MYRA

CASE STUDY

Resilient and digitally sovereign: How the district of Regensburg fends off cyberattacks with Myra Security

Case Study
Landkreis Regensburg

Lösungen
WAF,
Bot Management,
DDoS Protection, CDN

Resilient and digitally sovereign: How the district of Regensburg fends off cyberattacks with Myra Security

Executive Summary

The district of Regensburg already offers 1,823 digital administrative services for its citizens (as of August 2025). This puts Regensburg among the top 10 districts in the nationwide dashboard ranking under the Online Access Act (OZG).

To secure these administrative services, the district of Regensburg has been relying on professional application protection from Myra Security since February 2022. The collaboration ensures the availability of nearly 150 domains belonging to the district, affiliated municipalities, and several critical infrastructure facilities, while meeting the highest compliance requirements and strengthening digital sovereignty with Myra's technology, which is developed and operated in Germany.

Initial Situation

Authorities today face an increased threat level: politically motivated DDoS attacks and targeted attacks on web applications jeopardize the availability and integrity of digital services. The Allianz Risk Barometer 2025 cites cyber incidents and business interruptions as the greatest risks for organizations in Germany and Europe. Myra's defense systems register among the highest number of attacks on customers in the public sector.

In order to be sufficiently resilient, public administrations such as the district of Regensburg must meet high standards of security, data protection, and compliance. Scarce human and financial resources pose a challenge in this regard: according to the digital association Bitkom, there is still a shortage of more than 100,000 IT specialists in Germany.

Objectives and Implementation

In light of the consistently high threat level, the district of Regensburg decided to secure its public domains and online services using Myra's certified Security-as-a-Service platform. The primary objectives were:

- Real-time protection of websites, communication channels, and digital processes against DDoS and other Layer 7 attacks
- Fail-safe availability and consistently high performance even during attacks
- Compliance with strict data protection and regulatory requirements
- Promoting digital sovereignty through the use of European technologies

The selection of a suitable IT security service provider was carried out as part of a tender process based on strict technical and organizational criteria. Myra convinced as a European provider with a high level of certification (including BSI ISO 27001 based on IT-Grundschutz, BSI C5 Type 2, PCI DSS, KRITIS operator in accordance with Section 8a (3) of the BSI Act), legally compliant GDPR conformity, and an independent, secure infrastructure.

"We don't want any critical dependencies on non-European providers and rely on tested, certified security from Germany," explains Klaus Schwankl, Webmaster and Head of the Municipal Authority Network for the District of Regensburg.

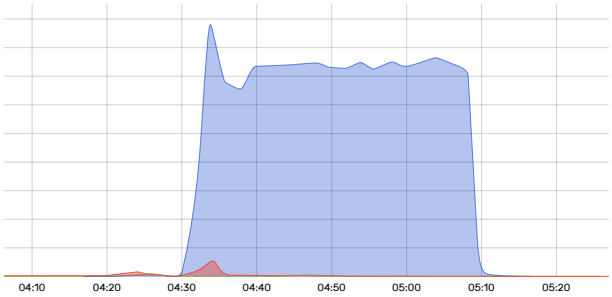
The implementation included a holistic defense concept with a DDoS-protected Content Delivery Network (CDN) that protects websites and services against overload attacks at the application level (Layer 7). In addition, the Myra Web Application Firewall (WAF) protects against OWASP Top 10 risks such as SQL injection or cross-site scripting, which aim to steal or manipulate data. Furthermore, Myra meets specific technical and organizational requirements for the district of Regensburg, such as DNS management and the automation of TLS/SSL certificate renewal.

> *We don't want any critical dependencies on non-European providers and rely on tested, certified security from Germany.*

Klaus Schwankl
Webmaster and Head of the Municipal Authority Network for the District of Regensburg

Benefits of the cooperation

In April 2024, the district of Regensburg was the target of a wave of attacks aimed at several domains. In that month alone, there were three attacks, all of which took place in the early hours of the morning and were mitigated by Myra. One of the attacks originated from 102 IPs and 26 AS networks in 13 countries and comprised a total of 681,000 malicious bot requests, over 99 percent of which were blocked.



"The Myra solution has proven itself in a real-world scenario: despite regular and sometimes massive attacks on our systems, there was no disruption at all. Our services remained available to citizens at all times," emphasizes Klaus Schwankl. "The automated system takes the pressure off our team and provides reliable 24/7 protection."

By working with Myra, the district of Regensburg benefits from the following advantages:

Holistic protection and high performance

- Highly effective DDoS mitigation and reliable protection against OWASP Top 10 risks
- Shorter loading times with reduced server load and improved availability
- High user satisfaction thanks to consistently high performance and reliability

Data protection, compliance, and digital sovereignty

- Legally compliant implementation of all data protection and regulatory requirements
- Compliance with the highest data protection standards through data processing in Germany
- Reducing critical dependencies by using a sovereign European data infrastructure

Efficiency and resource conservation

- Flexible scalability of the infrastructure
- Highly automated defense against attacks reduces internal personnel costs

Conclusion

The collaboration with Myra enables the district of Regensburg to operate its digital infrastructure with digital sovereignty, security, and high performance. The solutions not only offer protection against current and future cyberthreats, but also meet all regulatory and data protection requirements. The district of Regensburg is thus leading the way in strengthening the digital sovereignty of the public sector. "In Myra, we have found a service provider that fully meets our requirements for security, compliance, and digital sovereignty," Klaus Schwankl sums up. "The investment pays off every day – for us and for the citizens who rely on our digital services."