von über einer Million US-Dollar pro Vorfall – ein wirtschaftlicher Aderlass, der deutlich über dem globalen Durchschnitt liegt.

Das „New Normal“ der DDoS-Bedrohung

Die im aktuellen „European Cyber Report 2026“ (ECR 2026) dokumentierte Eskalation fügt sich nahtlos in dieses Bild ein. Was 2024 mit einer explosiven Steigerung der Angriffsfrequenz im Link11-Netzwerk um 137 % begann, hat sich 2025 zu einer neuen Normalität verfestigt. Ein weiterer Anstieg um 75 % im Vergleich zum Vorjahr zeigt, dass DDoS-Attacken keine punktuellen Störereignisse mehr sind, sondern eine permanente Grundbelastung digitaler Infrastrukturen darstellen. Dabei wurden Spitzenwerte von bis zu 1.247 Angriffen innerhalb von nur 24 Stunden registriert (Peak Day: 1. März 2025).

Die neue Qualität und Ausdauer der Angriffe ist dabei besonders ernst zu nehmen:

Durchbruch der Terabit-Schwelle: Während der Rekordwert von 1,4 Tbit/s im Jahr 2024 noch eine Ausnahme darstellte, etablierten sich Terabit-Angriffe im Jahr 2025 als wiederholbare Realität: **Es wurden drei Attacken jenseits der 1-Tbit/s-Marke registriert.**

Extreme Dauerbelastung: Die maximale Angriffsdauer hat sich von **2.689 Minuten im Jahr 2024 auf über 12.388 Minuten im Jahr 2025 vervielfacht.**

Systemische Wiederholung: **Mit einer Wahrscheinlichkeit von über 70 %** werden Unternehmen nach einem initialen Angriff erneut Ziel einer Attacke. Das Risiko ist heute serieller Natur.

Die Dimension wird in Anbetracht des kumulierten Volumens besonders eindrücklich: Eine Serie von Attacken erreichte einen Rekordangriff von 509 Terabyte – eine Datenmenge, die dem täglichen Datenvolumen einer Stadt mit 120.000 Einwohnern entspricht. Mit einer maximalen Bandbreite von 1,3 Tbit/s wird deutlich, dass die Bandbreite kein limitierender Faktor mehr ist, sondern von Angreifern als strategisches Mittel zur totalen Überlastung eingesetzt wird.

Geopolitik und systemische Kaskadeneffekte

Diese neue Angriffswirklichkeit ist untrennbar mit geopolitischer Volatilität verbunden. Getrieben durch die geopolitische Fragmentierung, wie das World Economic Forum (WEF)[3] sie beschreibt, und den massiven Einsatz von künstlicher Intelligenz auf Seiten der Angreifer, verschiebt sich die Bedrohung von der Ebene der Infrastruktur auf die Anwendungsebene. Wie die Analysen von PwC und KPMG[4] unterstreichen, zwingt diese neue Dynamik 92 % der Entscheider dazu, ihre Cyberstrategien anzupassen. Der Fokus liegt nicht mehr allein auf der punktuellen Abwehr, sondern auf einer ganzheitlichen, automatisierten Resilienz.

Staatlich tolerierte Akteure nutzen Cyberangriffe als politisches Instrument, wobei nationale Grenzen im digitalen Raum verschwimmen. Angriffe erfolgen zunehmend über kompromittierte Infrastrukturen in Drittstaaten, wodurch herkömmliche Abwehrmechanismen wie Geo-Blocking faktisch nutzlos werden.

Gleichzeitig verschärfen Konzentrationsrisiken in der digitalen Infrastruktur die Lage. Da nur wenige globale Cloud-Anbieter einen großen Teil der weltweiten Wertschöpfung tragen, wirken Angriffe auf diese Knotenpunkte wie ein Katalysator für massive Kaskadeneffekte. Der ECR 2026 verdeutlicht: Operative Resilienz existiert ohne belastbare Cyberresilienz nicht mehr.

Das technologische Wettrüsten

Ein zentraler Beschleuniger dieser Dynamik ist die künstliche Intelligenz (KI). Während KI-Systeme auf der defensiven Seite zur Erkennung eingesetzt werden, nutzen Angreifer sie, um DDoS-Kampagnen nahezu in Echtzeit zu orchestrieren und adaptive Laststeuerungen zu realisieren. Besonders kritisch ist, dass die Integration von KI-Systemen die eigene Angriffsfläche durch neue Verwundbarkeiten in Modellen und Daten erweitert. Es ist ein technologisches Wettrüsten entbrannt, das nicht mehr reaktiv beherrschbar ist.

Wer erst nach einem Angriff reagiert, hat bereits verloren – und das im Grunde in zweifacher Hinsicht, da die Wahrscheinlichkeit für Folgeattacken heute bei über 70 % liegt.

Im Report erfahren Sie im Detail:

1

Warum wir uns von der **„Peak-Abwehr“** hin zur Bewältigung tagelanger Dauerlasten entwickeln müssen.

2

Warum die **Herkunft als Filterkriterium** ausgedient hat und die verhaltensbasierte Analyse zum Standard wird.

3

Wie „Web Application & API Protection“ **schleichende Performance-Verluste** verhindert, die oft unterhalb der Alarmgrenzen unentdeckt bleiben..

DDoS im Strukturwandel: 2024 als Wendepunkt, 2025 als neue Realität

Das Jahr 2024 markierte einen klaren Wendepunkt in der globalen DDoS-Bedrohungslage. Mit einem Anstieg der Angriffe um 137 % gegenüber dem Vorjahr wurde deutlich, dass DDoS-Attacken nicht länger als seltene Ausnahmeszenarien betrachtet werden können. Die starke Zunahme war geprägt von einer hohen Dynamik: Es gab viele neue Angriffe, steigende Geschwindigkeiten und erste extreme Spitzen

+75%

2024 **2025**

Zunahme der DDoS-Angriffe im Link11-Netzwerk

Das Jahr 2025 knüpft an diese Entwicklung an, allerdings mit einer entscheidenden Verschiebung im Charakter der Bedrohung. Die Anzahl der Angriffe wächst zwar weiter, um 75 % im Vergleich zu 2024, jedoch nicht mehr explosionsartig, sondern strukturell. Das Angriffsniveau konsolidiert sich auf einem dauerhaft hohen Niveau. Das ist ein klares Signal: Nach der Eskalation im Jahr 2024 folgt im Jahr 2025 keine Entspannung, sondern die Etablierung eines neuen Normalzustands.

Während das Jahr 2024 noch stark durch einzelne Rekordereignisse und abrupte Peaks geprägt war, zeigt das Jahr 2025 über das Jahr hinweg eine deutlich höhere Gleichmäßigkeit der Angriffe. DDoS ist damit nicht länger ein kurzfristiges Krisenszenario, sondern entwickelt sich zu einem permanenten Risiko, das Planung, Budgetierung und Entscheidungen nachhaltig beeinflusst.

Entwicklung der Angriffsbandbreiten: Terabit ist kein Ausnahmefall mehr

Parallel zur Angriffsdauer ist auch bei den Bandbreiten eine deutliche Eskalation zu beobachten. Bereits das Jahr 2024 markierte einen Wendepunkt, als in Europa mit einem Angriff von 1,4 Tbit/s erstmals die Terabit-Schwelle überschritten wurde. Diese Zahl galt damals als Ausreißer, doch 2025 zeigt, dass sie den Beginn einer neuen Normalität markierte.

Die größte im Jahr 2025 abgewehrte Attacke erreichte eine Bandbreite von rund 1,33 Tbit/s, begleitet von mehr als 120 Millionen Paketen pro Sekunde. Damit lag sie nur knapp unter den bisherigen Rekordwerten und bestätigte die nachhaltige Verfügbarkeit enormer Angriffskapazitäten.

Zur Einordnung der Dimensionen: Diese Last entsprach pro Sekunde dem gleichzeitigen Transfer von über 3.300 einstündigen Podcasts oder dem parallelen Streaming von mehr als 16 UHD-Versionen der Extended Version der „Herr der Ringe"-Trilogie. Besonders relevant ist in diesem Zusammenhang, dass im Jahr 2025 gleich drei Angriffe mit einer Bandbreite von über einem Terabit pro Sekunde registriert wurden.

Im Vergleich zu 2024 verdeutlicht dies eine strategische Weiterentwicklung: Terabit-Angriffe waren zuvor eher seltene, hochgradig medienwirksame Einzelereignisse. Inzwischen etablieren sie sich zunehmend als wiederholendes Ereignis. Offensichtlich verfügen Angreifer über skalierbare Infrastrukturen, die es erlauben, solche Volumina nicht nur einmalig, sondern mehrfach abzurufen.

Größte DDoS-Kennzahlen in 2025

Volumen
262 TB

Bandbreite
1,3 TBIT/S

Pakete pro Sekunde
449 MIO

Parallel dazu verschiebt sich die Angriffslogik von reiner Volumengewalt hin zu koordinierten Präzisionsangriffen. Angreifer testen Schutzmechanismen systematisch, variieren Muster in Echtzeit und passen ihre Kampagnen dynamisch an beobachtete Abwehrreaktionen an. Der 1. März 2025, an dem 1.247 einzelne Angriffe innerhalb von 24 Stunden registriert wurden, verdeutlicht diese neue Qualität eindrucksvoll.

Für Unternehmen bedeutet das: Schutzmaßnahmen, die auf den „größten jemals gemessenen Angriff" ausgelegt sind, greifen zu kurz, wenn solche Extremwerte regelmäßig auftreten. Das Jahr 2025 zeigt eindeutig, dass die DDoS-Abwehr nicht mehr nur Spitzen abfedern muss, sondern dauerhaft hohe Lasten stabil verarbeiten können sollte. Von entscheidender Bedeutung ist die Fähigkeit, auch wiederholte Hochvolumenattacken ohne manuelle Eingriffe zu bewältigen. Das gilt besonders dann, wenn diese mit anderen Angriffstaktiken kombiniert werden.

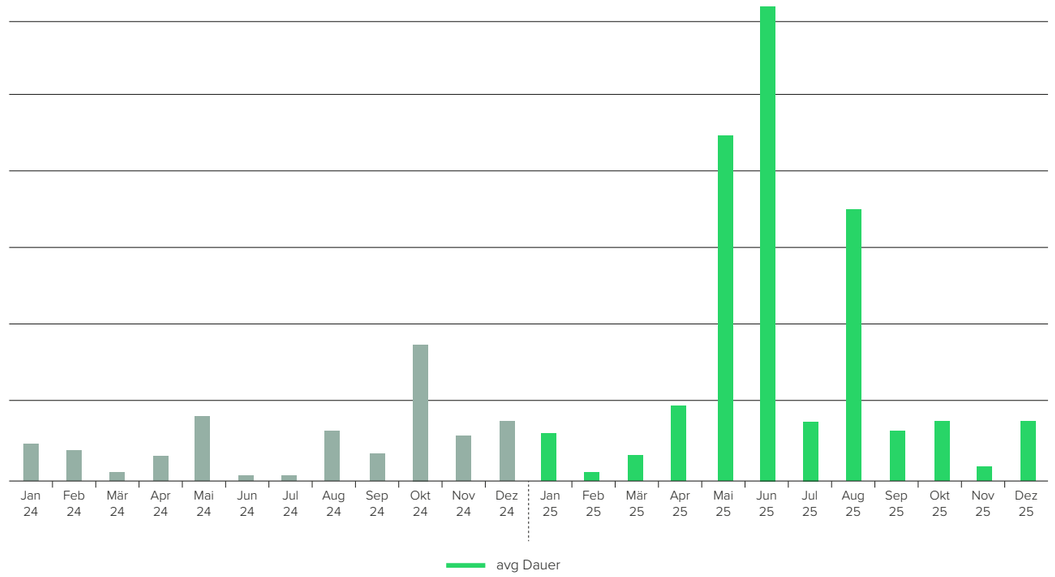
Entwicklung der Angriffsdauer: Von stundenlangen Störungen zu tagelanger Dauerbelastung

Die Analyse der Angriffsdauer im Link11-Netzwerk zeigt im Vergleich von 2024 und 2025 eine deutliche Verschiebung der Strategien der Angreifer: Während das Jahr 2024 von einem klaren Trend zu kürzeren, hochfrequenten Angriffen geprägt war, offenbaren die Zahlen aus dem Jahr 2025 eine neue Eskalationsstufe. Die Angreifer sind demnach wieder in der Lage, extrem langanhaltende DDoS-Attacken durchzuführen – allerdings unter veränderten Vorzeichen.

Im Jahr 2024 lag die längste mitigierte DDoS-Attacke bei 2.689 Minuten und stellte somit eine deutliche Reduktion gegenüber 2023 dar. Diese Entwicklung wurde damals als bewusste taktische Entscheidung interpretiert: Anstelle ressourcenintensiver Dauerangriffe setzten die Angreifer auf kurze, schnelle Störmanöver mit hoher Frequenz, um klassische Abwehrmechanismen zu überlasten.

2025 kehrt nun das Thema Angriffsdauer mit neuer Qualität zurück. Mit einer längsten registrierten Einzelattacke von 12.388 Minuten – also mehr als acht Tagen – wurde dieser Trend nicht nur gestoppt, sondern umgekehrt. Diese außergewöhnlich lange Dauer deutet darauf hin, dass Angreifer heute über deutlich stabilere Botnetze, eine bessere Orchestrierung und vor allem die Fähigkeit verfügen, Angriffe über lange Zeiträume unterhalb kritischer Schwellen aufrechtzuerhalten.

Durchschnittliche Angriffsdauer 2024 vs. 2025



Dauer der DDoS-Angriffe im Link11-Netzwerk

Längste Attacke 2024	**1,5** Tage	**2.689** Minuten
Längste Attacke 2025	**8** Tage	**12.388** Minuten
Gesamt 2025	**322** Tage	**464.971** Minuten

Noch gravierender ist jedoch die kumulierte Angriffszeit. Im Jahr 2025 war über alle Attacken hinweg 88 % der Zeit von aktiven DDoS-Angriffen geprägt. Das entspricht 322 Tagen oder 7.749 Stunden bzw. 464.971 Minuten unter Angriffslast. Damit ist der digitale Ausnahmezustand faktisch zum Normalzustand geworden. Es gibt keine klaren Ruhephasen mehr, sondern lediglich wechselnde Intensitätsstufen.

Auffällig ist dabei, dass die lange Angriffsdauer nicht zwangsläufig mit extremen Spitzenlasten einhergeht. Vielmehr handelt es sich häufig um anhaltenden, modulierten Druck auf Infrastruktur und Applikationen – ein Ansatz, der weniger Aufmerksamkeit erzeugt, jedoch operative Prozesse über Tage hinweg beeinträchtigt. Für Verteidiger bedeutet dies eine neue Herausforderung: Schutzmechanismen müssen nicht nur schnell reagieren, sondern auch über lange Zeiträume hinweg stabil und anpassungsfähig bleiben.

Dies bedeutet eine grundlegende Veränderung der operativen Realität. Incident-Response-Konzepte, die auf kurze Eskalationsphasen ausgelegt sind, stoßen bei tagelangen Angriffen an ihre Grenzen. DDoS-Angriffe werden somit nicht nur zu einer technischen, sondern auch zu einer organisatorischen Herausforderung.

Qualität und Ausdauer statt reiner Masse

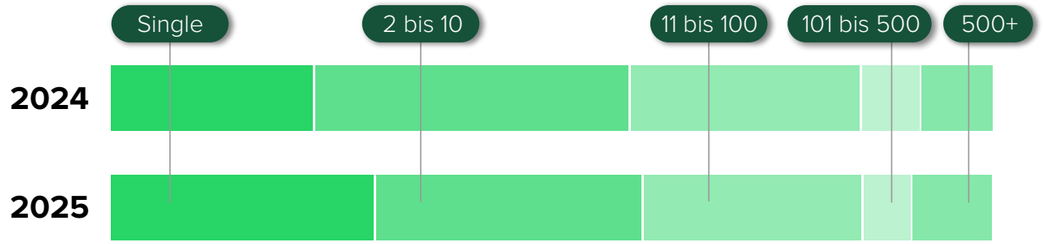
Die Kombination aus extremen Bandbreiten und außergewöhnlich langen Angriffsdauern verdeutlicht eine übergeordnete Entwicklung der Bedrohungslandschaft. Im Jahr 2025 verfolgen Angreifer nicht mehr ausschließlich das Ziel, maximale Spitzenlast zu erzeugen. Stattdessen kombinieren sie unterschiedliche Belastungsprofile, um Abwehrmechanismen systematisch zu testen und zu erschöpfen.

Im Vergleich zu 2024, als vor allem die hohe Frequenz kurzer Angriffe im Vordergrund stand, zeigt sich nun eine größere taktische Bandbreite. Kurze, schnelle Attacken bleiben zwar relevant, werden jedoch zunehmend von langanhaltenden Dauerbelastungen flankiert. Diese Hybridstrategie erhöht die operative Komplexität auf der Seite der Verteidiger erheblich und verschiebt den Fokus von der reinen Erkennung hin zur dauerhaften Resilienz.

Vom Einzelfall zur Serie

Eine weitere Erkenntnis des Jahresvergleichs ist die veränderte Angriffsdynamik auf Kundenebene. Im Jahr 2025 waren deutlich weniger Organisationen lediglich von einem einzelnen Angriff betroffen. Stattdessen wuchs der Anteil derer, die regelmäßig und mit hoher Frequenz angegriffen wurden.

Anzahl der DDoS-Angriffe pro Kunde



Besonders auffällig ist:

- Der Anteil der Kunden mit nur einem Angriff ging zurück.
- Alle Kategorien mit mehreren Angriffen nahmen zu.
- 8 % der Kunden waren 2025 vor mehr als 500 Angriffen geschützt

DDoS-Angriffe manifestieren sich damit nicht mehr als Ausnahme, sondern als dauerhafte Begleiterscheinung des digitalen Betriebs bestimmter Organisationen – mit unmittelbaren Auswirkungen auf Verfügbarkeit, Kosten und Betriebsstabilität. Das gilt besonders für exponierte Branchen und deren digitale Kerninfrastrukturen.

Diese Entwicklung macht deutlich: Während das Jahr 2024 noch stark von der Frage geprägt war, wie angegriffen wird, steht im Jahr 2025 zunehmend die Frage im Mittelpunkt, wie oft und wie dauerhaft Unternehmen betroffen sind.

Ein Angriff bleibt selten allein

Ein markanter Unterschied zwischen 2024 und 2025 liegt in der Wahrscheinlichkeit von Folgeangriffen.

- Konkret bedeutet dies, dass nach einem initialen Angriff im Durchschnitt 2,8 weitere Attacken folgen.
- Das entspricht einer Steigerung von rund 80 %.
- Die Wahrscheinlichkeit, erneut Ziel zu sein, liegt bei über 70 %.

Damit verändert sich die Angriffslogik grundlegend. DDoS-Angriffe werden nicht mehr als einzelner Störimpuls, sondern als Serie koordinierter Angriffe über einen längeren Zeitraum eingesetzt. Für betroffene Organisationen entsteht der Eindruck einer gezielten Belagerung mit permanentem Druck auf Verfügbarkeit, Personal und Entscheidungsfähigkeit.

Im Vergleich zu 2024 zeigt sich hier besonders deutlich, dass reaktive Schutzmaßnahmen nicht mehr ausreichen. Wer erst nach einem Angriff reagiert, ist 2025 bereits im Nachteil.

Resilienz als Daueraufgabe:
Was IT-Strategien jetzt leisten müssen

Ein direkter Vergleich der Jahre 2024 und 2025 zeichnet ein klares Bild: Während das Jahr 2024 als Jahr der Eskalation und der Rekorde in Erinnerung bleibt, steht das Jahr 2025 für die Normalisierung dieser Extremwerte.

Mehr Angriffe, längere Dauer, wiederholte Attacken und regelmäßig auftretende Terabit-Szenarien machen deutlich, dass DDoS kein operatives Randthema mehr ist. Für Entscheider ergeben sich daraus grundlegende strategische Konsequenzen:

- Resilienz wird zur Kernanforderung: Systeme müssen dauerhaft unter Angriff stabil bleiben.
- Automatisierung wird zwingend notwendig: Manuelle Reaktionen sind bei tagelangen Angriffen nicht skalierbar.
- Planungshorizonte verändern sich: DDoS-Abwehr ist keine temporäre Investition, sondern Teil der langfristigen IT-Strategie.

Der Vergleich der Jahre 2024 und 2025 zeigt somit nicht nur eine quantitative Verschärfung, sondern auch einen Paradigmenwechsel: DDoS ist nicht länger ein Ausnahmezustand, sondern eine dauerhafte Rahmenbedingung für die digitale Infrastruktur.

Geografische Muster von DDoS-Angriffen:
Was Herkunftsländer wirklich aussagen – und was nicht

Je professioneller DDoS-Angriffe durchgeführt werden, desto größer wird das Interesse an der geografischen Herkunft des Traffics. Dabei stellt sich regelmäßig die Frage, ob sich aus Länderzuordnungen konkrete Rückschlüsse auf Akteure, Motive oder Risiken ableiten lassen. Ein Vergleich der Jahre 2024 und 2025 zeigt: Die Antwort ist komplexer als auf den ersten Blick angenommen.

Bereits 2024 entfiel ein erheblicher Anteil der beobachteten DDoS-Angriffe auf wenige Länder mit stark ausgebauter digitaler Infrastruktur. Diese Verteilung setzte sich 2025 fort, verschob sich jedoch in Nuancen. Die USA bleiben das am häufigsten an Angriffen beteiligte Herkunftsland. Dies ist weniger Ausdruck politischer Motive, sondern vielmehr das Ergebnis einer hohen Dichte leistungsfähiger Infrastrukturen, großer Cloud-Umgebungen und zahlreicher kompromittierter Systeme, die als Teil von Botnetzen missbraucht werden.

Anteil am Angriffstraffic

Nr.	Land	Change
1	USA	-
2	Deutschland	2
3	UK	4
4	Frankreich	-2
5	Niederlande	5
6	Polen	-3
7	Italien	1
8	Singapur	13
9	Indien	-4
10	Spanien	3
11	Russland	11
12	Vietnam	-

Im Vergleich zeigt China ein anderes Profil: Die Anzahl der einzelnen Angriffe ist geringer, das von dort ausgehende Traffic-Volumen ist jedoch überdurchschnittlich hoch. Diese Diskrepanz verdeutlicht, dass die reine Häufigkeit von Angriffen wenig über deren tatsächliche Wirkung aussagt. Für IT-Entscheider ist vielmehr entscheidend, welche Last im Ernstfall auf die eigene Infrastruktur trifft.

Traffic Volumen

Nr.	Land	Change
1	China	-
2	USA	-
3	Deutschland	2
4	Russland	-1
5	Brasilien	1
6	Niederlande	10
7	Indien	2
8	Indonesien	-4
9	Frankreich	1
10	UK	4
11	Ukraine	-4
12	Bulgarien	13

Auffällig ist zudem die Entwicklung Russlands. Im Vergleich zu 2024 steigt 2025 die Zahl der von dort ausgehenden Angriffe, während das durchschnittliche Volumen pro Angriff geringer bleibt. Dieses Muster deutet auf eine hohe Anzahl koordinierter, aber technisch weniger massiver Angriffe hin, die insbesondere auf die Überlastung von Schutzmechanismen und Reaktionsprozessen abzielen.

Darüber hinaus rücken im Jahr 2025 Länder wie die Niederlande und Bulgarien stärker in den Fokus. Beide verfügen über leistungsfähige Hosting- und Transit-Infrastrukturen und werden immer häufiger als Ausgangspunkte für DDoS-Traffic genutzt.

Diese geografische Verschiebung unterstreicht, dass DDoS-Angriffe nicht an nationale Grenzen gebunden sind, sondern dort entstehen, wo Bandbreite, Rechenleistung und schlecht abgesicherte Systeme verfügbar sind.

Ein Vergleich der Jahre 2024 und 2025 macht somit deutlich: Die geografische Herkunft von Angriffen ist kein verlässlicher Indikator für Täter oder Motivation. Moderne DDoS-Angriffe sind hochgradig verteilt, international fragmentiert und von politischen Zuschreibungen technisch entkoppelt. Die Herkunftsländer spiegeln in erster Linie die Verfügbarkeit von Infrastruktur wider, nicht unbedingt geopolitische Intentionen.

Eine strategische DDoS-Abwehr sollte nicht ausschließlich auf Länder-Blocking oder einfache Geo-Filter setzen. Solche Maßnahmen greifen zu kurz und bergen das Risiko, legitimen Traffic zu beeinträchtigen. Effektiver Schutz erfordert eine globale, anbieterübergreifende Sicht auf Traffic-Muster sowie adaptive Mechanismen, die unabhängig von der geografischen Quelle reagieren können.

DDoS ist ein globales, strukturelles Phänomen. Wer es lokal oder national betrachtet, verkennt seine eigentliche Dynamik.

> *„DDoS-Angriffe sind heute keine seltenen Extremereignisse mehr, sondern eine permanente Hintergrundbelastung für digitale Infrastrukturen. Wer erst reagiert, wenn Systeme ausfallen, hat den Angriff bereits verloren. Moderne Resilienz beginnt daher lange vor der ersten Störung.“*



Karsten Desler, CTO

Warum kommt Geo-Blocking in einer verteilten Angriffslandschaft an seine Grenzen?

Lange als pragmatische Lösung geschätzt, verliert das Geo-Blocking im Jahr 2026 immer mehr seine Wirksamkeit. Der Hauptgrund dafür ist die Entkopplung von Angriff und geografischer Herkunft: Moderne DDoS-Kampagnen nutzen global verteilte Cloud-Plattformen und Content Delivery Networks (CDNs). Dadurch können Angreifer binnen Minuten Traffic aus dutzenden Ländern generieren – oft aus genau den Regionen, aus denen die legitimen Nutzer stammen.

Herkunftsländer spiegeln heute primär die Verfügbarkeit von Bandbreite und Rechenleistung wider, nicht den Standort der Akteure. Wer diese Infrastruktur-Knotenpunkte blockiert, gefährdet vor allem legitime Geschäftsbeziehungen. Da Layer-7-Angriffe zudem oft dieselben Netze wie regulärer Traffic nutzen, ist eine saubere technische Trennung ohne massive Einbußen der eigenen Erreichbarkeit unmöglich.

Angesichts steigender Dauer und Intensität ist DDoS kein punktuelles Ereignis mehr, sondern eine Dauerbelastung. Die moderne Abwehr sollte daher nicht nur auf der Herkunft, sondern auch auf dem Verhalten basieren: Anomalie-Erkennung und kontextbasierte Echtzeit-Analysen ersetzen starre Filter.

30 Jahre DDoS –

systemisches Geschäftsrisiko statt technischer Störung

1

1996–2000: Der Panix-DDoS-Angriff als Börsenthema

Als der New Yorker Internetprovider Panix im Jahr 1996 durch einen einfachen SYN-Flood rund 36 Stunden offline ging, wurde DDoS noch als technischer Zwischenfall betrachtet. Die Angriffe des sogenannten „Mafiaboy“ auf Yahoo, eBay und andere große Plattformen im Jahr 2000 machten jedoch deutlich, dass die Verfügbarkeit ein wirtschaftlicher Faktor ist. Analysten diskutierten erstmals öffentlich über DDoS als Risiko für Geschäftsmodelle – ein früher Vorbote dessen, was heute zur Normalität gehört.

2

2010er: IoT-Botnetze und neue Rekorde

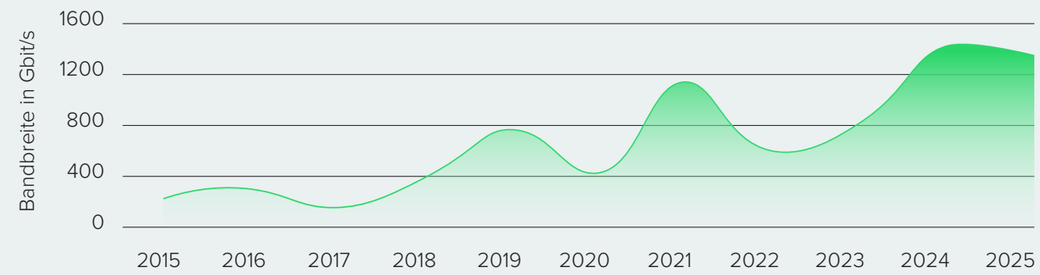
Anfang der 2010er-Jahre wurde mit Angriffen wie auf Spamhaus über den LINX-Knoten die 100-Gbit/s-Marke durchbrochen. Spätestens mit Mirai und dem Angriff auf Dyn, durch den große Teile des US-Internets, darunter Netflix, Twitter und GitHub, beeinträchtigt wurden, wurde klar: DDoS ist ein Massenphänomen. Hunderttausende unsicherer IoT-Geräte bildeten plötzlich globale Botnetze und zeigten damit die enge Verknüpfung zwischen technischem Fortschritt und neuen Angriffsflächen.

3

2020er: Terabit-Attacken, Hacktivismus und europäische Realität

In den 2020er-Jahren stellen Provider wie AWS, Azure und Cloudflare immer neue Rekorde im Terabit-Bereich auf. Gleichzeitig zeigen aktuelle europäische Daten, dass sich die Bedrohungslage weiter ausdifferenziert. Politisch motivierte DDoS-Attacken nehmen im Zuge geopolitischer Konflikte deutlich zu. Neben extremen Spitzenlasten nehmen vor allem lange, modulierte und koordinierte Angriffe zu. Verfügbarkeit wird damit zur Dauerbelastung und ist nicht mehr auf den Ausnahmezustand beschränkt .

Entwicklung der Bandbreite



	Typischer Wert	Bedeutung für das Business
Ausfallkosten / Stunde	ca. 50.000–250.000 €	Umsatzverluste, Vertragsstrafen, Supportaufwand
Vorfälle / Jahr	3–5 (bei exponierten Zielen deutlich mehr)	Wiederholte Betriebsunterbrechungen, Ressourcenbindung
Erkennungs- & Reaktionszeit	Sekunden bis Minuten	Entscheidet über Kundenerlebnis, SLAs und Reputation

Warum DDoS seit 30 Jahren funktioniert

Ein zentraler Grund für die anhaltende Wirksamkeit von DDoS-Angriffen liegt weniger in fehlender Technik als in den strukturellen Schwächen digitaler Infrastrukturen. Moderne Angriffe entstehen entweder aus wenigen, sehr leistungsfähigen Systemen oder aus einer kaum noch überschaubaren Masse kompromittierter Kleingeräte, insbesondere aus dem IoT-Umfeld. Jedes neu vernetzte Gerät vergrößert die Angriffsfläche. Ist es falsch konfiguriert oder nicht gepatcht, kann es Teil eines Botnetzes werden. So entsteht ein permanenter Nachschub an angreifbarer Infrastruktur, und DDoS erfindet sich mit jeder Technologiewelle neu.

Was heißt das konkret?

- Ist DDoS explizit im Business-Continuity- und Krisenhandbuch verankert (inklusive Kommunikationsplan)?
- Gibt es eine Always-on-Schutzlösung plus Notfall-Runbook für Eskalationen (ISP, Cloud, Spezialanbieter)?
- Werden reale DDoS-Szenarien regelmäßig geübt, einschließlich des Managements und der Fachbereiche?

Bis 2030 ist mit weiter steigenden Angriffszahlen und noch höheren Volumina zu rechnen. Unternehmen, die Verfügbarkeit nicht als eigene KPI im Risiko-Reporting berücksichtigen, unterschätzen das operative Risiko deutlich.

Web Application & API Protection

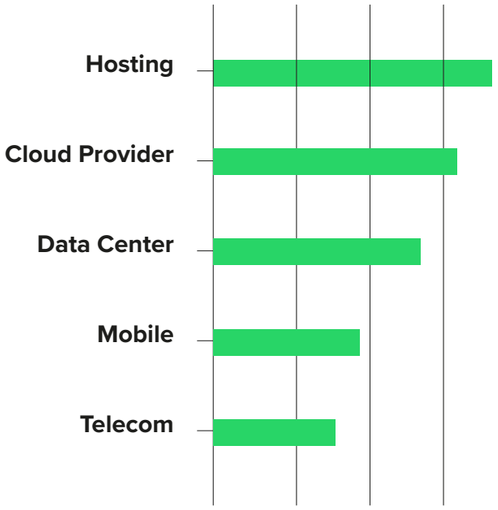
Weniger Lautstärke, mehr Wirkung

Webanwendungen und APIs sind heute zentrale Umsatz- und Wertschöpfungstreiber. Über sie werden Transaktionen abgewickelt, Services bereitgestellt und Kundenerlebnisse gestaltet. Genau deshalb stehen sie zunehmend im Fokus moderner Angriffe, allerdings nicht mehr mit dem Ziel, einen spektakulären Ausfall zu verursachen, sondern um digitale Geschäftsprozesse unauffällig zu beeinträchtigen.

Die Bedrohungslage hat sich dabei grundlegend verändert. Anstelle kurzer, lauter DDoS-Attacken treten nun Szenarien ein, die auf Ausdauer, Tarnung und betriebliche Wirkung ausgelegt sind. Die Angriffe operieren im Rahmen scheinbar normaler Nutzung, imitieren legitimes Verhalten und entfalten ihre Wirkung schrittweise. Die Performance sinkt, die Stabilität leidet und das Vertrauen erodiert – oft ohne dass ein klarer Sicherheitsalarm ausgelöst wird.

Angriffsinfrastruktur im Internet: Warum Cloud- und Hosting-Netze besonders häufig missbraucht werden

Eine zusätzliche Herausforderung ergibt sich aus der Infrastruktur, von der solche Angriffe ausgehen. Analysen der Netzwerkherkunft des Datenverkehrs zeigen deutliche Unterschiede zwischen verschiedenen Infrastrukturtypen. Während der Großteil des gesamten Internettraffics erwartungsgemäß aus klassischen Telekommunikationsnetzen stammt, findet sich eine besonders hohe Konzentration bösartiger Aktivitäten in Cloud- und Hosting-Infrastrukturen.



Der Grund liegt in der einfachen Verfügbarkeit dieser Ressourcen: Virtuelle Server lassen sich innerhalb weniger Minuten automatisiert starten und ebenso schnell wieder ersetzen. Angreifer können so kurzfristig Angriffsinfrastrukturen aufbauen und nach ihrer Nutzung wieder verschwinden lassen. Telekommunikations- oder Mobilfunknetze sind dagegen deutlich schwieriger zu missbrauchen, da hierfür zunächst reale Endgeräte kompromittiert werden müssten. Die Auswertung der Link11-Daten zeigt daher ein klares strukturelles Muster: Je einfacher sich Infrastruktur automatisiert bereitstellen lässt, desto höher ist typischerweise auch ihr Anteil an missbräuchlicher Nutzung.

Statt massiver Bandbreitenspitzen beobachten Organisationen heute:

- stark steigende Zahlen eindeutiger Clients ohne proportionalen Nutzwert,
- gezielte Ausnutzung ressourcenintensiver Endpunkte und
- globale oder regionale Botnetze mit realistisch wirkenden Identitäten sowie
- Low-and-Slow-Szenarien, die klassische Schwellenwerte nicht überschreiten.

Die Risiken sind erheblich. Anstelle klarer Ausfälle entstehen schleichende Service-Degradation, steigende Infrastruktur- und Betriebskosten sowie Umsatzverluste aufgrund abgebrochener Prozesse und sinkender Nutzerzufriedenheit. Besonders gefährlich ist dabei das trügerische Sicherheitsgefühl, wenn bestehende Schutzmechanismen keinen Vorfall melden, obwohl der Geschäftsbetrieb bereits beeinträchtigt ist.

Tarnung als legitime Bots oder warum Angreifer häufig Google imitieren

Ein häufig unterschätzter Bestandteil dieser Angriffe ist ihre gezielte Tarnung. Viele automatisierte Kampagnen versuchen nicht, vollständig unsichtbar zu bleiben, sondern imitieren bewusst legitime Bots. Besonders häufig geben sich Angreifer dabei als bekannte Suchmaschinen-Crawler aus. Analysen aus dem Link11-Netzwerk zeigen, dass rund 96 % des Traffics, der vorgibt, von einem Google-Bot zu stammen, tatsächlich gefälscht ist. Der Hintergrund ist pragmatisch: Viele Webseitenbetreiber lassen Suchmaschinen-Crawler bewusst ungefiltert passieren, um ihr Ranking nicht zu gefährden. Angreifer nutzen genau dieses Vertrauensmodell aus. Mit über 700.000 identifizierten Spoofing-Fällen im Link11-Netzwerk übertrifft der gefälschte Google-Bot-Traffic andere imitierte Bots – etwa von Facebook oder Amazon – deutlich. Diese Praxis verdeutlicht ein strukturelles Problem moderner Webinfrastrukturen: Vertrauensbasierte Ausnahmen können selbst zum Einfallstor für Angriffe werden.

96%

des eingehenden Traffics behaupten, von einem Google-Bot zu stammen.

Die folgenden drei Praxisbeispiele zeigen, warum „Web Application & API Protection“ (WAAP) heute weit mehr ist als eine reaktive Sicherheitsmaßnahme. Sie verdeutlichen, weshalb WAAP als operatives Steuerungsinstrument verstanden werden muss, das digitale Geschäftsprozesse schützt, stabilisiert und wirtschaftlich kalkulierbar hält.

> *„Was heute State of the Art ist, ist morgen ein ungepatchtes Legacy-System – und damit das nächste Problem.“*



Sean Power, Solution Engineer

Case Study 1 - Öffentlicher Sektor

Wenn mehr Besucher das System langsamer machen

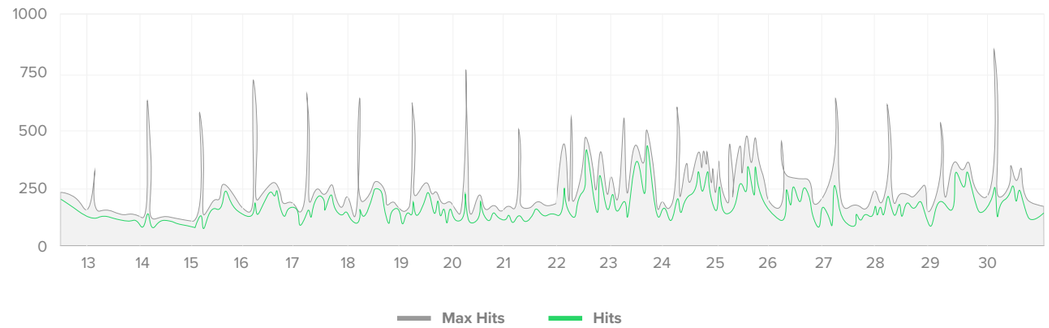
Technisch ergab sich jedoch ein anderes Bild. Weder die Anzahl der Requests noch die genutzte Bandbreite wuchsen proportional. Stattdessen verschlechterten sich die Antwortzeiten der Backend-Systeme sukzessive. Es kam zu Latenzspitzen und sporadischen Serverfehlern, ohne dass ein klarer Auslöser erkennbar war oder es zu erkennbaren Lastspitzen kam.

Die detaillierte Analyse des Anfrageverhaltens zeigte ein klar automatisiertes Muster. Die Clients riefen nahezu ausschließlich HTML-Ressourcen ab, verzichteten auf nachgeladene Inhalte und nutzten keine persistenten Sessions. Zwar waren viele Verbindungen kurzlebig, jedoch wurden sie in hoher Zahl parallel aufgebaut. Insgesamt entstand dadurch eine dauerhafte Belastung von CPU, Speicher und Connection-Handling auf den Origin-Systemen.

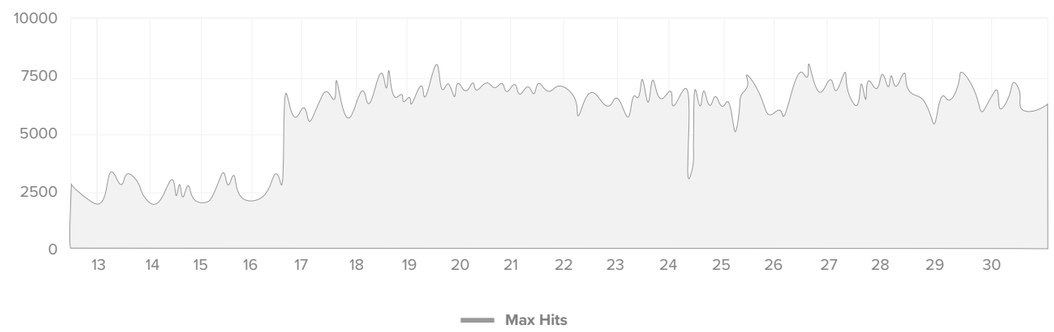
Aus geschäftlicher Sicht war dieser Angriff besonders kritisch, da er keinen Alarm auslöste. Es gab weder einen Ausfall noch eine massive Fehlerrate oder eine klare Angriffssignatur. Stattdessen litt die Plattform über einen längeren Zeitraum unter reduzierter Performance – ein Zustand, der im öffentlichen Umfeld schnell zu Vertrauensverlust, erhöhtem Supportaufkommen und politischem Druck führen kann.

Das Beispiel macht deutlich: Ohne verhaltensbasierte Analyse bleibt unklar, ob steigender Traffic tatsächlich einen Mehrwert erzeugt oder lediglich Ressourcen verbrennt.

Requests pro Tag



Eindeutige IPs pro Tag



Case Study 2 - Handelsplattform

Ein globales Botnetz als Belastungstest

Im zweiten Fall war eine internationale Handelsplattform Ziel eines klassischen, jedoch professionell orchestrierten Angriffs. Im Monitoring erschienen zwei massive Traffic-Spitzen in kurzer zeitlicher Folge. Bereits eine einzelne davon hätte ausgereicht, um eine ungeschützte Website lahmzulegen. Die größere Welle erreichte rund 16 Millionen Requests pro Minute bei einer Peak-Bandbreite von etwa 166 Gbit/s.

Auffällig war dabei nicht nur das Volumen, sondern auch die Art des Hochfahrens. Der Traffic stieg kontrolliert über mehrere Minuten hinweg an, statt schlagartig zu explodieren. Dieses Vorgehen deutet auf eine bewusste Erkundungsphase hin. Die Angreifer testeten, ob und wie schnell Schutzmechanismen greifen, bevor sie die volle Last freisetzten.

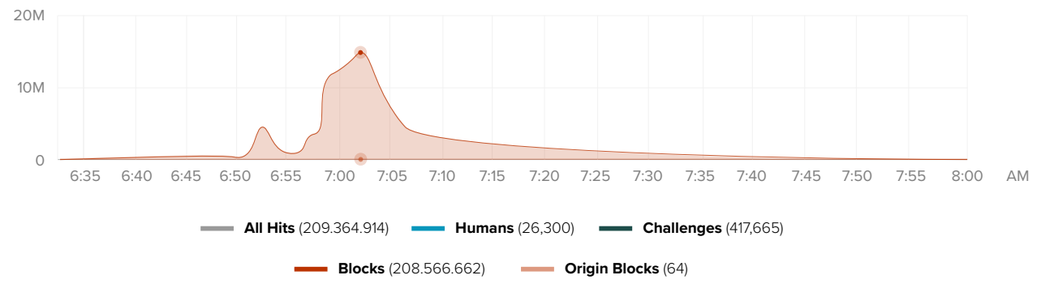
Die Herkunft der Anfragen war global verteilt. Tausende IP-Adressen aus unterschiedlichen Regionen – darunter zahlreiche Consumer-Netze großer Telekommunikationsanbieter – beteiligten sich an der Attacke. Dies spricht für ein gemischtes Botnetz aus kompromittierten Endgeräten und leistungsfähigen Servern oder Cloud-Instanzen.

Der eigentliche Schwachpunkt des Angriffs lag jedoch im Detail. Trotz der hohen Professionalität nutzten nahezu alle Bots identische User-Agent-Strings. Dieses scheinbar kleine Merkmal reichte aus, um den Traffic zuverlässig zu klassifizieren und zu blockieren. Die Plattform blieb erreichbar, die Latenz stabil und der Geschäftsbetrieb unbeeinträchtigt.

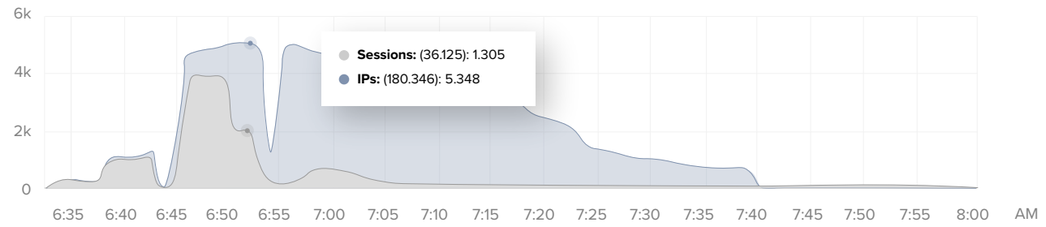
Strategisch zeigt dieser Fall zwei Dinge:

Zum einen wird deutlich, wie leistungsfähig und gut organisiert moderne Botnetze inzwischen sind. Zum anderen zeigt er, wie stark der Erfolg der Verteidigung von der Fähigkeit abhängt, Muster auf Anwendungsebene zu erkennen, und nicht an der reinen Bandbreite oder an IP-Listen. Für Handelsplattformen mit direktem Umsatzbezug ist diese Fähigkeit geschäftskritisch.

Durchgelassen vs. blockiert



Einmalige Sitzungen & IP



Case Study 3 - E-Commerce

Low-and-Slow mit echten Nutzern imitiert

Der dritte Fall veranschaulicht eine besonders schwer erkennbare Angriffsklasse. Bei einem großen europäischen Onlinehändler kam es über mehrere Wochen hinweg immer montags zu spürbaren Performance-Einbußen. Seiten luden langsamer und die Conversion-Rates sanken. Technisch ließ sich zunächst kein klassischer Angriff erkennen.

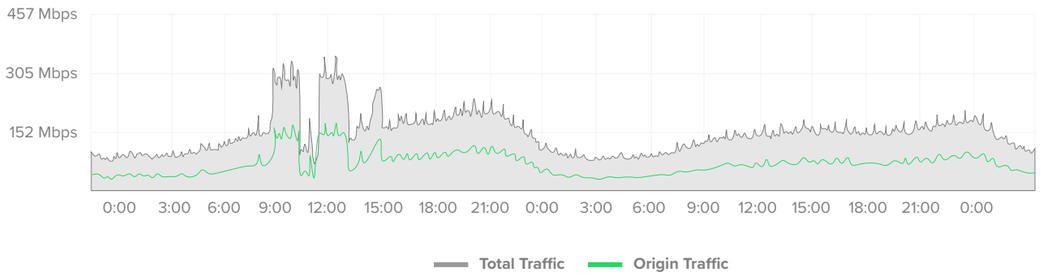
Die Volumen-Metriken blieben unauffällig. Erst eine zeitliche Korrelation zeigte, dass sich an diesen Tagen die Zahl der eindeutigen Clients nahezu verdoppelte, ohne begleitende Marketingaktionen oder externe Auslöser. Der Traffic stammte überwiegend aus Deutschland aus typischen Endkundennetzen mit realistischen Browser-Kennungen und technisch sauberem Verhalten.

Jede einzelne Quelle verursachte nur minimale Last. Doch die Verbindungen blieben ungewöhnlich lange offen und belasteten die Origin-Systeme zunehmend. Es handelte sich um einen typischen Low-and-Slow-Angriff mit einem entscheidenden Unterschied: Die Bots liefen auf echten, kompromittierten Endgeräten und verhielten sich nahezu wie menschliche Nutzer.

Erst ein kontrollierter Test mit global aktivierten CAPTCHAs brachte Klarheit. Innerhalb weniger Sekunden normalisierte sich die Last und der Großteil des Traffics verschwand. Für den Händler war dies der Beweis, dass es sich trotz scheinbarer Legitimität um automatisierte Prozesse handelte.

Der Business Impact war messbar. Langsame Ladezeiten führten zu Umsatzverlusten, obwohl nie ein klassischer Sicherheitsalarm ausgelöst worden war. Für den Betreiber war dies ein Weckruf: Verfügbarkeit allein reicht nicht aus, wenn Performance und Nutzererlebnis darunter leiden.

Angriffsvolumen in Mbit/s



Eindeutige Clients



Die Illusion der Legitimität:
Warum Traffic als Kennzahl heute trügerisch ist

Alle drei Beispiele folgen demselben Muster und markieren eine grundlegende Verschiebung in der Bedrohungslage für Webanwendungen und APIs. Entscheidend ist nicht mehr die Größe eines Angriffs, sondern seine Fähigkeit, sich nahtlos in scheinbar legitimen Traffic einzufügen. Moderne Angriffe setzen nicht auf Lautstärke, sondern auf Glaubwürdigkeit, Ausdauer und betriebliche Wirkung. Sie bleiben häufig unterhalb klassischer Alarmgrenzen und entfalten ihre Wirkung nicht innerhalb von Minuten, sondern über Tage oder Wochen hinweg.

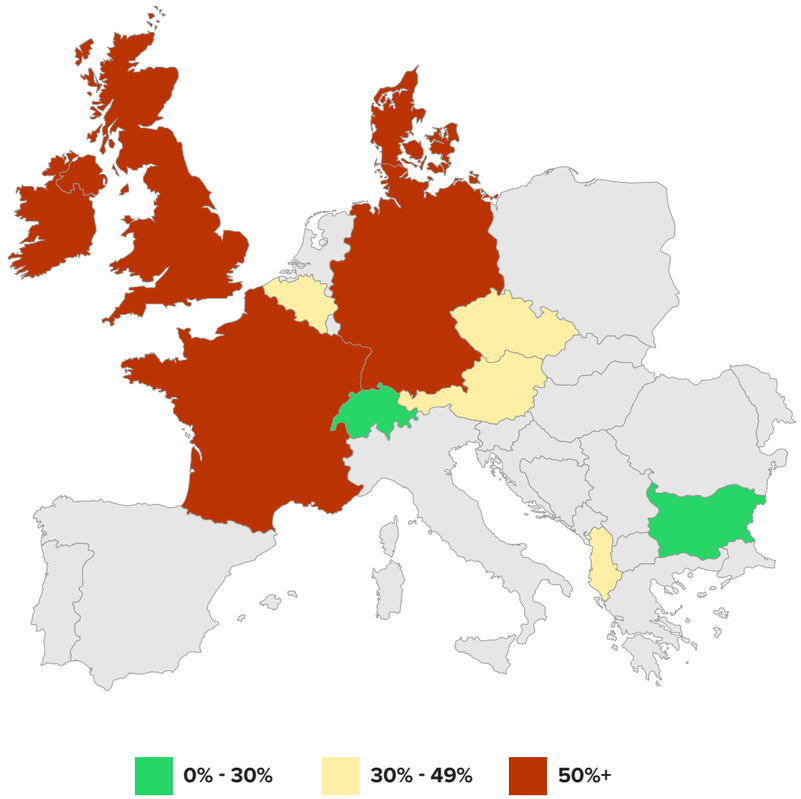
Damit verliert Traffic als isolierte Kennzahl seine Aussagekraft. Steigende Nutzerzahlen, globale Verteilung oder technisch saubere Protokolle sind heute kein verlässlicher Hinweis mehr auf echte Nachfrage oder legitime Nutzung. Im Gegenteil: Genau diese Merkmale werden gezielt instrumentalisiert, um Systeme schleichend zu belasten, Kosten zu treiben und die Performance zu degradieren, ohne dabei einen klaren Sicherheitsvorfall auszulösen.

Die geschäftlichen Risiken sind dabei erheblich. Anstelle klarer Ausfälle treten schleichende Service-Verschlechterungen, steigende Infrastruktur- und Betriebskosten ohne entsprechenden Mehrwert sowie Umsatzverluste durch langsame Ladezeiten, Abbrüche und eine sinkende Nutzerzufriedenheit auf. Besonders kritisch ist das trügerische Sicherheitsgefühl: Klassische Schutzmechanismen greifen nicht – und genau deshalb bleibt der Schaden oft lange unerkannt.

Bot-Aktivität in Europa

Auch die geografische Verteilung automatisierter Zugriffe zeigt, wie stark solche Angriffe inzwischen mit der Struktur digitaler Märkte verknüpft sind. In großen Internetmärkten wie Deutschland, Frankreich oder Großbritannien ist der Anteil automatisierter Bot-Aktivitäten deutlich höher als in kleineren europäischen Ländern. Dieses Muster lässt sich jedoch nicht allein mit der Zahl der Angreifer erklären.

Heatmap der Bot-Aktivitäten in Europa



Vielmehr spiegeln die Daten auch strukturelle Faktoren wider: Länder mit besonders großer digitaler Infrastruktur, vielen Rechenzentren und einer hohen Konzentration großer Onlineplattformen ziehen naturgemäß mehr automatisierten Traffic an – sowohl legitimen als auch schädlichen. Eine europäische Heatmap der Bot-Aktivitäten zeigt deshalb klare Cluster in Regionen mit besonders starker Internetnutzung und digitaler Wertschöpfung.

Die drei Fälle zeigen deutlich, warum „Web Application & API Protection“ (WAAP) nicht als reaktive Sicherheitsmaßnahme verstanden werden darf. WAAP ist ein operatives Steuerungsinstrument für digitale Geschäftsprozesse. Der eigentliche Mehrwert liegt nicht im Blockieren einzelner Angriffe, sondern in der Fähigkeit, legitimen Geschäftsverkehr zuverlässig von schädlicher Automation zu unterscheiden – in Echtzeit, kontextbezogen und über längere Zeiträume hinweg.

Aus strategischer Sicht verlagern sich Angriffe zunehmend von der Ebene der Infrastruktur auf die Anwendungsebene und von der reinen Überlastung hin zur gezielten Beeinflussung von Verfügbarkeit, Performance und Nutzererlebnis. Für IT- und Business-Entscheider bedeutet das eine Neubewertung: Web- und API-Sicherheit ist kein technisches Randthema mehr, sondern unmittelbar mit Umsatz, Reputation und Resilienz verknüpft.

WAAP ist deshalb eine klare Business-Entscheidung. Es entscheidet sich, ob digitale Services kalkulierbar, steuerbar und wirtschaftlich betrieben werden können oder ob sie zu einem dauerhaften Risiko werden, das erst dann sichtbar wird, wenn Vertrauen, Umsatz oder Marktposition bereits Schaden genommen haben.

> *„Die Größe eines Angriffs ist längst nicht mehr das entscheidende Kriterium. Erfolgreiche Angriffe sind heute subtil: Sie imitieren legitimen Traffic, bleiben unter klassischen Schwellenwerten und beeinträchtigen Systeme schleichend über Stunden oder Tage.“*



Jag Bains, VP Solution Engineering

Web Performance

DNS-Security: Warum die Integrität des Internets an der Namensauflösung hängt

DNS als Fundament und Angriffsziel digitaler Kommunikation

Kaum ein Protokoll ist so grundlegend für das Funktionieren des Internets und wurde zugleich so lange implizit als „vertrauenswürdig“ angenommen wie das Domain Name System (DNS). DNS übersetzt Domainnamen in IP-Adressen und ist somit der Einstiegspunkt für nahezu jede digitale Kommunikation. Webzugriffe, APIs, Cloud-Services und auch das E-Mail-Routing basieren auf DNS-Abfragen. Genau diese zentrale Rolle macht DNS zu einem strategischen Angriffsziel. Historisch wurde das Protokoll jedoch ohne eingebaute Authentifizierung entworfen. Eine Antwort gilt als korrekt, solange sie formal plausibel erscheint. Dadurch entstehen Angriffsmöglichkeiten für Manipulation, Umleitungen und Abhörangriffe, die massive Folgen für die Verfügbarkeit, Vertraulichkeit und das Vertrauen haben können.

Wenn Infrastrukturvertrauen missbraucht wird: Das strukturelle DNS-Problem

Dass es sich hierbei nicht um ein theoretisches Problem handelt, wurde unter anderem im Jahr 2014 deutlich, als Forscher der Carnegie Mellon University nachwiesen, dass E-Mails, die eigentlich über Server von Yahoo, Hotmail oder Gmail laufen sollten, über nicht autorisierte Mailserver umgeleitet wurden. Dabei wurde keine neue Zero-Day-Lücke ausgenutzt, sondern eine strukturelle Eigenschaft des DNS ausgenutzt: DNS prüft nicht von sich aus, ob eine Antwort wirklich von einem autoritativen Server stammt.

Wie spätere dem Akteur „Sea Turtle“[5] zugeschriebene Kampagnen zeigen, wird genau dieses Prinzip gezielt ausgenutzt. Das Ziel besteht darin, DNS-Auflösungen zu manipulieren und Verkehrsströme unbemerkt umzuleiten. In einer Welt, in der Angriffe zunehmend auf Manipulation, Umleitung und verdeckte Kontrolle statt auf reine Zerstörung setzen, wird diese fehlende Integrität zum systemischen Risiko.

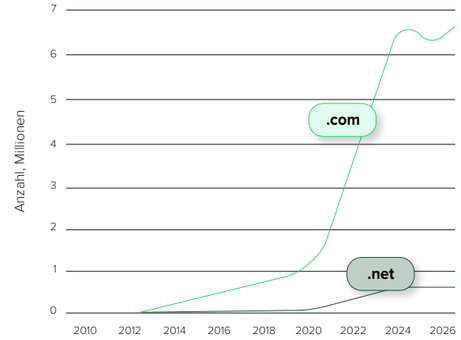
DNSSEC: Eine Vertrauensebene für ein historisch unsicheres Protokoll

Genau hier setzt DNSSEC (Domain Name System Security Extensions) an. DNSSEC ergänzt das bestehende DNS um eine Vertrauensebene, indem DNS-Antworten kryptografisch signiert werden. DNSSEC ermöglicht somit die Überprüfung, ob ein zurückgelieferter Eintrag tatsächlich vom zuständigen Nameserver stammt und unterwegs nicht verändert wurde. Dies geschieht technisch über digitale Signaturen (RRSIG), öffentliche Schlüssel (DNSKEY) und sogenannte Delegation-Signer-Einträge (DS). Sie bauen eine durchgehende Vertrauenskette von der Root-Zone über Top-Level-Domains bis zur einzelnen Domain auf. Die Root-Zone selbst wird in einer streng kontrollierten „Root Signing Ceremony“ signiert – ein bewusst transparent gestalteter Prozess, der das Fundament dieses globalen Vertrauensmodells bildet.

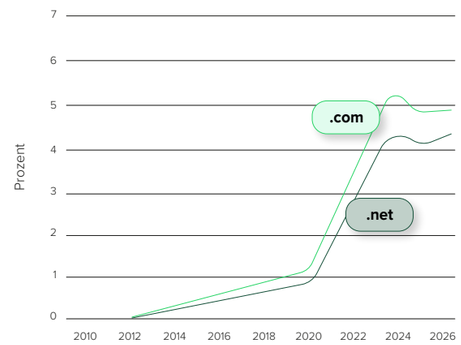
Domainnamen mit DS-Einträgen

Zwar nimmt die Verbreitung von DNSSEC kontinuierlich zu, doch insgesamt ist nach wie vor nur ein vergleichsweise kleiner Teil aller Domains tatsächlich durch DNSSEC geschützt.

Verbreitung von DNSSEC geschützter Domains



Anteil von DNSSEC geschützten Domains



Die Root Signing Ceremony

Das Domain Name System (DNS) fungiert als das Adressbuch des Internets. An dessen Spitze steht die Root-Zone, der Ausgangspunkt für jede Website-Anfrage weltweit. Um sicherzustellen, dass dieses „Adressbuch“ nicht manipuliert wird, findet regelmäßig ein hochgradig abgesicherter Prozess statt: die Root Signing Ceremony.

Warum ist das wichtig?

Ohne eine verifizierte Root-Zone könnten Angreifer DNS-Abfragen unbemerkt auf gefälschte Seiten umleiten. Bei der Zeremonie wird die Root-Zone mithilfe von DNSSEC (Sicherheitserweiterungen) mit einem digitalen Siegel versehen. Dieses Siegel garantiert weltweit die Authentizität und Integrität aller Internetadressen.

Der Prozess basiert auf dem „Mehr-Augen-Prinzip“.

Die Zeremonie ist kein bloßer Formalismus, sondern ein streng protokollierter Hochsicherheitsakt.

- Hochsicherheits-Standorte: Die Durchführung erfolgt in speziell gesicherten Rechenzentren unter Videoüberwachung und strikten Zutrittskontrollen.
- Internationale Treuhänder: Unabhängige Vertrauenspersonen aus aller Welt müssen physisch anwesend sein, um den Prozess zu autorisieren.
- Geteilte Schlüssel: Der kryptografische Hauptschlüssel ist physisch und digital auf verschiedene Systeme und Personen verteilt – niemand allein hat die volle Kontrolle.
- Totale Transparenz: Jeder Handgriff wird minutiös protokolliert und öffentlich nachvollziehbar dokumentiert.

Das Ergebnis ist eine lückenlose Vertrauenskette, die sicherstellt, dass eine Anfrage für „bank.de“ auch tatsächlich bei der echten Bank landet.

Integrität statt Illusion:
Was DNSSEC leistet und was nicht

Der sicherheitstechnische Mehrwert von DNSSEC ist klar: Zwar verhindert es keine DDoS-Angriffe und verschlüsselt auch keinen Traffic, aber es stellt sicher, dass Antworten nicht unbemerkt manipuliert werden können. Damit adressiert DNSSEC eine Klasse von Angriffen, die in klassischen Sicherheitsarchitekturen oft unerkannt bleiben.

Ohne DNSSEC lassen sich Angriffe auf die Namensauflösung kaum erkennen. Dazu zählen Cache-Poisoning-Angriffe, bei denen manipulierte DNS-Antworten in Zwischenspeichern landen und so ganze Nutzergruppen auf falsche Ziele umleiten, sowie Man-in-the-Middle-Angriffe, bei denen Antworten unterwegs verändert werden. Die Folge sind gezielte Umleitungen auf betrügerische oder schädliche Systeme, obwohl die URL unverändert und scheinbar korrekt bleibt.

Das Schutzmodell von DNSSEC wird durch Mechanismen wie NSEC und NSEC3 ergänzt. Diese machen auch die Nichtexistenz von Domains kryptografisch belegbar. Dadurch wird verhindert, dass Angreifer Nutzer durch gefälschte „Gibt es nicht“-Antworten täuschen oder gezielt von legitimen Diensten fernhalten. Gleichzeitig schließen diese Verfahren eine weitere, oft unterschätzte Schwachstelle: Ohne diese Schutzmechanismen könnten durch systematisches „Abklopfen“ des DNS-Namensraums – auch Domain Crawling genannt – vorhandene Subdomains und interne Strukturen abgeleitet werden. Genau diese Transparenz vergrößert die Angriffsfläche erheblich, da sie potenziellen Angreifern eine Art Lageplan der erreichbaren Dienste liefert. NSEC und NSEC3 begrenzen diese Informationslecks und reduzieren somit nicht nur die Manipulationsmöglichkeiten, sondern auch die strategische Vorbereitung von Angriffen.

DNS als verdeckter Angriffsvektor:
Tunneling, Command-and-Control und Missbrauch

Parallel dazu gewinnt DNS als Angriffs- und Exfiltrationskanal zunehmend an Bedeutung. Techniken wie DNS-Tunneling zeigen, dass DNS nicht mehr nur für die Namensauflösung, sondern auch für den verdeckten Transport von Daten oder die Steuerung von Malware genutzt wird. Für Sicherheitsverantwortliche wird DNS somit zu einem entscheidenden Beobachtungs- und Kontrollpunkt: Wer den DNS-Traffic nicht analysiert und absichert, lässt in seiner Sicherheitsarchitektur eine zentrale Schwachstelle bestehen.

Warum DNS-Security jetzt zur strategischen Pflicht wird

Warum gewinnt DNS-Security gerade jetzt an Relevanz? Erstens hängt das Überleben digitaler Geschäftsmodelle heute mehr denn je von durchgängiger Erreichbarkeit und korrekter Adressierung ab. Eine manipulierte Namensauflösung kann heute ganze Lieferketten, Plattformen oder Cloud-Ökosysteme treffen. Zweitens setzen Angriffe zunehmend auf subtile, schwer erkennbare Eingriffe, anstatt auf laute Ausfälle. Und drittens, weil die zunehmende Automatisierung und Skalierung von IT-Infrastrukturen Fehler und Fehlkonfigurationen vervielfacht. Was heute schnell ausgerollt wird, ist morgen oft ein ungepatchtes Legacy-Risiko – auch im DNS.

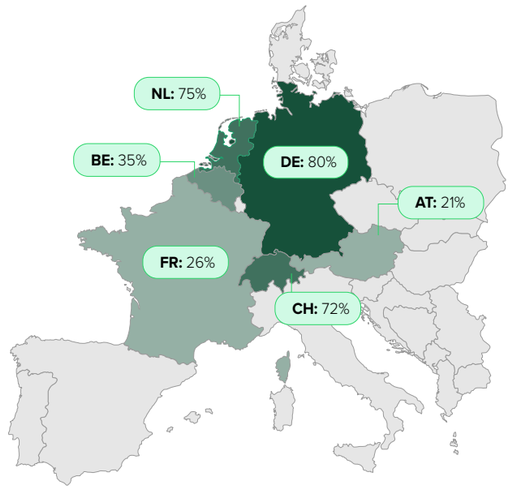
DNSSEC dient nicht nur der technischen Absicherung einzelner DNS-Abfragen, sondern stärkt grundsätzlich das Vertrauen in Internetdienste. Er sorgt dafür, dass Nutzer und Systeme sicher sein können, tatsächlich mit dem richtigen Server zu kommunizieren und nicht unbemerkt auf eine manipulierte oder umgeleitete Adresse weitergeleitet zu werden. Damit wird das Domain Name System erstmals überprüfbar und verlässlich, da Antworten nicht mehr unbemerkt verfälscht werden können. Die Internet Society[6] beschreibt DNSSEC deshalb nicht nur als Schutzmechanismus, sondern auch als wichtige Grundlage für zukünftige Sicherheitsfunktionen im Internet, die auf verlässlicher Namensauflösung basieren. Ein konkretes Beispiel dafür ist DANE (DNS-based Authentication of Named Entities)[7]: Dieses Verfahren nutzt DNSSEC-gesicherte DNS-Einträge, um kryptografische Informationen, etwa zu TLS-Zertifikaten, vertrauenswürdig zu verteilen. Dadurch wird das DNS-System vom reinen „Telefonbuch des Internets“ zu einem aktiven Vertrauensanker für weitere Sicherheitsprotokolle. Ohne DNSSEC fehlt diesen aufbauenden Mechanismen die notwendige Vertrauensbasis. Mit DNSSEC hingegen entsteht eine erweiterbare Sicherheitsarchitektur, die weit über die reine Absicherung der Namensauflösung hinausgeht.

DNSSEC als empfohlener Sicherheitsstandard

Nationale Sicherheitsbehörden wie das Bundesamt für Sicherheit in der Informationstechnik (BSI)[8] empfehlen DNSSEC ausdrücklich als Best-Practice-Maßnahme zur Absicherung der DNS-Infrastruktur. DNSSEC ist somit Teil einer ganzheitlichen Sicherheitsstrategie, die DNS-Server als kritische Infrastrukturkomponenten schützt und Manipulationen verhindert.

Gleichzeitig zeigen Umsetzungen und Studien, etwa zur DNSSEC-Unterstützung auf Seiten von Providern und in der Zugangsinfrastruktur, dass technische und organisatorische Hürden weiterhin bestehen. In der Regel erfolgt die DNS-Auflösung über Resolver von Internetanbietern oder großen Plattformbetreibern, die die Ergebnisse an die Endnutzer ausliefern. Das macht deutlich: DNS-Security kann nur dann wirksam skalieren, wenn alle Beteiligten im Ökosystem – Domaininhaber, Registrare, Provider und Plattformbetreiber – gemeinsam die Verantwortung für die Integrität und Validierung der Namensauflösung übernehmen.

DNSSEC-Validierungsrate nach Ländern (%)



Von der Grundfunktion zur Sicherheitskontrollschicht

Von der Grundfunktion zur Sicherheitskontrollschicht
Moderne DNS-Sicherheitsstrategien gehen über die reine Verfügbarkeit hinaus. Sie kombinieren DNSSEC zur Sicherung der Integrität mit Monitoring und Anomalie-Erkennung , um Missbrauch wie DNS-Tunneling zu verhindern, sowie proaktive Schutzmechanismen gegen volumetrische und logikbasierte Angriffe. Damit wird DNS vom „unsichtbaren Hilfsdienst“ zur sicherheitskritischen Kontrollschicht der digitalen Infrastruktur.

DNS-Security als Baustein für digitale Resilienz und Souveränität

Im Kontext der Mission, das Internet sicherer zu machen, ist DNS-Security keine optionale Zusatzfunktion mehr, sondern eine Grundvoraussetzung für Vertrauen im Netz. Verfügbarkeit ohne Integrität ist fragil und Integrität ohne Skalierbarkeit nicht zukunftsfähig. Die Absicherung der Namensauflösung ist somit nicht nur eine technische Maßnahme, sondern ein strategischer Baustein für digitale Souveränität, Resilienz und nachhaltiges Vertrauen in vernetzte Geschäftsmodelle.

„Ohne DNS-Integrität gibt es kein verlässliches Internet“



Lukas, warum gewinnt das Thema DNS-Integrität und DNSSEC gerade jetzt spürbar an Bedeutung?

DNS ist einer der grundlegendsten Bausteine des Internets und genau deshalb war es lange Zeit ein blinder Fleck in vielen Sicherheitsstrategien. Empfehlungen zu DNSSEC gibt es seit mehreren Jahren, auch von Behörden wie dem BSI. Was sich jetzt ändert, ist der Kontext: Digitale Geschäftsmodelle sind kritischer geworden, die Abhängigkeit von Online-Services steigt und die regulatorischen Anforderungen nehmen zu. Gleichzeitig sehen wir immer wieder Vorfälle, bei denen nicht die Anwendung selbst, sondern die zugrunde liegende Infrastruktur das Einfallstor war. In diesem Umfeld rückt die Frage nach der Vertrauenswürdigkeit der Namensauflösung zwangsläufig stärker in den Fokus.





Was leistet DNSSEC aus Management-Sicht, ohne zu tief in die Technik zu gehen?

Vereinfacht gesagt sorgt DNSSEC dafür, dass die digitalen Wegweiser im Internet verlässlich sind. Wenn ein Nutzer oder ein System nach einer Adresse fragt, stellt DNSSEC sicher, dass die Antwort tatsächlich von einer autoritativen Quelle stammt und nicht manipuliert wurde. Ohne diese Absicherung können Angreifer Nutzer unbemerkt umleiten, beispielsweise auf gefälschte Plattformen oder kompromittierte Systeme. DNSSEC ist somit keine Komfortfunktion, sondern eine grundlegende Maßnahme, um Vertrauen, Integrität und Verfügbarkeit digitaler Services abzusichern





Welche geschäftlichen Risiken entstehen, wenn Unternehmen auf DNSSEC verzichten?

Das größte Risiko besteht darin, dass Manipulationen unsichtbar bleiben. Angriffe wie „Cache Poisoning“, bei dem manipulierte Einträge in die Zwischenspeicher von DNS-Resolvern eingeschleust werden, oder betrügerische Umleitungen treffen nicht nur einzelne Nutzer. Sie können potenziell ganze Kundengruppen gleichzeitig betreffen. Die Folgen reichen von Reputationsschäden und Sicherheitsvorfällen bis hin zu massiven Betriebsunterbrechungen. Aus Unternehmenssicht ist das besonders kritisch, weil diese Art von Angriffen oft unterhalb der klassischen Sicherheitsradare stattfindet und gerade deshalb so wirksam ist.





Verschiedene Datensätze zeigen: Obwohl viele Netze DNSSEC prüfen könnten, ist nur ein kleiner Teil der Domains tatsächlich abgesichert. Woran liegt das?

Das ist ein typisches Muster bei der Sicherheit von Infrastrukturen. Die technische Basis ist oft vorhanden, aber für die Umsetzung sind Priorisierung, Ressourcen und klare Verantwortlichkeiten erforderlich. Bei DNSSEC kommt hinzu, dass Änderungen häufig sowohl beim DNS-Provider als auch beim Registrar koordiniert werden müssen. Alles, was keinen unmittelbaren Mehrwert liefert oder organisatorisch aufwendig ist, wird in Unternehmen gerne aufgeschoben. Gleichzeitig beobachten wir, dass gerade regulierte Branchen und der öffentliche Sektor hier schneller vorangehen, da die Compliance-Anforderungen den Handlungsdruck erhöhen.





Was ist deine klare Empfehlung an Entscheider, die Verfügbarkeit und Vertrauen ernst nehmen?

DNS sollte nicht länger als reines technisches Detail betrachtet werden, sondern als Teil der geschäftskritischen Vertrauenskette. Wer digitale Services betreibt, ist für deren Erreichbarkeit und Integrität verantwortlich. DNSSEC ist eine wirkungsvolle Grundlage dafür. Kurz gesagt: Ohne vertrauenswürdiges DNS gibt es keine verlässliche digitale Präsenz und genau deshalb gehört DNS-Integrität heute auf die Agenda von Organisationen, die Verfügbarkeit und Vertrauen ernst nehmen.



Fazit: Cyberresilienz wird zur strategischen Kernkompetenz

Die Analyse der aktuellen Daten zeigt deutlich, dass sich die Bedrohungslage im Cyberraum nicht nur quantitativ, sondern auch strukturell verändert. Angriffe werden häufiger, dauern länger und werden strategischer eingesetzt. Gleichzeitig verschiebt sich der Fokus von spektakulären Ausfällen hin zu gezielten Störungen digitaler Geschäftsprozesse.

Die wichtigsten Erkenntnisse des European Cyber Report 2026 auf einen Blick:

- Angriffe im Terabit Bereich werden von der Ausnahme zur Regel.
- Längster Angriff steigt von 1,5 auf 8 Tage im Jahresvergleich.
- Anzahl der Angriffe steigt um 75%, durchschnittliche Angriffsdauer steigt um 23,5 %.
- Geo-Blocking ist keine zeitgemäße Strategie mehr.
- DDoS erfindet sich auch nach 30 Jahren immer wieder neu.
- Angreifer-Bots tarnen sich als Google-Bots.
- DNS Security wird unterschätzt.

Diese Entwicklungen zeigen: Cyberangriffe sind schon lange nicht mehr nur technische Sicherheitsvorfälle, sondern operative Risiken für Umsatz, Reputation und Geschäftsmodelle. Entscheidend ist daher nicht nur die Fähigkeit, einzelne Angriffe abzuwehren, sondern auch, die digitale Infrastruktur dauerhaft resilient zu betreiben. Organisationen, die Cyberresilienz strategisch verankern, kombinieren eine belastbare Infrastruktur, automatisierte Schutzmechanismen und eine kontinuierliche Analyse des Datenverkehrs mit klaren Entscheidungs- und Krisenprozessen.

Der European Cyber Report 2026 soll dazu beitragen, diese Perspektive zu schärfen. Er versteht sich als Grundlage für Diskussionen, strategische Entscheidungen und den Austausch zwischen Sicherheitsexperten, IT-Verantwortlichen und der Unternehmensführung.

Denn eines wird immer deutlicher: Die Stabilität digitaler Infrastrukturen ist entscheidend für die Stabilität von Geschäftsmodellen. Wer heute systematisch Cyberresilienz aufbaut, schafft die Grundlage für nachhaltiges Vertrauen in die digitale Wirtschaft.

Ihr Ansprechpartner

Michael Scheffler
Vice President Sales

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



Nachweise

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

[2] 2026 Global Digital Trust Insights Survey: PwC

[3] Global Cybersecurity Outlook 2026 | World Economic Forum

[4] From Fragmentation to Trusted Growth: What Matters for Leaders in 2026

[5] Sea Turtle (Threat Actor)

[6] DNSSEC News, Guides and Tutorials - Internet Society

[7] DANE Grundlagen und Funktionsweise - LRZ Dokumentationsplattform

[8] BSI - Bundesamt für Sicherheit in der Informationstechnik - Umsetzung von DNSSEC

[S.21] https://www.verisign.com/resources/dnssec-tools/dnssec-scoreboard/

[S.23] https://stats.labs.apnic.net/dnssec

ACS - Allianz für Cyber-Sicherheit - ACS - Sichere Bereitstellung von DNS-Diensten v1.0



Hauptsitz

Link11 GmbH
Lindleystr. 12
60314 Frankfurt am Main