MYRA

MYRA WEB APPLICATION SECURITY REPORT:

Bedrohungslage H1 2023

Mit exklusiven DDoS Insights zu neuartigen Angriffsmustern

In Kooperation mit

zerobs

Defcon DDoS: Behörden in Alarmbereitschaft

EXECUTIVE SUMMARY

Öffentliche Verwaltung unter Beschuss

Der Trend zu Cyberattacken auf Behörden und öffentliche Organisationen setzt sich fort – das Security Operations Center (SOC) von Myra verzeichnete im ersten Halbjahr 2023 eine Zunahme von schädlichem Traffic auf die digitalen Lösungen von Behörden. So gerieten im April die Webseiten und Portale mehrere Landespolizeien sowie verschiedene Institutionen auf Länderebene ins Visier von Angreifern. Neben der Bundes- und Landesverwaltung sind immer öfter auch Kommunen von Cyberangriffen betroffen. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) wies zuletzt auf der Potsdamer Konferenz für Nationale Cybersicherheit auf die kritische Bedrohungslage für Kommunen hin.

Cybercrime-Katalysator: DDoS als Dienstleistung

Cybercrime-Dienstleister im Darknet verschärfen die angespannte Lage zusätzlich. Über DDoS-for-hire-Portale können selbst Angreifer ohne technische Kenntnisse einfache DDoS-Attacken ab 10 Dollar pro Stunde buchen, die meist ausreichen, um Webinstanzen ohne dedizierte Schutzsysteme ausfallen zu lassen.[1] Im April hatte das Landeskriminalamt Hessen (HLKA) in Zusammenarbeit mit dem BKA die Server des DDoS-for-hire-Anbieters „FlyingHost" beschlagnahmt. Über den Dienst sollen unter anderem Attacken auf Unternehmen und Behörden in Hessen und Baden-Württemberg ausgeführt worden sein.

Bedrohung von Webdiensten nimmt zu

Insgesamt verlagern Cyberkriminelle vermehrt ihre Attacken auf die äußerste Netzwerkschicht (Layer 7), um dort Webapplikationen, Internetportale und kritische Schnittstellen (APIs) direkt anzugehen. DDoS-Angriffe zählen hier zu den Hauptursachen für Cybervorfälle.[2] Attacken auf Layer 7 sind für die betroffenen Unternehmen meist sehr schwer zu identifizieren und abzuwehren. Insbesondere, wenn es sich dabei um ausgeklügelte Angriffsmethoden wie die HALO-Attacke handelt – mehr dazu auf Seite 4.

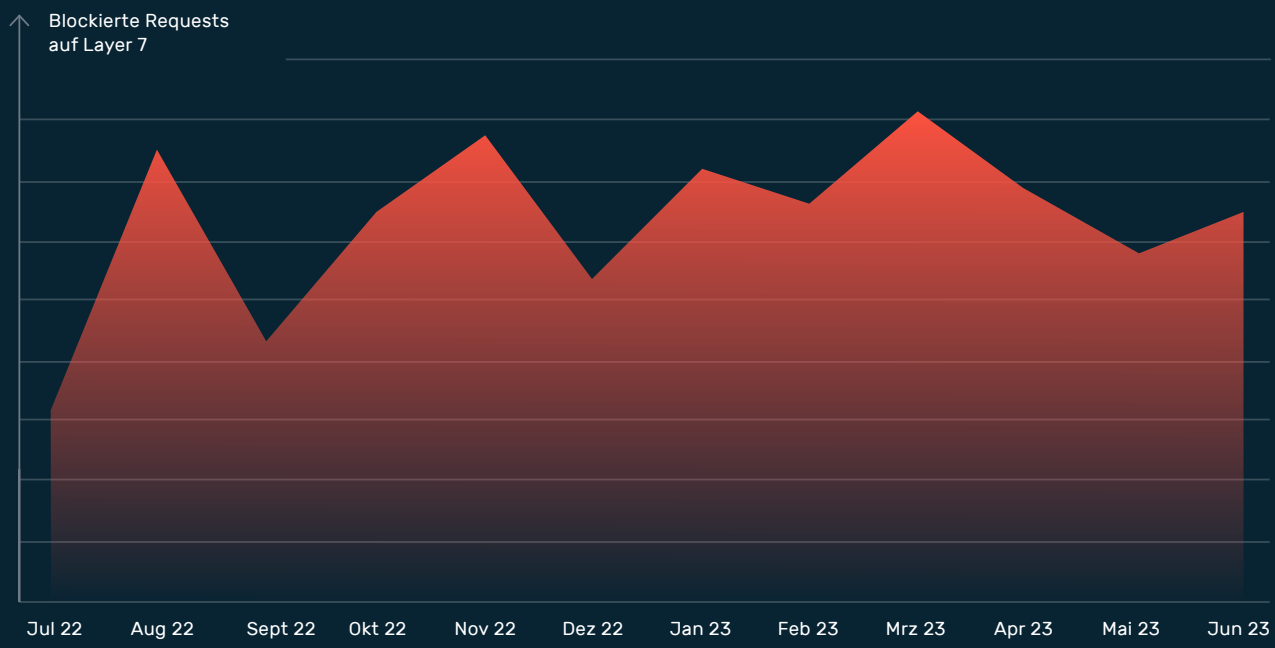
Die geopolitischen Entwicklungen haben zu einer massiven Verschärfung der digitalen Bedrohungslage geführt. Im ersten Halbjahr 2023 äußerte sich dies insbesondere durch eine gestiegene Angriffsaktivität im Bereich DDoS. Aktuell betrachten 7 von 10 IT-Verantwortliche in Deutschland DDoS-Attacken als Security-Risiko mit erheblichen Auswirkungen.[3] Umso entscheidender ist die Implementierung dedizierter Schutzlösungen, um kritische Webprozesse konsequent vor solchen Attacken zu schützen. Zumal viele Unternehmen durch die Umsetzung der EU-Richtlinie NIS-2 ohnehin dazu verpflichtet sind, maßgerechte IT-Sicherheitslösungen nach dem Stand der Technik einzusetzen. Entsprechend wächst der Druck auf Organisationen aller Sektoren, Informationssicherheit zur Chefsache zu erklären – die Bedrohungslage mahnt dazu, der Gesetzgeber verpflichtet dazu.

1 PrivacyAffairs.com: Dark Web Price Index 2023
2 Verizon: Verizon Data Breach Investigations Report 2023
3 Lünendonk/KPMG: Von Cyber Security zu Cyber Resilience 2023

DDoS-Bedrohungslage auf unverändert hohem Niveau

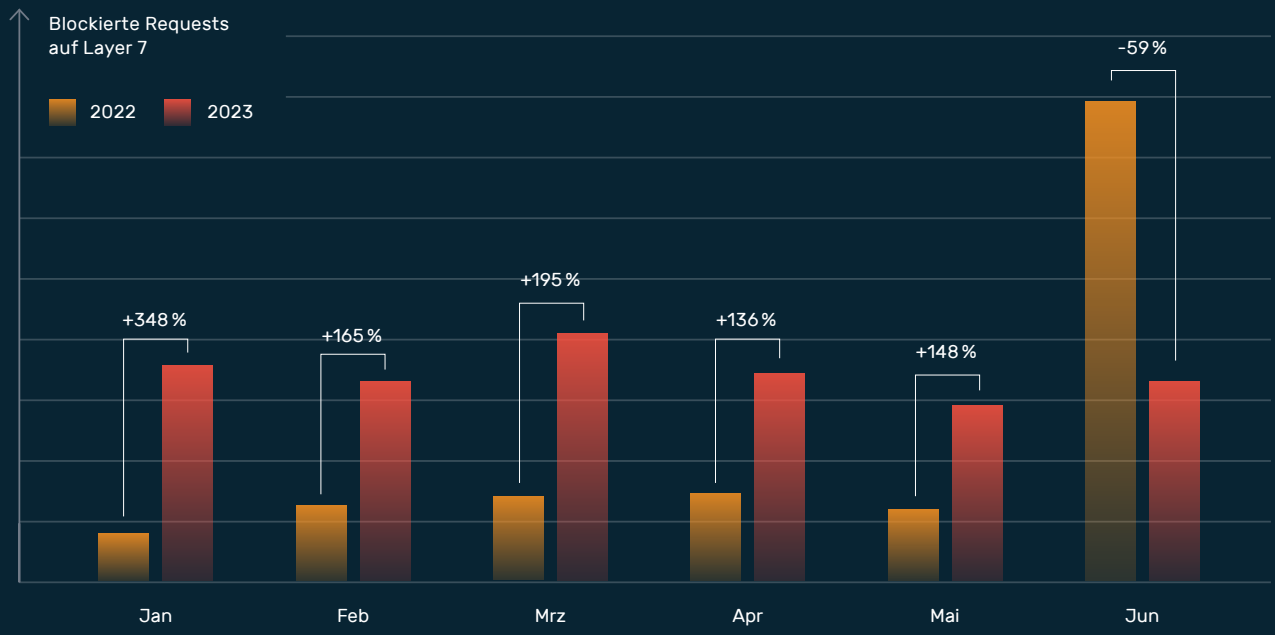
Die Analyse der Mitigationszahlen aus dem SOC von Myra offenbart zwei wesentliche Erkenntnisse: Zum einen verharrt die DDoS-Bedrohungslage auf dem hohen Niveau, auf dem sie sich seit Mitte 2022 eingependelt hat – eine saisonale Entspannung zeichnet sich nicht ab. Zum anderen blieben massive Ausschläge, wie sie ebenfalls im vergangenen Jahr zu beobachten waren, bislang aus. Die meisten schädlichen Anfragen registrierte das Myra SOC im März, die niedrigste Anzahl abzuwehrender Requests im Mai.

Angriffsaktivität von Juli 2022 bis Juni 2023



Im direkten Vergleich zum ersten Halbjahr 2022 ergibt sich insgesamt eine deutliche Verschärfung der Bedrohungslage, die Anzahl schädlicher Requests stieg um knapp die Hälfte (47,1 %) an. Dieses Ergebnis umfasst jedoch den massiven Ausschlag aus dem Juni 2022, der aus einer orchestrierten Angriffskampagne auf deutsche Behörden hervorging. Um diesen Ausschlag bereinigt hat sich die Anzahl blockierter Anfragen im betrachteten Zeitraum fast verdreifacht (+186 %). Selbst im Mai 2023, dem Monat mit der niedrigsten Anzahl abgewehrter Requests im ersten Halbjahr, ist im Jahresvergleich die Angriffsaktivität um 148 % angewachsen.

Angriffsaktivität: H1 2022 vs H1 2023



Behörden im Fokus der Angreifer

Zu den präferierten Zielen von Cyberkriminellen zählen auch im ersten Halbjahr 2023 wieder Organisationen aus der öffentlichen Verwaltung – damit setzt sich auch hier ein Trend aus dem vergangenen Jahr fort. Etwa zwei kritische Attacken pro Monat und Kunde verzeichnete das Myra SOC für den Bereich der öffentlichen Verwaltung. Ohne dedizierte Schutzlösungen hätten diese Angriffe unweigerlich zum Ausfall der anvisierten Webseiten, Bürgerportale und IT-Fachverfahren geführt.

> *Die Sicherheit der deutschen Behörden war schon immer im Fadenkreuz.*
>
> **Christian Dörr**
> *Leiter des Fachgebiets Cybersecurity am Hasso-Plattner-Institut*

Die Einschätzungen der Wissenschaft und der zuständigen Behörden decken sich mit den Erkenntnisse aus dem Myra SOC. „Die Sicherheit der deutschen Behörden war schon immer im Fadenkreuz. Das Risikoniveau ist aufgrund des Ukraine-Krieges wahrscheinlich von hoch auf sehr hoch gestiegen“, sagte Christian Dörr, Leiter des Fachgebiets Cybersecurity am Hasso-Plattner-Institut Potsdam, im April auf der Potsdamer Konferenz für Nationale Cybersicherheit. BSI-Vizepräsident Gerhard Schabhüser rief an gleicher Stelle vor allem die kleineren Kommunen dazu auf, IT-Dienstleistungen an qualifizierte Profis auszulagern: „Macht Eure IT nicht selbst, sondern nutzt Dienstleister.“

DDoS Insights von zeroBS

Das auf DDoS-Attacken spezialisierte Pentesting-Unternehmen zeroBS untersucht und analysiert laufend neue Angriffsvektoren, um die potenzielle Schlagkraft von neuen Cyberwaffen einschätzen zu können. Zuletzt beschäftigten sich die DDoS-Stresstester mit dem sogenannten HALO-Angriff, einer Angriffsmethode, die insbesondere von versierten Akteuren eingesetzt wird. Der Name leitet sich vom HALO-Drive ab, einer theoretischen Antriebsform für die interstellare Raumfahrt, bei der ein Laserstrahl um ein Schwarzes Loch geschleudert wird, um Energie zu gewinnen.

Bei der HALO-Attacke handelt es sich um einen Reverse-HTTP-Amplification-Angriff, der zu einem erheblichen Upstream-Verkehr beim anvisierten Ziel führt und die ausgehende Datenverbindung blockiert. Dazu sendet der Angreifer gültige Anfragen an Ressourcen, die größer sind als die Anfrage selbst – in der Regel JavaScript- oder CSS-Code, Bilder, PDFs und dergleichen. Beim Einsatz eines Botnetzes mit 5.000 Bots und 1 RPS (Requests Per Second) waren die Fachleute von zeroBS in der Lage, mit Dateien von durchschnittlich 1 MByte Größe einen Upstream von 70 GBit/s zu generieren. Durch die niedrige RPS-Rate können bei der HALO-Attacke gängige WAF- und Bot-Management-Lösungen umgangen werden, während die schädliche Bandbreite den Upstream vollständig auslastet.

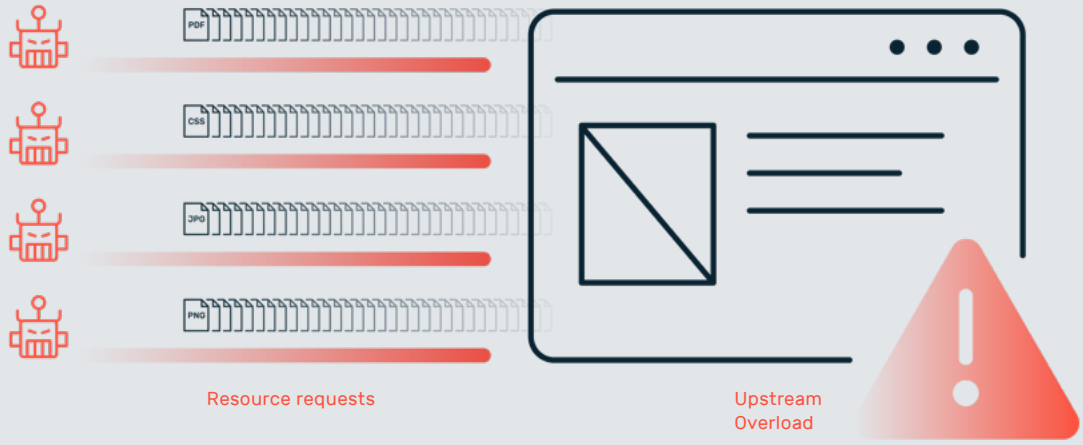
Best Practice Mitigation

Um das Risiko von Reverse-HTTP-Amplification-Angriffen einzudämmen, müssen Organisationen den eingehenden und ausgehenden Datenverkehr genau überwachen. Eine weitere, wesentliche Mitigationsempfehlung ist der Einsatz eines leistungsfähigen Content Delivery Network (CDN) für alle statischen Ressourcen, idealerweise weltweit aufgestellt und via Anycast-Routing erreichbar.

HALO-Angriff im Überblick

Dieser Reverse-HTTP-Amplification-Angriff ist für betroffene Unternehmen äußerst schwierig zu mitigieren, da nicht wie üblich die Überlastungsgefahr vom eingehenden Traffic ausgeht, sondern vom Upstream nach außen. Diese Art von Angriff bietet den Akteuren gleich mehrere Vorteile:

- Erlaubt Umgehung von WAF & Bot Management aufgrund geringer RPS pro Bot.
- Amplification im Inneren des Zielnetzwerks ermöglicht die Umgehung der Mitigation und die Option, spezifische Ziele anzugreifen.
- Unübliche Angriffsart, die häufig zu Problemen bei Erkennung und Mitigation führt.



Bei der HALO-Attacke fluten Bots den anvisierten Dienst mit Anfragen zu frei verfügbaren Dateien, bis der Upstream-Kanal des Webservers überlastet ist.

Attack of the clones

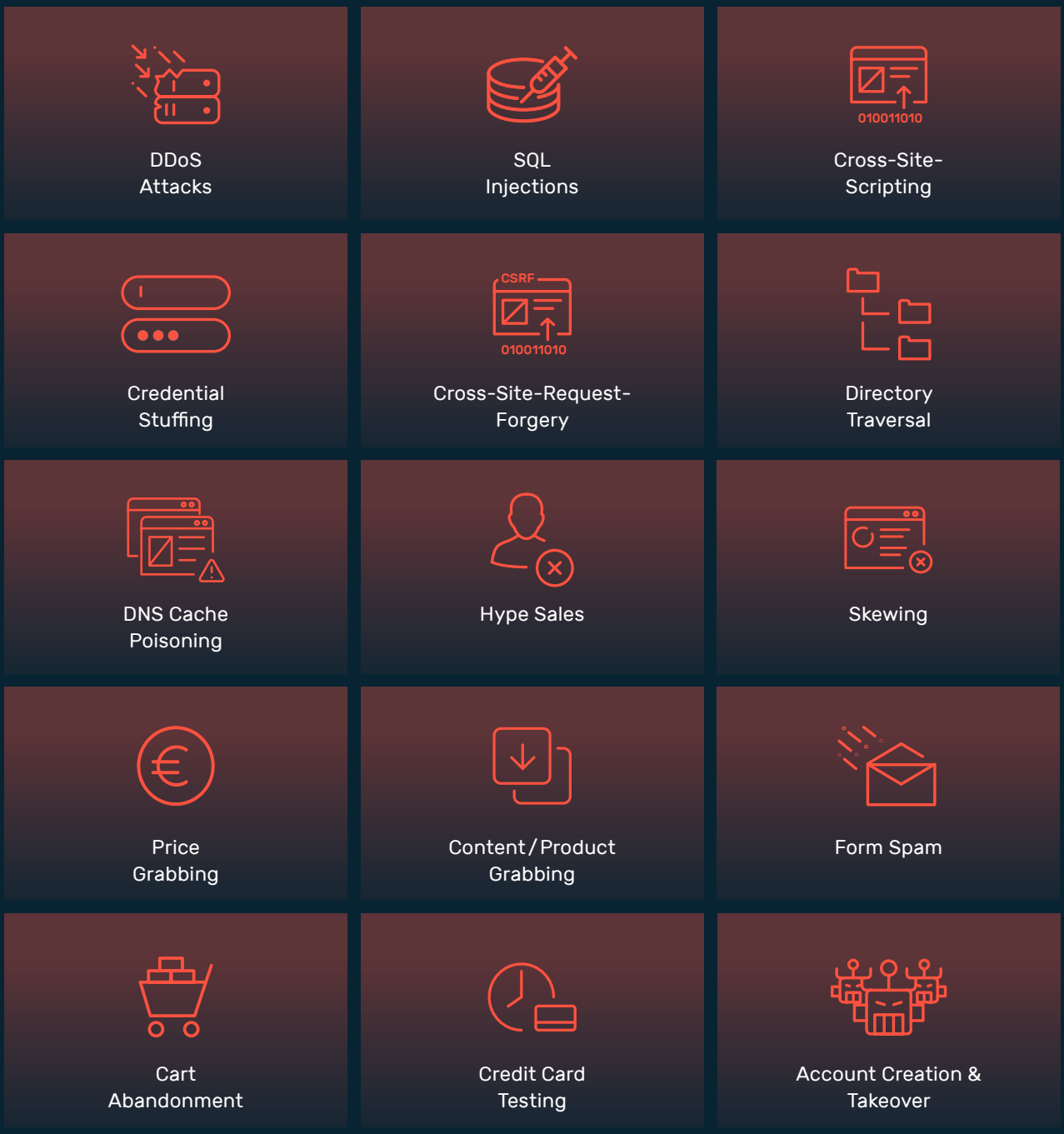
Folgendes Gedankenexperiment verdeutlicht das enorme Schadenspotenzial der HALO- Angriffsmethode: Als Ausgangspunkt für einen Angriff auf eine Coding-Plattform soll ein großes Botnetz wie Meris oder Mirai dienen, bestehend aus 50.000 Bots. Für dieses Botnetz erstellen die Angreifer eine Liste aller öffentlich zugänglichen Repositories der Plattform mit mehr als 1 MByte Quellcode. Nun werden die Bots angewiesen, während des Angriffs in einer Endlosschleife einen Klonbefehl für zufällig ausgewählte Repositories durchzuführen.

Ausgehend von konservativen Durchschnittsmessungen von 100 MBit/s Download-Verkehr pro Bot würde der gesamte Upstream-Verkehr der Plattform die enorme Höhe von 5 TBit/s erreichen. Es ist davon auszugehen, dass dieses Traffic-Aufkommen eine erhebliche Belastungsprobe der Systeme darstellen würde. Selbst bei einem um den Faktor 10 kleineren Botnet mit 5.000 Bots, das durchaus als Standard-Botnetz gelten kann, ließen sich durch die Methode immer noch 500 GBit/s Traffic erzeugen.

Dieses Szenario verdeutlicht die potenziellen Auswirkungen und das Ausmaß von DDoS-Angriffen, wenn sie sorgfältig ausgeführt werden. Indem Hersteller von Schutzlösungen und Unternehmen das potenzielle Ausmaß solcher Angriffsmethoden verstehen und bei der Implementierung von Sicherheitsmaßnahmen proaktiv bleiben, können Sie die Auswirkungen von DDoS-Angriffen minimieren und die Stabilität und Zuverlässigkeit ihrer digitalen Infrastruktur schützen.

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.



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 | 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

Die Bundesregierung | Bundeszentrale für gesundheitliche Aufklärung (BZgA) | ITSG | msc Munich Security Conference | CANCOM | DSV IT Service | flatex DEGIRO | Liechtensteinische Landesbank 1861

Made in Germany

Jetzt individuelle Maßnahmen ableiten und Resilienz erhöhen

Sie haben Fragen zu den Ergebnissen unserer Untersuchung oder wünschen eine persönliche Schutzberatung? Unsere IT-Fachleute stehen Ihnen gerne zur Verfügung.

Myra Security GmbH

+49 89 414141 - 345

www.myrasecurity.com

info@myrasecurity.com