



CYBERSECURITY REPORT 2025

Testing the Resilience of Digital Society

In cooperation with:



Preface

The year 2024 has once again shown how dynamic and complex the current cyber threat landscape is. While we have seen the situation worsen, there have also been signs of some relief. This development makes it clear that efforts to secure digital business processes are having an effect. At the same time, the utmost vigilance and continuous development of protective measures are still required.

This report covers a wide range of challenges, from the increasing number and complexity of DDoS attacks and the vulnerability of digital supply chains to the risks associated with democratic elections. Particularly worrying is the growing threat to critical infrastructures and the public sector, which form the foundation of our social life.

Despite the current development and the serious situation, there is reason to be confident. Technical advances in automation and the use of artificial intelligence (AI) are opening up new possibilities for more efficient and precise cyber defense. At the same time, we are seeing a growing willingness on the part of public authorities and companies to invest more in their digital resilience.

However, a holistic approach is needed to protect our society from cyber threats in a sustainable and efficient way. This includes not only technological measures, but also a fundamental awareness of cybersecurity at all levels. Regulatory frameworks such as NIS-2, the Cyber Solidarity Act or the Cyber Resilience Act are important cornerstones for an EU-wide protective shield.

The challenges may be great, but the bundling of expertise and resources, as well as the continuous development of protective technologies, offer the potential for a resilient digital future. Let us approach this task with determination and optimism – for a secure and prosperous digital society in Europe.



Christof Klaus
 Director Global Network Defense
 at Myra Security

Contents

Preface	2	Measuring Protection with the DDoS Resiliency Score	14
Executive Summary.....	3	Automation Meets Precision: The Challenges of Efficient Cyber Defense	16
Threat Level Between All-Time High and Decline	7	Sources and References.....	18
Cyberhotspot: Critical Infrastructure and Public Sector.....	8		
Cyber Risks in the Context of the 2025 Federal Elections	11		

Executive Summary

25 %

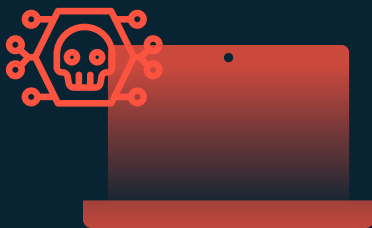


Dynamic Cyber Threat Landscape

In the first half of 2024, there was a significant increase of 53% in malicious traffic compared to the previous year, with a peak in July. From that point on, the number of attacks gradually decreased and was below the previous year's level from October onwards. While geopolitical conflicts and major social events such as the 2024 Olympics and the super election year acted as catalysts, successful operations by international investigative authorities helped to defuse the situation. Despite the turnaround, a 25% increase in malicious requests was recorded over the entire year.

The Supply Chain Challenge

The global outages resulting from the failed CrowdStrike update and the thwarted backdoor attack on XZ-utils have highlighted the vulnerability of digital infrastructure. Particularly in the case of IT systems with robust security, an attack by cybercriminals that takes a detour via external service providers is often the more efficient route.

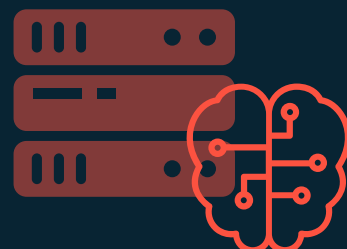


Cybercrime as a Cost Driver

As the frequency and intensity of attacks on digital infrastructure increases, the losses and associated costs will also skyrocket. Across Germany, cybercrime-related damage amounting to 178.6 billion euros is currently anticipated.

AI: From Vision to Practice

The hype surrounding artificial intelligence (AI) in cybersecurity will give way to a more pragmatic view in 2024, with an increasing focus on concrete, measurable benefits. These can be found specifically in the automation of routine tasks such as attack detection – here, the use of AI accelerates the identification of threats by up to 10% in most cases.

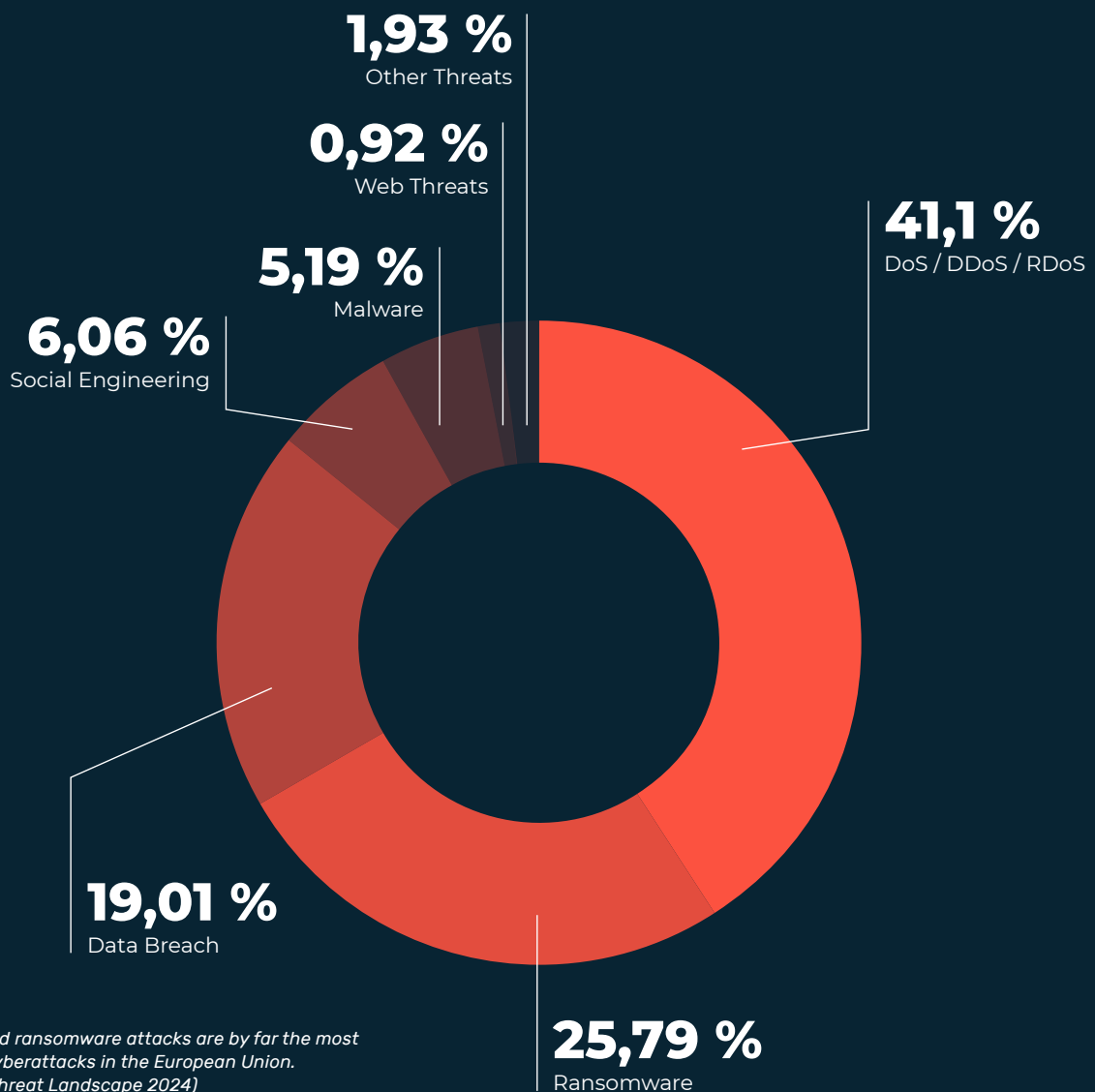


In 2024, the cybersecurity situation as a whole has seen dynamic development. After initially worsening, a gradual improvement was observed as time went on. Specifically, there was a significant year-on-year increase of 53% in malicious traffic flows in the first half of the year. These were primarily DDoS attacks and bot-based attacks on vulnerabilities in online applications and databases.

This increase can be attributed to several factors, including geopolitical tensions such as the Israeli-Palestinian conflict, the ongoing war in Ukraine, and the Taiwan question. These factors led to increased hacktivism and activities by state-sponsored actors. In addition, major events such as the Olympic Games in Paris and the elections in Russia, India, the EU, the US, and the state elections in Germany provided targets for orchestrated cyberattacks.

In July, the Myra systems recorded the highest number of attacks. After this peak, there was a turnaround: from August onwards, the number of attacks fell each month. In October, the number of blocked requests was below the previous year's figure for the first time. This positive development can be partly attributed to successful operations by international investigative authorities, which led to the shutdown of central "cybercrime as a service" platforms. Regardless of the turnaround, a 25% increase in malicious requests can be observed over the entire year. Overall, the risk situation in the area of malicious traffic flows has thus intensified, as in previous years.

Cyber threat situation in Europe: primary attack vectors by number of incidents



DDoS attacks and ransomware attacks are by far the most most reported cyberattacks in the European Union. (Source: ENISA Threat Landscape 2024)

Backdoors and Breakdowns: The Growing Risks of Digital Supply Chains

The events of 2024 show that even well-protected IT infrastructures are vulnerable to weaknesses in digital supply chains. Attackers are increasingly exploiting this by targeting widely used software libraries.

A notable example of this was the backdoor attack attempt on XZ Utils, a common collection of archiving programs for Linux. This supply chain attack was discovered by chance on March 28, 2024, when a PostgreSQL developer noticed unusual CPU utilization during SSH connections.

The attackers had infiltrated the open-source project for over three years to insert malicious code that enabled remote access. The vulnerability received the highest CVSS (Common Vulnerability Scoring System) rating of 10. The complexity and long-term planning indicate state-sponsored actors.

However, the risks for digital supply chains do not only come from malicious attacks; faulty software patches also pose a problem. The global shutdowns of airports, hospitals, banks, government agencies and countless businesses in the wake of the CrowdStrike mishap on July 19 are an impressive illustration of this.

The faulty update caused the failure of approximately 8.5 million Windows systems worldwide. The estimated total cost of the failure for Fortune 500 companies in the US is around 5.4 billion US dollars. Worldwide, the total damage is estimated at around 15 billion US dollars.



Cyber risk situation Germany

On average,
companies experience

49 cyberattacks per year



Consequences

25 % suffer losses over € 500,000

46 % lose customers

47 % have problems with customer
acquisition

Source: Hiscox

“ Cyber security will increasingly advance from an abstract cost factor to a concrete sales argument, because customers can only rely on my performance if I as a company have sufficiently secure processes. ”



Prof. Dr. Dennis-Kenji Kipker
Research Director cyberintelligence.institute
and Myra Advisory Board Member

The Cost of Cybercrime Is Skyrocketing

The escalation of the cyber threat situation over the past few months is also reflected in the increased losses. The German Federal Criminal Police Office (BKA) has recorded an alarming increase in losses caused by organized cybercrime. The amount of damage has almost tripled compared to the previous year and reached 1.7 billion euros. This means that cybercrime accounts for almost two-thirds of the total losses caused by organized crime, which amount to 2.7 billion euros – more than twice as much as in the previous year. BKA President Holger Münch emphasizes: “The fight against organized crime remains a central focus of our work. It causes extensive damage and poses a significant threat to the state, the economy and society through the influence it exerts and the violence it uses.”¹

Meanwhile, the industry association Bitkom provides a broader view of the extent of the damage. Its research has shown that the damage caused to the German economy by cyber security incidents amounts to 178.6 billion euros annually.²

The German Insurance Association (GDV) reports a similar trend. According to their figures, the number of cyber attacks reported to insurers rose by 19% to around 4,000 cases. The insurance companies made payments totaling around 180 million euros, which corresponds to an increase of 50% over the previous year. The average loss per attack was 45,370 euros³

KI-Konsolidierung in der Cybersicherheit

Meanwhile, the initial hype surrounding artificial intelligence (AI) in cybersecurity in 2024 gives way to a more sober assessment. Although one in two IT decision-makers still believes that AI can significantly improve their organization's IT security, the focus is now increasingly on specific business cases that deliver measurable benefits.⁴ The automation of routine tasks is emerging as the greatest advantage of AI in cybersecurity. The use of intelligent algorithms enables companies to analyze large amounts of data in the shortest possible time and thus identify attack patterns early on. Nine out of ten organizations have accelerated attack detection by up to 10% by using AI.⁵ The capacities saved as a result can be used by security teams to address more complex tasks. In view of the ongoing shortage of skilled workers in IT security, AI offers a welcome relief here. In Germany, 62% of organizations report personnel bottlenecks in the area of cybersecurity; specifically, there is currently a shortage of around 120,000 IT security professionals.⁶

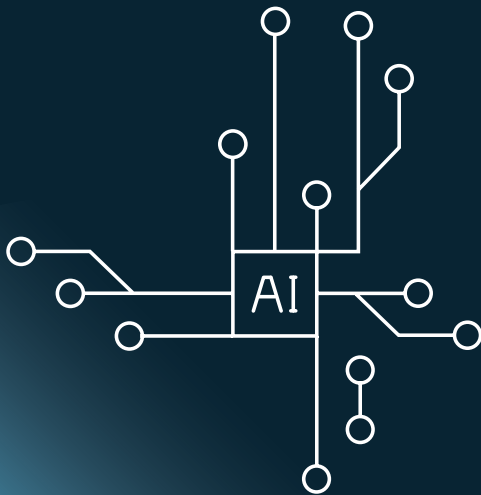
“The sabotaged presidential elections in Romania provide the blueprint: an AI botnet is enough to completely undermine our democracy. The time for warnings is over – either we upgrade our digital resilience now or we lose control of our democratic processes.”



Sergej Epp
CISO at Sysdig and
Myra Advisory Board Member

On the other hand, cybercriminals use AI technology to disguise attacks and exploit security vulnerabilities in the shortest possible time. This puts increasing pressure on IT security teams to install available patches as quickly as possible and to reduce the attack surface when vulnerabilities become known. Accordingly, 8 out of 10 companies in Germany assume that the widespread availability of AI has sustainably exacerbated the threat situation for the economy.⁷

The high level of dynamism in this field of technology also poses enormous challenges for European digital policy. On the one hand, it is important to promote innovation and strengthen the competitiveness of European companies. On the other hand, risks must be effectively contained and ethical standards maintained. The implementation of the AI Act initiated by the EU Commission offers an opportunity to pursue these goals in a gradual and structured manner.

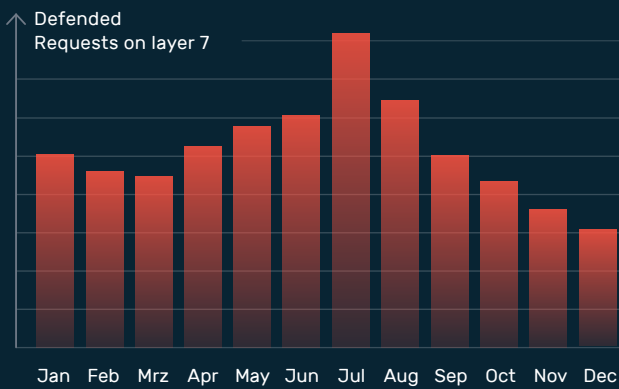


Threat Level Between All-Time High and Decline

Managing cyber incidents caused by malicious traffic is an immense challenge for an increasing number of organizations in Germany and Europe. Almost half of all cyber incidents in Europe (41,1 %) are due to a DDoS attack, followed by ransomware attacks at 27.3 %.⁸

The analyses from the Myra SOC (Security Operations Center) underscore this trend. Over the entire year, an increase of around 25% in malicious requests was observed here. In particular, a significant increase was recorded in the first half of the year up to and including July. The malicious traffic flows consist of DDoS attacks, bot attacks and malicious attempts to access databases via cross-site scripting (XSS), cross-site request forgery (CSRF) or SQL injection.

Attack activity 2024

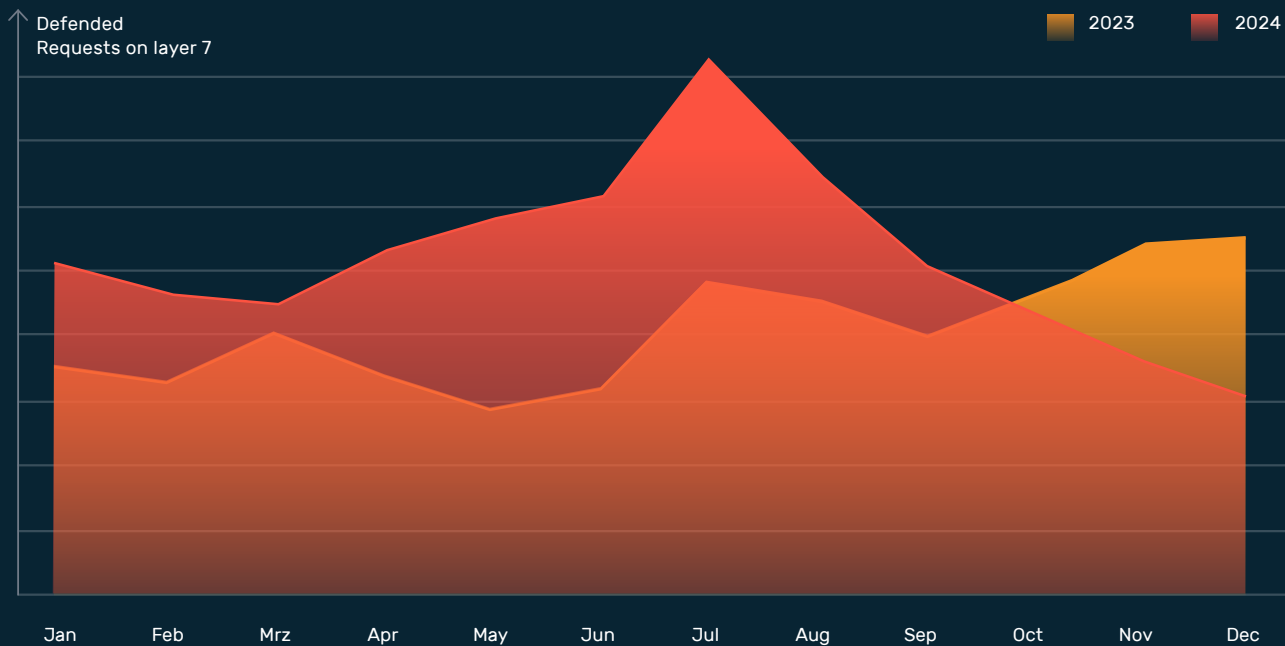


Malicious traffic flows at application level peaked in the middle of 2024.

July 2024 marked the month with the highest number of mitigations since the start of the analysis. In the period from January to July, the number of requests blocked rose by 53% compared to the previous year. After July, however, a trend reversal can be observed. From this point on, the number of attacks in the monthly analysis decreased step by step and has been below the previous year's figure since October. Compared to the intensive summer months, the situation visibly eased towards the end of the year.

The observed development of cyber attacks in 2024 can be explained by a combination of various factors. On the one hand, the first half of the year was strongly influenced by geopolitical conflicts, which led to an increase in hacktivism and the activity of state-sponsored actors. Examples include the Israel-Gaza conflict, the ongoing war in Ukraine and the Taiwan issue.

Year-on-year comparison



In 2024 as a whole, the Myra defense systems recorded a 25% increase in malicious requests. The trend reversed in July, since when the number of attacks has been falling - from October onwards, the figures were even lower than in the previous year.

In addition, major social events such as the Olympic Games in Paris and the elections in Russia, India, the EU, and the US, as well as the state elections in Saxony, Thuringia, and Brandenburg, provided an opportunity for orchestrated attacks. It should be noted that cyber actors usually launch their attack campaigns months before the actual date of the respective target event – especially in the case of elections, in order to exert influence by means of disinformation and uncertainty (More on this in the chapter “Cyber risks in the context of the 2025 federal elections” on p. 11 ff.).

The successful actions taken by international investigative authorities against professional cybercriminals are also important in this context. For example, in May, a globally coordinated operation against botnets shut down over 100 servers and more than 2,000 domains that were used to distribute malware.⁹ Other successful operations such as “PowerOFF” led to the closure of the closure of Digitalstress, the world’s most active underground marketplace for DDoS services, and the seizure of 27 of the most-used stresser services, which allowed cybercriminals to easily book overload attacks¹⁰






Cyberhotspot: Critical Infrastructure and Public Sector

Meanwhile, the risk of threats to critical infrastructures (KRITIS) and public administration facilities has by no means diminished in 2024 – quite the opposite. The spread of hacktivism and the increasing activities of politically motivated and state-sponsored cyber actors pose additional challenges for these sectors in particular.

Since incidents at public authorities or critical infrastructure facilities tend to become public knowledge quickly, these organizations are attractive targets from an attacker’s perspective, as they can be used to cause damage and spread uncertainty in society. The affected organizations are well aware of this situation: 9 out of 10 critical infrastructure operators currently assume that the threat situation is intensifying (87%).¹¹

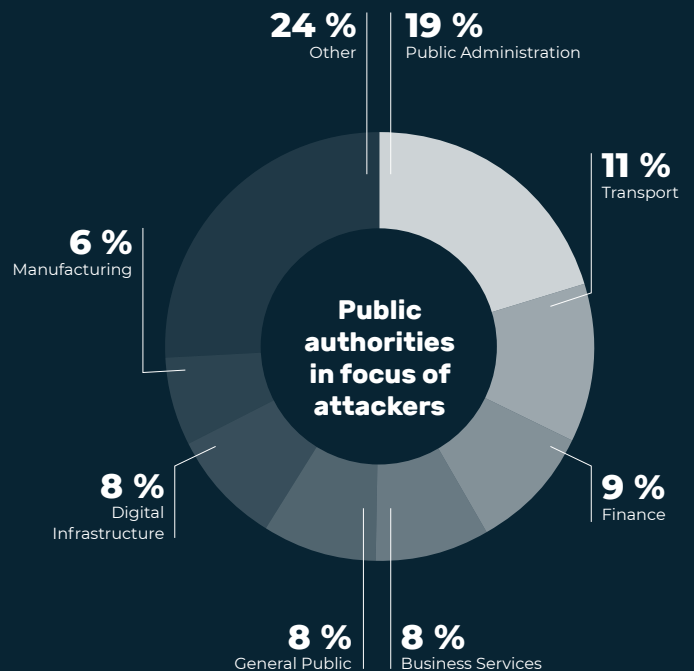
The most dangerous Software vulnerabilities 2024

(MITRE CWE Top 25)

1	Cross-site Scripting	
2	Out-of-bounds Write	
3	SQL Injection	
4	Cross-site Request Forgery (CSRF)	
5	Path Traversal	

The list is based on the analysis of more than 31,000 CVE entries and serves as a guide for developers and security teams, to prioritize and address critical security risks.

Cyber threat situation Europe: Target sectors by number of incidents



Public authorities in the focus of cyber criminals: One in five cyberattacks in Europe targets a public sector organization. (Source: ENISA Threat Landscape 2024)

Critical Infrastructure: Increasing Numbers of Cases

In the first three quarters of 2024, 612 incidents had already been reported by critical infrastructure operators. This high number underscores the urgency of continuously improving protective measures and adapting them to new threat scenarios. Attacks or incidents that lead to the failure of or adverse effects on critical services are particularly worrisome.

One example of the vulnerability of digital infrastructure was the global outage of Windows systems caused by a faulty CrowdStrike update in July. The US cybersecurity firm made faulty changes to its in-house product Falcon Sensor, which led to system failures in Windows environments. As a result of the incident,

thousands of flights had to be canceled, planned operations in hospitals postponed and countless digital services remained disabled for hours. Among those affected were banks, retailers, media and telecommunications companies, as well as government agencies

The CrowdStrike incident clearly shows how important redundantly secured systems and digital sovereignty are in today's IT landscape. Operators of critical infrastructures cannot afford a single point of failure – especially if it is outside of their own digital supply chain and beyond their control.

The crowdstrike failure 2024 in facts and figures:



Affected systems:
8.5 million Windows devices



Duration of the outage of affected services:
approx. 10 hours



Estimated damage:
over 15 billion US dollars



Flight cancellations:
5,078 canceled flights worldwide



Date:
July 19, 2024



Affected systems in German companies:
One third of all PCs, half of all servers

62 %

of the companies surveyed in Germany were directly affected

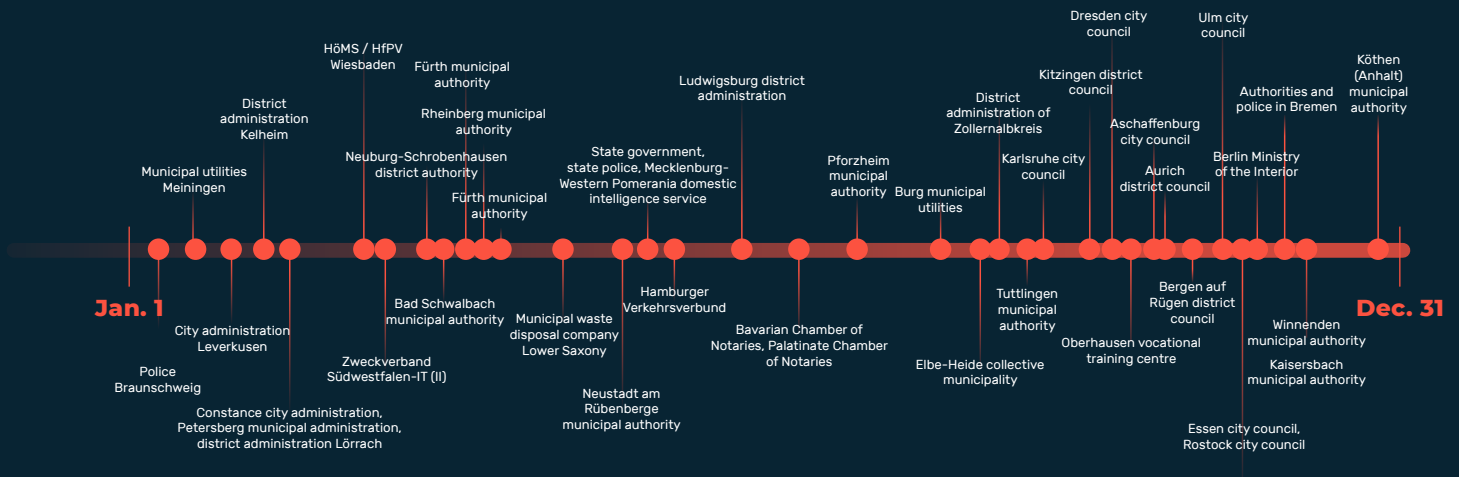
48 %

of the companies surveyed in Germany were indirectly affected via partners

Public Administration Targeted

DDoS attacks are the weapon of choice for hacktivists and politically motivated cyber groups seeking to provoke cyber incidents for publicity purposes. In Europe, the public sector is by far the most affected by denial-of-service attacks: 33% of all reported DDoS attacks target the websites and services of public authorities. Political motivation or an activist agenda is suspected in 40% of DDoS attacks, for example in connection with the war in Ukraine. It is also noteworthy that 56.8% of the DDoS attacks analyzed resulted in the complete failure of the target.¹²

Cybersecurity incidents impacting public authorities and local government



Selection of publicized cyber incidents in the public sector for the year 2024.

In 2024, Europe was hit by several waves of orchestrated attack campaigns. In March, France was hit by a major attack wave, in which the attackers, according to their own statements, disabled 17,000 IP addresses and devices, as well as more than 300 domains.¹³ There were also major campaigns in Switzerland around the Ukraine Peace Conference in June and in Austria in the run-up to the parliamentary elections in September.¹⁴ In October, the attacks shifted to Belgium as a possible response to promised arms deliveries to Ukraine.¹⁵

Most attacks were directed against (police) authorities and public administration organizations, followed by financial institutions and transportation¹⁶ – the same as in Germany. The larger waves of attacks in Germany occurred in the months of March to June and October to December. In most cases, the DDoS attacks were carried out by well-known cyber groups such as NoName057(16), Anonymouse Sudan or Cyber Army Russia.

Due to the ongoing trend towards cybercrime-as-a-service, DDoS attacks involve little effort and low costs for the threat actors. This circumstance enables both a high frequency and an increased scope of attacks. On the side of the affected organizations, however, defense is only possible with dedicated protection systems at all relevant network layers. In the case of large-scale DDoS campaigns, the same result can therefore always be observed: protected environments withstand the attacks, while unprotected ones collapse – with all the consequences that result from this.

NIS-2 Delayed

In response to the ongoing tense cyber threat situation, the EU Commission has launched the NIS-2 directive for the horizontal protection of critical infrastructures. However, its implementation, which was planned for October 17, 2024, is being delayed in many member states, including Germany. Due to the collapse of the coalition government, experts now expect NIS-2 in Germany to be launched only from fall 2025. This delay is regrettable, as the directive aims to increase the level of cybersecurity across the European Union and strengthen the resilience of critical sectors.

Nevertheless, many companies are already preparing for the upcoming requirements. Research by industry associations shows that almost half of the companies surveyed have already taken measures to ensure their cybersecurity in accordance with the new directive – there is no lack of awareness among businesses of the urgency of the issue.

EU Rules for More Cybersecurity

While the NIS-2 directive is still being implemented in Germany and many other EU member states, the Cyber Solidarity Act (CSA) and the Cyber Resilience Act (CRA) promise to strengthen cybersecurity in the European Union in the near future.

The CSA regulation governs the handling and response of member states in the context of major cyber incidents. The aim of the regulation is to improve cooperation between EU countries in the event of major cyber attacks and to enable rapid and effective countermeasures.

At the same time, the Cyber Resilience Act sets new cybersecurity standards for products with digital components and requires manufacturers to ensure security throughout the entire lifecycle.

Together, these laws create a robust framework for protecting critical infrastructure and foster collaboration between EU member states, thereby increasing the resilience of the public sector and the economy to cyberattacks.

Cyber Risks in the Context of the 2025 Federal Elections

New elections to the German Bundestag are scheduled for mid-February 2025. It is important to protect these elections reliably and efficiently against threats. Recent years have shown that electoral processes are generally a preferred target of politically or ideologically motivated cyber actors. For example, published research by the Romanian secret service revealed that the country's electoral infrastructure was the target of more

than 85,000 cyber attacks in the context of the presidentialelections.¹⁷ Due to this influence on the electoral process, Romania's supreme court was forced to declare the first round of the presidential elections invalid.¹⁸ Similar patterns of attack were also observed in the elections in the Republic of Moldova and in Austria (see mitigation case p.13).¹⁹



Meanwhile, in Germany, the Federal Office for the Protection of the Constitution warned at the end of November 2024 of the risks posed by other states exerting influence on the upcoming federal election. "Actions of disinformation and discrediting, cyber attacks, espionage and sabotage are to be expected," the agency warned. "Their aim is to secretly influence decision-makers and officials in other states under false pretenses, but also to interfere with the free formation of opinion and will."²⁰

Although elections in Germany are largely analog, the associated infrastructures of government agencies, authorities, parties, and their service providers are indeed vulnerable. The methods used are varied.

Traditional malware, such as ransomware Trojans or wiperware, can corrupt or destroy important data related to the electoral process, such as voter registration data. DDoS attacks and website defacements undermine confidence in the electoral process, especially if they affect or manipulate the transmission and display of election results. Supply chain attacks can be used to sabotage election-related digital infrastructure by exploiting vulnerabilities in suppliers. Through the use of social engineering and phishing, cyber actors can obtain sensitive information for use in disinformation campaigns, for example.²¹

“ We definitely want to ensure that not only is the election secure, but that people also have confidence in the election. ”

BSI President Claudia Plattner

In addition, hybrid threats such as Foreign Information Manipulation and Interference (FIMI) are on the rise. Research by the European External Action Service (EEAS) has shown that FIMI campaigns are coordinated across platforms and many different channels to create the illusion of authentic discussion and interest, and to disguise the origin of FIMI content. In the 750 incidents analyzed, more than 4,000 channels were active 9,800 times. These were both websites and social media profiles, groups and pages. The most common platforms involved were Telegram and X (formerly Twitter). However, FIMI activity was observed on virtually all other major, emerging, and niche platforms²²

The creation of content for FIMI activities and its distribution on social networks is increasingly done with the help of AI. The widespread availability of large language models (LLMs) and AI-based bots are catalysts that allow disinformation campaigns to spread rapidly and on a large scale. Equally problematic is the growing number of deepfakes. These are AI-manipulated videos, photos, and audio recordings that are nearly indistinguishable from the original content - in practice, only one in ten users is confident that they can identify deepfakes²³



Case Study: Widespread DDoS Attacks Before the Austrian Parliamentary Elections

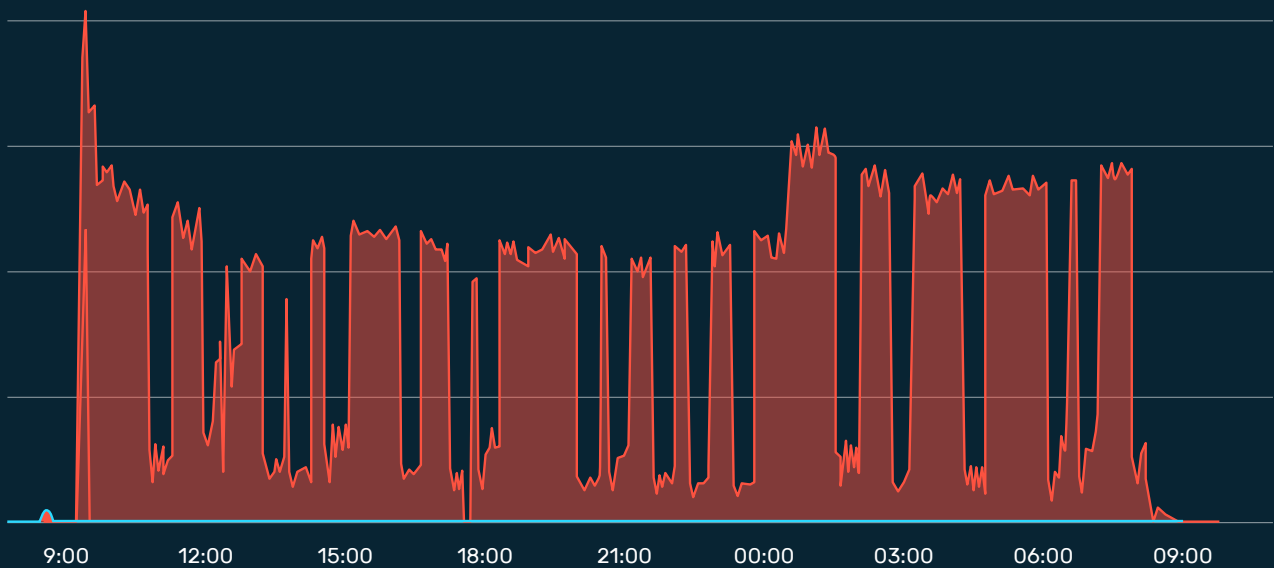
In September 2024, a significant increase in DDoS attacks on Austrian organizations was observed over an extended period of time in connection with the parliamentary elections. On September 16, the Austrian Computer Emergency Response Team (CERT.at) warned of a large-scale DDoS attack campaign against authorities and organizations in the country.

Particularly affected were the websites of ministries, administrative authorities, energy suppliers, public transportation systems and political parties. The attacks led to temporary outages at several important institutions, including, according to media reports, the websites of the ÖVP and SPÖ parties, the Ministry of Defense, the Court of Auditors and the Public Employment Service (AMS).

Thanks to Myra’s protection systems, a central state authority was able to fend off a 24-hour attack, thereby avoiding any consequences. This underscores the importance of robust protective measures against DDoS attacks.



Mitigation of a 24-hour attack



The graphic shows a typical DDoS attack that was averted as part of the attack campaign on Austrian organizations in September 2024. The attack occurred in several waves over a period of almost 24 hours.

DDoS Resiliency Score Makes Defense Measurable

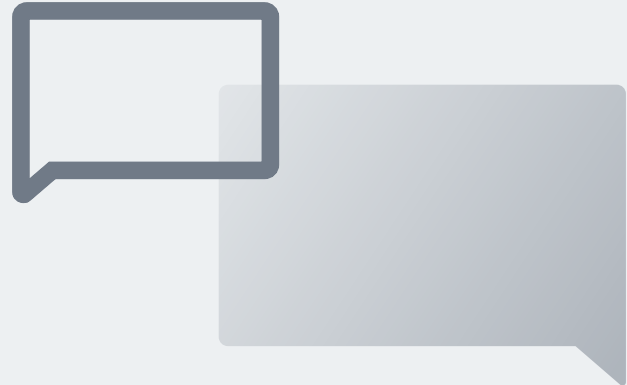


When it comes to DDoS protection, not all solutions are equal. This is a fact that companies around the world experience every day when their digital business processes are shut down by a DDoS attack despite supposedly solid protection.

Holistic protection requires more than the basic defense that many hosting and cloud providers offer by default for the network and transport layers (layers 3/4). In particular, attacks at the application layer are becoming increasingly complex and cannot be distinguished from valid traffic by layer 3/4 protection systems.

The DDoS Resiliency Score (DRS) was developed to raise awareness among companies for these and other challenges in defending against DDoS attacks – a framework that allows an objective evaluation of protective measures and highlights potential for improvement.

In the following interview, Markus Manzke, Chief Technology Officer (CTO) of zeroBS and DRS Board Member, explains how the framework makes the protection readiness of organizations transparently measurable and what advantages it offers for optimizing defenses.



Markus Manzke,
Chief Technology Officer (CTO) at zeroBS and
DRS Board Member

What exactly is the DDoS Resiliency Score (DRS)?

The DRS is a standard for objectively and quantitatively measuring and evaluating strategies for defending against DDoS attacks. It provides a standardized scale to quantify the strength and complexity of attacks and the ability to withstand them. The DRS enables companies to assess the resilience of their systems against DDoS risks.

Why is such a score necessary?

Despite the abundance of available data and solutions, there is still no standardized scale for evaluating DDoS mitigation measures. The DRS fills this gap and enables organizations to assess their readiness against various types and sizes of DDoS attacks in a granular way.

How can organizations use the DRS in practice?

On the one hand, the DRS can be used to objectively and structurally assess an organization's readiness for DDoS attacks. This assessment enables a better evaluation of the protective measures available and simplifies communication between technical teams and management. This results in data-based decision-making processes.

On the other hand, B2B IT companies such as protection providers, scrubbing centers, Internet service providers (ISPs), cloud providers or even hosting companies can use the DRS to meet regulatory requirements (DORA, TIBER, NIS-2) regarding service quality or IT risk management.



What factors does the DRS address?

The DRS is based on seven ascending levels of DDoS attacks. Each level brings with it additional attack types, more sophisticated attack vectors, and larger traffic volumes. Accordingly, the requirements for the defense increase, with each level requiring a shorter response time for mitigation and lower latency.

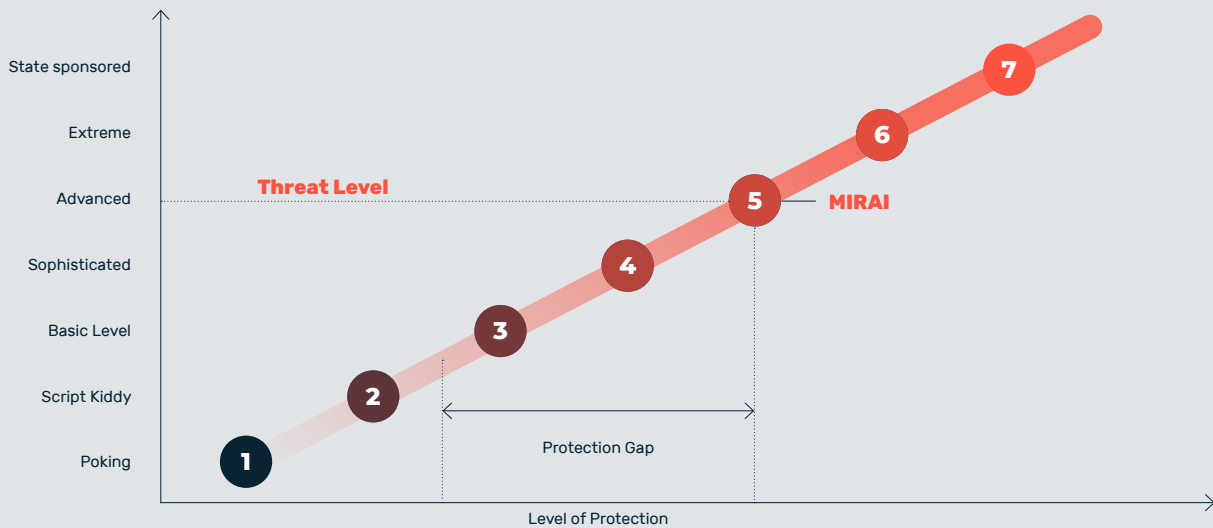
Who is the DRS designed for?

The DRS can be used by various groups: security consultants can use the standard to provide better service to end customers; DDoS stress test providers can use the DRS to perform objective and comparable tests; protection providers can integrate the DRS into their development cycle to meet SLAs and compliance requirements.

What other advantages does the DRS offer protection providers?

By using the DRS, providers can reduce the effort required for incident management, minimize downtime, and optimize staffing requirements. This results in cost savings, reduced risks associated with service delivery and SLA violations, and a competitive advantage.

DDoS Resiliency Score (DRS) at a Glance



Level	Name	Volume	Requests per Second (RPS)	Number of Attack Vectors
1	Poking	100 MBit	1.000	1
2	Script Kiddy	1 GBit	5.000	2
3	Basic Level	100 GBit	10.000	5
4	Sophisticated	500 GBit	100.000	10
5	Advanced	1.000 GBit	1 Mio	Unlimited
6	Extreme	Unlimited	Unlimited	Unlimited
7	State sponsored	Unlimited	Unlimited	Unlimited

DRS takes a quantitative approach to measuring DDoS resilience. With each level from 1 to 7, the requirements for the mitigation volume, the number of requests, and the attack vectors used increase. In the two upper levels for extremes and state professionals, increasingly complex attack methods and the sophistication level are crucial.

Automation Meets Precision: The Challenges of Efficient Cyber Defense



Christof Klaus
Director Global Network Defense
at Myra Security

The increasing professionalization of cybercriminals and the use of modern technologies such as artificial intelligence for malicious purposes requires an adaptation of the defense strategy – efficient countermeasures are needed now.

Myra's solution: highly automated systems capture, process and analyze global data traffic in the Myra DNS in real time to identify anomalies in fractions of a second and initiate appropriate countermeasures. This approach makes it possible to significantly increase the efficiency of defense measures despite the increasing complexity of attacks.

In the following interview, Christof Klaus, Director Global Network Defense at Myra Security, explains what is important for a fast and effective cyber defense and what role AI plays on the part of attackers and defenders.

What technologies does Myra use to quickly and efficiently fend off attacks?

We use a variety of different mechanisms to detect and defend against attacks. Insights into attacks and access patterns are always obtained from the most appropriate sources. Either a countermeasure is then initiated at this point, or the data generated here is merged with insights gained elsewhere and then evaluated in a larger context.

What are the challenges in developing a highly automated protection system?

The challenges in developing these systems are also many and varied. Some of them can be counteracted by well-planned investments in hardware. This directly addresses aspects such as computing power, bandwidths, speeds, interfaces and the like. Other challenges, especially in the field of analytics, can only be solved by software solutions developed in a very targeted manner. In addition to the pure performance requirements for such solutions, architectural aspects such as horizontal scalability and redundancy, as well as flexibility and targeted adaptability, are of the utmost importance.

How does Myra technology help to detect and defend against unknown and complex attack patterns at an early stage?

Two aspects are particularly important when defending against attacks. First and foremost, it is necessary to recognize the attack itself. In most cases, there are very clear changes from "normal operation" in these cases, whether it's a sharp

“ *The fact is that, today, you have to protect yourself holistically against all types of attack, because an unmitigated attack – at any level – always has negative effects on the overall system.* **”**

increase in traffic or, for example, an accumulation of WAF triggers. The second – much more complex – requirement is then to distinguish "good" from "bad" traffic and selectively filter out the bad traffic. Another aspect that enables us to proceed particularly effectively and quickly here is that the deployment of highly specific blocking rules – precisely tailored to the respective attack – takes place within fractions of a second across the entire CDN.

How does automated defense in the area of network and infrastructure protection differ from application protection?

The most obvious difference between infrastructure and application protection is the amount of data available for selectively fending off an attack. With application protection, the respective application protocols and parameters provide a detailed account of what happens when a page is accessed and how visitor behavior is to be interpreted.

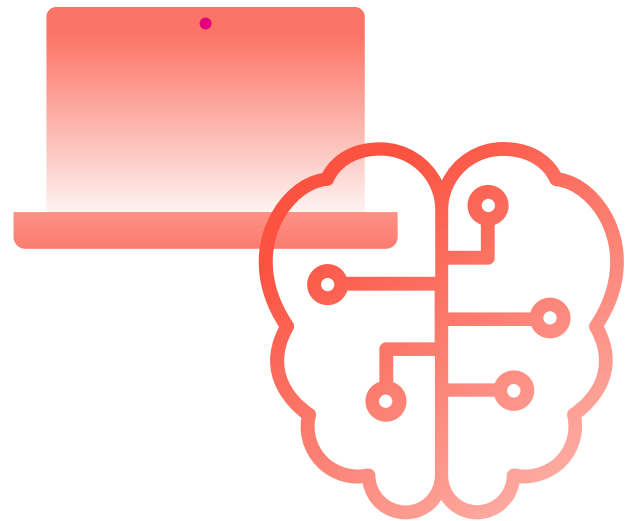
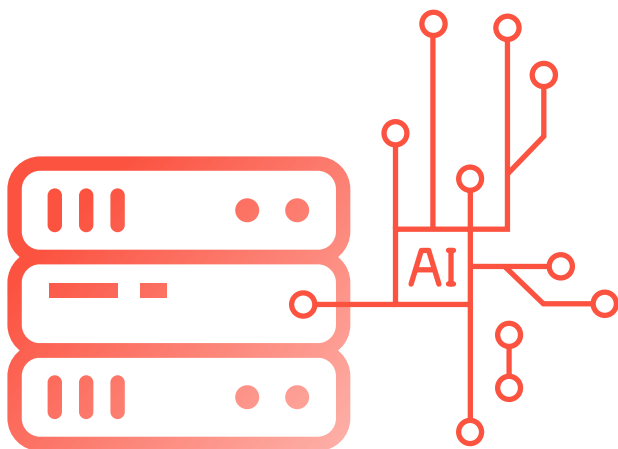
Traffic at the infrastructure level is not decrypted and thus offers a significantly smaller amount of information for rule formation. A GET flood or a cachebuster attack on HTTPS only looks like a lot of traffic on port 443 at the unencrypted network level and is therefore difficult to distinguish. In this case, other parameters such as IP reputation, GeoIP databases and other analysis tools must be used to defend against the malicious traffic. The fact is that nowadays, holistic protection against all types of attack is essential, because an unmitigated attack – regardless of the level – always has negative effects on the overall system.

Let's look at the other side of the coin: what challenges arise from the increasing misuse of AI as an attack tool?

In particular, AI-based systems offer a speed advantage over human actors. An AI can access and apply information about a vulnerability within a very short time after it has been published. Furthermore, it is possible to combine these new attacks with techniques such as WAF evasion and other attack vectors in a fully automated way until a successful result is achieved. This increases the pressure on service providers to fix published vulnerabilities in the shortest possible time and to put solid defense systems in place to remain secure.

How do attackers use AI for attacks, aside from phishing?

Another advantage of AI, in addition to the time factor already mentioned, is the ability to modify attack patterns during the attack. Particularly in the area of application protection, we are seeing attempts to make it more difficult to identify the attacker by randomly changing entire parameter groups during an attack. This significantly increases the sophistication required of the mitigation systems in order to still be able to defend effectively.



What are the limits of automation and AI in cybersecurity, and where is human intervention still necessary?

AI systems can work extremely quickly and efficiently. However, they are often only able to do so in the exact areas in which they have been trained. New fields of application are difficult for them to access or only within the framework of "general" adaptations. So whenever an overall view, an understanding of the interaction of individual services, in-depth expert knowledge or simply dealing with previously unknown situations is required, humans remain unsurpassed in their adaptability. This applies to both attackers and defenders.

Sources and References

- 1 BKA: Organisierte Kriminalität - Bundeslagebild 2023
- 2 Bitkom Wirtschaftsschutz 2024
- 3 <https://www.gdv.de/gdv/medien/medieninformationen/mehr-cyberschaeden-praevention-wichtiger-denn-je-181946>
- 4 Bitkom Wirtschaftsschutz 2024
- 5 Capgemini Research Institute 2024: New defenses, new threats: What AI and Gen AI bring to cybersecurity
- 6 ISC2 Cybersecurity Workforce Study 2024
- 7 Bitkom Wirtschaftsschutz 2024
- 8 ENISA Threat Landscape Report 2024
- 9 <https://www.europol.europa.eu/media-press/newsroom/news/largest-ever-operation-against-botnets-hits-dropper-malware-ecosystem>
- 10 <https://www.europol.europa.eu/media-press/newsroom/news/law-enforcement-shuts-down-27-ddos-booters-ahead-of-annual-christmas-attacks>
- 11 Bitkom Wirtschaftsschutz 2024
- 12 ENISA Threat Landscape Report 2024
- 13 <https://www.dw.com/de/gro%C3%9Fe-cyberattacke-trifft-ministerien-in-frankreich/a-68499200>
- 14 <https://www.ncsc.admin.ch/ncsc/de/home/aktuell/im-fokus/2024/kfu.html>
- 15 <https://www.vrt.be/vrtnws/de/2024/10/07/websites-belgischer-behoerden-im-visier-eines-cyberangriffs-eine/>
- 16 ENISA Threat Landscape Report 2024
- 17 <https://www.bleepingcomputer.com/news/security/romanas-election-systems-targeted-in-over-85-000-cyberattacks/>
- 18 <https://www.spiegel.de/ausland/rumaenien-praesidentschaftswahl-muss-wiederholt-werden-a-5040d09f-e6ae-4ca4-8a60-122a9c7b4ce0>
- 19 <https://www.krone.at/3580528>
- 20 <https://www.tagesschau.de/inland/verfassungsschutz-warnung-cyberangriffe-bundestagswahl-100.html>
- 21 ENISA Compendium on Elections Cybersecurity and Resilience 2024
- 22 European Union External Action - 2nd EEAS Report on Foreign Information Manipulation and Interference Threats
- 23 <https://www.ofcom.org.uk/online-safety/illegal-and-harmful-content/deepfakes-demean-defraud-disinform/>

Fortify Your Digital Defenses With Myra



Security

Avoid data theft, system outages, and disrupted communications. Our robust defense system protects your critical processes with unwavering vigilance.



Performance

Experience high-performance delivery of your content, even during traffic peaks. Maintain optimal performance and provide your users with a seamless experience.



Business Continuity

Myra ensures the utmost protection for your business by utilizing direct and geo-redundant connections to your infrastructure, without relying on external factors.



Compliance

Meet the requirements of IT security and data protection teams with ease. Myra is your trusted partner, offering unrivaled expertise in the strictest compliance regimes.

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



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.



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