LINK11

EUROPEAN CYBER REPORT

2026

www.link11.com

Dear readers,

Digital infrastructure is now the backbone of almost all business models. Platforms, cloud services, APIs, and data-driven processes connect companies, customers, and partners. This level of networking creates great economic opportunities, but also dependencies.

Cybersecurity is therefore no longer just a technical issue, but also a strategic task. International studies show that cyber incidents are among the greatest business risks. At the same time, attacks are becoming more automated and coordinated, and are designed to have an operational impact.

This is particularly evident in DDoS attacks: what used to be considered isolated website disruptions is now a structural risk to value creation. Modern attack campaigns combine enormous bandwidths with high frequencies, long durations, and increasingly sophisticated camouflage mechanisms. In addition, many attacks are shifting from infrastructure to applications, APIs, and digital processes.

The „European Cyber Report 2026“ analyzes these changes based on real attack data from the Link11 network and the international cyber landscape. The aim is to make structural trends visible, as this is the only way to plan for resilience.

The key finding: cyber resilience does not arise at the moment of attack. It is the result of long-term architectural decisions, responsibilities, and continuous risk awareness.

The analyses and classifications in this report are intended to help you question and further develop your security strategy. Digital availability is a competitive factor. Securing it is a joint task for technology, organization, and leadership.

I hope you find this report insightful.

Herzliche Grüße
Jens-Philipp Jung, CEO, Link11



Contents

Executive Summary 04

DDoS in structural change 06

30 years of DDoS 12

Web Application & API Protection 14

Web Performance 21

Interview with Lukas Frank 24

Conclusion 26

Executive Summary

The new era of cyber resilience

In the global risk landscape of 2026, cybersecurity has finally transformed from a purely technical discipline into a critical core factor of corporate management. International analyses such as the „Allianz Risk Barometer 2026“i clearly show that, with 42% of mentions, cyber incidents rank first among global business risks across all industries. The fact that these are no longer abstract dangers is confirmed by the „PwC Digital Trust Insights 2026“.ii In Germany alone, 37% of companies have already reported losses of over one million US dollars per incident – an economic drain that is well above the global average.

The „new normal“ of the DDoS threat

The escalation documented in the current „European Cyber Report 2026“ (ECR 2026) fits seamlessly into this picture. What began in 2024 with an explosive 137% increase in the frequency of attacks on the Link11 network became the new normal in 2025. A further increase of 75% compared to the previous year shows that DDoS attacks are no longer isolated incidents, but rather represent a permanent basic load on digital infrastructures. Peak values of up to 1,247 attacks were recorded within just 24 hours (peak day: March 1, 2025).

The new quality and persistence of the attacks must be taken particularly seriously.

Breaking the terabit threshold: While the record value of 1.4 Tbit/s in 2024 was still an exception, terabit attacks became a recurring reality in 2025: **Three attacks exceeding the 1 Tbit/s mark were recorded.**

Extreme duration: The maximum attack duration multiplied from **2,689 minutes in 2024 to over 12,388 minutes in 2025.**

Systemic repetition: Repeat attacks show a **probability of over 70%** that companies will be targeted again. The risk today is serial in nature.

The cumulative volume makes the scale particularly impressive: a series of attacks on Record Attack reached 509 terabytes – a data volume equivalent to the daily data volume of a city with 120,000 habitants. With a maximum bandwidth of 1.3 Tbit/s, it is clear that bandwidth is no longer a limiting factor, but is being used by attackers as a strategic means of total overload.

Geopolitics and systemic cascade effects

This new reality of attack is inextricably linked to geopolitical volatility. Driven by geopolitical fragmentation, as described by the World Economic Forum (WEF),iii and the massive use of artificial intelligence on the part of attackers, the threat is shifting from the infrastructure level to the application level. As analyses by PwC and KPMGiv underscore, this new dynamic is forcing 92% of decision-makers to adapt their cyber strategies. The focus is no longer solely on selective defense, but rather on holistic, automated resilience.

State-tolerated actors use cyberattacks as a political tool, blurring national borders in the digital space. Attacks are increasingly carried out via compromised infrastructures in third countries, rendering conventional defense mechanisms such as geo-blocking virtually useless.

At the same time, concentration risks in digital infrastructure are exacerbating the situation. Since only a few global cloud providers account for a large share of global value creation, attacks on these hubs act as a catalyst for massive cascade effects. ECR 2026 makes it clear: operational resilience no longer exists without robust cyber resilience.

The technological arms race

A key accelerator of this dynamic is artificial intelligence (AI). While AI systems are used on the defensive side for detection, attackers use them to orchestrate DDoS campaigns in near real time and implement adaptive load control. What is particularly critical is that the integration of AI systems expands the attack surface through new vulnerabilities in models and data. A technological arms race has broken out that can no longer be controlled reactively.

Those who only react after an attack has occurred have already lost – especially since the probability of follow-up attacks is now over 70%.

In this report, you will learn in detail:

1. Why we need to move away from **„peak defense“** and toward managing continuous loads that last for days.
2. Why **origin as a filter criterion** has become obsolete and behavior-based analysis is becoming the standard.
3. How web application and API protection prevents **creeping performance losses** that often remain undetected below traditional alarm thresholds.

DDoS in structural change: 2024 as a turning point, 2025 as a new reality

The year 2024 marked a clear turning point in the global DDoS threat landscape. With a 137% increase in attacks compared to the previous year, it became evident that DDoS attacks can no longer be considered rare, exceptional scenarios. The sharp increase was characterized by high dynamics: there were many new attacks, increasing speeds, and the first extreme peaks.

+75%

2024 **2025**

Increase in DDoS attacks on the Link11 network

The year 2025 continued this trend, but with a decisive shift in the nature of the threat. The number of attacks continues to grow (up by 75% compared to 2024) but no longer explosively, rather structurally. The level of attacks is consolidating at a permanently high level. This is a clear signal: after the escalation in 2024, 2025 will not see a relaxation, but rather the establishment of a new normal.

While 2024 was still strongly characterized by individual record events and abrupt peaks, 2025 shows a significantly higher consistency of attacks throughout the year. DDoS is thus no longer a short-term crisis scenario, but is developing into a permanent risk that will have a lasting impact on planning, budgeting, and decision-making.

Development of attack bandwidths: Terabits are no longer an exception

Parallel to the duration of attacks, a significant escalation can also be observed in bandwidths. An attack of 1.4 Tbit/s in Europe exceeded the terabit threshold for the first time in 2024, making a significant turning point. At the time, this figure was considered an outlier, but 2025 shows that it marked the beginning of a new normal.

The largest attack mitigated in 2025 reached a bandwidth of around 1.33 Tbit/s, accompanied by more than 120 million packets per second. This was only slightly below the previous record values and confirmed the sustained availability of enormous attack capacities.

To put the dimensions into perspective, this load corresponded to the simultaneous transfer of over 3,300 one-hour podcasts per second or the parallel streaming of more than 16 UHD versions of the extended version of The Lord of the Rings trilogy. Particularly relevant in this context is the fact that in 2025, three attacks with a bandwidth of over one terabit per second were recorded.

Compared to 2024, this illustrates a strategic development: Terabit attacks were previously rare, highly media-effective isolated incidents. Now, they are increasingly becoming a recurring event. Attackers clearly have scalable infrastructures that allow them to access such volumes not just once, but multiple times.

Largest DDoS figures in 2025

Volume

262 TB

Bandwidth

1.3 TBIT/S

Packets per second

449 MIO

At the same time, the logic behind attacks is shifting from pure volume to coordinated precision attacks. Attackers systematically test protective mechanisms, vary patterns in real time, and dynamically adapt their campaigns to observed defensive responses. This is perhaps illustrated best by figures from March 1, 2025, when 1,247 individual attacks were recorded within 24 hours.

For companies, this means that protective measures designed for the „largest attack ever measured“ fall short when such extreme values occur regularly. The year 2025 clearly shows that DDoS defense no longer needs to cushion peaks, but should be able to handle high loads stably over the long term. The ability to cope with repeated high-volume attacks without manual intervention is crucial. This is especially true when these attacks are combined with other attack tactics.

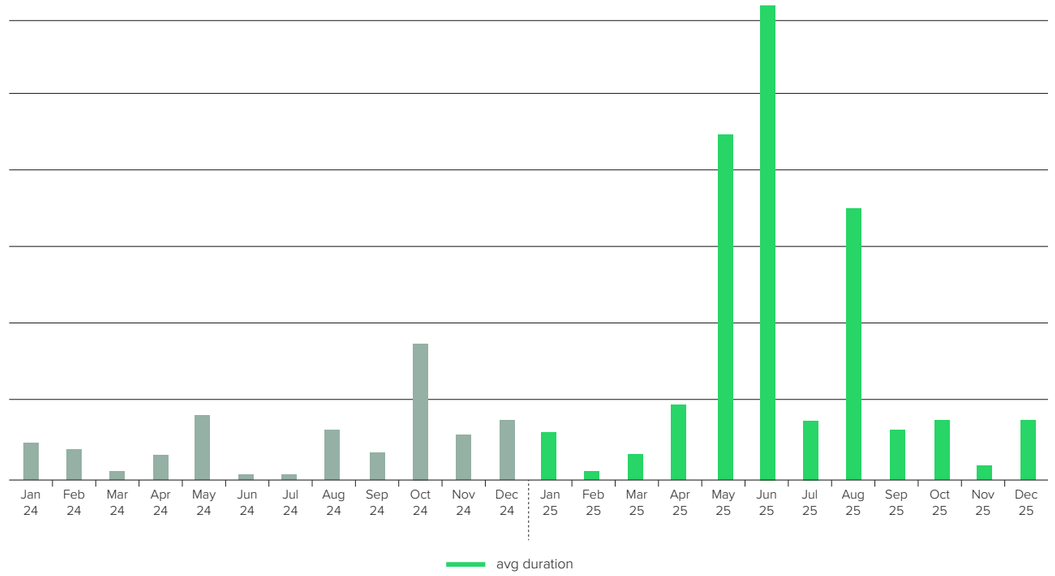
Development of attack duration: From hours-long disruptions to days-long continuous stress

Analysis of attack duration in the Link11 network shows a clear shift in attacker strategies between 2024 and 2025: While 2024 was characterized by a clear trend toward shorter, high-frequency attacks, the figures from 2025 reveal a new level of escalation. Attackers are once again capable of carrying out extremely long-lasting DDoS attacks – but under different circumstances.

In 2024, the longest mitigated DDoS attack lasted 2,689 minutes, representing a significant reduction compared to 2023. At the time, this development was interpreted as a deliberate tactical decision: instead of resource-intensive continuous attacks, attackers relied on short, fast disruption maneuvers with high frequency to overload classic defense mechanisms.

In 2025, the issue of attack duration is now returning with a new quality. With the longest recorded single attack lasting 12,388 minutes – more than eight days – this trend has not only been halted, but reversed. This exceptionally long duration indicates that attackers now have significantly more stable botnets, better orchestration, and, above all, the ability to sustain attacks below critical thresholds over much longer periods.

Average attack duration in 2024 vs. 2025



Duration of DDoS attacks on the Link11 network

Longest attack 2024	**1.5** Days	**2,689** Minutes
Longest attack 2025	**8** Days	**12,388** Minutes
Total 2025	**322** Days	**464,971** Minutes

Even more serious, however, is the cumulative attack time. In 2025, 88% of the time across all attacks was characterized by active DDoS attacks. This corresponds to 322 days, 7,749 hours, or 464,971 minutes under attack load. This means that the digital state of emergency has effectively become the norm. There are no longer any clear periods of calm, only varying levels of intensity.

It is striking that the long duration of attacks is not necessarily accompanied by extreme peak loads. Rather, it is often a case of sustained, modulated pressure on infrastructure and applications – an approach that attracts less attention but impairs operational processes over a period of days. For defenders, this presents a new challenge: protection mechanisms must not only respond quickly, but also remain stable and adaptable over long periods of time.

This represents a fundamental change in operational reality. Incident response concepts designed for short escalation phases reach their limits when attacks last for days. DDoS attacks are thus shifting from not only technical challenges, but also organizational ones.

Quality and endurance instead of pure mass

The combination of extreme bandwidths and exceptionally long attack durations highlights an overarching development in the threat landscape. In 2025, attackers no longer pursue the sole goal of generating maximum peak loads. Instead, they combine different load profiles to systematically test and exhaust defense mechanisms.

Compared to 2024, when the focus was primarily on high frequency, short attacks, there is now a greater tactical range. Short, fast attacks remain relevant, but are increasingly flanked by long-lasting continuous loads. This hybrid strategy significantly increases operational complexity on the defender's side and shifts the focus from pure detection to lasting resilience.

From isolated incidents to series

Another finding from the year-on-year comparison is the change in attack dynamics at the customer level. In 2025, significantly fewer organizations were affected by a single attack. Instead, the proportion of those who were attacked regularly and with high frequency grew.

Number of DDoS attacks per customer



Particularly striking is the fact that

- The proportion of customers with only one attack declined.
- All categories with multiple attacks increased.
- In 2025, 8% of customers were protected against more than 500 attacks within a year.

DDoS attacks are thus no longer an exception, but a permanent feature of the digital operations of certain organizations – with immediate implications for availability, costs, and operational stability. This is particularly true for exposed industries and their core digital infrastructures.

This development makes it clear that, while 2024 was still heavily influenced by the question of how attacks are carried out, the focus in 2025 is increasingly on how often and how permanently companies are affected.

An attack rarely stands alone

A striking difference between 2024 and 2025 lies in the probability of follow-up attacks.

- Specifically, this means that after an initial attack, an average of 2.8 further attacks follow.
- This corresponds to an increase of around 80%.
- The probability of being a target again after an attack is over 70%.

This fundamentally changes the logic of attacks. DDoS attacks are no longer used as a single disruptive impulse, but as a series of coordinated attacks over a longer period of time. For affected organizations, this creates the impression of a targeted siege with constant pressure on availability, personnel, and decision-making capabilities.

Compared to 2024, it is particularly clear that reactive protective measures are no longer sufficient. Those who only react after an attack will already be at a disadvantage in 2025.

Resilience as an ongoing task:
What IT strategies must now deliver

A direct comparison of 2024 and 2025 paints a clear picture: while 2024 will be remembered as a year of escalation and record highs, 2025 represents the normalization of these extreme values.

More attacks, longer duration, repeated attacks, and regularly occurring terabit scenarios make it clear that DDoS is no longer a marginal operational issue. This has fundamental strategic consequences for decision-makers:

- Resilience becomes a core requirement: Systems must remain stable under sustained attack.
- Automation becomes imperative: Manual responses are not scalable for attacks lasting several days.
- Planning horizons are changing: DDoS defense is not a temporary investment, but part of a long-term IT strategy.

A comparison of the years 2024 and 2025 thus shows not only a quantitative increase, but also a paradigm shift. DDoS is no longer an exceptional situation, but rather a permanent condition for digital infrastructure.

Geographic patterns of DDoS attacks: What countries of origin really say – and what they don‘t

The greater the number of professionally DDoS attacks that are carried out, the greater the interest in the geographical origin of the traffic. This regularly raises the question of whether country attributions allow concrete conclusions to be drawn about actors, motives, or risks. A comparison of the years 2024 and 2025 shows that the answer is more complex than it might appear at first glance.

As early as 2024, a significant proportion of the DDoS attacks observed were attributable to a few countries with highly developed digital infrastructure. This distribution continued in 2025, but shifted slightly. The US remains the country of origin most frequently involved in attacks. This is less a reflection of political motives and more the result of a high density of powerful infrastructures, large cloud environments, and numerous compromised systems that are misused as part of botnets.

Share of attack traffic

Nr.	Country	Change
1	USA	-
2	Germany	2
3	UK	4
4	France	-2
5	Netherlands	5
6	Poland	-3
7	Italy	1
8	Singapore	13
9	India	-4
10	Spain	3
11	Russia	11
12	Vietnam	-

In comparison, China shows a different profile: the number of individual attacks is lower, but the volume of traffic originating there is above average. This discrepancy illustrates that the sheer frequency of attacks says little about their actual impact. For IT decision-makers, what matters more is the load that will be placed on their own infrastructure in the event of an emergency.

Traffic volume

Nr.	Country	Change
1	China	-
2	USA	-
3	Germany	2
4	Russia	-1
5	Brazil	1
6	Netherlands	10
7	India	2
8	Indonesia	-4
9	France	1
10	UK	4
11	Ukraine	-4
12	Bulgaria	13

Russia‘s development is also striking. Compared to 2024, the number of attacks originating there increased in 2025, but the average volume per attack was lower. This pattern indicates a high number of coordinated but technically less massive attacks, which are aimed in particular at overloading protection mechanisms and response processes.

In addition, countries such as the Netherlands and Bulgaria come more into focus in 2025. Both have powerful hosting and transit infrastructures and are increasingly being used as starting points for DDoS traffic. This geographical shift underscores the fact that DDoS attacks are not bound by national borders, but originate wherever bandwidth, computing power, and poorly secured systems are available.

A comparison of 2024 and 2025 thus makes it clear that the geographical origin of attacks is not a reliable indicator of perpetrators or motivation. Modern DDoS attacks are highly distributed, internationally fragmented, and technically decoupled from political attributions. The countries of origin primarily reflect the availability of infrastructure, not necessarily geopolitical intentions.

Strategic DDoS defense should not rely exclusively on country blocking or simple geo-filtering. Such measures fall short and carry the risk of affecting legitimate traffic. Effective protection requires a global, cross-provider view of traffic patterns and adaptive mechanisms that can respond independently of the geographic source.

DDoS is a global, structural phenomenon. Viewing it locally or nationally fails to recognize its true dynamics.

> *“DDoS attacks are no longer rare extreme events, but a permanent background burden on digital infrastructures. If you only react when systems fail, you have already lost the attack. Modern resilience therefore begins long before the first disruption.”*



Karsten Desler, CTO

Why is geo-blocking reaching its limits in a distributed attack landscape?

Long valued as a pragmatic solution, geo-blocking is increasingly losing its effectiveness in 2026. The main reason for this is the decoupling of attacks from their geographical origin: modern DDoS campaigns use globally distributed cloud platforms and content delivery networks (CDNs). This allows attackers to generate traffic from dozens of countries within minutes – often from the very regions where legitimate users are located.

Today, countries of origin primarily reflect the availability of bandwidth and computing power, not the location of the actors. Blocking these infrastructure hubs primarily jeopardizes legitimate business relationships. Since Layer 7 attacks often use the same networks as regular traffic, a clean technical separation is impossible without massive losses in one‘s own accessibility.

Given the increasing duration and intensity, DDoS is no longer a one-off event, but a constant burden. Modern defense should therefore be based not only on origin, but also on behavior: anomaly detection and context-based real-time analysis are replacing rigid filters.

30 years of DDoS –

systemic business risk rather than technical disruption

1

1996–2000: The Panix DDoS attack as a stock market topic

When New York-based internet provider Panix went offline for around 36 hours in 1996 due to a simple SYN flood, DDoS was still considered a technical incident. However, the attacks by the so-called „Mafiaboy“ on Yahoo, eBay, and other major platforms in 2000 made it clear that availability is an economic factor. Analysts publicly discussed DDoS as a risk to business models for the first time – an early harbinger of what is now considered normal.

2

2010s: IoT botnets and new records

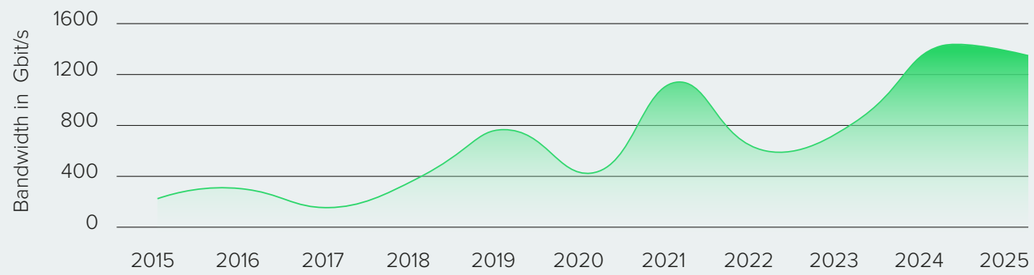
In the early 2010s, attacks such as those on Spamhaus via the LINX node broke the 100 Gbit/s mark. By the time Mirai and the attack on Dyn, which affected large parts of the US internet, including Netflix, Twitter, and GitHub, it became clear that DDoS was a mass phenomenon. Hundreds of thousands of unsecure IoT devices suddenly formed global botnets, demonstrating the close link between technological progress and new areas of vulnerability.

3

2020s: Terabit attacks, hacktivism, and European reality

In the 2020s, attacks on providers such as AWS, Azure, and Cloudflare are setting new records in the terabit range. At the same time, current European data shows that the threat situation is becoming more differentiated. Politically motivated DDoS attacks are increasing significantly in the wake of geopolitical conflicts. In addition to extreme peak loads, long, modulated, and coordinated attacks are on the rise. Availability is thus becoming a permanent burden and is no longer limited to exceptional circumstances.

Development of bandwidth



	Typical value	Significance for the business
Downtime costs/ hour	Approx. $50,000–$250,000	Loss of revenue, contractual penalties, support costs
Incidents per year	3–5 (significantly more for exposed targets)	Repeated operational interruptions, resource commitment
Detection & response time	Seconds to minutes	Determines customer experience, SLAs, and reputation

Why DDoS has been effective for 30 years

A key reason for the continued effectiveness of DDoS attacks relates less to a lack of technology and more to structural weaknesses in digital infrastructures. Modern attacks originate either from a few very powerful systems or from a barely manageable mass of compromised small devices, especially from the IoT environment. Every newly networked device increases the attack surface. If it is incorrectly configured or not patched, it can become part of a botnet. This creates a permanent supply of vulnerable devices, and DDoS reinvents itself with every wave of technology.

What does that mean specifically?

- Is DDoS explicitly anchored in the business continuity and crisis manual (including communication plan)?
- Is there an always-on protection solution plus an emergency runbook for escalations (ISP, cloud, specialist providers)?
- Are real DDoS scenarios practiced regularly, including management and specialist departments?

By 2030, the number of attacks is expected to continue to rise and volumes to increase even further. Companies that do not include availability as a separate KPI in their risk reporting are significantly underestimating the operational risk.

Web Application & API Protection

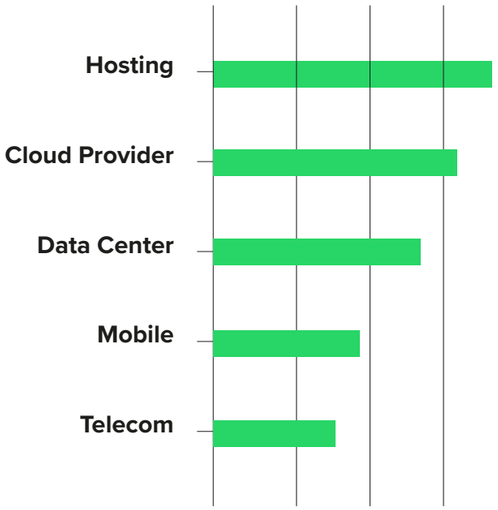
Less noise, more impact

Web applications and APIs are now key drivers of revenue and value creation. They are used to process transactions, provide services, and shape customer experiences. This is precisely why they are increasingly the focus of modern attacks, although the aim no longer to cause spectacular failure, but rather to discreetly disrupt digital business processes.

The threat landscape has changed fundamentally. Instead of short, loud DDoS attacks, we now see scenarios designed for endurance, camouflage, and operational impact. The attacks operate within the context of seemingly normal use, imitate legitimate behavior, and unfold their effects gradually. Performance declines, stability suffers, and trust erodes – often without triggering a clear security alarm.

Attack infrastructure on the Internet: Why cloud and hosting networks are particularly frequently abused

An additional challenge arises from the infrastructure where such attacks originate. Analysis of the network origin of data traffic shows clear differences between types of infrastructure. While the majority of all internet traffic originates from traditional telecommunications networks, as expected, there is a particularly high concentration of malicious activity in cloud and hosting infrastructures.



The reason for this is the easy availability of these resources: virtual servers can be started automatically within a few minutes and replaced just as quickly. Attackers can thus set up attack infrastructures at short notice and make them disappear again after use. Telecommunications or mobile networks, on the other hand, are much more difficult to misuse, as real end devices would first have to be compromised. The evaluation of Link11 data therefore shows a clear structural pattern: the easier it is to automatically provision infrastructure, the higher its share of misuse typically is.

Instead of massive bandwidth spikes, organizations today are seeing:

- a sharp increase in the number of unique clients without proportional utility,
- targeted exploitation of resource-intensive endpoints,
- global or regional botnets with realistic-looking identities, and
- low-and-slow scenarios that do not exceed classic thresholds.

The risks are considerable. Instead of clear failures, there is creeping service degradation, rising infrastructure and operating costs, and lost revenue due to interrupted processes and declining user satisfaction. Particularly dangerous is the false sense of security when existing protection mechanisms do not report an incident, even though business operations are already being affected.

Disguised as legitimate bots, or why attackers often imitate Google

A frequently underestimated component of these attacks is their targeted disguise. Many automated campaigns do not attempt to remain completely invisible, but deliberately imitate legitimate bots. In particular, attackers often pose as well-known search engine crawlers. Analysis from the Link11 network shows that around 96% of traffic that pretends to come from a Google bot is actually fake. The reason for this is pragmatic: many website operators deliberately allow search engine crawlers to pass through unfiltered so as not to jeopardize their ranking. Attackers, then, exploit precisely this model of trust. With over 700,000 identified cases of spoofing in the Link11 network, fake Google bot traffic significantly exceeds other imitated bots, such as those from Facebook or Amazon. This practice highlights a structural problem in modern web infrastructure: trust-based exceptions can themselves become a gateway for attacks.

The following three practical examples show why web application and API protection (WAAP) is now much more than a reactive security measure. They illustrate why WAAP must be understood as an operational control tool that protects and stabilizes digital business processes and keeps them economically predictable.

96%

of incoming traffic claim to originate from a Google bot.

„What is state of the art today is tomorrow‘s unpatched legacy system – and thus the next problem.“



Sean Power, Solution Engineer

Case Study 1 - Public sector

When more visitors slow down the system

The first case focuses on a web platform in the public sector. Its operators had observed an unusual increase in unique visits over a period of several weeks. At times, the number of unique IP addresses was more than twice as high as during normal operation. At the management level, this signal could easily have been interpreted as growing user interest.

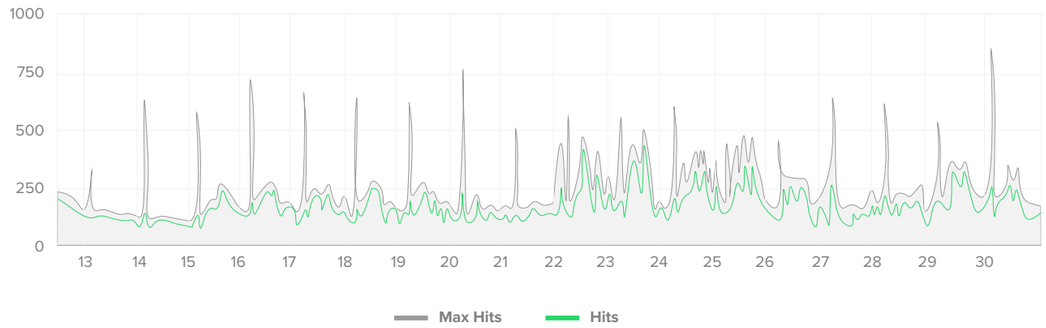
Technically, however, the picture was different. Neither the number of requests nor the bandwidth used grew proportionally. Instead, the response times of the backend systems gradually deteriorated. There were latency spikes and sporadic server errors without any clear trigger or noticeable load peaks.

A detailed analysis of the request behavior revealed a clear automated pattern. The clients retrieved almost exclusively HTML resources, did not reload content, and did not use persistent sessions. Although many connections were short-lived, they were established in large numbers in parallel. Overall, this resulted in a permanent load on the CPU, memory, and connection handling on the origin systems.

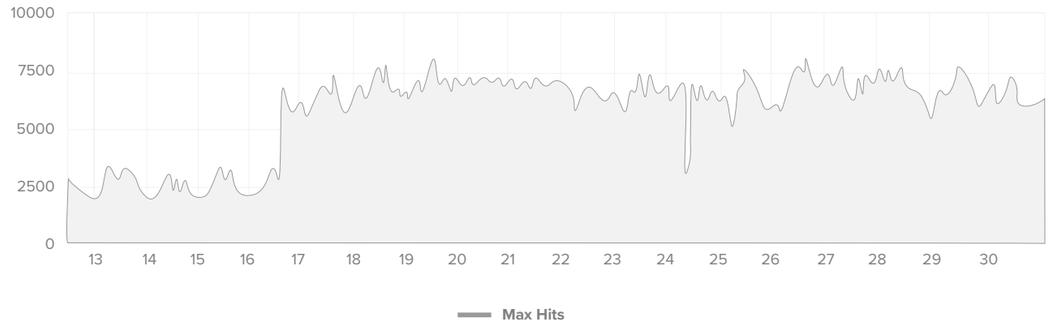
From a business perspective, this attack was particularly critical because it did not trigger any alarms. There was no outage, no massive error rate, and no clear attack signature. Instead, the platform suffered from reduced performance over a longer period of time – a situation that can quickly lead to a loss of trust, increased support requests, and political pressure in the public sector.

This example makes it clear that without behavior-based analysis, it remains unclear whether increasing traffic actually generates added value or merely burns resources.

Requests per day



Unique IPs per day



Case Study 2 - Trading platform

A global botnet as a stress test

In the second case, an international trading platform was the target of a classic but professionally orchestrated attack. Monitoring revealed two massive traffic spikes in quick succession. Even one of these would have been enough to cripple an unprotected website. The larger wave reached around 16 million requests per minute with a peak bandwidth of approximately 166 Gbit/s.

What was striking was not only the volume, but also the nature of the ramp-up. Traffic increased in a controlled manner over several minutes instead of exploding suddenly. This approach indicates a deliberate exploration phase. The attackers tested whether and how quickly protective mechanisms would take effect before unleashing the full load.

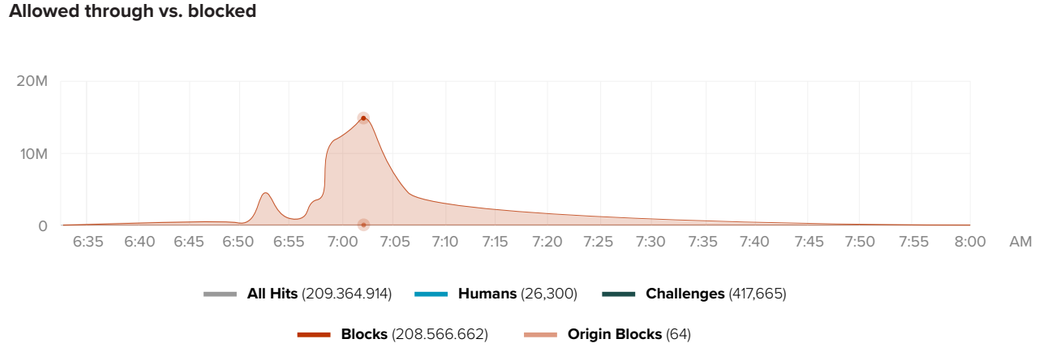
The origin of the requests was distributed globally. Thousands of IP addresses from different regions – including numerous consumer networks of large telecommunications providers – participated in the attack. This suggests a mixed botnet of compromised end devices and powerful servers or cloud instances.

However, the real weakness of the attack lay in the details. Despite the high level of professionalism, almost all bots used identical user agent strings. This seemingly minor feature was enough to reliably classify and block the traffic. The platform remained accessible, latency remained stable, and business operations were unaffected.

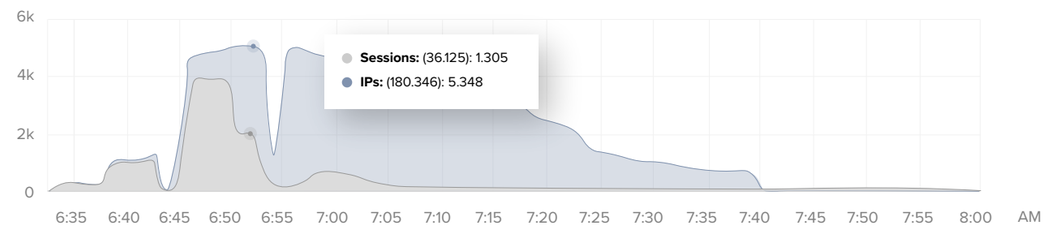
Strategically, this case shows two things:

On the one hand, it highlights how powerful and well-organized modern botnets have become. On the other hand, it shows how much the success of defense depends on the ability to recognize patterns at the application level, rather than on pure bandwidth or IP lists. For trading platforms with a direct link to revenue, this difference is business-critical.

Allowed through vs. blocked



Einmalige Sitzungen & IP



Case Study 3 - E-Commerce

low-and-slow imitated with real users

The third case illustrates a particularly difficult-to-detect class of attack. A large European online retailer experienced noticeable performance losses every Monday for several weeks. Pages loaded more slowly and conversion rates declined. Technically, no classic attack could be detected at first.

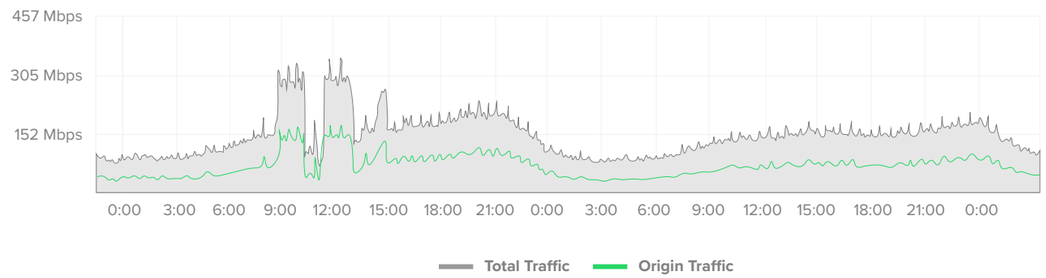
The volume metrics remained unremarkable. Only a temporal correlation showed that on these days, the number of unique clients nearly doubled without accompanying marketing campaigns or external triggers. The traffic came predominantly from Germany and consisted of typical end-customer networks with realistic browser identifiers and technically clean behavior.

Each individual source caused only minimal load. However, the connections remained open for an unusually long time and increasingly burdened the origin systems. It was a typical low-and-slow attack with one crucial difference: the bots ran on real, compromised end devices and behaved almost like human users.

Only a controlled test with globally activated CAPTCHAs provided clarity. Within seconds, the load normalized and most of the traffic disappeared. For the retailer, this was proof that, despite their apparent legitimacy, these were automated processes.

The business impact was measurable. Slow loading times led to lost sales, even though no classic security alarm had ever been triggered. For the operator, this was a wake-up call: availability alone is not enough if performance and user experience suffer as a result.

Attack volume in Mbit/s



Unique clients



The illusion of legitimacy:
Why traffic as a metric is now misleading

All three examples follow the same pattern and mark a fundamental shift in the threat landscape for web applications and APIs. It is no longer the size of an attack that matters, but its ability to blend seamlessly into seemingly legitimate traffic. Modern attacks rely not on volume, but on credibility, persistence, and operational impact. They often remain below traditional alarm thresholds and unfold their effects not within minutes, but over days or weeks.

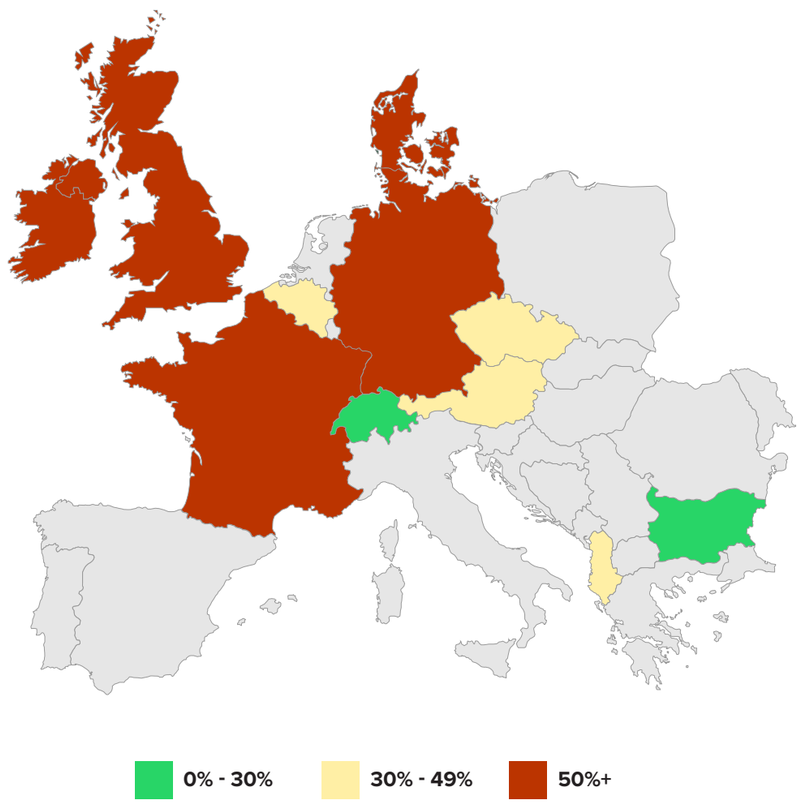
This means that traffic as an isolated metric loses its significance. Rising user numbers, global distribution, or technically clean protocols are no longer a reliable indication of genuine demand or legitimate use. On the contrary, it is precisely these characteristics that are deliberately exploited to gradually overload systems, drive up costs, and degrade performance without triggering a clear security incident.

The business risks involved are considerable. Instead of clear failures, there are creeping service deteriorations and rising infrastructure and operating costs without corresponding added value, and revenue losses due to slow loading times, interruptions, and declining user satisfaction. Particularly critical is the deceptive sense of security: traditional protection mechanisms do not work – and that is precisely why the damage often remains undetected for a long time.

Bot activity in Europe

The geographical distribution of automated access also shows how closely such attacks are now linked to the structure of digital markets. In large internet markets such as Germany, France, and the UK, the proportion of automated bot activity is significantly higher than in smaller European countries. However, this pattern cannot be explained solely by the number of attackers.

Heat map of bot activity in Europe



Rather, the data also reflects structural factors: Countries with particularly large digital infrastructures, many data centers, and a high concentration of large online platforms naturally attract more automated traffic – both legitimate and malicious. A European heat map of bot activity therefore shows clear clusters in regions with particularly high internet usage and digital value creation.

These three cases clearly show why web application and API protection (WAAP) should not be viewed as a reactive security measure. WAAP is an operational control tool for digital business processes. The real added value lies not in blocking individual attacks, but in the ability to reliably distinguish legitimate business traffic from malicious automation – in real time, contextually, and over extended periods.

From a strategic perspective, attacks are increasingly shifting from the infrastructure level to the application level and from pure overload to targeted manipulation of availability, performance, and user experience. For IT and business decision-makers, this means a reassessment: web and API security is no longer a marginal technical issue, but is directly linked to revenue, reputation, and resilience.

WAAP is therefore a clear and favorable business decision. It determines whether digital services can be operated in a predictable, controllable, and economical manner, or whether they become a permanent risk that only becomes apparent once trust, revenue, or market position have already been damaged.

„The size of an attack is no longer the decisive criterion. Successful attacks today are subtle: they imitate legitimate traffic, remain below classic thresholds, and insidiously compromise systems over hours or days.“



Jag Bains, VP Solution Engineering

Web Performance

DNS security: Why the integrity of the internet depends on name resolution

DNS as the foundation and target of digital communication

Hardly any other protocol is as fundamental to the functioning of the internet or is implicitly assumed to be „trustworthy“ for as long as the Domain Name System (DNS). DNS translates domain names into IP addresses and is therefore the entry point for almost all digital communication. Web access, APIs, cloud services, and even email routing are based on DNS queries. It is precisely this central role that makes DNS a strategic target for attack. Historically, however, the protocol was designed without built-in authentication. A response is considered correct as long as it appears formally plausible. This creates opportunities for manipulation, redirection, and eavesdropping attacks, which can have massive consequences for availability, confidentiality, and trust.

When infrastructure trust is abused:
The structural DNS problem

That this is not a theoretical problem became clear in 2014 when, among other things, researchers at Carnegie Mellon University demonstrated that emails that were supposed to run through Yahoo, Hotmail, or Gmail servers were being redirected through unauthorized mail servers. This did not exploit a new zero-day vulnerability, but rather a structural feature of the DNS: DNS does not check on its own whether a response really comes from an authoritative server.

As later campaigns attributed to the actor „Sea Turtle“v show, this principle is being exploited in a targeted manner. The goal is to manipulate DNS resolutions and redirect traffic flows unnoticed. In a world where attacks increasingly rely on manipulation, redirection, and covert control rather than pure destruction, this lack of integrity becomes a systemic risk. .

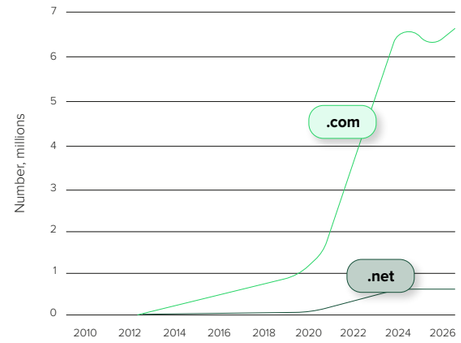
DNSSEC: A layer of trust for a historically insecure protocol

This is precisely where DNSSEC (Domain Name System Security Extensions) comes in. DNSSEC adds a layer of trust to the existing DNS by cryptographically signing DNS responses. DNSSEC thus makes it possible to verify whether a returned entry actually originates from the responsible name server and has not been altered en route. Technically, this is done using digital signatures (RRSIG), public keys (DNSKEY), and so-called delegation signer records (DS). They establish a continuous chain of trust from the root zone through top-level domains to individual domains. The root zone itself is signed in a strictly controlled „root signing ceremony“ – a deliberately transparent process that forms the foundation of this global trust model.

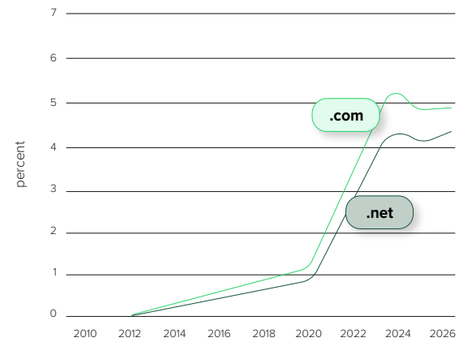
Domain names with DS entrie

Although DNSSEC is becoming increasingly widespread, overall only a relatively small proportion of all domains are actually protected by DNSSEC.

Distribution of DNSSEC-protected domains



Percentage of domains protected by DNSSEC



The Root Signing Ceremony

The Domain Name System (DNS) acts as the address book of the internet. At its top is the root zone, the starting point for every website request worldwide. To ensure that this „address book“ is not manipulated, a highly secure process takes place regularly: the Root Signing Ceremony.

Why is this important?

Without a verified root zone, attackers could redirect DNS queries to fake sites without being noticed. During the ceremony, the root zone is digitally sealed using DNSSEC (security extensions). This seal guarantees the authenticity and integrity of all internet addresses worldwide.

The process is based on the „multiple eyes principle.“

The ceremony is not a mere formality, but a strictly protocoled high-security act.

- High-security locations: The ceremony takes place in specially secured data centers under video surveillance and strict access controls.
- International trustees: Independent trustees from around the world must be physically present to authorize the process.
- Shared keys: The cryptographic master key is physically and digitally distributed across different systems and individuals – no one person has full control.
- Total transparency: Every step is meticulously logged and publicly documented in a traceable manner.

The result is a seamless chain of trust that ensures that a request for „bank.com“ actually ends up at the real bank.

Integrity instead of illusion:
What DNSSEC does and does not do

The security benefits of DNSSEC are clear: While it does not prevent DDoS attacks or encrypt traffic, it ensures that responses cannot be manipulated without being noticed. DNSSEC thus addresses a class of attacks that often go undetected in traditional security architectures.

Without DNSSEC, attacks on name resolution are almost impossible to detect. These include cache poisoning attacks, in which manipulated DNS responses end up in caches and thus redirect entire user groups to false targets, as well as man-in-the-middle attacks, in which responses are altered en route. The result is targeted redirection to fraudulent or malicious systems, even though the URL remains unchanged and appears to be correct.

The DNSSEC protection model is supplemented by mechanisms such as NSEC and NSEC3. These also make the non-existence of domains cryptographically verifiable. This prevents attackers from deceiving users with fake „does not exist“ responses or deliberately keeping them away from legitimate services. At the same time, these procedures close another, often underestimated vulnerability: without these protection mechanisms, existing subdomains and internal structures could be deduced by systematically „scanning“ the DNS namespace – also known as domain crawling. It is precisely this transparency that significantly increases the attack surface, as it provides potential attackers with a kind of map of the accessible services. NSEC and NSEC3 limit these information leaks and thus reduce not only the possibilities for manipulation, but also the strategic preparation of attacks.

DNS as a covert attack vector: Tunneling, command-and-control, and abuse

At the same time, DNS is becoming increasingly important as a channel for attacks and exfiltration. Techniques such as DNS tunneling show that it is no longer used only for name resolution, but also for the covert transport of data or the control of malware. For security managers, DNS is thus becoming a crucial observation and control point: those who do not analyze and secure DNS traffic leave a central vulnerability in their security architecture.

Why DNS security is now becoming a strategic imperative

Why is DNS security becoming more relevant now? First, the survival of digital business models depends more than ever on consistent accessibility and correct addressing. Manipulated name resolution can now affect entire supply chains, platforms, or cloud ecosystems. Secondly, attacks increasingly rely on subtle, difficult-to-detect intrusions rather than loud failures. And thirdly, the increasing automation and scaling of IT infrastructures multiplies errors and misconfigurations. What is rolled out quickly today is often an unpatched legacy risk tomorrow – even in DNS.

DNSSEC not only serves to technically secure individual DNS queries, but it also fundamentally strengthens trust in internet services. It ensures that users and systems can be sure that they are actually communicating with the correct server and are not being redirected to a manipulated or diverted address without their knowledge. This makes the Domain Name System verifiable and reliable for the first time, as responses can no longer be falsified without being noticed. The Internet Societyvi therefore describes DNSSEC not only as a protective mechanism, but also as an important foundation for future security functions on the internet that are based on reliable name resolution. A concrete example of this is DANE (DNS-based Authentication of Named Entities).vii This procedure uses DNSSEC-secured DNS entries to distribute cryptographic information, such as TLS certificates, in a trustworthy manner. This transforms the DNS system from a mere „phone book of the internet“ into an active trust anchor for further security protocols.

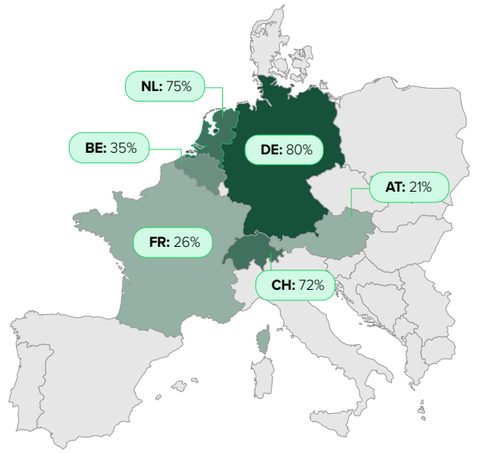
Without DNSSEC, these building blocks lack the necessary foundation of trust. With DNSSEC, on the other hand, an expandable security architecture is created that goes far beyond simply securing name resolution.

DNSSEC as the recommended security standard

National security authorities such as the German Federal Office for Information Security (BSI)viii expressly recommend DNSSEC as a best practice measure for securing the DNS infrastructure. DNSSEC is therefore part of a holistic security strategy that protects DNS servers as critical infrastructure components and prevents manipulation.

At the same time, implementations and studies show that technical and organizational hurdles remain, particularly for DNSSEC support on the part of providers and in the access infrastructure. As a rule, DNS resolution is performed by resolvers from internet providers or large platform operators, which deliver the results to end users. This makes it clear that DNS security can only scale effectively if all participants in the ecosystem – domain owners, registrars, providers, and platform operators – jointly assume responsibility for the integrity and validation of name resolution.

DNSSEC validation rate by country (%)



From basic functionality to security control layer

Modern DNS security strategies go beyond mere availability. They combine DNSSEC to ensure integrity with monitoring and anomaly detection to prevent abuse such as DNS tunneling, as well as proactive protection mechanisms against volumetric and logic-based attacks. This transforms DNS from an „invisible support service“ into a security-critical control layer of the digital infrastructure.

DNS security as a building block for digital resilience and sovereignty

In the context of the mission to make the internet more secure, DNS security is no longer an optional extra, but a basic prerequisite for trust in the network. Availability without integrity is fragile, and integrity without scalability is not sustainable. Securing name resolution is therefore not just a technical measure, but a strategic building block for digital sovereignty, resilience, and sustainable trust in networked business models.

„*Without DNS integrity,*
there is no reliable internet.“



Lukas, why are the topics of DNS integrity and DNSSEC becoming noticeably more important right now?

DNS is one of the most fundamental building blocks of the internet, which is precisely why it has long been a blind spot in many security strategies. Recommendations on DNSSEC have been around for several years, including from authorities such as the BSI. What is changing now is the context: digital business models have become more critical, dependence on online services is increasing, and regulatory requirements are growing. At the same time, we are seeing more and more incidents where it is not the application itself but the underlying infrastructure that has been the gateway for attacks. In this environment, the question of the trustworthiness of name resolution is inevitably coming into sharper focus.





From a management perspective, what does DNSSEC do without going too deeply into the technology?

Put simply, DNSSEC ensures that digital signposts on the internet are reliable. When a user or system requests an address, DNSSEC ensures that the response actually comes from an authoritative source and has not been manipulated. Without this protection, attackers can redirect users unnoticed; for example, to fake platforms or compromised systems. DNSSEC is therefore not just a convenience feature, but a fundamental measure to ensure the trust, integrity, and availability of digital services.





What business risks arise when companies do without DNSSEC?

The biggest risk is that manipulations remain invisible. Attacks such as „cache poisoning,“ in which manipulated entries are injected into the caches of DNS resolvers, or fraudulent redirects do not only affect individual users. They can potentially affect entire customer groups at the same time. The consequences range from reputational damage and security incidents to massive business interruptions. From a company's perspective, this is particularly critical because these types of attacks often take place under the radar of classic security systems and are therefore incredibly effective.





Various data sets show that although many networks could check DNSSEC, only a small proportion of domains are actually secured. Why is that?

This is a typical pattern in infrastructure security. The technical basis is often in place, but implementation requires prioritization, resources, and clear responsibilities. With DNSSEC, there is the additional factor that changes often have to be coordinated with both the DNS provider and the registrar. In many businesses, anything that does not deliver immediate added value or is organizationally complex tends to be postponed. At the same time, we are seeing that regulated industries and the public sector in particular are moving faster in this area, as compliance requirements increase the pressure to act.





What is your clear recommendation to decision-makers who take availability and trust seriously?

DNS should no longer be viewed as a purely technical detail, but as part of the business-critical chain of trust. Anyone who operates digital services is responsible for their accessibility and integrity. DNSSEC is an effective foundation for this. In short, without trustworthy DNS, there can be no reliable digital presence, which is precisely why DNS integrity should be on the agenda of organizations that take availability and trust seriously.



Conclusion: Cyber resilience is becoming a core strategic competence

Analysis of current data clearly shows that the threat situation in cyberspace is changing not only quantitatively but also structurally. Attacks are becoming more frequent, lasting longer, and being used more strategically. At the same time, the focus is shifting from spectacular outages to targeted disruptions of digital business processes.

Here are the key findings of the European Cyber Report 2026 at a glance:

- Attacks in the terabit range are becoming the norm rather than the exception.
- The average length of an attack increased from 1.5 to 8 days year-on-year.
- The number of attacks increased by 75%, and the average attack duration increased by 23.5%.
- Geo-blocking is no longer a viable strategy.
- Even after 30 years, DDoS continues to reinvent itself.
- Attacker bots are hiding behind Google bots.
- DNS security is underestimated.

These developments demonstrate that cyberattacks are operational risks to revenue, reputation, and business models, not just technical security incidents. Therefore, it is crucial to not only be able to fend off individual attacks but also to operate digital infrastructure in a permanently resilient manner. Organizations that strategically embed cyber resilience combine resilient infrastructure, automated protection mechanisms, and continuous data traffic analysis with clear decision-making and crisis processes.

The European Cyber Report 2026 aims to help sharpen this perspective. It is intended as a basis for discussion and exchange between security experts, IT managers, and corporate management to aid strategic decisions.

Because one thing is becoming increasingly clear: the stability of digital infrastructures is crucial to the stability of business models. Those who systematically build cyber resilience today are laying the foundation for sustainable trust in the digital economy.

Your contact person

Michael Scheffler
Vice President Sales

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



Sources

[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



Head Office

Link11 GmbH
Lindleystr. 12
60314 Frankfurt am Main