MYRA

CYBERSECURITY REPORT H1 2024:

Critical Processes in Focus

In collaboration with:

zeroBS

Introduction

In times of increasing geopolitical tensions, cybersecurity is becoming increasingly important for the well-being of society. In the year 2024, new challenges and risks await, but also opportunities for companies, public institutions and individuals alike.

Hacktivism is experiencing a worrying upswing, driven by global conflicts and social crises. Politically motivated groups are increasingly using cyberattacks as a tool to achieve their goals and demands. At the same time, we are observing a progressive professionalization of attack methods and technologies. Cybercriminals are using increasingly sophisticated techniques to exploit vulnerabilities in systems and networks.

The continuing trend towards "cybercrime as a service" is particularly alarming. This form of cybercrime is aimed at the direct monetization of attacks by offering them as a service via darknet forums. This gives a broad audience of criminal actors access to cyberattacks. With targeted attacks on authorities and other public institutions or politicians, cybercriminals pursue the goal of creating uncertainty in the public perception. In the 2024 super-election year, this could have far-reaching consequences for democratic processes.

Artificial intelligence (AI) plays an ambivalent role in cybersecurity beyond the current hype surrounding the technology. On the one hand, AI enables improved defensive measures and automated security processes. On the other hand, it opens new opportunities for cybercriminals to launch even more sophisticated attacks.

In view of these developments, companies and public institutions are confronted with enormous challenges. The implementation of new regulations such as the NIS-2 Directive and the ongoing discussions about data protection and cross-border data transfers are adding to the pressure.

In this report from Myra Security, IT decision-makers get a comprehensive overview of the current trends and challenges in the field of cybersecurity – with a particular focus on the risks of malicious traffic. We will show how organizations can strengthen their defense strategies to counter the many threats.

Content

Executive Summary

DDoS Threat Landscape and Attack Trends

The number of malicious web requests rose by 53.2% in the first half of 2024 compared to the same period last year.

New attack techniques such as “HTTP/2 Continuation Flood” pose an increased threat.

Public administrations and critical infrastructure are increasingly the target of cyberattacks across Europe. The number of attacks in the EU rose by 31% year-on-year.

Attacks on websites, web applications and APIs are the most difficult for organizations to defend against due to increasing technical complexity.

Artificial Intelligence in Cybersecurity

Artificial intelligence (AI) plays an ambivalent role in cybersecurity. AI offers significant opportunities to improve security measures, but also poses risks, as it can also be used by cybercriminals. AI-based attacks are a concern for many companies, while at the same time AI systems are used for the automated identification of anomalies and real-time monitoring.

Cyber incidents are the

#1 risk factor

Allianz Risk Barometer 2024

Economic Impact: €148 billion in Damages

The professionalization of cybercriminals and the growing use of cybercrime-as-a-service platforms are increasingly exacerbating the threat situation. The costs of cybercrime are enormous, with an estimated €148 billion per year for the German economy and €8.6 trillion worldwide for 2024 – this corresponds to around half of the European Union’s gross domestic product in 2023.

Compliance Challenges

- NIS-2 is just around the corner: The EU NIS-2 Directive is intended to ensure a uniformly high level of cybersecurity throughout the EU. It expands the scope of application considerably from October 2024 and imposes stricter requirements. In Germany alone, around 30,000 organizations will be affected. However, many companies are not yet sufficiently prepared for the implementation, which represents a challenge for SMEs in particular.
- GDPR vs. FISA 702: The GDPR has led to improvements in data security, but due to controversial legislation there are still legal uncertainties regarding cross-border data transfers, particularly between the EU and the U.S.

7 out of 10
organizations expect serious damage from DDoS attacks.

Lünendonk 2023

More than half
of all organizations see their existence threatened.

Bitkom 2023

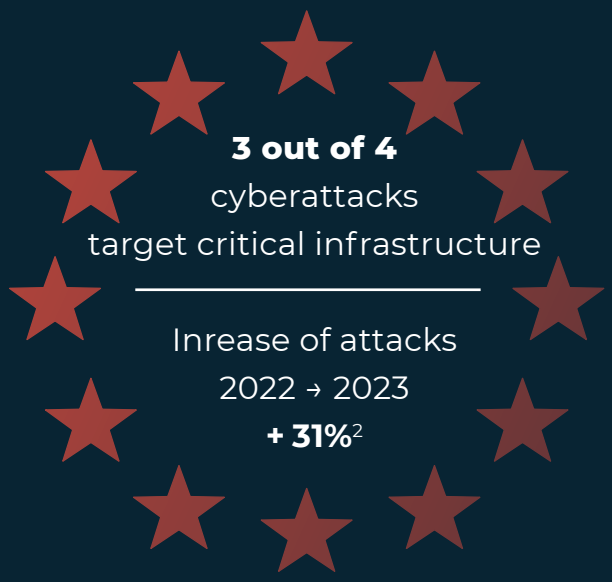
Trends and Forecasts

The cybersecurity landscape will continue to be characterized by geopolitical tensions, the increasing professionalization of cybercriminals, and the development of new attack techniques. Companies and organizations must continuously adapt and improve their security measures and improve them to keep pace with the evolving threats. Legislators and supervisory authorities need to provide the appropriate frameworks to make society resilient to these risks.

Critical Processes in Focus

Cyber incidents affecting organizations in the critical infrastructure sector are on the rise. In the first quarter of 2024 alone, 181 incidents were reported to the German Federal Office for Information Security (BSI). On average, one in six critical infrastructure organizations recorded a cyber incident – the sectors particularly affected were energy, finance and insurance, transportation and healthcare.[1]

Threat Situation in the EU



Public administration institutions are also under increasing pressure. As a result of geopolitical developments since the start of the war in Ukraine, public authorities are increasingly facing attack campaigns from politically motivated groups.

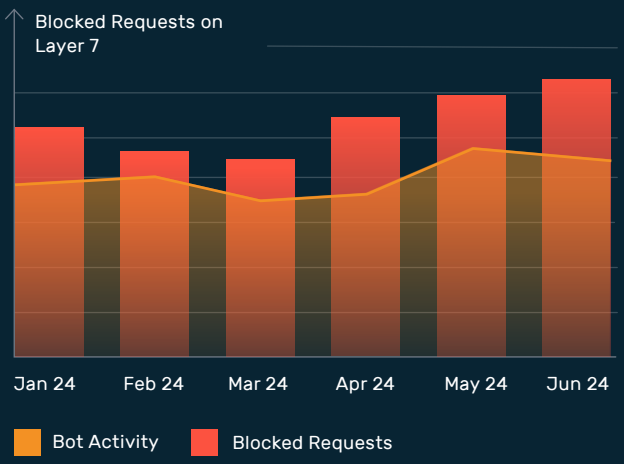
In March, a massive wave of DDoS attacks hit French government websites. The attackers reportedly disrupted 17,000 IP addresses and devices, as well as more than 300 domains. In early April, hacktivists launched a large-scale DDoS campaign that caused the partial outage of websites of several German state and police authorities in Berlin, Brandenburg, Mecklenburg-Western Pomerania, Lower Saxony, Saarland, Saxony-Anhalt, Schleswig-Holstein and Thuringia.

DDoS Attacks, Cyberattacks and Bad Bots: Malicious Requests Increase by 53.2%

These trends can also be seen in the mitigation data from Myra's Security Operations Center (SOC). As a cybersecurity service provider for highly regulated industries, Myra can provide a detailed picture of developments in the financial, insurance, healthcare, government, and critical infrastructure sectors.

For the first quarter of 2024, the number of malicious requests on websites, online portals and web APIs increased by 29.8% compared to 2023. In the second quarter, the growth was even more pronounced at 80%. Over the entire first half of 2024, the increase in malicious requests was 53.2% compared to the same period of the previous year. This malicious traffic is made up of DDoS attacks, attacks on vulnerabilities in online applications and bot-based attacks. Particularly for May and June, traffic monitoring from the Myra SOC shows a high level of activity from malicious bots.

Attacks and Bot Activity



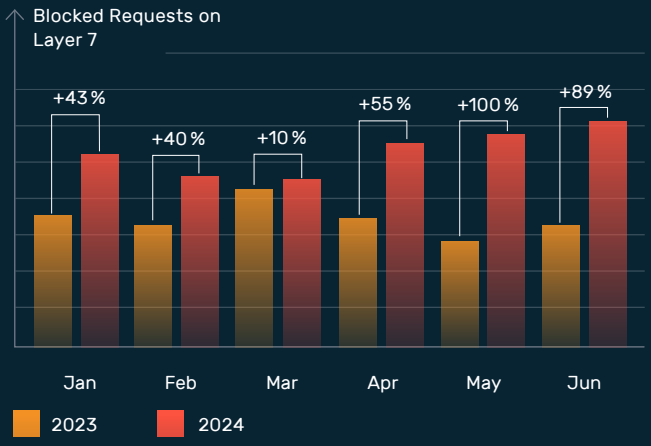
After a slight downward trend in the first quarter of 2024, the number of malicious requests has been rising steadily again since April. Autonomous access by malicious bots largely follows this trend, although a slight decline can be observed at the end of the second quarter.

One of the reasons for the tense threat situation is the increasing professionalization of cybercriminals, which the BSI has already pointed out. Through cybercrime-as-a-service platforms, criminal services such as DDoS attacks are provided cheaply via the darknet – simple attacks are available there for as little as $10.[3] This means that attacks are also possible for actors without any special technical skills.

Another example of the mass distribution of attack tools is the DDoSia project of the criminal group NoName057(16). The tool is made available to followers of the group via Telegram messenger. Once installed, the client computer acts as part of a botnet to carry out DDoS attacks.

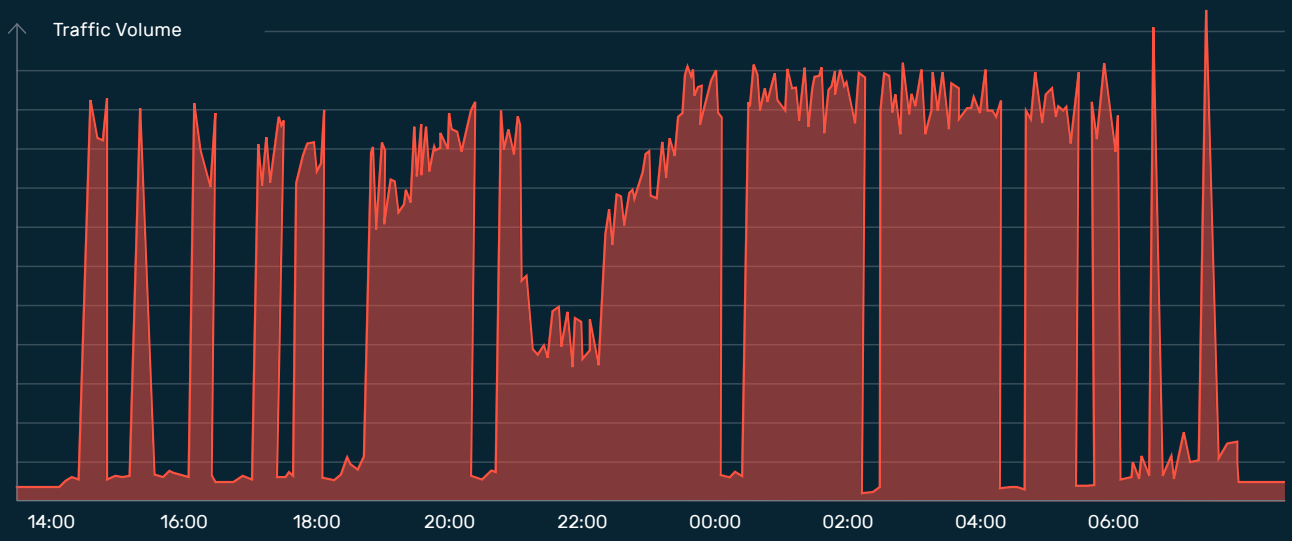
A look at the Myra SOC shows just how massive the impact of DDoSia has become: In June, Myra's defense systems automatically defended against a 17-hour DDoS attack on the digital processes of a German critical infrastructure company. The attack took place in several waves and led to a hundredfold increase in traffic volume.

Attack Activity: H1 2023 vs. H1 2024



A year-on-year comparison shows a massive increase in blocked requests, particularly in the second quarter of 2024. In May, Myra's protection systems blocked twice as many malicious requests as in 2023.

Progression Analysis of a DDoSia Attack

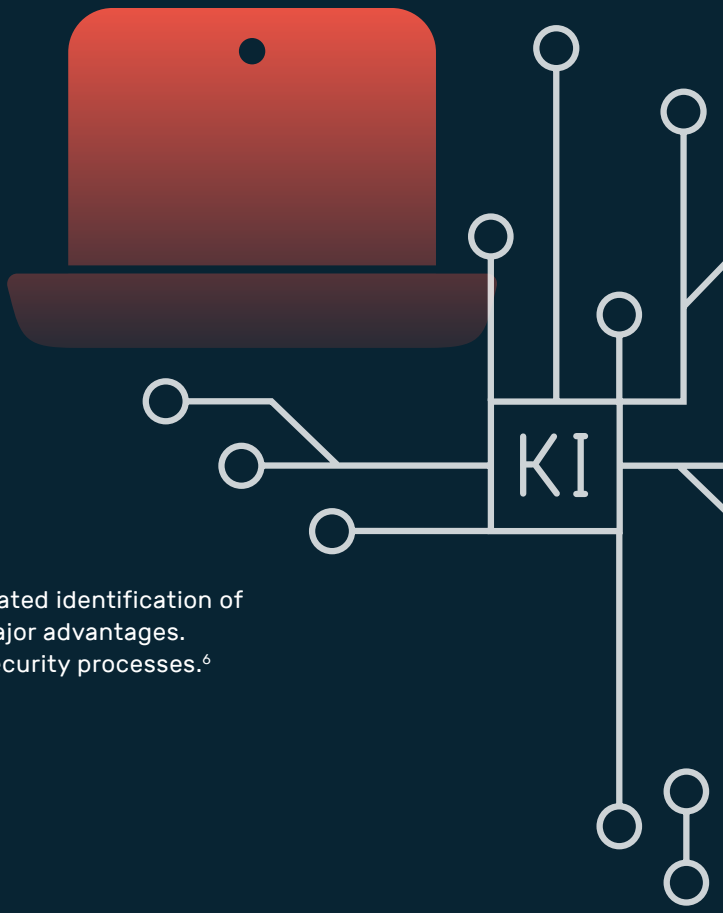


The attack originating from the DDoSia botnet took place in several waves over a period of 17 hours.

AI and Cybersecurity: A Blessing and a Curse

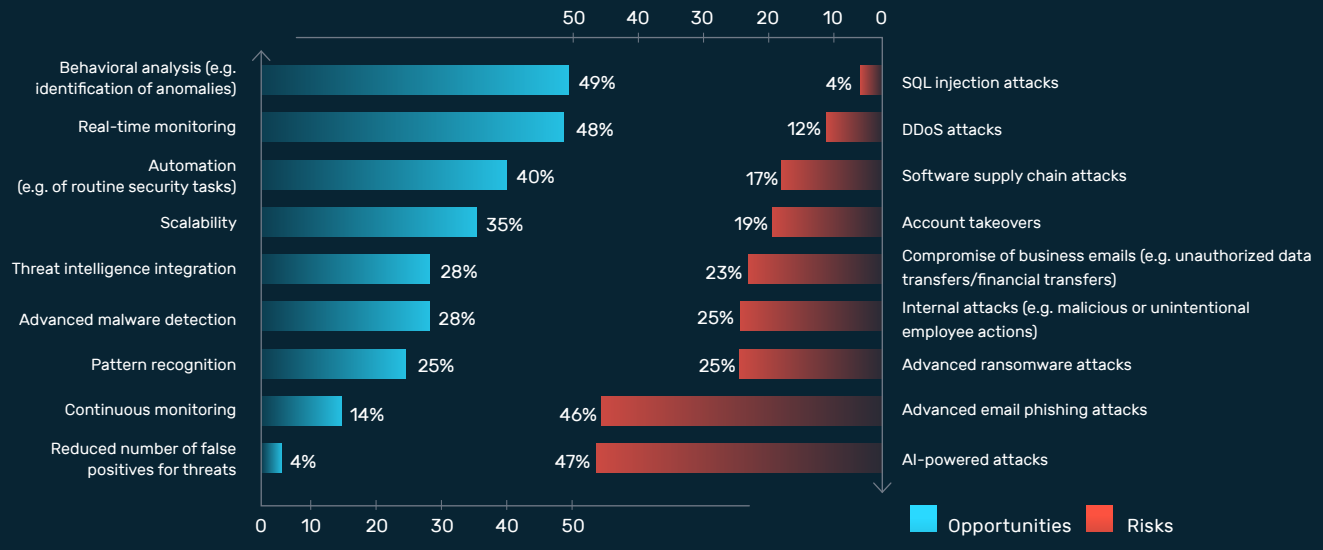
Artificial intelligence (AI) holds enormous opportunities, but also considerable risks for cybersecurity. In some scenarios, AI systems can detect threats more quickly and mitigate them more effectively than humans. At the same time, AI systems are a powerful attack tool for cybercriminals.

The ongoing development of AI solutions is further intensifying the threat situation. While large language models (LLMs) such as GPT 3.5 are currently mostly used by attackers for phishing campaigns, new generations of LLMs are also suitable for the automated creation of malicious code for newly discovered software errors. It becomes a time-critical undertaking to fix and close security vulnerabilities if AI-supported analyses of security advisories are sufficient to create targeted exploits for the affected software.[4] No wonder that AI-based attacks cause concern for every second company.[5]



On the other hand, AI systems can greatly improve the security of critical digital processes. Especially in the automated identification of anomalies and real-time monitoring, security experts see major advantages. In addition, AI can also be used to automate many routine security processes.[6]

Opportunities and Risks of AI in Cybersecurity



Cybersecurity experts see high potential in the use of AI in cybersecurity, particularly in terms of detection, real-time monitoring, and the automation of routine measures. On the other hand, there are risks from AI-supported attacks and advanced email phishing.

Cybercrime, Hacktivism and Billions in Costs

The fight against organized cybergroups continues to keep national and international investigative authorities on their toes. In May, the German Federal Criminal Police Office, in cooperation with law enforcement agencies from the Netherlands, France, Denmark, the UK, Austria and the U.S., struck a major blow against various cybergroups as part of "Operation Endgame" – 100 servers were confiscated, 1,300 domains were blocked, and 10 arrest warrants were issued. The infrastructure operators were also ordered to forfeit assets in the amount of €69 million. In addition, 99 crypto wallets with a current total volume of more than €70 million were confiscated from numerous crypto exchanges.

However, as the Lockbit raid in February shows, such successes are often only short-lived.[7] Within just a few days, the cybercriminals around Lockbit returned with new attack tools. This makes the authorities' actions against cybercriminals similar to the fight against the hydra – the monster from Greek mythology that grows back two heads when one is cut off.

With this in mind, it is not surprising that the costs caused by cybercrime are reaching immense proportions. While the damage to the German economy amounts to €148 billion, the global costs are estimated at €8.6 trillion for the year 2024.[8,9]

The Challenge of NIS-2 Compliance

In response to the threat situation, which has been intensifying for years, the EU has launched the next evolutionary stage of its cybersecurity strategy with the NIS-2 Directive. The directive significantly expands the original scope of application and defines stricter requirements for companies and organizations in critical sectors such as energy, transport, healthcare and digital infrastructure.

NIS-2 Scope at a Glance

The NIS-2 Directive increases the number of highly regulated organizations. Depending on the size of the company and the sector to which it belongs, different strict guidelines for IT risk management, the reporting of cyber incidents and secure collaboration with service providers must be followed.

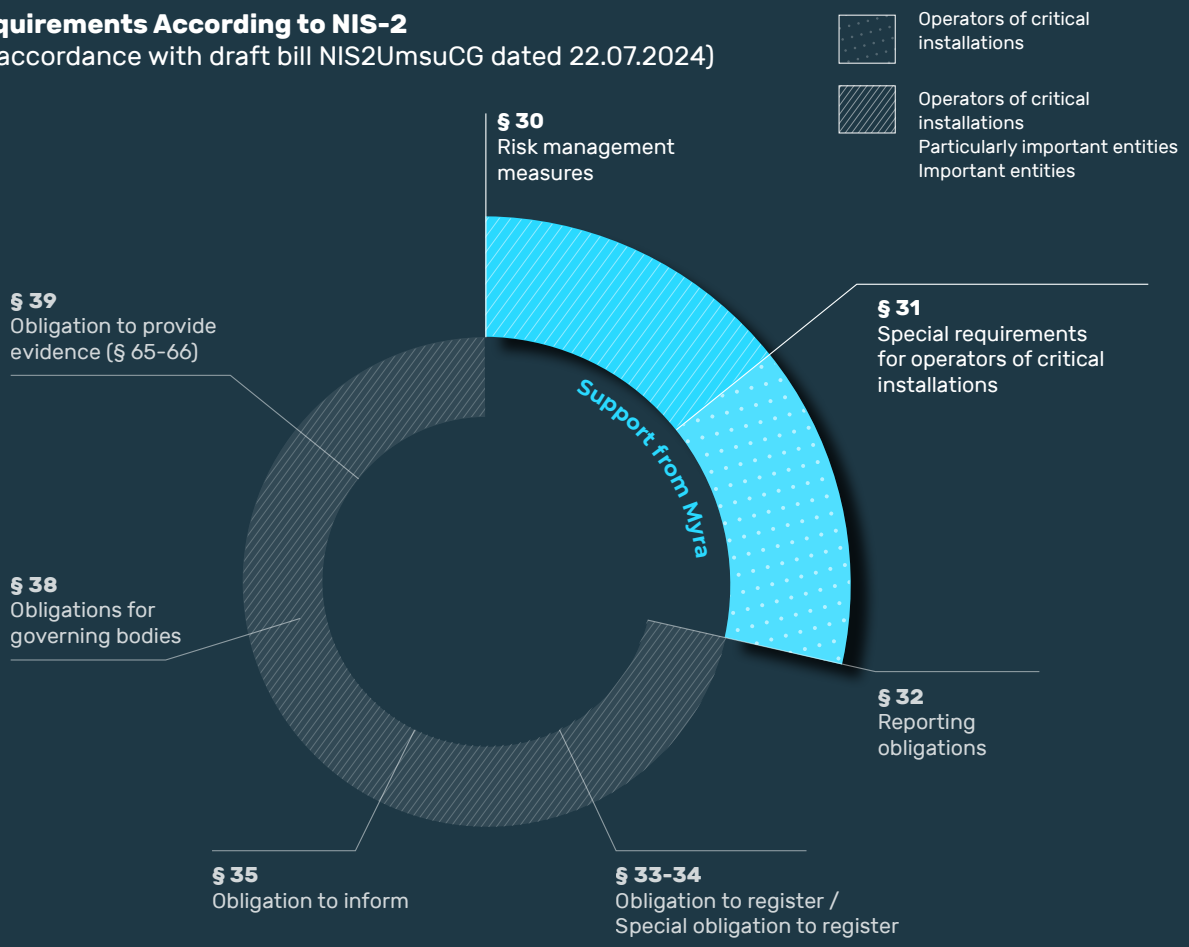
The aim is to ensure a consistently high level cybersecurity across the EU and strengthen resilience against cyberattacks.

NIS-2 goes beyond the mere expansion of the scope of application. The directive places a strong focus on cybersecurity risk management, the reporting of security incidents and information security along the supply chain. Companies must take comprehensive measures in accordance with NIS-2 to protect their systems and data and react quickly and effectively in the event of an attack.

NIS-2 must be transposed into German law and applied by mid-October. Nevertheless, many of the approximately 30,000 affected companies in Germany have not yet sufficiently addressed the future requirements, according to a survey conducted by the eco association. One in three companies stated in the survey that they had not yet taken any measures for NIS-2 implementation. Only 13.2% of IT decision-makers have expanded IT risk management in line with NIS-2.

The new requirements pose a challenge for SMEs in particular, as implementation requires many additional resources and the necessary specialist staff are difficult to find. Bitkom anticipates a shortage of IT specialists in 2024 of around 153,000 vacancies across all sectors in Germany.[10] On average, companies search for more than seven months until they have found and recruited a suitable IT specialist.[11]

Requirements According to NIS-2
(in accordance with draft bill NIS2UmsuCG dated 22.07.2024)



Risk management is at the heart of NIS-2. In accordance with § 30 NIS2UmsuCG, it comprises the performance of risk analyses, the security of information systems, the management of security incidents and the maintenance of operations, including recovery and crisis management.

In addition, the affected organizations must secure supply chains, ensure security during development and maintenance, evaluate risk management and train staff in cyberhygiene and cybersecurity. Cryptography, personnel security, access controls and multi-factor authentication are further supplementary measures.

According to § 31, the risk management of operators of critical installations must meet higher requirements and include more complex measures. In addition, the NIS2UmsuCG requires the use of state-of-the-art attack detection systems.

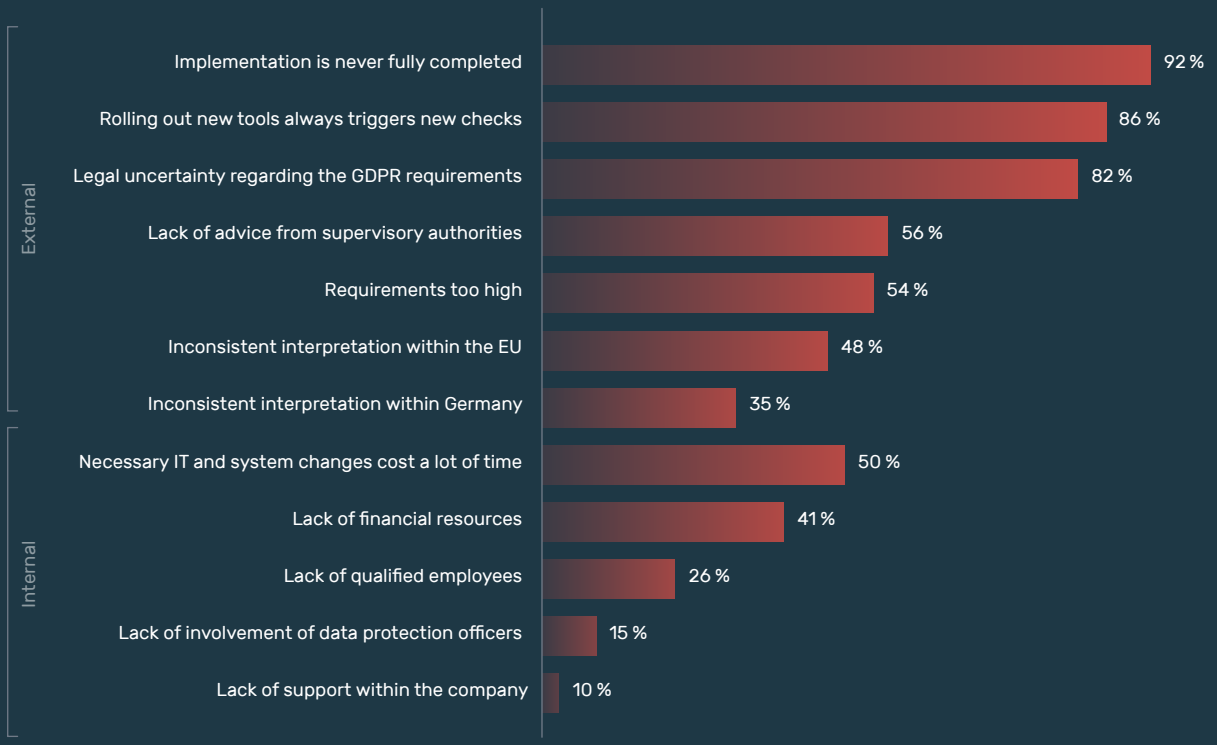
GDPR and US Data Transfer

While NIS-2 aims to improve cybersecurity, the General Data Protection Regulation (GDPR) is intended to ensure better protection of sensitive information – with success. Since the introduction of the GDPR in 2018, 61% of German companies have optimized their data protection measures. Nevertheless, many organizations are still unsure about how to deal with cross-border data transfer, especially in light of legal uncertainties in transatlantic data traffic.[12]

The GDPR defines strict standards for the processing of personal data. In contrast, Section 702 of the Foreign Intelligence Surveillance Act (FISA), which was extended in April 2024, obliges U.S. organizations to cooperate with investigative authorities in the United States and hand over data on non-U.S. citizens. This controversial positioning of legislation in Europe and the U.S. inevitably leads to legal tensions and uncertainty. In the past, two data protection agreements between Europe and the United States, Safe Harbor (2015) and Privacy Shield (2020), have already been overturned by the European Court of Justice (ECJ). The current adequacy decision based on the new EU-U.S. Data Privacy Framework (DPF) is also the subject of controversy among experts. Data protection activist Max Schrems has already announced that he will take legal action against the DPF, as it offers "no substantial change to U.S. surveillance law."

In this context, it is hardly surprising that almost all companies based in Germany (99%) prefer a provider with data centers in Germany when using cloud services.[13]

Company Survey: The Biggest Challenges in Implementing the GDPR[14]



In terms of external challenges, IT decision-makers see the ongoing implementation of data protection requirements, the constant testing of new tools and the continuing legal uncertainty as the main issues. Internally, the greatest challenges are the resources required in terms of time, costs, and personnel.

DDoS Threat Insights by zeroBS

7 questions about DDoS threats to zeroBS CTO Markus Manzke

Markus Manzke is Chief Technology Officer (CTO) of zeroBS, a pentesting company based in Germany. zeroBS helps its customers to understand and address the risks involved in operating Internet-based infrastructures. zeroBS is purely technology-driven and operates its own solutions for the various types of availability tests (Avydos, DDoS stress tests). Markus has over 15 years of experience as a security specialist in the German e-commerce ecosystem and is involved in some open-source solutions such as Naxsi (nginx-based WAF) and EmergingThreats (open-source Snort Signatures). He is a regular speaker at security conferences (CeBIT, SLAC, various BSides, Solutions HH).

DNS attacks seem to be on the rise, what are the most common methods?
An increase in DNS flood attacks has been observed by various manufacturers since 2023. This involves DNS servers being put under so much load that they cease to work and the target under attack is virtually digitally erased.

Which attack vectors cause companies the most difficulties when it comes to defense?
The most successful attacks currently occur on the application layer, as this has an extremely high degree of complexity due to a combination of the attack surface (number and distribution of targets) and the technology used (classic web applications, APIs, API-generated websites).

Have DDoS attacks carried out by state actors increased?

Direct state actors are rarely seen in DDoS attacks. An increase in hacktivism driven by geopolitical events can be seen worldwide (Europe, USA, Israel, Middle East, Southeast Asia) though.

Are there any new attack tools or techniques that are particularly worrying?
On the one hand, the focus has shifted to APIs, which are still easy to attack by IoT botnets. We are also seeing a sharp increase in attacks using browsers and proxy farms that undermine traditional defense mechanisms and geo-blocking. We continue to expect a strong increase in protocol attacks against HTTP/2, as two new attack vectors have been published in the past six months (RapidReset, Continuation Flood) and new vectors are to be expected.

What role do AI and machine learning already play in the execution of and defense against DDoS attacks?
We already see AI in use, primarily on the defense side, to defend against new types of attacks. On the one hand, AI support works well against IoT botnets; on the other hand, it can be used effectively by intelligent attackers to “learn” the attack traffic.

To what extent is the maximum defense bandwidth really decisive in mitigating attacks?
If you look at the reports of the well-known manufacturers, the bandwidth of 90% of attacks is less than 100 GB/s, and the high-volume attacks are carried out at 300 to 500 GB/s. There are a few attacks per year that are in the TB range, but these are isolated cases. The maximum bandwidth only plays a role when such an attack actually takes place or at least becomes highly probable.

What developments and trends do you expect regarding DDoS attacks in the near future?
As the geopolitical situation will not change in the foreseeable future, hacktivism will remain a serious factor. Furthermore, we expect a further increase in the professionalization of attack methods (browsers, proxies, APIs, WAF, stack/protocols) as well as the attackers’ choice of target.

Markus Manzke
Chief Technology Officer (CTO)
of zeroBS

HTTP/2 Attack “Continuation Flood”

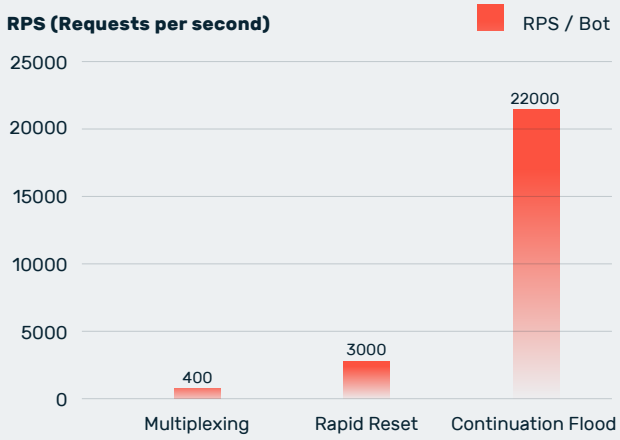
In early April 2024, a new DDoS attack technique called “HTTP/2 Continuation Flood” was discovered, which exploits vulnerabilities in numerous HTTP/2 protocol implementations.

In many cases, Continuation Flood poses a greater threat than the “Rapid Reset” method discovered last year: all it takes is a single computer (and in certain cases even a single TCP connection or a handful of frames) to overload a web server. The malicious requests of the attack are not even visible in HTTP access log files because – similar to Slowloris attacks – the requests are never completed.

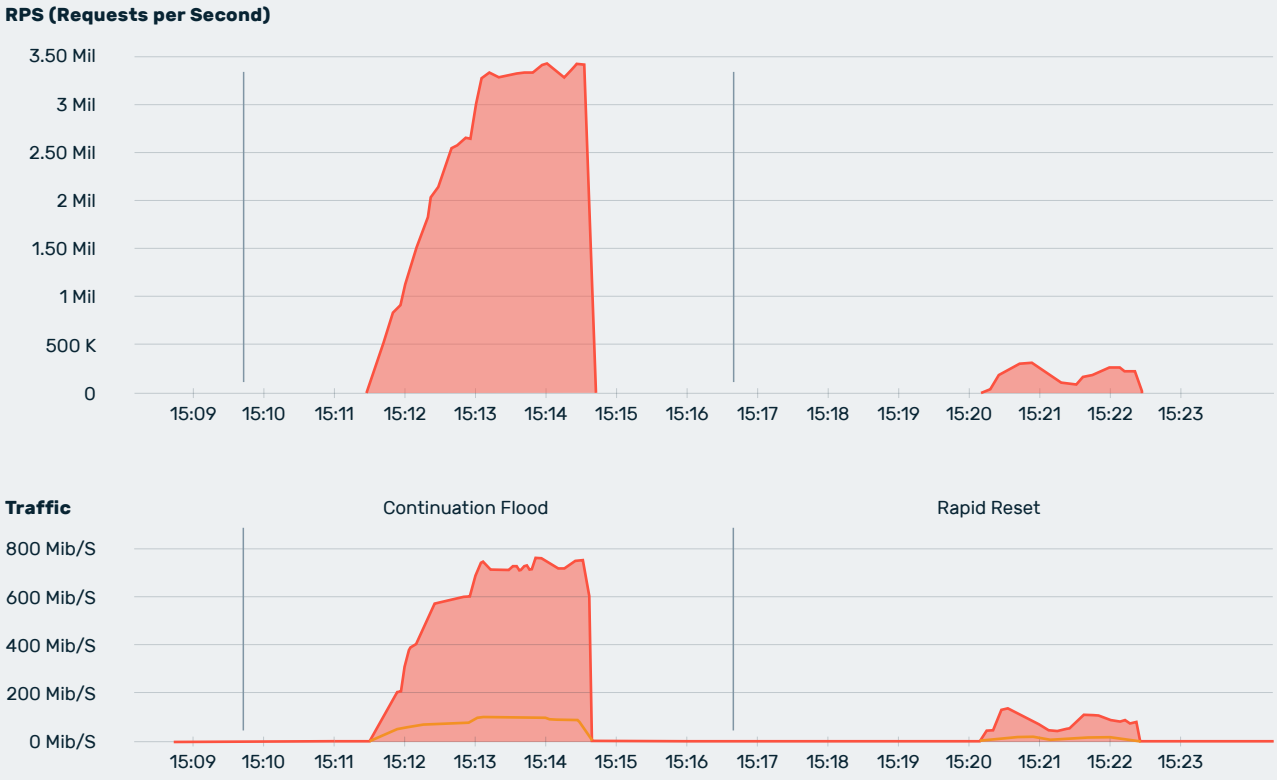
zeroBS has examined the new attack vector and can confirm its effectiveness against several tested systems. When comparing a Continuation Flood with Rapid Reset, the enormous malicious potential becomes clear: While Rapid Reset was almost eight times stronger than normal HTTP/2 multiplexing attacks, the Continuation Flood is seven times stronger than Rapid Reset in terms of pure requests per second (RPS) per bot - or 55 times stronger than multiplexing.

Up to 55 times stronger: Compared to conventional multiplexing attacks and the Rapid Reset method from the previous year, the enormous power of the Continuation Flood is evident.

HTTP/2 Attack Vector in Comparison



Continuation Flood Analysis



Both in terms of packet rate (RPS) and traffic volume, the Continuation Flood outperforms the Rapid Reset method by far.

Companies face a wide range of digital threats every day. Myra offers effective protection solutions to meet this challenge.

Myra's Security-as-a-Service platform is designed to secure business-critical online processes. Our customers benefit from highly efficient protection solutions to defend against DDoS attacks, malicious bot access, zero-day exploits, attacks on databases and many other threats.

DDoS Attacks

SQL Injection

Cross-Site Scripting (XSS)

Credential Stuffing

Cross-Site Request Forgery (CSRF)

Directory Traversal

DNS Cache Poisoning

Hype Sales

Skewing

Price Grabbing

Content / Product Grabbing

Form Spam

Cart Abandonment

Credit Card Testing

Account Creation & Takeover

Comprehensive protection against harmful traffic

In the area of application and infrastructure security, Myra provides all of the capabilities defined by Gartner - from DDoS protection across all relevant OSI layers to Secure CDN, Web Application and API Protection (WAAP) as well as DNS Security.

Core capabilities	
Detection and mitigation of Layer 3 volumetric attacks	✓
Amplification/reflection attacks (via DNS, NTP, SSDP, CLDAP, Memcached etc.)	✓
Carpet bombing	✓
ICMP flood attacks etc.	✓
Detection and mitigation of Layer 4 protocol attacks, causing resource exhaustion	✓
Flood attacks (UDP, TCP SYN, ACK, SYN/ACK, RST, UDP fragmentation etc.)	✓
Detection and mitigation of Layer 7 application layer attacks	✓
HTTP flood attacks (GET, POST, HEAD, Recursive GET flood etc.)	✓
Low-and-slow attacks (Slowloris etc.), ReDoS, Denial of Wallet attacks	✓
Detection and mitigation of multivector attacks	✓

Optional capabilities	
Real-time logging and reporting interface	✓
Security Operations Center (SOC) and Managed Security Services (MSS)	✓
CDN	✓
Web Application and API Protection (WAAP)	✓
Bot mitigation	✓
Domain Name System (DNS) security	✓

Sources

1 BSI: https://www.bsi.bund.de/DE/Themen/Regulierte-Wirtschaft/Kritische-Infrastrukturen/KRITIS-in-Zahlen/kritis-in-zahlen_node.html
2 IBM: 2024 X-Force Threat Intelligence Index
3 Privacy Affairs Dark Web Price Index 2023
4 Richard Fang, Rohan Bindu, Akul Gupta, Daniel Kang: LLM Agents can Autonomously Exploit One-day Vulnerabilities | Cornell University
5 Capterra Sicherheitsreport 2024
6 Capterra Sicherheitsreport 2024
7 Europol: https://www.europol.europa.eu/media-press/newsroom/news/law-enforcement-disrupt-worlds-biggest-ransomware-operation
8 Bitkom Wirtschaftsschutz 2023
9 Statista Market Insights
10 Bitkom 2024: IT-Fachkräfte 2040:Wo steht die deutsche Wirtschaft?
11 Bitkom 2024: Trotz Krieg und Krisen: In Deutschland fehlen 137.000 IT-Fachkräfte
12 Bitkom Research 2023: https://www.bitkom.org/Presse/Presseinformation/5-Jahre-DS-GVO-nur-Note-ausreichend#_
13 Bitkom Research 2024: https://www.bitkom.org/Presse/Presseinformation/Unternehmen-treiben-mit-Cloud-Digitalisierung-voran
14 Bitkom Research 2023: Wo steht die deutsche Wirtschaft beim Datenschutz?

Why CISOs choose Myra

Security

Cyberattacks result in data theft, system outages and disrupted communications. Myra defends your digital business processes against cyberattacks in real time.

Performance

Traffic peaks caused by sales campaigns, live video streaming or unforeseen events can overload web applications. Myra ensures high-performance delivery of your content.

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

Legal and company-specific requirements for IT security and data protection call for audited processes. Myra is your compliance partner for the strictest requirements.

BSI-certified IT security

Myra Technology is certified by the German Federal Office for Information Security (BSI) in accordance with the ISO 27001 standard based on IT-Grundschutz. In addition, we are one of the leading security service providers worldwide to meet all 37 criteria set by the BSI for qualified DDoS protection providers. We are setting the standard in IT security.

ISO 27001 BSI zertifiziert auf der Basis von IT-Grundschutz Zertifikat Nr.: BSI-IGZ-0479-2021 | PCI DSS Certified | BSIG KRITIS-qualifiziert | BSI C5 Testat Typ 2 | Trusted Cloud | ISAE 3402 IDW PS 951 Type 2 | DIN EN 50600 zertifiziert Betriebssicheres Rechenzentrum

Certified by the German 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 §3 BSI Act | BSI C5 Type 2 | Certified Trusted Cloud Service | IDW PS 951 Type 2 (ISAE 3402) audited service provider | Certification of data centers according to DIN EN 50600

Myra protects what matters. In the digital world.

Bundesministerium für Gesundheit | BZgA Bundeszentrale für gesundheitliche Aufklärung | lib 1861 | msc Munich Security Conference | CANCOM | DSV IT Service | Barmenia Einfach. Menschlich. | flatex DEGIRO

Made in Germany

Myra Security is the new benchmark for global IT security.

Would you like to find out more about how you can use our solutions to increase your revenue, minimize your costs and protect your applications from malicious attacks? Our team of experts will be happy to advise you individually and develop a customized solution for your company. Why not arrange a no-obligation consultation today?

Request a free consultation →

Myra Security GmbH

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