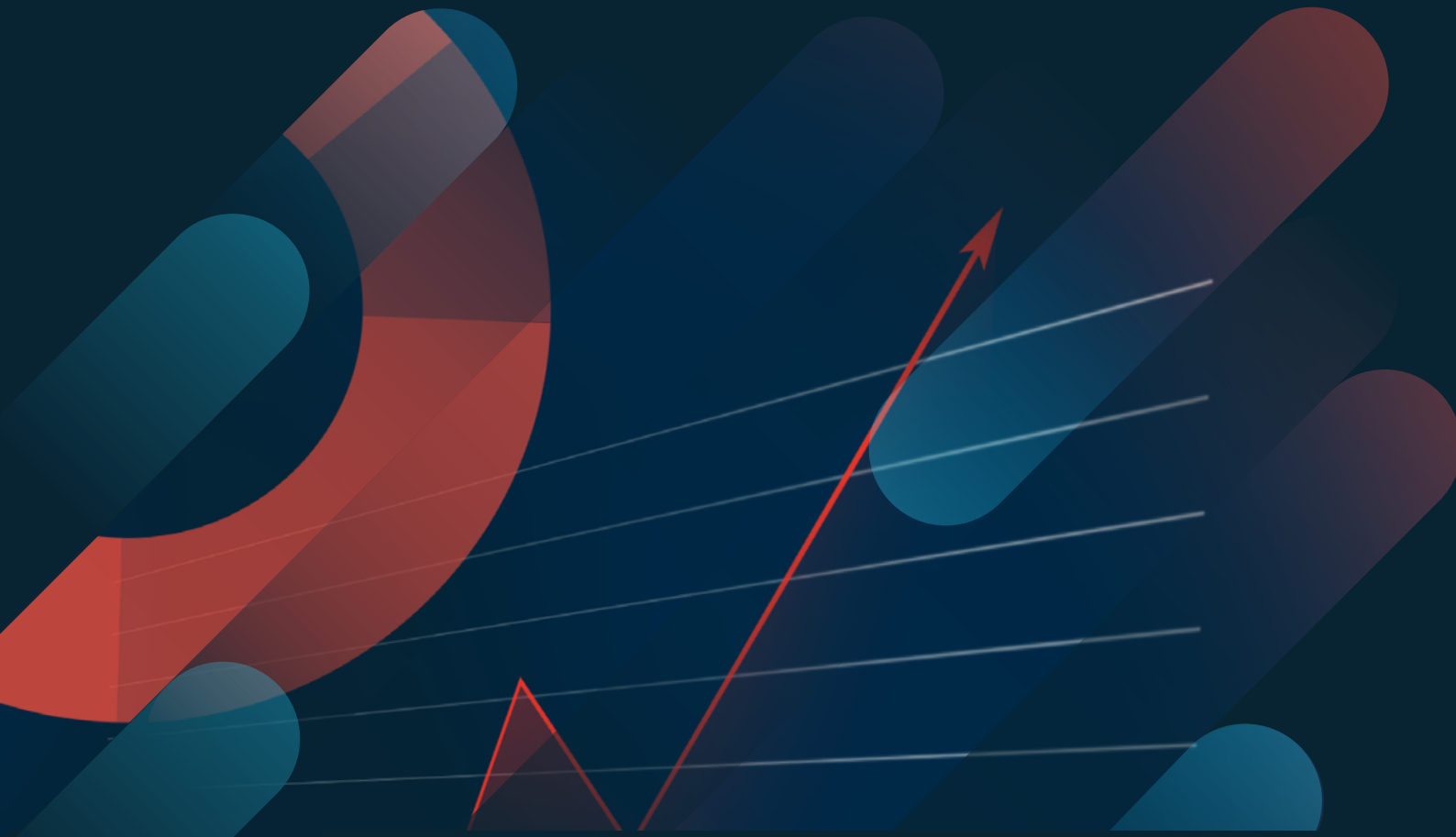


MYRA

MYRA WEB APPLICATION SECURITY REPORT:

Bedrohungslage 2023

In Zusammenarbeit mit:

zerobs

Tatort Layer 7: Ambitionierte Angreifer setzen Firmen unter Druck

EXECUTIVE SUMMARY

Insbesondere versierte Angreifer setzen auf Attacken auf die Applikationsschicht (Layer 7), die vielen Unternehmen noch immer erhebliche Schwierigkeiten bei der Abwehr bereiten.

DDoS-Attacken auf Layer 7 haben im zweiten Halbjahr 2022 massiv zugelegt. Insgesamt stieg die Anzahl blockierter Requests im Jahresvergleich um 178 Prozent. Ein Grund für den Anstieg sind unter anderem eine Reihe orchestrierter DDoS-Angriffe auf verschiedene deutsche Behörden.

Führende Unternehmen testen und optimieren laufend ihre IT-Sicherheit. Neben der Qualität der eingesetzten Abwehrtechnologie ist vor allem die professionelle Implementierung derselben sowie die Einführung von entsprechenden Mitigations-prozessen entscheidend, um die eigene Cyberresilienz nachhaltig zu erhöhen.

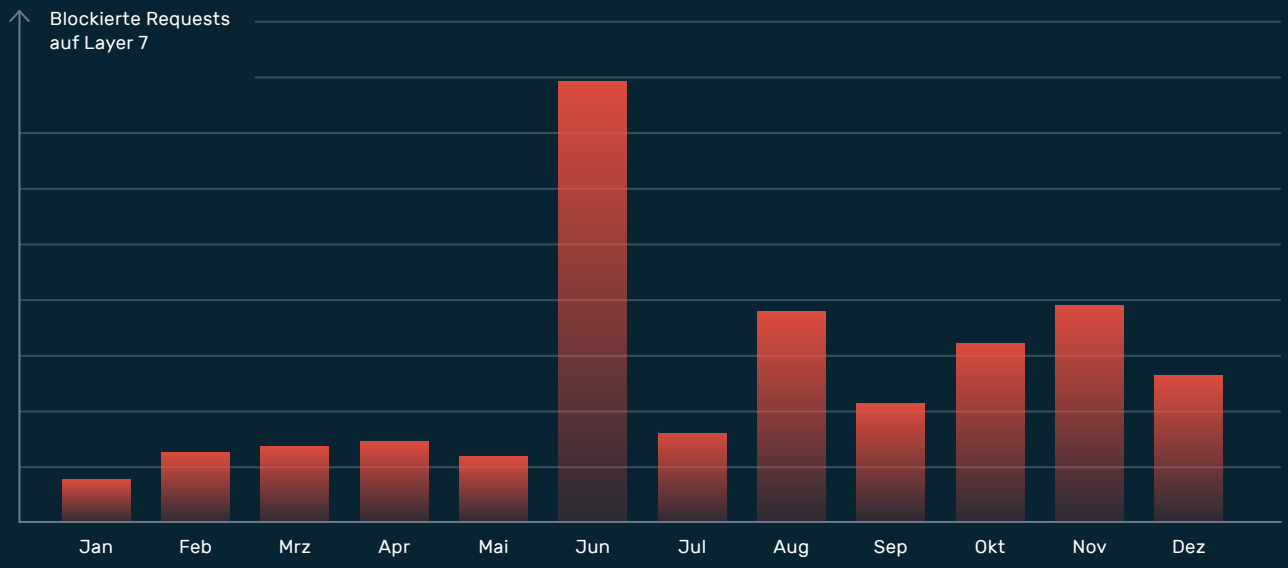
Cyberkriminelle nutzen zunehmend mehrstufige Erpressungsmethoden zur Monetarisierung ihrer Attacken. Dabei kommen auch Kombinationen von DDoS-Angriffen und Ransomware-Infektionen zum Einsatz.

Durch die fortdauernde Verlagerung von lokalen Diensten und Programmen in die Cloud verändert sich auch die digitale Bedrohungslandschaft grundlegend. Cyberkriminelle fokussieren ihre Attacken zunehmend auf die äußerste Netzwerkschicht und nehmen die dort befindlichen Webanwendungen, Internetseiten und Online-Schnittstellen (APIs) ins Visier. Im Security Operations Center (SOC) von Myra lässt sich diese Entwicklung in Echtzeit verfolgen. Täglich registrieren und analysieren unsere Cybersecurity Service Engineers Angriffe auf die digitalen Geschäftsprozesse von Unternehmen und Verwaltungsbehörden. Der folgende Report beschreibt die Cyberbedrohungslage für Deutschland, Österreich und die Schweiz (DACH) auf Basis der aggregierten Mitigationsdaten des Jahres 2022.

Massiver Anstieg von DDoS-Angriffen

Die Bedrohungslage auf der Anwendungsebene hat sich insbesondere seit der zweiten Jahreshälfte massiv verschärft. Ausschlaggebend für den sprunghaften Anstieg schädlicher Anfragen im Juni war in erster Linie eine Reihe orchestrierter DDoS-Angriffe auf verschiedene deutsche Behörden. Für den weiteren Verlauf des Jahres dokumentiert das Myra SOC ein anhaltend hohes Bedrohungsniveau. Der Halbjahresvergleich ergibt einen Anstieg der Angriffsaktivitäten um 24 Prozent.

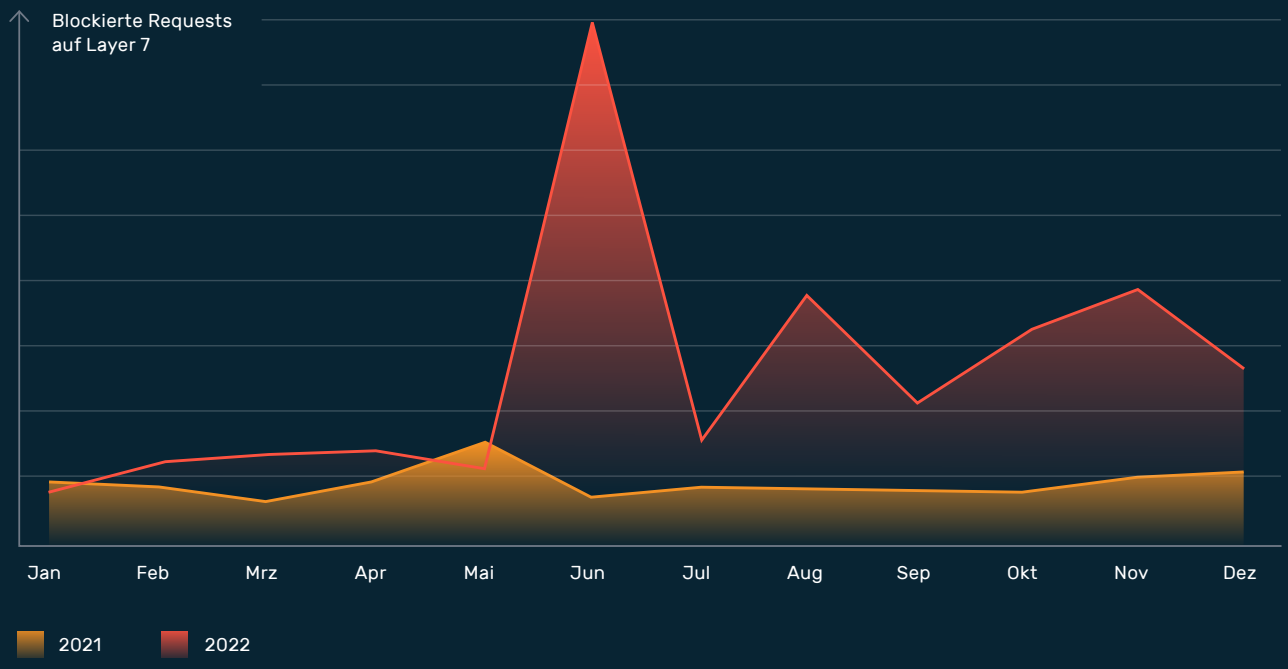
Angriffsaktivitäten 2022



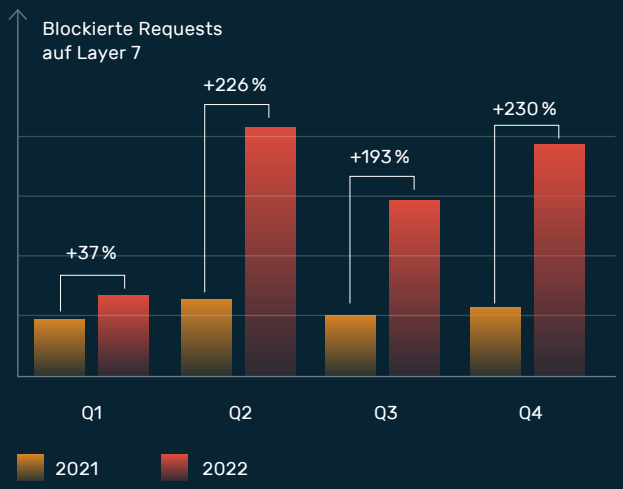
Die Zahl der blockierten Requests ist ebenso im Vergleich zum Vorjahr signifikant angestiegen. Allein für das erste Halbjahr 2022 belegen die Mitigationsdaten einen Anstieg der Angriffsaktivitäten um 144 Prozent gegenüber dem Vorjahreszeitraum. Über das gesamte Jahr betrachtet beträgt der Zuwachs sogar 178 Prozent.

Damit verschärft sich die aktuelle Bedrohungslage selbst im Vergleich zum mitigationsintensiven Pandemiejahr 2020 deutlich, in dem starke Angriffe auf den Finanzsektor dominierten. Hier lässt sich 2022 im direkten Vergleich mit 2020 ein Zuwachs der blockierten Anfragen um 143 Prozent festhalten.

Jahresvergleich 2021 vs 2022



Quartalsvergleich 2021 vs 2022

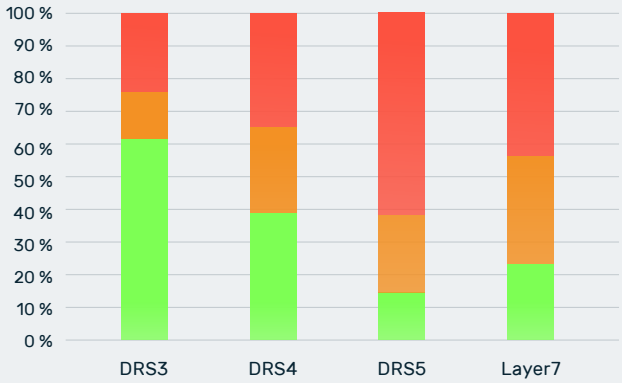


Im Quartalsvergleich von 2021 zu 2022 wird die Entwicklung noch deutlicher: Im zweiten Quartal hat sich die Summe blockierter Requests mehr als verdreifacht (plus 226 Prozent). Im dritten Quartal war weiterhin nahezu eine Verdreifachung gegenüber dem Vorjahreszeitraum zu beobachten (plus 193 Prozent). Der höchste Anstieg im Vorjahresvergleich ist mit 230 Prozent im vierten Quartal zu verzeichnen.

DDoS Insights von zeroBS

Die DDoS-Testing-Fachleute von zeroBS prüfen die DDoS-Schutzverfahren von Unternehmen mit hohen Verfügbarkeitsanforderungen in Verbindung mit Schutztechnologien führender Anbieter und Provider.

Im Jahr 2022 hat zeroBS mehr als 400 DDoS-Stresstests durchgeführt und dabei eine Vielzahl Vektoren, Protokolle und Methoden erprobt; vom simplen Script-Kiddie-Angriff bis zum ausgefeilten Red Teaming mit Open Source Intelligence (OSINT), Zielsuche, Einsatz von Browserbots und Machine Learning zur Überwindung von Browser Challenges und Captchas sowie Programmierung angepasster Traffic-Generatoren.



Dabei beobachteten die Pentester, dass neben Attacken per TCP DirectPath / TCP-Handshakes vor allem Layer-7-Angriffe die meisten Schwierigkeiten bei der Mitigation bereiten. Deswegen werden diese Arten von Angriffen auch bevorzugt von versierten Akteuren eingesetzt. Größtenteils resultierten die Probleme aus Konfigurationsfehlern. Insgesamt lässt sich festhalten: Je höher das Anforderungsniveau ausfiel, desto wahrscheinlicher waren Angriffe erfolgreich – insbesondere bei steigender Komplexität der IT-Systeme.

Testergebnisse

- **Erfolgreich:** Angriff mitigiert, maximale Mitigationszeit 30 Sekunden
- **Problematisch:** Angriff entweder nur teilweise oder manuell mitigiert, hoher Impact für mindestens 10 Minuten
- **Fehlgeschlagen:** keine Mitigation

DDoS Resiliency Score (DRS)

DRS 3: umfasst u.a. Stresser/Booter-Services, DDoS-as-a-Service

DRS 4: umfasst u.a. Aktivistengruppen (Killnet, Noname), DDoS-Erpressergangs

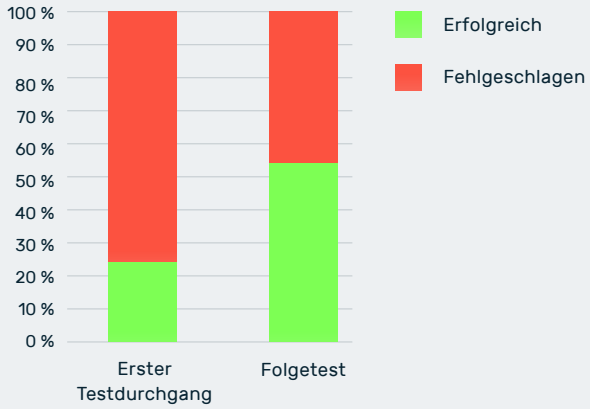
DRS 5: umfasst u.a. Advanced Attacker, DDoS-For-Hire, Profis

Weshalb führende Unternehmen regelmäßig testen

Testen zahlt sich aus. Fehlkonfigurationen werden schnell erkannt und können behoben werden. Potenzielle Angriffspunkte können getestet werden, bevor Angreifer dies tun.

Die Fachleute von zeroBS haben mehrere Problemfelder identifiziert, an denen wirksame DDoS-Mitigation scheitern kann. Neben einer sauberen Architektur und Implementierung sind auch die organisatorischen Workflows oder die Netztopologie entscheidend.

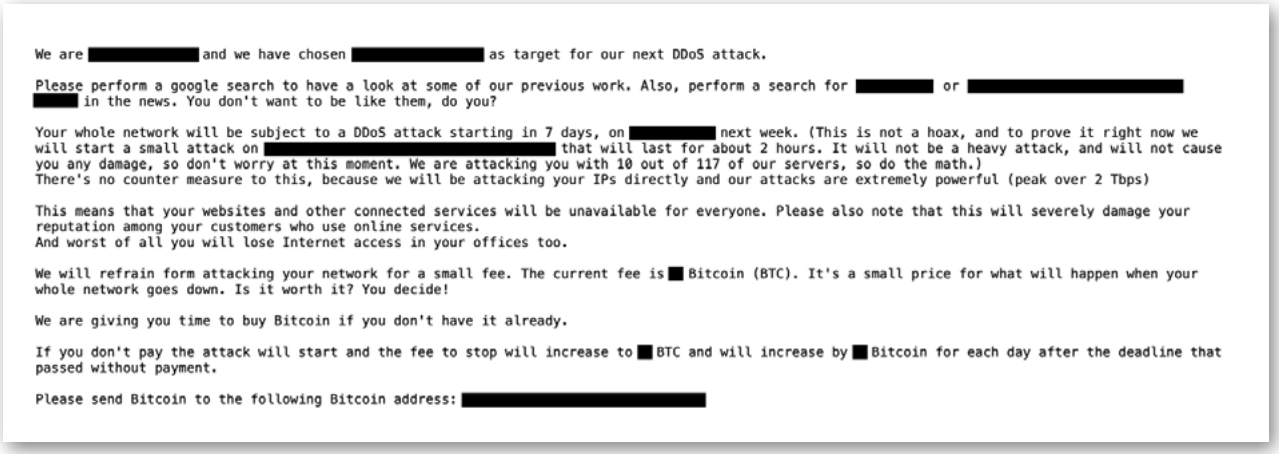
Es empfiehlt sich daher, das eigene DDoS-Schutzlevel kontinuierlich zu testen und an die sich laufend ändernden Bedingungen anzupassen. Da die Angreifer nicht schlafen, sondern im Gegenteil sehr aktiv sind und sich ständig weiterentwickeln, sollte jede Organisation mindestens jährlich das eigene Schutzniveau gegen DDoS-Bedrohungen evaluieren. Die Auswertung der Testreihen belegt, dass geprüfte Unternehmen ihre Cyberresilienz bereits in Folgetests deutlich steigern konnten.



Cybererpressung per DDoS und Ransomware

Incident-Analysen aus dem SOC von Myra ergeben zudem eine weitere Zunahme von DDoS-basierten Erpressungen (Ransom Denial of Service oder kurz RDoS). Die von einem RDoS-Angriff betroffenen Unternehmen erhalten im Vorfeld der Attacke ein Erpresserschreiben, das zur Zahlung eines Lösegelds auffordert.

Meist erfolgt zeitgleich eine erste Attacke auf die Webinfrastruktur der jeweiligen Firma. Dadurch wollen die Angreifer zeigen, dass sie es ernst meinen. Wer der Aufforderung der Erpresser nicht nachkommt, muss mit schweren Folgeattacken rechnen. Bereits seit Jahren nutzen Cyberkriminelle diese Methode, um DDoS-Angriffe direkt zu monetarisieren.



We are [redacted] and we have chosen [redacted] as target for our next DDoS attack.

Please perform a google search to have a look at some of our previous work. Also, perform a search for [redacted] or [redacted] in the news. You don't want to be like them, do you?

Your whole network will be subject to a DDoS attack starting in 7 days, on [redacted] next week. (This is not a hoax, and to prove it right now we will start a small attack on [redacted] that will last for about 2 hours. It will not be a heavy attack, and will not cause you any damage, so don't worry at this moment. We are attacking you with 10 out of 117 of our servers, so do the math.)
There's no counter measure to this, because we will be attacking your IPs directly and our attacks are extremely powerful (peak over 2 Tbps)

This means that your websites and other connected services will be unavailable for everyone. Please also note that this will severely damage your reputation among your customers who use online services.
And worst of all you will lose Internet access in your offices too.

We will refrain form attacking your network for a small fee. The current fee is [redacted] Bitcoin (BTC). It's a small price for what will happen when your whole network goes down. Is it worth it? You decide!

We are giving you time to buy Bitcoin if you don't have it already.

If you don't pay the attack will start and the fee to stop will increase to [redacted] BTC and will increase by [redacted] Bitcoin for each day after the deadline that passed without payment.

Please send Bitcoin to the following Bitcoin address: [redacted]

Typisches Erpresserschreiben

Seit einiger Zeit erweitern Cyberkriminelle dieses Muster auch um weitere Angriffsebenen wie dem Einsatz von Ransomware. Durch Verschlüsselungstrojaner werden dabei die Daten des Ziels in Geiselhaft genommen. Sollte das Unternehmen die Forderungen der Erpresser nicht erfüllen, folgen zusätzlich DDoS-Attacken, um noch mehr Druck aufzubauen.

Ebenfalls beobachtet das Myra SOC den Einsatz von DDoS-Attacken zur Verschleierung weiterer Angriffe. Dazu zählen neben Ransomware auch Brute-Force-Angriffe oder Advanced Persistent Threats (APT), bei denen sich Angreifer zu Spionage- oder Manipulationszwecken unbemerkt über längere Zeit in einem System einnisten.

Unternehmen stehen täglich einer Fülle von Bedrohungen gegenüber. Myra bietet effektive Schutzlösungen, um dieser Herausforderung zu begegnen.

Die Myra Application Security ist zur Absicherung geschäftskritischer Onlineprozesse konzipiert. Unsere Kunden profitieren von hocheffizienten Schutzlösungen zur Abwehr von DDoS-Attacken, schädlichen Bot-Zugriffen, Zero-Day-Schwachstellen, Angriffen auf Datenbanken und vieler weiterer Angriffsarten.

DDoS Attacks

SQL Injections

Cross-Site-Scripting

Credential Stuffing

Cross-Site-Request-Forgery

Directory Traversal

DNS Cache Poisoning

Hype Sales

Skewing

Price Grabbing

Content / Product Grabbing

Form Spam

Cart Abandonment

Credit Card Testing

Account Creation & Takeover

Myra schützt das reale Leben vor digitalen Gefahren

Myra bietet als deutscher Technologiehersteller eine sichere, zertifizierte Security-as-a-Service-Plattform zum Schutz digitaler Geschäftsprozesse. Die smarte Myra-Technologie überwacht, analysiert und filtert schädlichen Internet-Traffic, noch bevor virtuelle Angriffe einen realen Schaden anrichten.

Unsere Kernkompetenzen

Security

Durch Cyberangriffe werden Daten gestohlen, Systemausfälle provoziert und Kommunikationskanäle gestört. Myra wehrt Angriffe auf Ihre digitalen Prozesse in Echtzeit ab.

Performance

Traffic-Peaks durch Sales-Kampagnen, Livestreaming oder unplanbare Ereignisse überfordern Web-Anwendungen. Myra liefert Ihren Content immer hochperformant aus.

Compliance

Gesetzliche und unternehmens-spezifische Vorgaben zu IT-Sicherheit und Datenschutz erfordern auditierte Prozesse. Myra ist Ihr Garant für strengste Anforderungen.

BSI-zertifizierte IT-Sicherheit

Die Myra-Technologie ist vom Bundesamt für Sicherheit in der Informationstechnik (BSI) nach dem Standard ISO 27001 auf Basis von IT-Grundschutz zertifiziert. Zudem erfüllen wir als einer der führenden Anbieter alle 37 Kriterien des BSI für qualifizierte KRITIS-Sicherheitsdienstleister. Damit setzen wir den Maßstab in der IT-Sicherheit.

ISO 27001 BSI zertifiziert auf der Basis von IT-Grundschutz Zertifikat Nr.: BSI-IGZ-0479-2021 | PCI DSS Certified | BSIG KRITIS-qualifiziert | EU-DSGVO konform | BSI C5 Testat Typ 2 | Trusted Cloud Service | ISAE 3402 IDW PS 951 Type 2 | 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 | KRITIS-qualifiziert nach §3 BSI-Gesetz | Konform mit der (EU) 2016/679 Datenschutz-Grundverordnung | 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

Myra ist der Spezialanbieter für Kunden aus hochregulierten Bereichen

Bundesministerium für Gesundheit | Bundeszentrale für gesundheitliche Aufklärung (BZgA) | Liechtensteinische Landesbank 1861 | msc Munich Security Conference

CANCOM | DSV IT Service | ITSG | flatex DEGIRO

Made in Germany

Myra Security ist der neue Maßstab für globale IT-Sicherheit.

Myra bietet als deutscher Technologiehersteller eine sichere, zertifizierte Security-as-a-Service-Plattform zum Schutz digitaler Geschäftsprozesse.
Die smarte Myra-Technologie überwacht, analysiert und filtert schädlichen Internet-Traffic, noch bevor virtuelle Angriffe einen realen Schaden anrichten.

Jetzt individuelle Sicherheitsanalyse anfordern

Myra Security GmbH

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