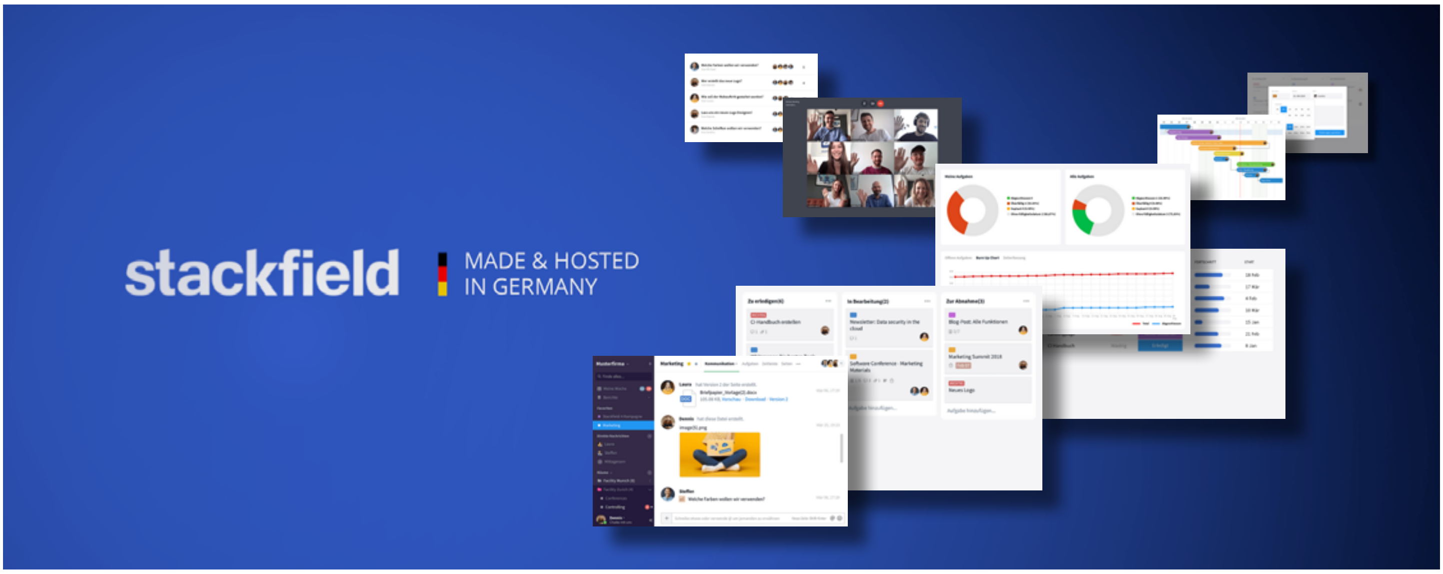
MYRA

CASE STUDY

GDPR-Compliant DDoS Protection According to German Standards

Case Study
Stackfield

Solutions
DDoS Protection



Collaboration Platform Stackfield Relies on Managed Security Services from Myra

Executive Summary

Stackfield was founded in 2012 by CEO Cristian Mudure in Munich with the aim of making collaboration and communication in companies as simple, clear and above all as safe as possible. The top priority is to secure customers‘ data with the best possible safeguards, such as end-to-end encryption. The company’s servers are located exclusively in Germany. Stackfield thus ensures that when using the tool, all data remains within the EU.

The company also applies these high standards of data protection to its partners: Stackfield only works with subcontractors that are based in the EU. The search for a DDoS protection provider ended with Myra Security not least for this reason. The experienced German specialist provider of managed security services is also committed to the highest quality and data protection standards. Myra protects Stackfield’s web applications from highly complex DDoS attacks at the application level and thus from malicious disruptions to business processes.

Starting Point and Goals

In light of the escalating cybersecurity threat landscape, Stackfield began searching for a DDoS mitigation service provider in 2018. The goal was to proactively protect against overload attacks and thereby meet their self-imposed highest standards for IT security and data protection.

As a German company, the Security-as-a-Service provider Myra is subject to the European legal framework and stands for the highest GDPR compliance. Additionally, Myra offers data processing limited to Germany upon request and a commitment to the highest security standards, which is manifested in a variety of certifications. The company also provides first-class service and years of expertise.

Shortly after contacting Myra, the alignment in shared values on both sides became clear: „Long before GDPR came into effect, we exclusively relied on German providers,“ says Christian Mudure, founder and CEO of Stackfield. „For this reason, this point was a decisive criterion in selecting a provider, alongside technical expertise.“

In May 2018, Stackfield signed a term contract for the use of DDoS protection for web applications and the Myra Content Delivery Network (CDN). Cristian Mudure is still fully satisfied with this decision today: „What primarily convinced us about Myra was the fact that it is a reputable German provider. The price-performance level is absolutely appropriate.“

Implementation

Myra protects the domain stackfield.com against cyberattacks at the application level (layer 7). The Myra DDoS protection can be implemented independently of the existing infrastructure and quickly, as no additional hardware or software is required. Myra handles almost the entire setup and configuration of the protection solution, minimizing the effort on the customer's side.

The technical implementation for Layer 7 WAF protection system is possible through two main methods: Either by adjusting the DNS entry via the CNAME record, or by transferring the authoritative DNS server to Myra using an import of existing zones. Once the customer's corresponding TLS certificates have been made available in the Myra Dashboard via API or upload, the TLS connection can be terminated, and a Deep Packet Inspection can be performed. Finally, the expert team at the Myra Network Operations Center (NOC) sets important filter rules.

„The implementation was very quick and straightforward," recalls Christian Mudure. „A few individual adjustments beyond the standard were required, which Myra implemented quickly and competently."

The biggest challenge in securing Stackfield was the team chat feature: As an all-in-one collaboration tool with messenger functionality, the immediate provision of new information is of great importance for Stackfield. Request/response-based protocols like HTTP are not suitable for this type of information delivery, as clients have to repeatedly make requests to check if new information is available. The bi-directional WebSocket protocol offers a solution to this problem; Myra has built a connection protection for these long-lived connections on Layer 4.

The Myra CDN ensures that all static and dynamic elements of the Stackfield website are delivered at lightning speed. Caching of content minimizes traffic on Stackfield's own servers. Myra offers the option to limit CDN delivery to servers in Germany, thus meeting Stackfield's high data protection requirements.

Summary

Since the implementation, Stackfield has benefited from a comprehensive protection concept for its domain. With the special adaptation for the messenger feature of the collaboration tool in the form of a bi-directional WebSocket protocol, Myra has fully met all of the customer's special requirements. The Myra CDN ensures consistently high performance for all functions, such as project management, team chat, or audio and video conferences. Stackfield is completely satisfied with the collaboration with Myra. „If there have been suspicious activities in the past, we were immediately informed about them," says Christian Mudure. „Our entire IT department is absolutely convinced by Myra's response speed and service."

Through the collaboration with Myra, Stackfield benefits from the following advantages:

- Highest availability through Myra's multiply redundant infrastructure
- Accelerated content delivery with low latencies through global CDN
- Low implementation and maintenance effort: no additional hardware or software required
- Local 24/7 support from Germany via the Myra NOC (Network Operations Center) at the headquarters in Munich
- Access to expertise and industry experience of a highly certified specialist provider
- Certified security according to BSI ISO 27001 based on IT-Grundschutz
- Legally compliant GDPR conformity

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

ISAE 3402 IDW PS 951 TYPE 2

KRITIS Nachweis gemäß § 8a. Abs. 3 BSIG

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 §3 BSI Act | BSI C5 Type 2 | Certified Trusted Cloud Service | KRITIS operator in accordance with Section 8a (3) BSI Act