MYRA

CYBERSECURITY REPORT H1 2025

Facing Offensive AI with Resilience and Sovereignty

Preface

The first half of 2025 marks a new turning point in the development of the cyber threat landscape in Germany. The increasing intensity of DDoS attacks highlights how much the threat situation in the digital space continues to escalate. At the same time, ongoing geopolitical conflicts and the return of Donald Trump to the US presidency are causing additional uncertainty, particularly with regard to Europe's digital sovereignty.

These developments clearly demonstrate that traditional defense methods are insufficient. The growing use of artificial intelligence by attackers poses a significant risk to companies and institutions. As a result, attacks are becoming more targeted, intense, and sophisticated. Banks, critical infrastructures, and the public sector are particularly vulnerable, as attackers are increasingly misusing global cloud infrastructures to hide and amplify their attacks.

Against this backdrop, it is urgent that we reduce our technological dependencies and strengthen our ability to act in the digital space. Digital sovereignty and resilient IT architectures are essential for minimizing cyber risks and ensuring compliance with strict regulations. Investing in European solutions and continuously developing expertise will enable the German economy and public administration to remain secure and capable in the future—provided decision-makers are willing to do so.

To summarize: cyber resilience and digital sovereignty are no longer niche topics, but a social imperative whose importance has increased further due to the current threat situation. This Cybersecurity Report from Myra highlights the most relevant developments and shows how companies and public institutions can strengthen their resilience with targeted measures in order to effectively counter current and future threats.

Christof Klaus
Director Global Network Defense
at Myra Security

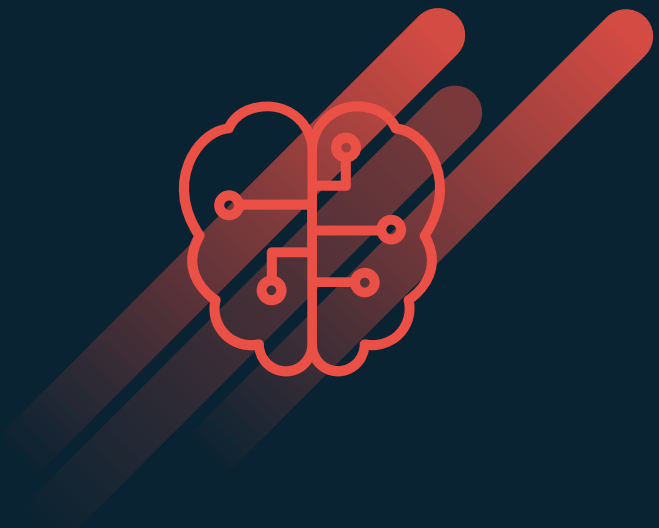
Contents

Executive Summary

In 2025, the cybersecurity situation in Germany will remain tense and highly dynamic. Although the number of attacks documented and defended by Myra declined in the first half of the year (**-18.5 percent** compared to the previous year), the intensity, targeting, and technical sophistication of the attacks continue to increase. Highly regulated industries such as the financial industry, critical infrastructures, and the public sector are particularly affected: **40 percent of all attacks target banks** and other financial service providers. Attackers are also deliberately exploiting global cloud infrastructures to conceal their attacks and increase their impact. The strongest attacks were recorded by defense systems for the technology industry, while **the longest attacks lasted for almost two days.**

Escalation of Cyber Risks Through Offensive AI

The widespread availability and gradual integration of artificial intelligence (AI) into attack tools is significantly exacerbating the cyber threat landscape: Attackers can identify vulnerabilities more quickly, precisely, and cost-effectively and orchestrate automated, adaptive attack campaigns that increasingly circumvent traditional protective measures. In the area of DDoS attacks in particular, AI-optimized techniques enable **dynamic adaptation of attack vectors** and effective management of botnets, significantly increasing the efficiency and impact of such attacks. **AI-based bots and crawlers also cause considerable server load** on websites through mass automated requests, which can lead to outages. The vast majority of companies recognize the growing threat: 82 percent see AI as enabling more targeted exploitation of vulnerabilities, while 89 percent believe that **the use of AI will enable cybercriminals to carry out more efficient and precise attacks.**



Hybrid Threat Situation and Geopolitical Dimension

Meanwhile, the lines between financially and politically motivated attacks are becoming increasingly blurred. **Hacktivist groups and state-sponsored actors use cyberattacks as a means of hybrid warfare** to sow uncertainty and promote social division. According to information from the German Armed Forces and the Federal Office for Information Security (BSI), **Germany is the target of such hybrid attacks on a daily basis**, which target not only IT systems but also the stability of public order as a whole.[1] Only a highly resilient IT infrastructure can withstand this threat—and such infrastructure is currently only available to a limited extent in Germany. The Federal Audit Office recently warned of serious security gaps in the federal government's data centers: *"The federal government's IT is not prepared for the current threats."*[2] German authorities and businesses often lack the necessary redundancies, crisis resilience, and sovereignty.

Sovereignty Is the Foundation for Cyber Resilience

Digital sovereignty describes the ability of companies, organizations, and states to maintain control over their data, digital infrastructures, and key technologies and to minimize dependencies on non-European providers. This digital independence is essential, especially against the backdrop of unreliable partnerships outside Europe. Only through sovereign IT architectures, the targeted use of European solutions, and compliance with strict data protection and compliance standards can **resilience to cyber threats** be strengthened in the long term. Although both politicians and businesses have recognized the importance of digital sovereignty, this is not yet reflected in sufficient investment in European cloud, AI, and security solutions. There is often a lack of knowledge about powerful alternatives. Regulatory initiatives such as the **NIS 2 Directive**, the **DORA Regulation**, and the **Cyber Resilience Act** are pointing the way toward holistic cyber resilience along the entire digital value chain.

Resilient into the Future

Strengthening digital sovereignty is therefore not an abstract vision of the future, but an urgent necessity for Germany's security and competitiveness. It is a prerequisite for effective data protection, legally compliant compliance, and the resilience of critical infrastructures. Companies and public authorities must systematically reduce their dependence on non-European technologies, expand their own expertise and solutions, and strengthen strategic partnerships within Europe. This is the only way to shape a sustainable, secure, and self-determined digital future.

The main section of this cybersecurity report provides detailed analysis, interviews, and practical recommendations on the topics covered. Aggregated figures from Myra's Security Operations Center (SOC) offer a comprehensive overview of trends and attack methods from a Central European and DACH perspective, with a particular focus on highly regulated industries and critical infrastructure.

Losses and Risk at Record Levels

The need for better protection systems is illustrated by the relevant loss statistics, which have reached new record levels. For example, the damage caused by cybercrime to the German economy amounts to 178.6 billion euros - an increase of more than 20% compared to the previous year. **8 out of 10 companies are affected** by data theft, espionage or sabotage.[3] 47 percent of German companies see **cyber incidents as their greatest business risk**, ahead of business interruptions and natural disasters.[4] Around 3 out of 4 managers are certain that the risk of danger to their own company has increased in the past two years, and more than half expect the situation to worsen massively in the future.[5]

Mitigation Trends and Attack Patterns

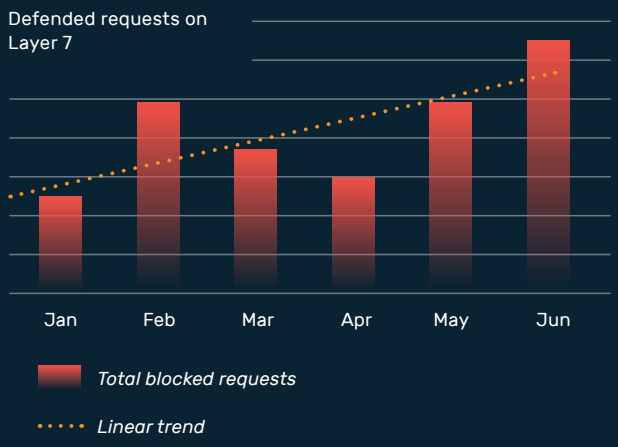
In the first half of 2025, the threat landscape of malicious traffic streams remained extremely dynamic. Though the total number of attacks declined slightly, massive waves of attacks and increasingly sophisticated methods indicate that the quality and targeting of attacks are on the rise. Attackers particularly target companies in highly regulated industries, which are increasingly exposed to complex and prolonged attacks. Cybercriminals exploit global cloud infrastructures and employ modern obfuscation techniques, making it much more difficult to reliably identify and defend against attacks.

Specifically, it can be said that the number of malicious requests to web applications, online portals, and APIs remained at a consistently high level during the period under review. Although the total number of attacks fell by 18.5 percent compared to the same period last year, current developments and the long-term trend signal a qualitative intensification of the threat situation.

Massive waves of attacks in individual months underscore this trend:

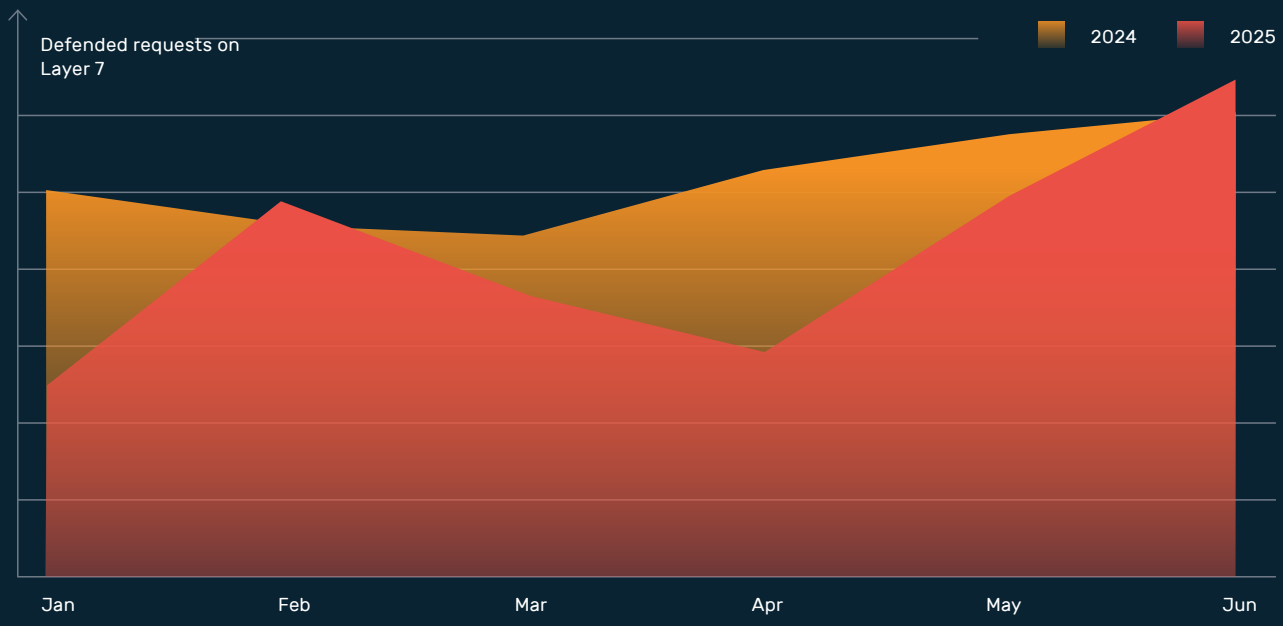
- **February 2025:** An increase of 6 percent in malicious requests was already recorded in the spring, which can be attributed primarily to a targeted attack campaign against Bavarian authorities.
- **June 2025:** A significant increase of 6.6 percent compared to the same month last year also points to increased attack activity at the end of the half-year.

Attack Activity H1 2025



These data show that despite an overall statistical decline, the intensity and targeting of attacks are increasing.

Attack Activity Year-On-Year



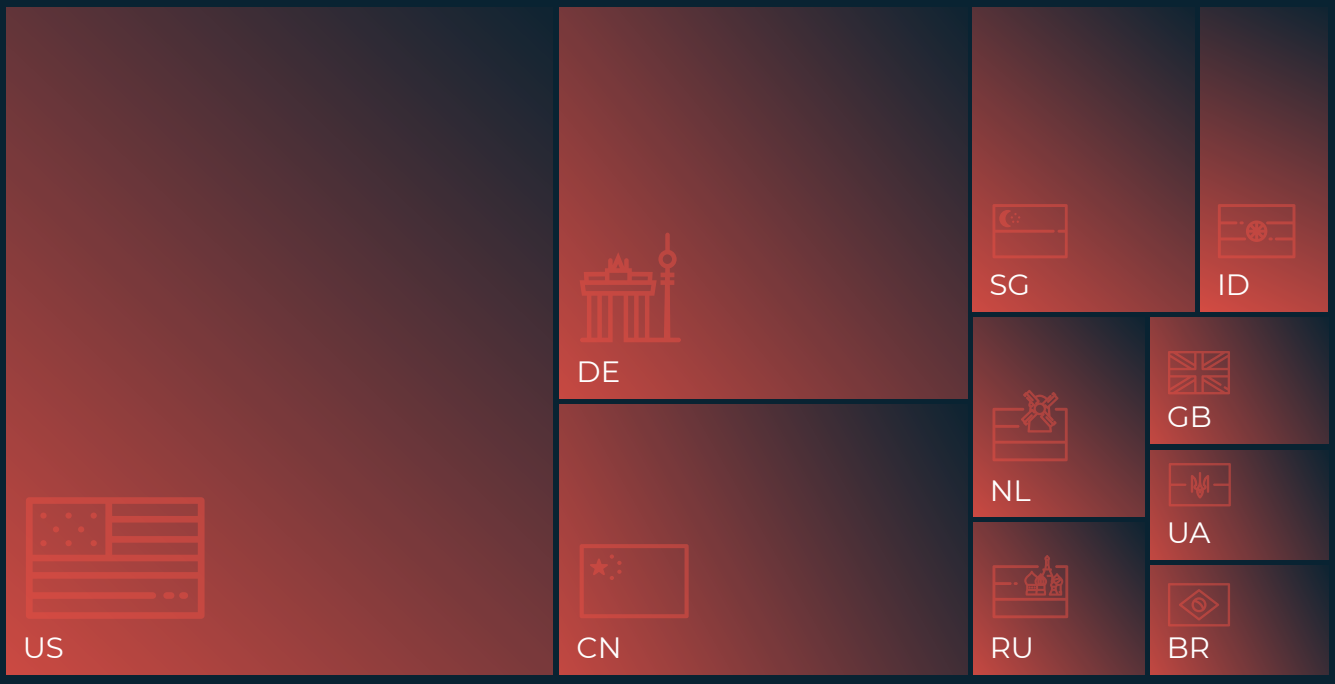
Compared to the same period last year, there were 18.5% fewer malicious requests in the first half of 2025. Nevertheless, there were significant peaks in February (+6%) and June (+6.6%), which even exceeded the already high level of mitigation of the previous year.

Origin Analysis and Limitations in Attribution

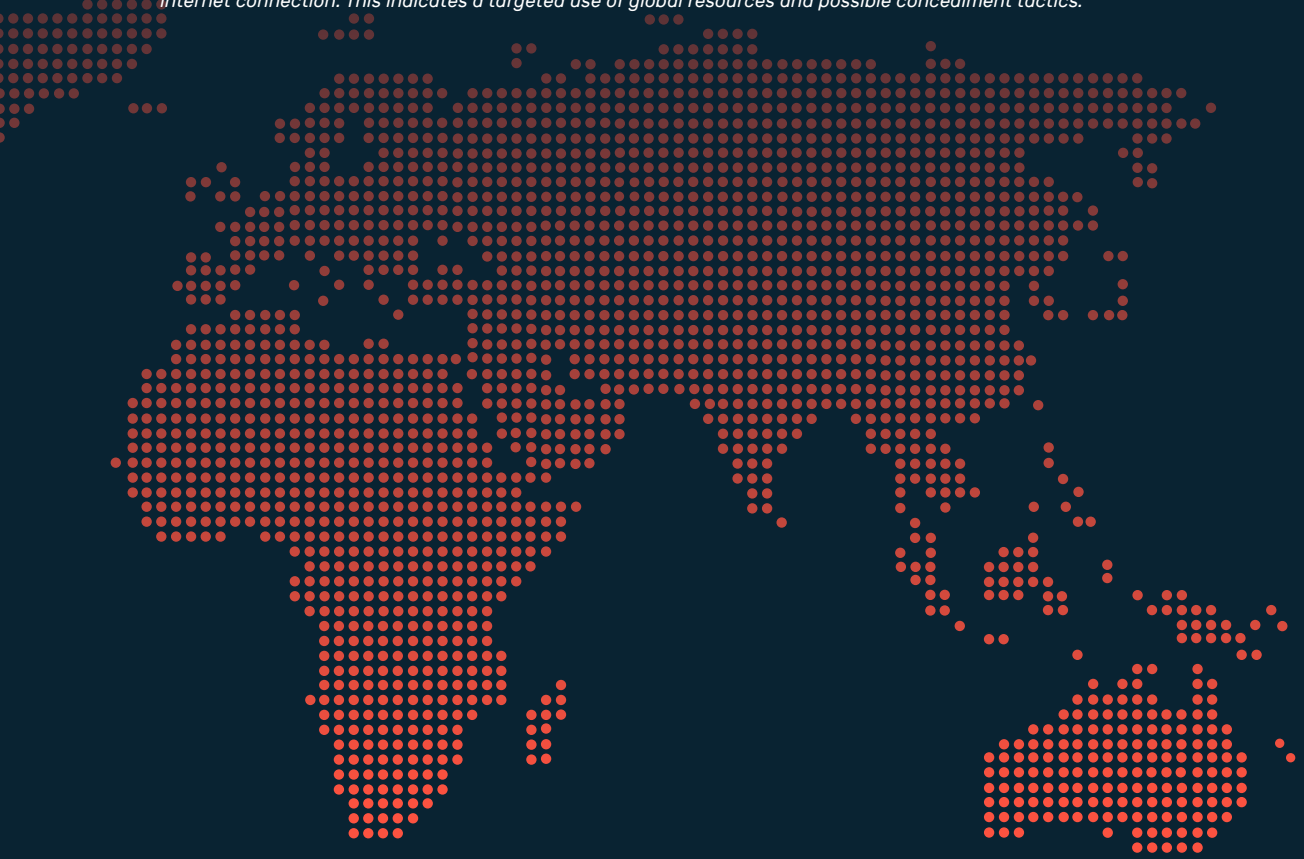
Analysis of the attack data processed by Myra provides insights into global traffic sources, although a differentiated interpretation is required.

Geographical distribution of requests: The majority of malicious requests originated in the US. Looking at the ten countries with the highest number of requests, the United States accounts for 42 percent. Germany follows at a considerable distance with 19 percent, and China with 12 percent. Russia ranks seventh with only 3 percent.

Top 10 Origin Countries

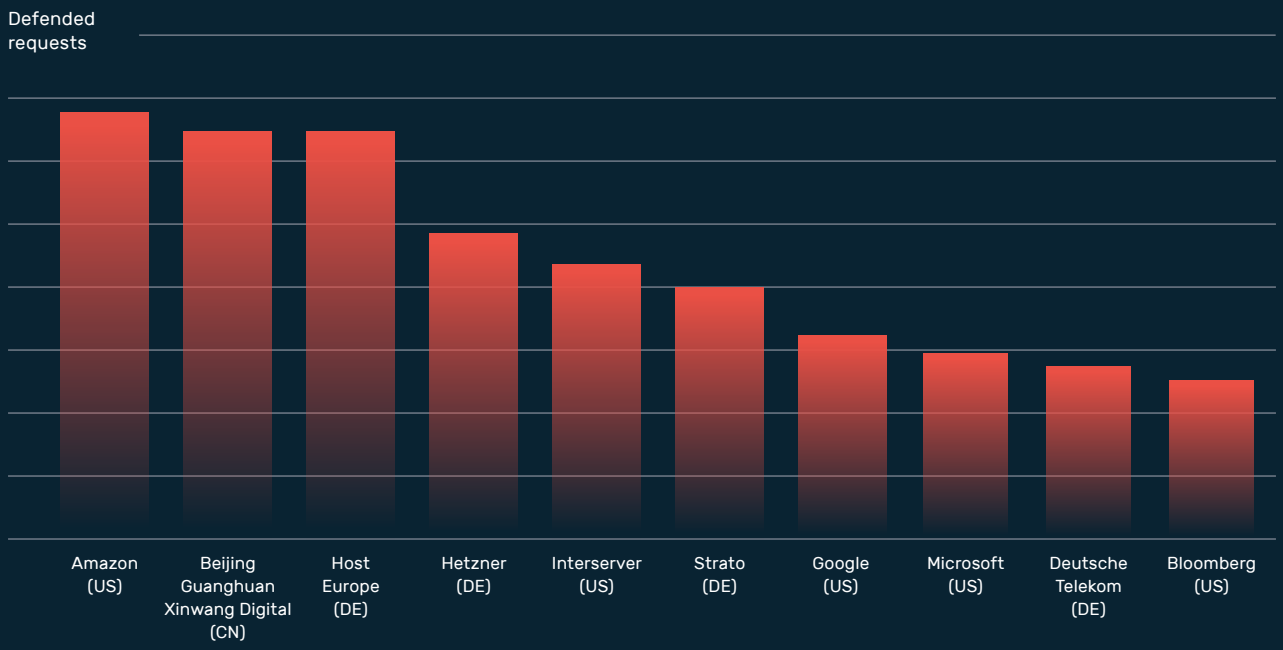


The analysis shows that cyber criminals usually direct their attack campaigns via countries with a powerful technical infrastructure and fast internet connection. This indicates a targeted use of global resources and possible concealment tactics.



Distribution by autonomous systems (AS):
A breakdown of malicious requests by network infrastructure shows a high concentration on a few large cloud providers and hosters. Most malicious requests originated from the networks of the US hyperscaler Amazon, closely followed by Beijing Guanghuan Xinwang Digital from China and Host Europe from Germany. This underlines the importance of large, globally active infrastructure providers as platforms for attackers who specifically misuse providers' resources for their own purposes.

Top 10 Origin AS



The analysis of the original AS in the top 10 ranking shows that a large proportion of attacks originate from the networks of US hyperscalers. In addition, cyber actors also use regional networks with high credibility, such as Hetzner, Host Europe or Deutsche Telekom. As a result, traditional origin filters are becoming increasingly ineffective.

Attribution notes: The information about countries of origin or AS used does not allow any reliable conclusions to be drawn about the actual location or identity of the attackers. Cybercriminals deliberately use techniques such as IP spoofing, reflection attacks, and globally distributed botnets to conceal their true origin. In addition, compromised servers or cloud resources are often used as springboards, making the attacks appear to originate from completely different regions (for more information, see the info box on page 8).

The evaluation of the top origin AS or countries is therefore primarily used to classify and analyze traffic flows. It can help to identify patterns and target protective measures.

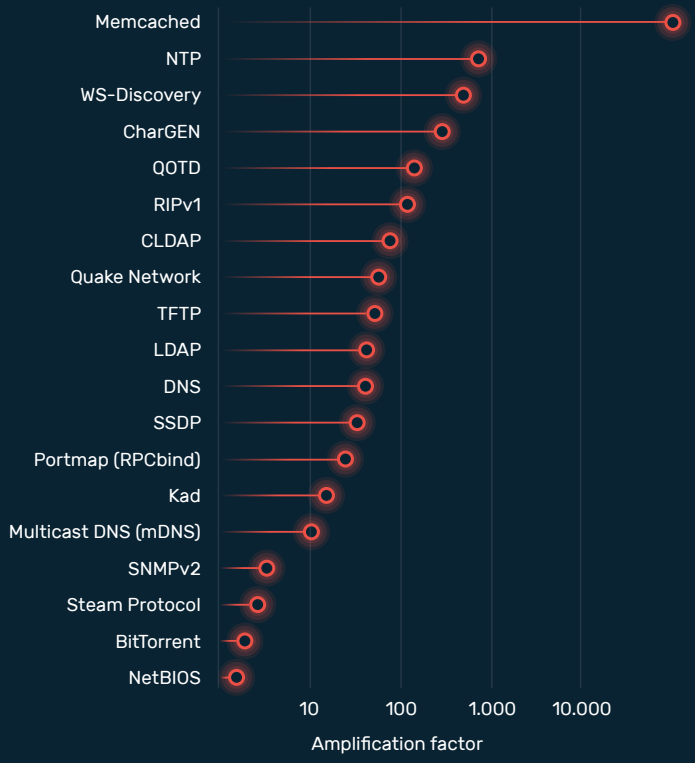
However, it is not suitable for identifying specific attackers or their locations. Attribution in cyberspace remains one of the industry's biggest challenges and always requires critical and multi-layered analysis.

These Industries Are Attacked

In the first half of 2025, Myra's defense systems recorded a significant focus of attacks on companies in the financial sector, which were the most frequent targets of attackers, accounting for 40 percent of all attacks. This was closely followed by technology companies, which accounted for 38 percent of all mitigated attacks. Insurance companies (7 percent) and public administration organizations (4 percent) followed at a considerable distance.

It is striking that the most massive attacks occurred in the technology sector, followed by telecommunications and public administration. The duration of individual attacks was also particularly noteworthy: the longest documented attack lasted almost two days (46.08 hours), illustrating the increasing endurance and tenacity of modern attackers.

UDP-Based Amplification Attacks



Many DDoS attacks are carried out via highly amplifying reflectors such as DNS services, which respond to the attackers' short requests with large data packets. In this way, such reflection attacks increase the power of the attacks many times over.[6]

How Cyber Criminals Hide Their Attacks

IP spoofing: Attackers manipulate the source IP address in packet headers to conceal their identity. This involves generating fake IP packets with deliberately falsified sender addresses to prevent tracing and circumvent security systems. This technique is particularly popular in DDoS attacks, where randomly generated source IPs make filtering difficult.

Reflection attacks: Here, attackers misuse public services such as DNS, NTP, or SNMP. They send requests with a fake sender address (victim IP) to these services. The responses generated are then forwarded to the victim – often with considerable amplification, as response packets can be larger than requests. This method does not require control over the servers used.

Globally distributed botnets: Attackers control compromised devices ("bots") worldwide, which are coordinated via command-and-control servers. These botnets generate attack traffic from thousands of sources, rendering geographical or AS-based attributions useless.

Who Are the Attackers? An Overview of Modern Cyber Actors

Various groups with different motives and approaches are behind the attacks on websites, APIs, and infrastructure. It should be noted, however, that nine out of ten attackers have financial motives, and espionage plays a central role in around one-fifth of attacks.[7]

State-supported actors: State-supported cyber actors use attacks primarily for espionage. They plan for the long term and use a wide range of attack tools - from DDoS attacks to advanced malware. Their targets are not only other states, but also companies and organizations in order to gain access to sensitive information or financial resources.

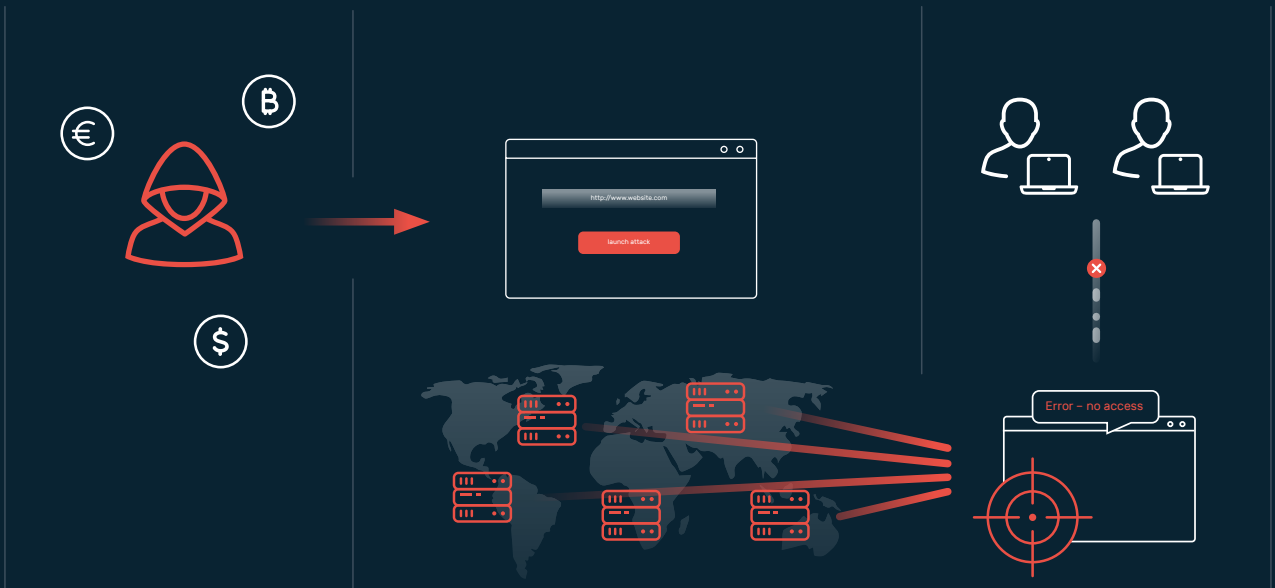
Script kiddies: A script kiddie is an inexperienced cyber actor who uses ready-made hacking tools, scripts, and services without really understanding how they work. They typically use publicly available software to exploit vulnerabilities or disrupt systems. Despite their limited expertise, script kiddies can cause considerable damage through automated attacks.

Cybercriminals: Cybercriminals are responsible for the majority of all attacks. They usually act opportunistically and rely on broad-based attacks to compromise specific data or critical infrastructure. Their goal is to cause maximum damage — whether through direct theft of digital assets, extortion of victims, or the profitable sale of stolen information.

Insider threats: Internal actors also pose a significant risk, regardless of whether their actions are intentional or unintentional. In practice, many security incidents can be traced back to human error, misconfigurations, or inadequate security policies. Companies should therefore include not only external threats but also potential risks from insiders in their security strategy.

Hacktivists: Hacktivist groups use cyberattacks to pursue political or social goals. Their main aim is to attract attention, cause disruption in public life, and stir up uncertainty. The technical capabilities and attack methods of these groups vary greatly. In addition, hacktivists are occasionally exploited by state actors, for example for targeted disinformation campaigns or to influence public opinion.

Sequence of a DDoS Attack Using DDoS as a Service



1.
Criminals hire a DDoS attack service on the Internet and specify the target IP address. Payment is usually made in cryptocurrencies.

2.
The booter service launches the DDoS attack via its attack infrastructure.

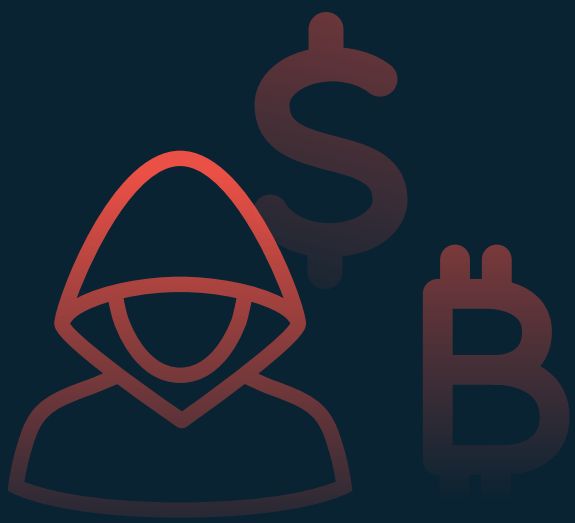
3.
The DDoS attack overloads the target's servers, making them inaccessible to regular users.

Inexpensive Attacks with Enormous Power: DDoS as a Service

DDoS-as-a-service offerings provided by cybercriminals on the darknet or platforms such as Telegram are contributing significantly to the escalation of the threat situation. There, actors rent out the power of their botnets for as little as a few US dollars per day. Even inexpensive attacks are often enough to paralyze unprotected web processes for the duration of the attack.

The effectiveness of such DDoS-as-a-service offerings was recently demonstrated in the attack on the blog of cybersecurity expert Brian Krebs (KrebsOnSecurity): On May 12, 2025, the attack using the Aisuru botnet reached a peak load of 6.3 Tbit/s. In public Telegram chat channels, the people behind Aisuru offered the botnet for rent in subscription tiers ranging from 150 US dollars per day to 600 US dollars per week, advertising attacks of up to 2 Tbit/s.[8]

Overall, the price structure for these services is alarmingly low, ranging from a low double-digit amount to several hundred US dollars, depending on the duration and severity of the attacks carried out. Payment is usually made anonymously in the form of cryptocurrencies such as Bitcoin.



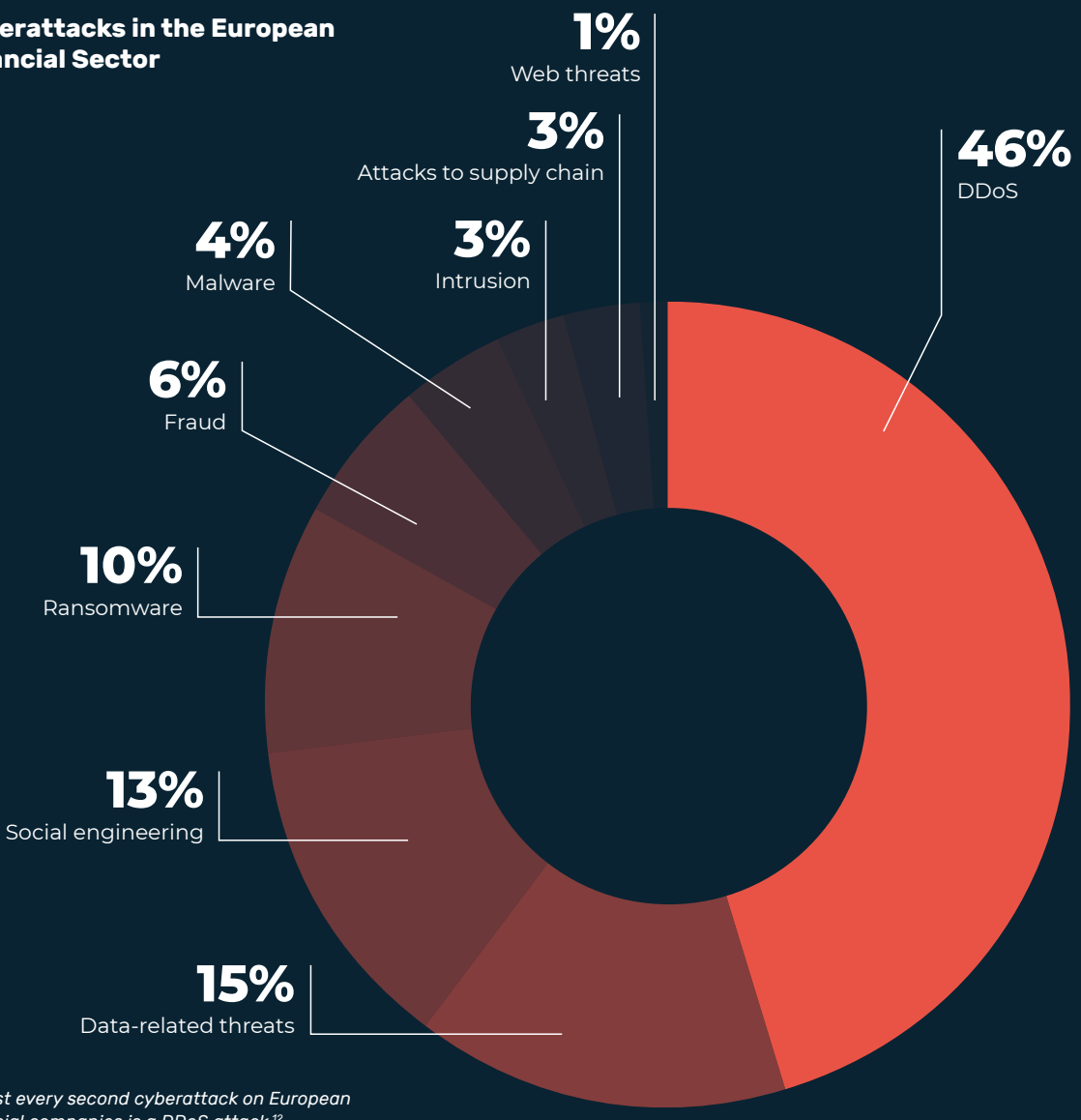
Financial Sector in the Focus of Cybercrime

The financial sector has been a primary target for cybercriminals for years – a fact that can be explained by the high concentration of sensitive data and significant assets in this sector. Where large amounts of value are managed and transactions are processed in real time, potential attackers are particularly interested. Cyber incidents therefore represent the central risk for financial institutions.[9]

DDoS attacks are the weapon of choice for cybercriminals targeting banks and financial services providers in most cases: In Europe, 46 percent of all attacks on the financial sector are carried out using this attack vector.[10] Such attacks aim to disrupt the availability of online banking, payment services, and stock exchange platforms, which not only causes financial damage but also permanently damages customer trust. The Myra SOC recorded the highest number of attacks in the financial sector in the past six months, underscoring the particular vulnerability of this sector.

Against this backdrop, the German Federal Financial Supervisory Authority (BaFin) has declared strengthening operational resilience to be one of its top strategic priorities for the coming years. The aim is to increase the industry's resilience to cyber threats, minimize downtime, and ensure confidence in the stability of the financial system.[11]

Cyberattacks in the European Financial Sector

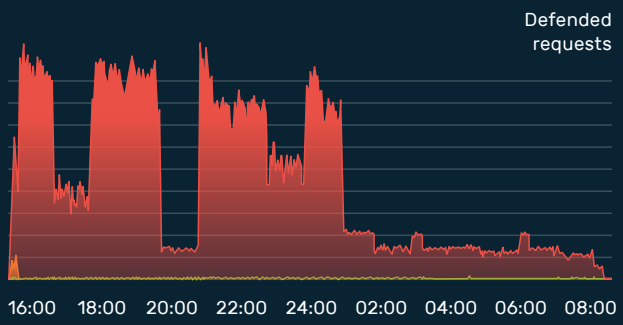


Almost every second cyberattack on European financial companies is a DDoS attack.[12]

DDoS Attack Campaign Defended in the First Half of 2025

After numerous administrative portals of German cities were hit by a coordinated DDoS attack campaign at the end of April, cybercriminals shifted their attacks to German banks and financial service providers in May – several Myra Security customers were also affected by the wave of attacks.

Over a period of more than 16 hours, cyber actors attacked the financial institutions' systems in several waves. The attackers used various methods and vectors, including Slowloris, and targeted different network layers. Myra's protection systems blocked more than 240 million requests during this period, preventing critical infrastructure from being overwhelmed.



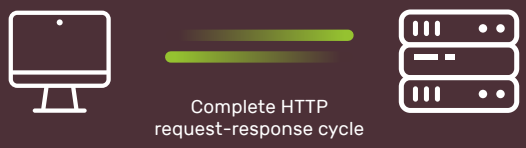
The coordinated cyberattack on German financial institutions took place in several waves over a period of more than 16 hours.

Thanks to the certified security technology and expertise of the Myra SOC, all affected financial services were kept available and performing at all times. The attacks were detected and defended on all relevant network layers. Automated processes enabled an immediate response to the changing attack patterns.

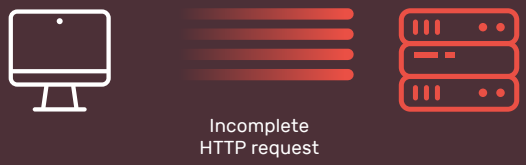
> *Our defense systems took fully automatic action against the attackers and blocked their attacks on all relevant network layers.*
>
> *The complexity of the attacks was particularly striking: among other things, the attackers used Slowloris as an attack vector. This involves opening numerous connections to a web server and keeping them open for as long as possible. This gradually exhausts server resources without the attack being noticed due to unusually high bandwidth – legitimate traffic is effectively blocked, while the attack remains difficult to detect for classic protection mechanisms.*
>
> *Our multi-layered defense mechanisms also identify these low-and-slow attacks at an early stage and initiate mitigation before the availability of the targeted services is compromised.*

Christof Klaus
Director Global Network Defense
at Myra Security

Ordinary HTTP Request - Response Connection



DDoS attack via Slowloris



Slowloris: Inconspicuous Attack with Great Effect

In a slowloris attack, a special form of denial-of-service attack, an attacker opens numerous connections to a web server and keeps them open for as long as possible with incomplete HTTP requests. This blocks the server's available connections, preventing legitimate users from establishing a connection even though the server still has free capacity. Unlike classic DDoS attacks, Slowloris requires very little bandwidth and often goes unnoticed because the attack looks like normal, but extremely slow, traffic.

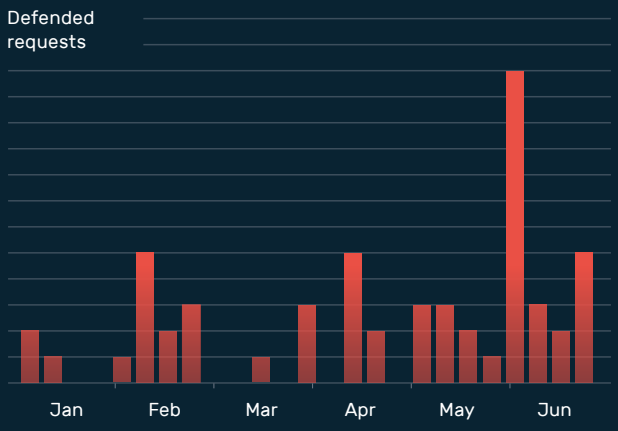
Authorities, Cities and Municipalities Under Constant Attack

According to the German government, a total of 80 IT security incidents were recorded at federal authorities last year – 17 of which could not be successfully defended.[13] In addition to federal institutions, state and local authorities were also targeted by serious cyber attacks. Myra's defense systems recorded some of the highest numbers of attacks on customers in the public sector. Globally, cyber incidents in the public services and government sector rank second among the biggest risks.[14]

Particularly striking was a wave of attacks with a geopolitical background that hit numerous German authorities and cities in April 2025. For example, the capital city portal berlin.de was paralyzed by massive DDoS attacks.

In February, Bavarian authorities, the Federal Finance Court, and the police were also affected by cyberattacks and had to accept temporary restrictions on their online operations.

Cyber threat landscape Public Sector



These attacks resulted in digital administrative services for citizens being partially unavailable and internal processes being significantly disrupted. The attackers deliberately exploited political tensions to stir up uncertainty and undermine trust in government structures.

The attacks make it clear that the public sector remains an attractive target for cybercriminals and politically motivated attackers. The attacks are real, the consequences are tangible, and the need for action remains high.

Cyberattacks are causing outages and performance problems in federal, state and local authority digital processes across Germany.[15]

Cyber Incidents in the Public Sector

June 20, 2025
Municipal administration Lotte

June 3, 2025
Municipal administration Ostercappeln

June 2, 2025
Wittenberg district administration

May 26, 2025
Remscheid city administration

May 22, 2025
Lake Constance district administration

May 9, 2025
IT Service Center Berlin

May 6, 2025
Nationwide (BOS digital radio)

May 5, 2025
Ellwangen Town Council

April 30, 2025
Stuttgart City Hall

April 29, 2025
City of Dresden

April 26, 2025
City of Berlin

April 25, 2025
City of Nuremberg

March 31, 2025
Municipal IT service provider AKDB

March 16, 2025
Kirkel municipal administration

March 5, 2025
Municipality of Schwerte

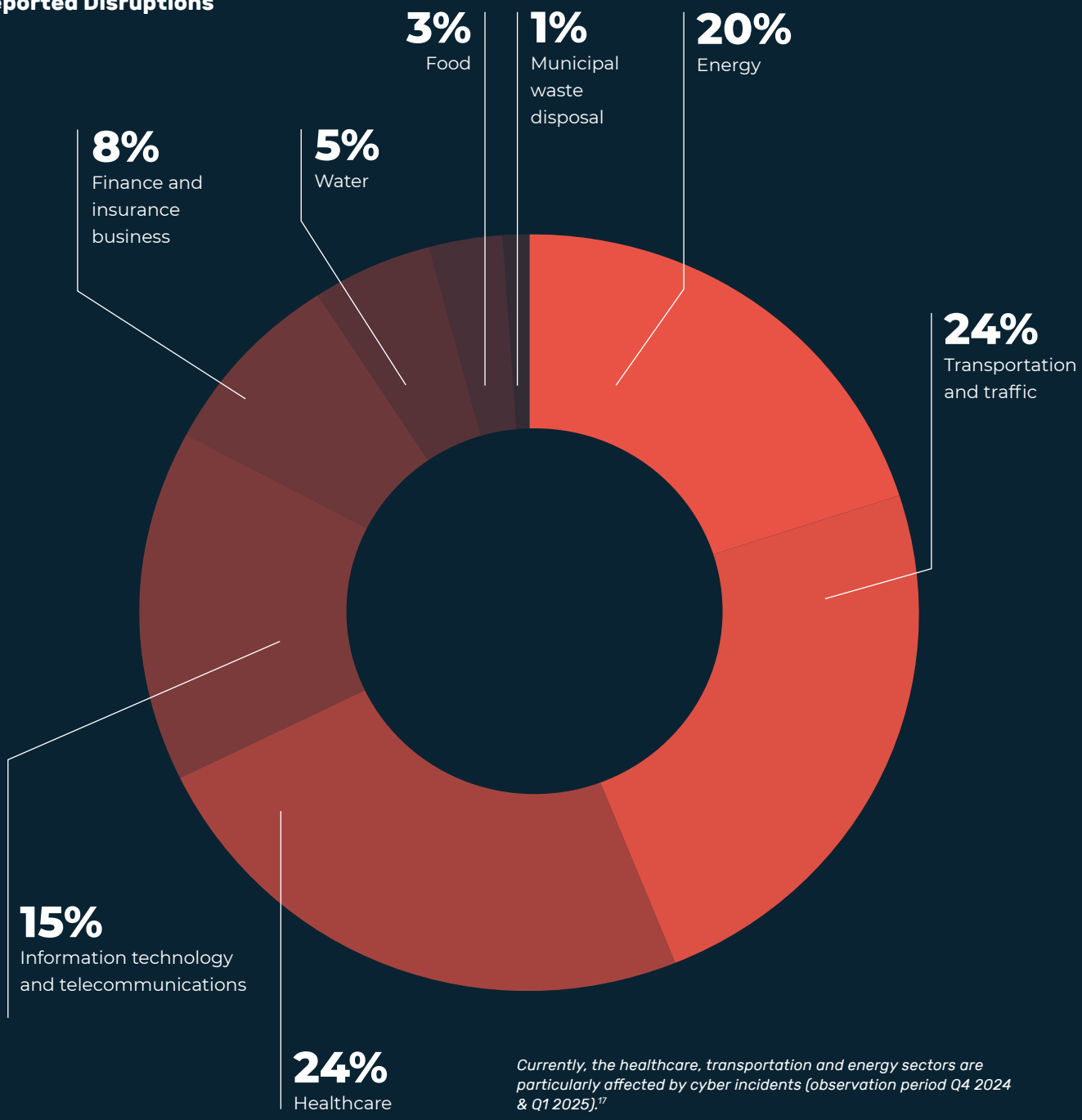
February 13, 2025
City administrations Garching

Critical Infrastructure: Growing Threat Meets Slow NIS 2 Implementation

While the wait for NIS 2 implementation in Germany continues to drag on, the threat to critical infrastructure organizations (KRITIS) is becoming increasingly acute. According to official statistics, a total of 769 incidents were reported to the BSI last year – an increase of 43 percent compared to the previous year.[16] These figures make it clear that cyberattacks on Germany's critical infrastructure are not an abstract danger, but an acute threat to the functionality and security of our society.

Only **4 EU countries have implemented NIS-2** on time: **Belgium, Italy, Croatia** and **Lithuania**

Critical Infrastructure: Reported Disruptions



Currently, the healthcare, transportation and energy sectors are particularly affected by cyber incidents (observation period Q4 2024 & Q1 2025).[17]

The energy, transport, health, IT, and telecommunications sectors are particularly targeted by attackers, sometimes with serious consequences.

Meanwhile, the BSI sees the energy supply sector in particular as a "growing target for cybercriminals," as BSI President Claudia Plattner stated in May. The decentralized structure with numerous small power plants, wind farms, and solar installations is creating more and more access points for targeted infiltration, sabotage, and manipulation.[18]

Even sectors that are supposedly less affected, such as water, food, or waste disposal, pose a major risk to society in the event of a significant disruption. It should be noted that no area in the critical infrastructure sector is immune to attacks, as exemplified by the attack on a dam in southwestern Norway (see next page).

A Warning Shot from Norway: How Vulnerable Are Europe's Infrastructures?

A recent incident in Norway highlights the real risks to critical infrastructure: In April 2025, unknown attackers managed to open the water release valves of a dam at the Risevatnet reservoir in the south-west of the country for several hours without being noticed. The cybercriminals gained access to the control systems, which were accessible via the internet, using a weak password. After successfully authenticating themselves, they were able to bypass the security controls and gain direct access to the operational technology (OT) environment. As a result, all valves were opened completely and the water discharge increased by 497 liters per second above the prescribed minimum flow rate. Fortunately, the attack did not cause any further damage.

However, the incident serves as a warning shot and highlights how vulnerable critical infrastructure is to inadequate security measures.

A glance at the global search engine Shodan, which is used to find networked devices, reveals that the vulnerability exploited at the Risevatnet reservoir is not an isolated case: thousands of building automation and control systems worldwide are directly accessible from the internet – many of them without adequate security measures.

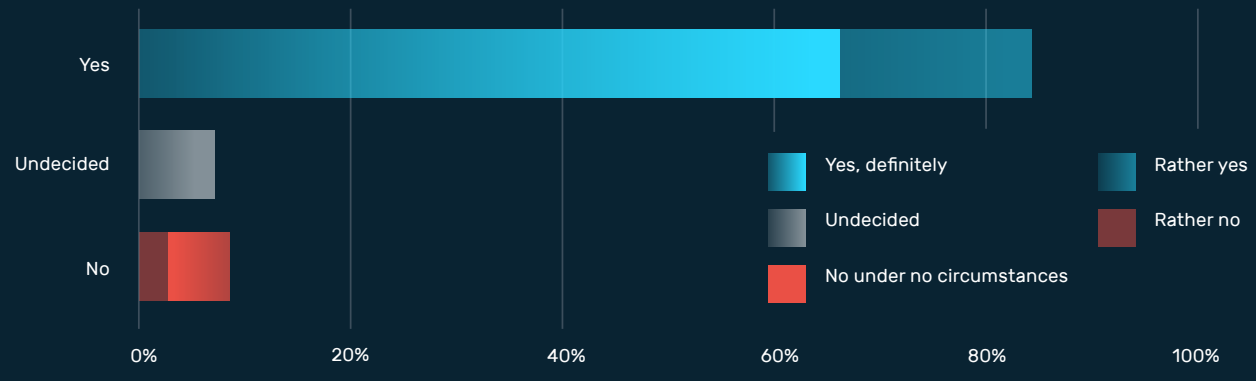
Calls for Digital Sovereignty Are Getting Louder

The tense situation in the area of critical infrastructure is also reflected in the opinions of IT decision-makers. This is the finding of a recent Civey study commissioned by Myra. More than four-fifths of those surveyed believe that critical infrastructure in Europe should rely exclusively or primarily on European software solutions in the future. This shows a clear consensus, especially among those responsible for IT security.

At the same time, however, the survey also reveals that there is a huge gap between aspiration and reality. Actual dependence on international software providers remains high, and the implementation of digital sovereignty is progressing only slowly.[19]

The implication is clear: while the threat level is increasing and calls for European independence are growing louder, practical implementation is falling short of expectations. Commitments alone do not make infrastructure secure. What has long been decided in the minds of IT managers must now be consistently translated into budgets, procurement guidelines, and implementation plans.

In your opinion, should states and operators of critical infrastructure in Europe rather use European providers for digital products in order to be independent of non-European providers?



Digital Sovereignty Is the Key to Sustainable Digital Transformation and Compliance

The mitigation data from the Myra SOC speaks for itself: the cyber threat situation in Germany is more tense than ever before. Companies are not only facing an increasing number of attacks, but also the challenge of defending themselves against them technically and organizationally without violating data protection and compliance requirements.

At the same time, critical dependencies and risks in the digital supply chain must be avoided. When it comes to securing their own cyber resilience, organizations in Germany and Europe are increasingly looking to local offerings to strengthen their digital sovereignty. This trend is gaining momentum, especially against the backdrop of geopolitical tensions and uncertainties. As a result of the policies of the US administration under President Donald Trump, every second company in Germany now feels compelled to rethink its own cloud strategy.[20]

In conversation with Prof. Dr. Louisa Specht-Riemenschneider, Federal Commissioner for Data Protection and Freedom of Information (BfDI), and Prof. Dr. Dennis-Kenji Kipker, cybersecurity expert and member of the Myra Advisory Board, we shed light on the complex interplay between digital sovereignty, data protection, and cyber resilience.

Prof. Dr. Kipker, cyberattacks repeatedly show us how vulnerable digital infrastructures in Germany still are. In your opinion, what are the biggest challenges in defending against cyber attacks – such as DDoS?

We must bear in mind that defending against DDoS attacks has long been more than just a technical issue – it's about supply chains, compliance, liability, and digital sovereignty. This is because defending against overload attacks – for example, through traffic analysis and filtering – requires service providers to look deep into data traffic and intervene. This entails not only technical risks, but also significant compliance risks, especially when personal or business-critical data is involved.

As a company, I have to ensure that the service providers I use are trustworthy and comply with all regulatory requirements in order to minimize liability risks and guarantee system availability. The basis for this is sound risk management, which involves putting the service provider through a comprehensive due diligence process.

Working with international service providers, especially those based in the U.S., often raises questions because different legal systems come into play. What compliance risks does this entail?

In practice, working with US providers carries significant risks, as these companies are primarily subject to US jurisdiction. Even if servers are located in the EU, US authorities can access data, or rather, order access to it – think CLOUD Act, FISA 702, or Patriot Act. The political developments in the US, which we are now seeing in Donald Trump's second term, are further exacerbating this problem.

At the same time, the legal basis for GDPR-compliant transatlantic data transfers is extremely fragile. The existing adequacy decision between the EU and the US is based solely on an executive order by Joe Biden, which can be revoked at any time by his successor. And Trump has already announced in his Agenda 47, his US presidential agenda, that he wants to essentially reverse everything Biden has done.

This process has already begun with the dismissal of the Democratic members of the Privacy Oversight Board, a central component of the EU-US Data Privacy Framework that serves as the basis for the current adequacy decision. Companies that rely on US service providers are therefore exposed to significant compliance and liability risks.

What strategic advice do you give organizations to make themselves future-proof?

My advice is clear: companies must reduce their dependence on non-European providers and

consistently rely on original European solutions. This applies not only to DDoS protection, but to the entire digital supply chain. Regulatory requirements—such as those imposed by the NIS 2 Directive or the Cyber Resilience Act—will continue to increase. Those who switch to European providers early on will not only minimize compliance risks, but also promote the digital sovereignty and resilience of their own companies. This is no longer an optional step, but a necessity.

Prof. Dr. Specht-Riemenschneider, in recent years, Germany's dependencies in areas such as health, energy, and IT have become increasingly apparent. How can these dependencies be reduced and Germany's sovereignty strengthened?

The dependencies are often known, but are addressed too late or not with the necessary consistency. A key reason for this is that economic efficiency and short-term cost savings have long been priorities, while strategic resilience and digital sovereignty only come to the fore in times of crisis.

Digital and technical sovereignty requires forward-looking digital and industrial policies that specifically strengthen European technologies and infrastructures. This means investing in key technologies such as cloud computing, AI, and semiconductors that embody European values. But it also means greater European cooperation to leverage economies of scale and strengthen our own ability to act through pooled demand.

In addition, regulatory frameworks must be designed in such a way that they enable innovation that complies with fundamental rights without creating new dependencies. In short, we need less reaction and more strategic foresight.

With the EU-US data protection framework under threat, how can we reduce our reliance on non-European technologies and secure control over data in the EU?

I am watching events in the US with concern and hope that the EU will make wise decisions. At the same time, I would like to see European companies finally recognize their knowledge advantage in the field of data protection-friendly technologies as a competitive advantage. With my organization, I am ready to support this with information and advice and to pave the way for it.

Europe has the technology and expertise, but there is a lack of implementation of sovereign IT solutions. Where do you see a need for action?

For me, the key question is: what is holding us back? Digital policy must pursue a vision, a goal that can guide legislative action. Value-based digitalization could be such a goal. Supervision can be a catalyst through information, advice, and active support such as real-world laboratories. I am happy to offer this. But it is up to the legislature to establish the appropriate rules that enable innovation while protecting fundamental rights. I believe we need targeted investment in solutions that carry our European values into a digital future.

Want to learn more?
Scan the QR codes to access the full interviews.

In conversation with Prof. Dr. Dennis-Kenji Kipker | Data control and availability are imperatives, not just recommendations.

In conversation with Prof. Dr. Louisa Specht-Riemenschneider (BfDI) | Digital awakening: Europe's path to sovereignty

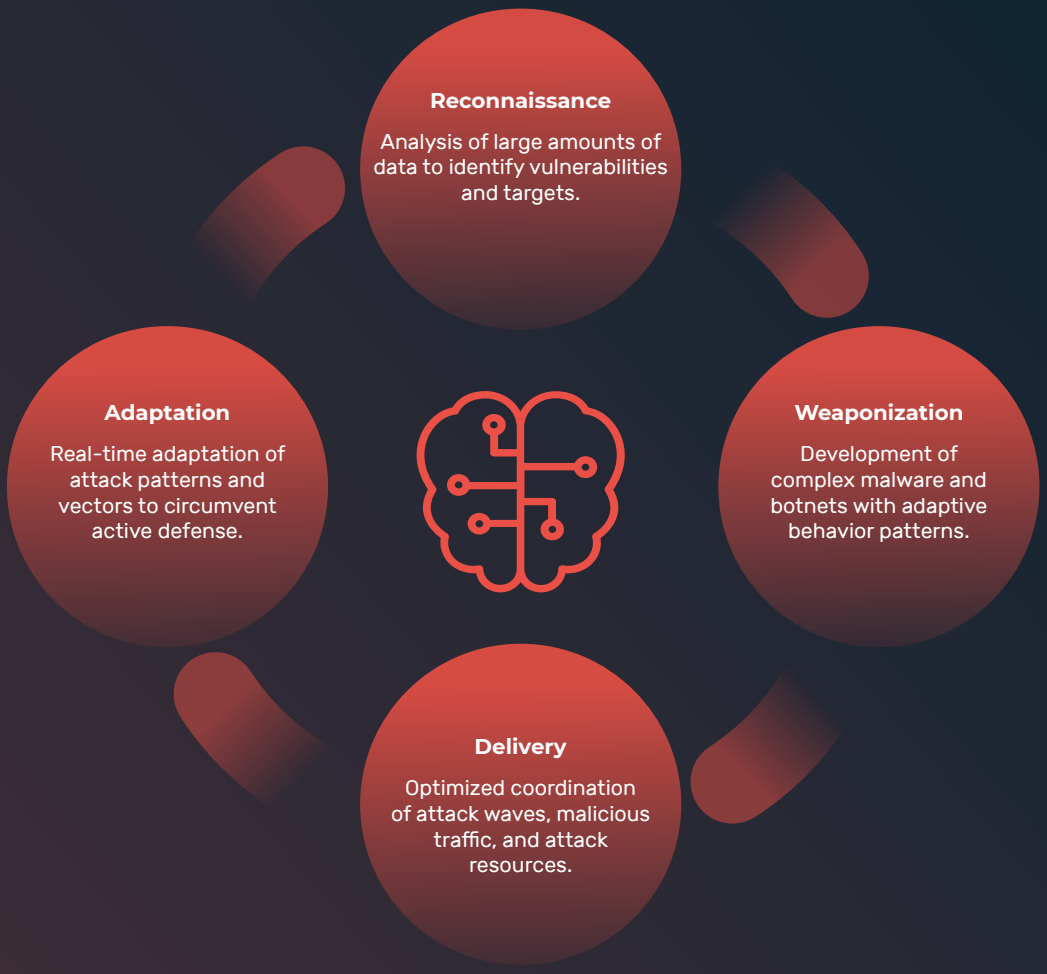
Offensive AI Escalates the Threat Situation

Fast, precise, inexpensive: the widespread availability of AI is revolutionizing cybercriminal attack campaigns worldwide. By integrating AI into attack tools (offensive AI), cyber actors can more quickly and easily identify gaps in companies' defenses and exploit the attack vector that offers the highest success rate.

Whereas experienced black hat hackers used to be needed to spend several days identifying specific security leaks for attacks such as XSS, SQLi, or unprotected domains, today a novice with well-trained AI can do the same in a matter of hours. AI makes it possible to orchestrate adaptive and long-lasting attack campaigns that target entire industries for months on end without the perpetrators being identifiable. This greatly exacerbates the cyber threat landscape, as attacks become more numerous, more precise, and more powerful. In practice, AI takes over classic tasks such as reconnaissance (information gathering), evaluation of attack paths, impact analysis, and selection of the most effective points of attack.

The following chapter provides a qualitative overview of the most relevant AI cyber risks in the context of malicious data streams. The findings presented are based on empirical data and experience from the Myra SOC.

Artificial Intelligence Reinforces Every Phase of an Attack



AI supports attack campaigns by automating and optimizing classic tasks such as scouting targets, analysing possible attack paths and evaluating the most promising points of attack. This allows attacks to be carried out more quickly and in a more targeted manner.

The Role of AI in the Further Development of DDoS Attacks

The use of AI-powered attack tools has made the DDoS threat much worse. Cybercriminals are using AI-optimized amplification attacks to ensure their attacks have the greatest impact with the fewest resources. For instance, they can dynamically adjust attack vectors in seconds.

Additionally, cyber actors benefit from AI-powered solutions through the largely automated, efficient orchestration of attacks, botnets, and attack vectors. Intelligent attack systems can bypass defense mechanisms, such as rate limiting and firewalls.

These systems can detect vulnerabilities and adapt their attack patterns, enabling the development of evasive tactics. Additionally, particularly complex and difficult-to-detect attacks can be carried out, gradually undermining classic protective measures. Lastly, AI enables the autonomous and effective management of botnets, significantly increasing their resilience and attack potential.

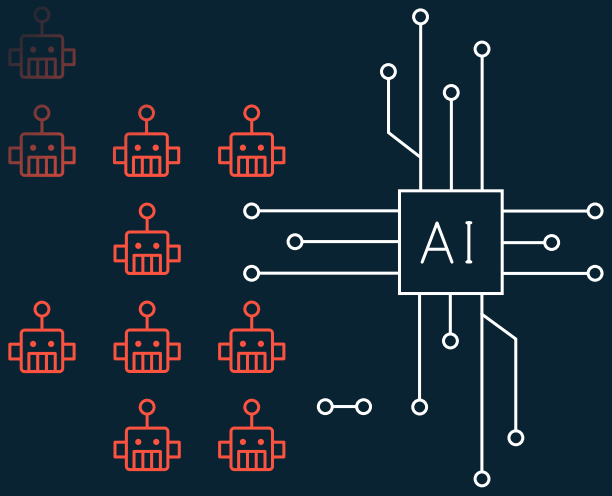
How AI Increases the Risk Potential of Malicious Requests

Distributed Denial of Service (DDoS):
AI-supported automation makes large-scale DDoS attacks easier and more efficient to implement.

SQL Injection:
AI accelerates the automated detection and exploitation of SQL injection vulnerabilities.

Zero-day attacks:
Zero-day attacks exploit unknown vulnerabilities and are particularly difficult to defend against.

Cross-site scripting (XSS):
With AI, XSS attacks can be automated and further developed using payloads that are difficult to recognize.

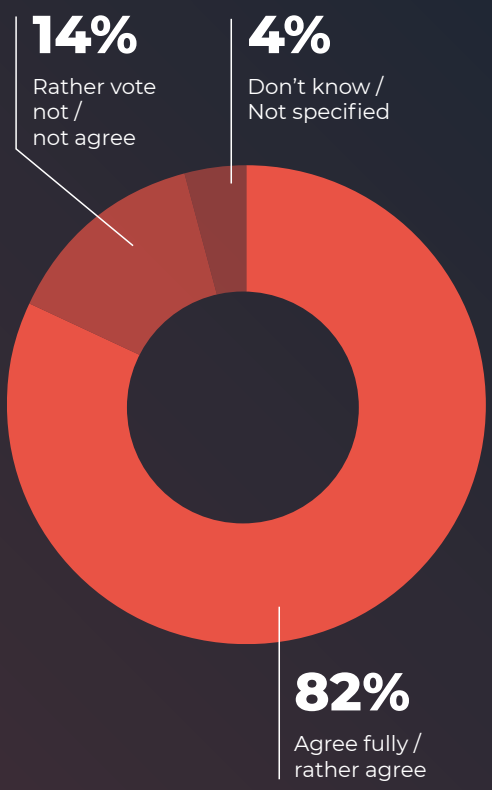


Risks from AI Bots and Crawlers

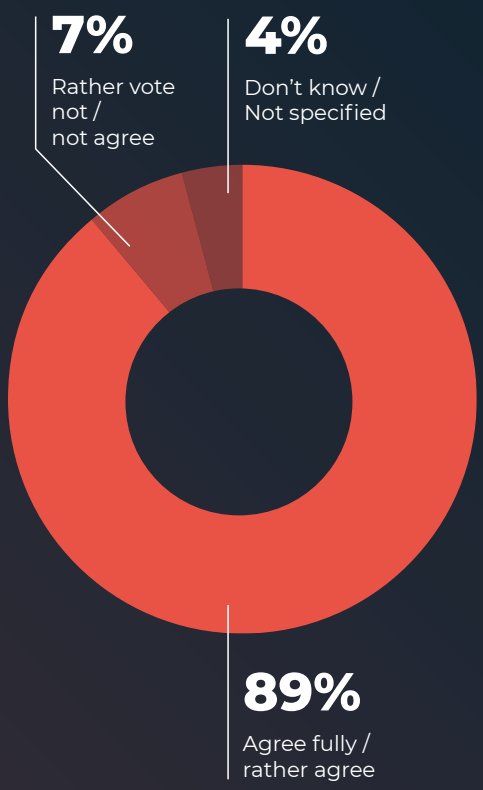
AI-based bots and crawlers search the internet automatically and cause enormous server loads. An example from published data from the cloud hosting service Vercel impressively shows the extent of this. In December 2024 alone, GPTBot generated 569 million requests and ClaudeBot 370 million, which corresponds to around 20 percent of Googlebot requests in the same period. Such immense activity can overload web servers and lead to outages, as demonstrated by an incident at the Git hosting service SourceHut, in which aggressive LLM crawlers paralyzed the company's servers in March 2025.

To What Extent Do You Agree with These Statements About the Use of AI in Cyber Attacks?

Artificial intelligence enables attackers to exploit specific vulnerabilities in our systems.



Artificial intelligence helps make cyberattacks more efficient and targeted.



Companies agree: AI makes attackers significantly more powerful. More than four-fifths believe that AI makes it easier to exploit IT vulnerabilities, while nine out of ten organizations expect AI-enabled attacks to become both more efficient and more targeted.[21]

List of Sources

1 https://www.security-insider.de/deutschland-ziel-cyberangriffe-drohnen-russland-a-ce7e9670547109240427f094798ebc58/
2 https://www.spiegel.de/politik/deutschland/cybersicherheit-rechnungshof-warnt-vor-mangelndem-schutz-der-bundes-it-a-6baacfe5-2e6b-4e8b-a64b-e10d9cf2585e
3 Bitkom Wirtschaftsschutz 2024
4 Allianz Risk Barometer 2025
5 EY Datenklaustudie 2025 | Forensic & Integrity Services
6 https://www.cisa.gov/news-events/alerts/2014/01/17/udp-based-amplification-attacks
7 Verizon: 2025 Data Breach Investigations Report
8 https://krebsonsecurity.com/2025/05/krebsonsecurity-hit-with-near-record-6-3-tbps-ddos/
9 Allianz Risk Barometer 2025
10 ENISA: Threat Landscape: Finance Sector 2025
11 BaFin: Strategische Ziele 2026-2029
12 ENISA: Threat Landscape: Finance Sector 2025
13 Antwort der Bundesregierung auf die Kleine Anfrage der Abgeordneten Manuel Höferlin, Maximilian Funke-Kaiser, Konstantin Kuhle, weiterer Abgeordneter und der Fraktion der FDP – Drucksache 20/14372
14 Allianz Risk Barometer 2025
15 https://kommunaler-notbetrieb.de
16 https://www.zeit.de/digital/2025-01/parlamentarische-anfrage-zahl-cybersicherheitsvorfaelle-kritische-infrastruktur-gestiegen
17 https://www.bsi.bund.de/DE/Themen/Regulierte-Wirtschaft/Kritische-Infrastrukturen/KRITIS-in-Zahlen/kritis-in-zahlen_node.html
18 https://www.tagesschau.de/inland/innenpolitik/bsi-energie-cyberangriffe-100.html
19 Myra Security: State of Digital Sovereignty 2025
20 Bitkom Cloud Report 2025
21 TÜV Cybersecurity Studie 2025

That's Why CISOs Choose Myra

Security

Cyber attacks steal data, cause system failures, and disrupt communication channels. Myra defends your digital processes against attacks in real time.

Performance

Traffic spikes caused by sales campaigns, live streaming, or unforeseeable events can overwhelm web applications. Myra always delivers your content with high performance.

Business Continuity

Myra ensures maximum protection for your business by using direct and geo-redundant connections to your infrastructure without relying on external factors.

Compliance

Legal and company-specific requirements for IT security and data protection require audited processes. Myra is your guarantee for the strictest requirements.

Cyberresilienz

Myra strengthens the robustness of your infrastructure against cyber threats so that attacks do not impair or halt business operations.

Digital Sovereignty

With Myra, you can manage your digital supply chain independently while maintaining control over critical processes and data at all times.

BSI-certified IT Security

Myra technology is certified by the German Federal Office for Information Security (BSI) to the standard ISO 27001 based on IT-Grundschutz. We are one of the leading security service providers worldwide to meet all 37 criteria the BSI has set for KRITIS qualified DDoS mitigation service providers.

ISO 27001 BSI zertifiziert auf der Basis von IT-Grundschutz Zertifikat Nr.: BSI-IGZ-0667-2024 | PCI DSS Certified | BSIG KRITIS-qualifiziert | BSI C5 Testat Typ 2 | Trusted Cloud Service 10043 | Certified IDW PS 951 ISAE 3402 | KRITIS Nachweis gemäß § 8a. Abs. 3 BSIG | Certified ISO 9001:2015 Company

Certified by the Federal Office for Information Security (BSI) in accordance with ISO 27001 on the basis of IT-Grundschutz | Certified in accordance with Payment Card Industry Data Security Standard (PCI DSS) | Qualified for critical infrastructure in accordance with Section 3 BSI Act | BSI C5 Type 2 | Certified Trusted Cloud Service | IDW PS 951 Type 2 (ISAE 3402) audited service provider | KRITIS operator in accordance with Section 8a (3) BSI Act | ISO 9001 quality management

We Protect What Matters. In the Digital World.

1&1 versatel | Barmenia Einfach. Menschlich. | Baden-Württemberg Staatsministerium | msc Munich Security Conference | Sparkasse | llb 1861 | flatex DEGIRO | Stadt Regensburg

Made in Germany

We Protect What Matters. In the Digital World.

Want to learn more about how our solutions can increase your revenue, minimize your costs, and protect your applications from malicious attacks?

Our team of experts is ready to help you develop a customized solution for your business. Schedule a no-obligation consultation today!

Cyber attacks are expensive, a non-binding conversation costs nothing

Myra Security GmbH

+49 89 414141 - 345
www.myrasecurity.com
info@myrasecurity.com