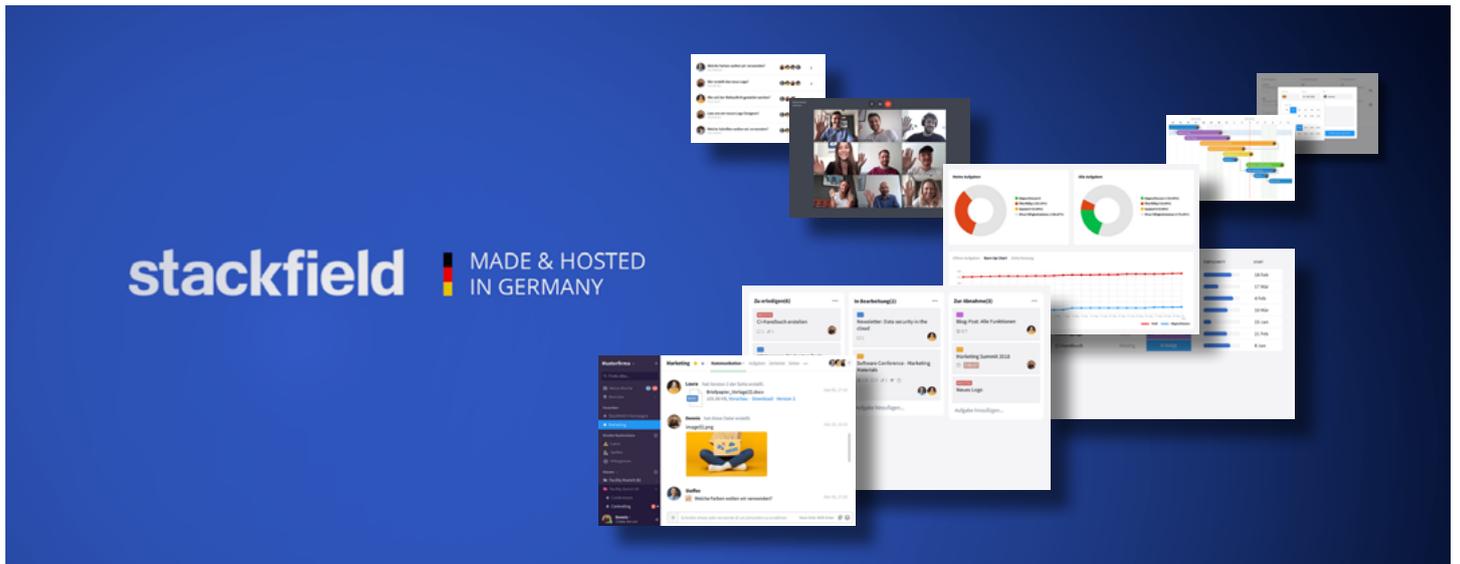




CASE STUDY

# DSGVO-konformer DDoS-Schutz nach deutschen Standards





# Collaboration-Plattform Stackfield setzt auf Managed Security Services von Myra

## Executive Summary

Stackfield wurde 2012 von CEO Cristian Mudure in München mit dem Ziel gegründet, die Zusammenarbeit und Kommunikation in Unternehmen so einfach, übersichtlich und vor allem so sicher wie möglich zu gestalten. Oberste Priorität ist, die Daten der Kunden mit den bestmöglichen Schutzmaßnahmen wie einer Ende-zu-Ende-Verschlüsselung abzusichern. Die Server des Unternehmens befinden sich ausschließlich in Deutschland. Stackfield stellt damit sicher, dass bei der Nutzung des Tools alle Daten innerhalb der EU bleiben.

Diese hohen Maßstäbe beim Thema Datenschutz legt das Unternehmen auch an seine Partner an: Stackfield arbeitet nur mit Subunternehmen zusammen, die ihren Sitz in der EU haben. Die Suche nach einem DDoS-Schutzanbieter endete nicht zuletzt aus diesem Grund bei Myra Security. Der erfahrene deutsche Spezialanbieter von Managed Security Services fühlt sich ebenfalls höchsten Qualitäts- und Datenschutzstandards verpflichtet. Myra schützt Stackfields Webapplikationen vor hochkomplexen DDoS-Attacken auf Anwendungsebene und damit vor böswillig herbeigeführten Unterbrechungen der Geschäftsprozesse.

## Ausgangssituation und Zielsetzung

Vor dem Hintergrund der sich verschärfenden Cyberbedrohungslage machte sich Stackfield 2018 auf die Suche nach einem DDoS-Mitigations-Dienstleister. Ziel war, sich präventiv vor Überlastungsangriffen zu schützen und damit den selbst formulierten höchsten Ansprüchen an die IT-Security und den Datenschutz gerecht zu werden.

Der Security-as-a-Service-Anbieter Myra unterliegt als deutsches Unternehmen dem europäischen Rechtsrahmen und steht für höchste DSGVO-Konformität. Dazu kommen die auf Wunsch rein auf Deutschland begrenzte Datenverarbeitung und das Commitment zu höchsten Sicherheitsstandards, das sich bei Myra in einer Vielzahl von Zertifizierungen manifestiert, sowie erstklassiger Service und jahrelange Expertise.

Schon kurz nach der Kontaktaufnahme zu Myra wurde die Übereinstimmung in den gelebten Werten auf beiden Seiten klar: „Schon lange vor Inkrafttreten der DSGVO haben wir ausschließlich auf deutsche Anbieter gesetzt“, so Christian Mudure, Gründer und CEO von Stackfield. „Aus diesem Grund war dieser Punkt neben der technischen Expertise ein entscheidendes Kriterium bei der Auswahl eines Anbieters.“

Stackfield unterzeichnete im Mai 2018 einen Laufzeitvertrag über den Einsatz des DDoS-Schutzes für Webapplikationen und des Myra Content Delivery Network (CDN). Cristian Mudure ist mit dieser Entscheidung noch heute voll und ganz zufrieden: „An Myra hat uns in erster Linie die Tatsache überzeugt, dass es sich um einen seriösen, deutschen Anbieter handelt. Das Preis-Leistungsniveau ist absolut angemessen.“

## Umsetzung

Myra sichert die Domain stackfield.com gegen Cyberattacken auf Anwendungsebene (Layer 7) ab. Der Myra DDoS-Schutz lässt sich unabhängig von der bestehenden Infrastruktur und kurzfristig implementieren, da keinerlei zusätzliche Hard- oder Software erforderlich ist. Myra übernimmt nahezu die komplette Einrichtung und Konfiguration der Schutzlösung, so dass der Aufwand auf Kundenseite minimal ist.

Die technische Aufschaltung auf Layer 7 für das WAF-Schutzsystem ist prinzipiell über zweierlei Wege möglich: Entweder erfolgt eine Anpassung des DNS-Eintrags über den CNAME-Eintrag oder der autoritative DNS-Server wird mithilfe eines Imports bestehender Zonen an Myra übertragen. Sobald nun die entsprechenden TLS-Zertifikate des Kunden per API oder Upload im Myra Dashboard zur Verfügung gestellt wurden, kann die TLS-Verbindung terminiert und eine Deep Packet Inspection durchgeführt werden. Abschließend setzt das Expertenteam des Myra Network Operations Center (NOC) noch wichtige Filterregeln.

„Die Implementierung lief sehr schnell und unkompliziert“, erinnert sich Christian Mudure. „Es waren ein paar individuelle Anpassungen abseits des Standards erforderlich, die seitens Myra schnell und kompetent umgesetzt wurden.“

Die größte Herausforderung bei der Absicherung von Stackfield war das Team-Chat-Feature: Als All-in-One Collaboration Tool mit Messenger-Funktion ist die sofortige Bereitstellung von neuen Informationen für Stackfield von großer Bedeutung. Request/Response-basierte Protokolle wie HTTP eignen sich für diese Art der Informationsbereitstellung nicht, da Clients immer wieder Anfragen stellen müssen, um zu prüfen, ob neue Informationen vorhanden sind. Das bi-direktionale Websocket-Protokoll bietet eine Lösung für dieses Problem; Myra hat auf Layer 4 einen Verbindungsschutz für diese langlebigen Verbindungen aufgebaut.

Das Myra CDN sorgt dafür, dass alle statischen und dynamischen Elemente der Stackfield-Website blitzschnell ausgeliefert werden. Das Caching der Inhalte minimiert den Traffic auf Stackfields eigenen Servern. Myra bietet die Möglichkeit, die CDN-Auslieferung auf Server in Deutschland zu beschränken und erfüllt damit die hohen Datenschutzansprüche von Stackfield.

## Resümee

Seit der Aufschaltung profitiert Stackfield von einem umfassenden Schutzkonzept für seine Domain. Mit der speziellen Anpassung für das Messenger-Feature des Collaboration-Tools in Form eines bi-direktionalen Websocket-Protokolls hat Myra alle Sonderwünsche des Kunden vollumfänglich erfüllt. Das Myra CDN sichert eine gleichbleibend hohe Performance aller Funktionen, wie Projektmanagement, Team-Chat oder die Audio- und Videokonferenzen. Stackfield ist mit der Zusammenarbeit mit Myra rundum zufrieden. „Wenn es in der Vergangenheit verdächtige Aktivitäten gab, wurden wir umgehend darüber informiert“, so Christian Mudure. „Unsere gesamte IT-Abteilung ist von der Reaktionsgeschwindigkeit und dem Service von Myra absolut überzeugt.“

### Durch die Zusammenarbeit mit Myra profitiert Stackfield von folgenden Vorteilen:



- höchste Verfügbarkeit durch mehrfach redundante Infrastruktur von Myra
- beschleunigte Content-Auslieferung mit niedrigen Latenzen durch globales CDN
- geringer Implementierungs- und Wartungsaufwand: keine zusätzliche Hard- und Software erforderlich
- lokaler 24/7-Support aus Deutschland über das Myra-NOC (Network Operations Center) am Hauptsitz in München
- Zugang zu Expertise und Branchenerfahrung eines hochzertifizierten Spezialanbieters
- zertifizierte Sicherheit nach ISO 27001 auf Basis von IT-Grundschutz des BSI
- Rechtssichere DSGVO-Konformität

ISO 27001 BSI zertifiziert  
auf der Basis von IT-Grundschutz  
Zertifikat Nr.: BSHGZ-0479-2021



DIN EN 50600  
zertifiziert  
BETRIEBSSICHERES  
RECHENZENTRUM

Zertifiziert vom Bundesamt für Sicherheit in der Informationstechnik (BSI) nach ISO 27001 auf Basis von IT-Grundschutz | Zertifiziert nach Payment Card Industry Data Security Standard (PCI DSS) | KRITIS-qualifiziert nach §3 BSI-Gesetz | BSI-C5-Testat Typ 2 | Geprüfter Trusted Cloud Service | IDW PS 951 Typ 2 (ISAE 3402) geprüfter Dienstleister | Zertifizierung von Rechenzentren nach DIN EN 50600