MYRA

CASE STUDY

Ausfallsicher und souverän: Wie der Landkreis Regensburg mit Myra Security Angriffswellen trotzt

Case Study
Landkreis Regensburg

Lösungen
WAF,
Bot Management
DDoS Protection, CDN

Ausfallsicher und souverän: Wie der Landkreis Regensburg mit Myra Security Angriffswellen trotzt

Executive Summary

Der Landkreis Regensburg bietet bereits 1.823 digitale Verwaltungsdienstleistungen für seine Bürgerinnen und Bürger an (Stand: August 2025). Damit ist Regensburg im bundesweiten Dashboard-Ranking im Rahmen des Onlinezugangsgesetzes (OZG) unter den Top 10 der Landkreise.

Zur Absicherung dieser Verwaltungsdienste setzt der Landkreis Regensburg seit Februar 2022 auf den professionellen Applikationsschutz von Myra Security. Die Zusammenarbeit sichert die Verfügbarkeit von knapp 150 Domains des Landkreises, angeschlossener Kommunen sowie einiger KRITIS-Einrichtungen, erfüllt dadurch höchste Compliance-Anforderungen und stärkt die digitale Souveränität durch den Einsatz der in Deutschland entwickelten und betriebenen Myra-Technologie.

Ausgangslage

Behörden sehen sich heutzutage einer verschärften Bedrohungslage ausgesetzt: politisch motivierte DDoS-Angriffe und gezielte Attacken auf Webanwendungen gefährden die Verfügbarkeit und Integrität digitaler Dienste und Fachverfahren. Das Allianz Risk Barometer 2025 nennt Cybervorfälle und Betriebsunterbrechungen als die größten Risiken für Organisationen in Deutschland und Europa. Die Abwehrsysteme von Myra verzeichnen mit die meisten Angriffe auf Kunden aus dem öffentlichen Sektor.

Um ausreichend resilient zu sein, müssen öffentliche Verwaltungen wie der Landkreis Regensburg hohe Anforderungen an Sicherheit, Datenschutz und Compliance erfüllen. Knappe personelle und finanzielle Ressourcen stellen dabei eine Herausforderung dar: Nach Angaben des Digitalverbands Bitkom fehlen in Deutschland weiterhin mehr als 100.000 IT-Fachkräfte.

Zielsetzung und Umsetzung

Angesichts der konstant hohen Bedrohungslage entschied sich der Landkreis Regensburg dazu, seine öffentlichen Domains und Onlinedienste durch die zertifizierte Security-as-a-Service-Plattform von Myra abzusichern. Primäre Ziele waren:

- Echtzeit-Schutz der Webseiten, Kommunikationskanäle und digitalen Prozesse vor DDoS und anderen Layer-7-Attacken
- Ausfallsichere Verfügbarkeit und konstant hohe Performance auch während Angriffen
- Erfüllung strenger Datenschutz- und Compliance-Anforderungen
- Förderung digitaler Souveränität durch Nutzung europäischer Technologien

Die Auswahl eines geeigneten IT-Security-Dienstleisters erfolgte im Rahmen einer Ausschreibung nach strengen technischen und organisatorischen Kriterien. Myra überzeugte als europäischer Anbieter mit hohem Zertifizierungsniveau (u. a. BSI ISO 27001 auf Basis von IT-Grundschutz, BSI C5 Typ 2, PCI DSS, KRITIS-Betreiber gemäß § 8a Abs. 3 BSI-Gesetz), rechtssicherer DSGVO-Konformität und einer unabhängigen, sicheren Infrastruktur.

„Wir wollen keine kritischen Abhängigkeiten zu außereuropäischen Anbietern und setzen auf geprüfte, zertifizierte Sicherheit aus Deutschland", erklärt Klaus Schwankl, Webmaster und Leiter des kommunalen Behördennetzes des Landkreises Regensburg.

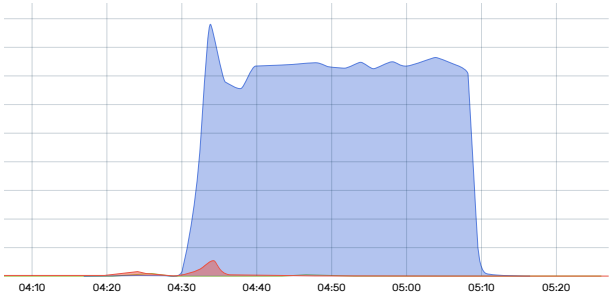
Die Implementierung umfasste ein holistisches Abwehrkonzept mit DDoS-geschütztem Content Delivery Network (CDN), das Webseiten und Services gegen Überlastungsangriffe auf Anwendungsebene (Layer 7) sichert. Zusätzlich schützt die Myra Web Application Firewall (WAF) vor OWASP-Top-10-Risiken wie SQL Injection oder Cross-Site Scripting, die auf den Diebstahl oder die Manipulation von Daten abzielen. Darüber hinaus erfüllt Myra spezielle technische und organisatorische Anforderungen für den Landkreis Regensburg wie das DNS-Management und die Automatisierung der TLS/SSL-Zertifikatserneuerung.

> *Wir wollen keine kritischen Abhängigkeiten zu außereuropäischen Anbietern und setzen auf geprüfte, zertifizierte Sicherheit aus Deutschland.*

Klaus Schwankl
Webmaster und Leiter des kommunalen Behördennetzes des Landkreises Regensburg

Mehrwerte der Kooperation

Im April 2024 war der Landkreis Regensburg Ziel einer Angriffswelle, die gegen mehrere Domains gerichtet war. Allein in diesem Monat kam es zu drei Attacken, die alle in den frühen Morgenstunden stattfanden und von Myra abgewehrt wurden. Einer der Angriffe ging von 102 IPs und 26 AS-Netzen aus 13 Ländern aus und umfasste insgesamt 681.000 bösartige Bot-Anfragen, die zu über 99 Prozent blockiert wurden.



„Die Myra-Lösung hat sich im Ernstfall bewährt: Trotz regelmäßiger und teils massiver Angriffe auf unsere Systeme kam es zu keinerlei Beeinträchtigung. Unsere Dienste blieben für Bürgerinnen und Bürger jederzeit erreichbar", betont Schwankl. „Die automatisierte Abwehr entlastet unser Team und sorgt für einen zuverlässigen Schutz rund um die Uhr."

Durch die Zusammenarbeit mit Myra profitiert der Landkreis Regensburg von folgenden Vorteilen:

Holistischer Schutz und hohe Performance

- Hocheffektive DDoS-Abwehr und verlässlicher Schutz vor OWASP-Top-10-Risiken
- Kürzere Ladezeiten bei reduzierter Serverlast und verbesserter Verfügbarkeit
- Hohe Nutzerzufriedenheit dank konstant hoher Performance und Ausfallsicherheit

Datenschutz, Compliance und digitale Souveränität

- Rechtssichere Umsetzung aller Datenschutz- und Compliance-Vorgaben
- Erfüllung höchster Datenschutzstandards durch Datenverarbeitung in Deutschland
- Reduzierung kritischer Abhängigkeiten durch Nutzung einer souveränen europäischen Dateninfrastruktur

Effizienz und Ressourcenschonung

- Flexible Skalierbarkeit der Infrastruktur
- Hochautomatisierte Angriffsabwehr reduziert internen Personalaufwand

Fazit

Die Zusammenarbeit mit Myra ermöglicht dem Landkreis Regensburg, seine digitale Infrastruktur souverän, sicher und performant zu betreiben. Die Lösungen bieten nicht nur Schutz vor aktuellen und zukünftigen Cyberbedrohungen, sondern erfüllen auch sämtliche regulatorischen und datenschutzrechtlichen Anforderungen. Damit geht der Landkreis Regensburg bei der Stärkung der digitalen Souveränität des öffentlichen Sektors als Vorbild voran. „Mit Myra haben wir einen Dienstleister gefunden, der unsere Anforderungen an Sicherheit, Compliance und digitale Souveränität voll erfüllt", resümiert Schwankl. „Die Investition zahlt sich täglich aus – für uns und für die Bürgerinnen und Bürger, die auf unsere digitalen Dienste vertrauen."