MYRA

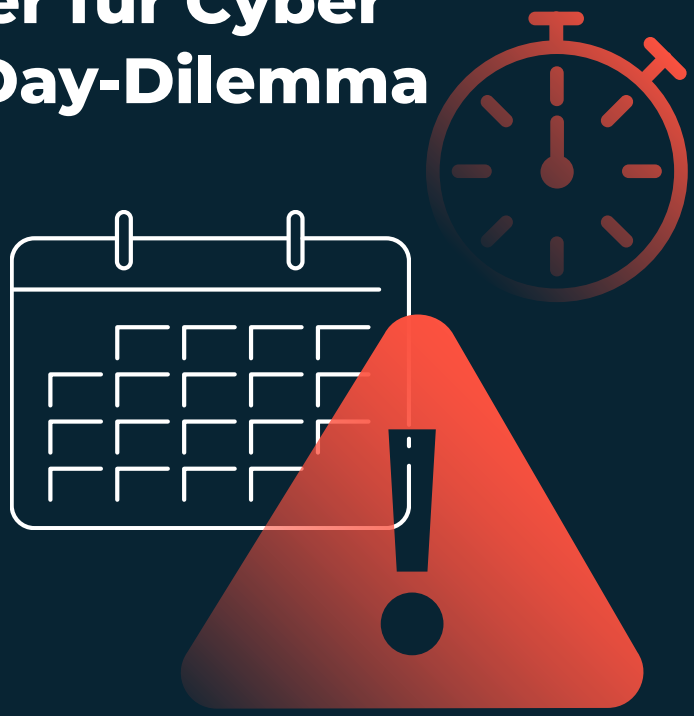
MYRA WEB APPLICATION SECURITY REPORT:

Bedrohungslage 2024

In Zusammenarbeit mit:

zerobs

Brandbeschleuniger für Cyber Threats: das Zero-Day-Dilemma



KEY FINDINGS

Gefährdungslage durch DDoS nimmt massiv zu

Im Security Operations Center (SOC) von Myra wurden im Jahresverlauf 2023 rund 60 Prozent mehr schädliche Anfragen auf Webseiten, Internetportale und Online-Schnittstellen abgewehrt als im Vorjahr. Inzwischen halten es 67 Prozent aller IT-Führungskräfte für sehr wahrscheinlich, dass ihr Unternehmen einem schwerwiegenden DDoS-Angriff (Distributed Denial of Service) zum Opfer fallen wird.[1]

Neue Angriffsvektoren verstärken Attacken und erschweren die Abwehr

Nicht nur die Anzahl der Attacken auf die Webinfrastruktur von deutschen Organisationen steigt, auch die Stärke und Komplexität der Angriffe nimmt zu. Neue Angriffsvektoren wie HTTP/2 RapidReset oder DRDoS-Attacken (Distributed Reflected Denial of Service) via SLP nutzen Sicherheitslücken in bestehenden Systemen und Protokollen, um verwundbare Ressourcen gezielt auszuschalten.

206 Milliarden Euro Schäden durch Cybervorfälle

Angriffe auf die digitalen Systeme deutscher Unternehmen haben im vergangenen Jahr zu Schäden in Höhe von 206 Milliarden Euro geführt. Durch die anhaltend hohe Bedrohungslage fühlen sich mehr als die Hälfte aller Organisationen in ihrer Existenz bedroht.[2] Das Schadensausmaß einer Cyberattacke beträgt bei Unternehmen mit 50 bis 250 Arbeitskräften im Schnitt 102.739 Euro.[3]

Striktere Compliance-Vorgaben, härtere Strafen

Durch neue regulatorische Regelwerke wie NIS2, den Cyber Resilience Act (CRA) oder DORA (Digital Operational Resilience Act) definieren Aufsichtsbehörden striktere Vorgaben für die erforderliche Absicherung digitaler Systeme. Die neuen Regeln gelten für einen zunehmend größeren Kreis von Unternehmen einschließlich deren Dienstleister entlang der gesamten digitalen Wertschöpfungskette. Wer den Vorgaben nicht nachkommt, muss mit empfindlichen Strafen rechnen. 2023 musste rund jedes fünfte von einer Cyberattacke betroffene Unternehmen ein Bußgeld aufgrund regulatorischer Verfehlungen bezahlen.[4]

1 Lünendonk Studie 2023
2 Bitkom Wirtschaftsschutz 2023
3 HDI Cyberstudie 2023
4 HDI Cyberstudie 2023

Zeitenwende in der Informationssicherheit

Im vergangenen Jahr mussten sich Organisationen in Deutschland vielen neuen Herausforderungen stellen. Die geopolitischen Entwicklungen sorgten nicht nur für einen enormen Anstieg der Energiepreise und eine hohe Inflation, auch bei der Cybersicherheit verschärfte sich die Bedrohungslage. Laut Untersuchungen der Allianz stellen Cybervorfälle das größte Risiko für Organisationen in der Bundesrepublik dar.[5] Staatlich unterstützte Cybergruppierungen nahmen im vergangenen Jahr gezielt deutsche Unternehmen und Verwaltungsbehörden mit orchestrierten Attacken ins Visier – weiträumige Ausfälle von Online-Diensten und Services waren die Folge.

Gleichzeitig agieren die Angreifer immer professioneller. Kriminelle bieten DDoS-Attacken, Ransomware-Angriffe und mehr als Dienstleistung (Cybercrime as a Service) im Darknet an. Dadurch wird es auch technisch unversierten Akteuren möglich, schwere Schäden anzurichten. Oft genügt eine Sicherheitslücke in den eingesetzten Systemen, um das gesamte Firmennetz zu gefährden – und davon gibt es mehr denn je. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) zählt in seinem aktuellen Lagebericht mehr als 2.000 Schwachstellen, die durchschnittlich pro Monat entdeckt wurden. Jede sechste davon gilt als kritisch. Pro Tag identifiziert die Behörde mehr als 21.000 infizierte Systeme.

Top Geschäftsrisiken in Deutschland
(Allianz Risk Barometer 2024)

1	Cybervorfälle
2	Betriebsunterbrechung
3	Änderungen von Gesetzen und Vorschriften
4	Mangel an qualifizierten Arbeitskräften
5	Makroökonomische Entwicklung

Durch die freie Verfügbarkeit generativer KI-Modelle wie ChatGPT, Bard oder LlaMa stehen Cyberkriminellen neue Werkzeuge zur Ausnutzung von Sicherheitslücken und zur Erstellung von Schadcode bereit – täglich werden mehr als eine Viertelmillion neue Schadprogrammvarianten von Sicherheitsbehörden identifiziert. Das Bundeskriminalamt (BKA) erwartet für die Zukunft eine weitergehende kriminelle Ausnutzung von KI-Methoden zur gezielten (Weiter-)Entwicklung von Angriffswerkzeugen und -vektoren.[6]

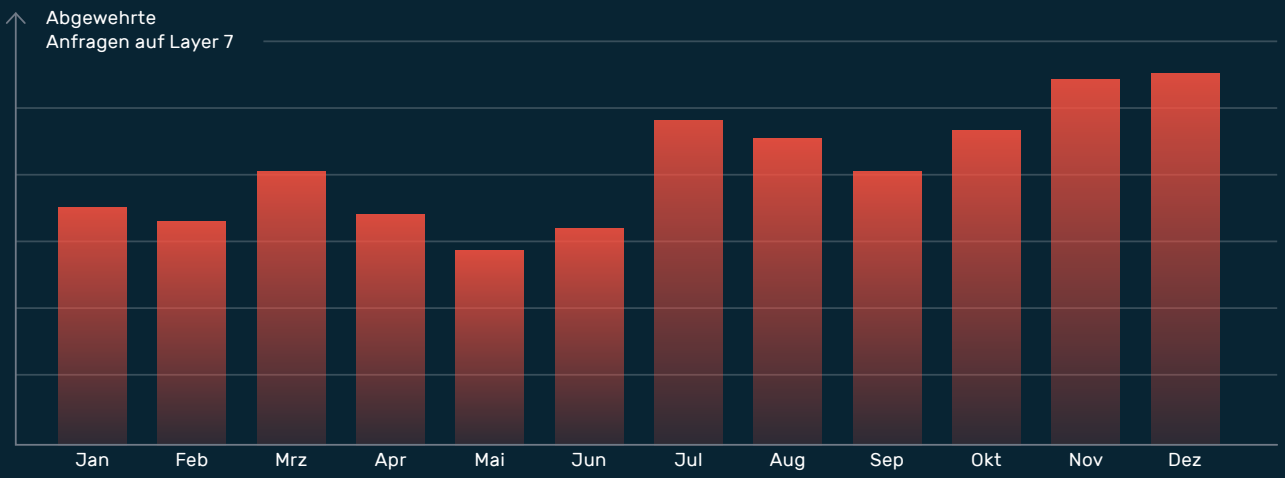
Um auf die angespannte Bedrohungslage angemessen zu reagieren, müssen Unternehmen und Organisationen der öffentlichen Verwaltung auf eine holistische und ebenso flexible Absicherung ihrer Systeme setzen. Insbesondere Webapplikationen, APIs und Webinfrastrukturen werden immer öfter von Angreifern ins Visier genommen – hier sind Schutzsysteme unverzichtbar, um kritische Geschäftsprozesse konsequent zu sichern.

Auf den folgenden Seiten erhalten Sie detaillierte Einblicke aus dem Myra SOC zur Entwicklung der Bedrohungslage auf der Applikationsebene im Jahr 2023. Außerdem analysiert unser Partner zeroBS den neuartigen Angriffsvektor HTTP/2 RapidReset und liefert hierzu praxisnahe Messergebnisse, welche die enorme Schlagkraft der DDoS-Angriffsmethode verdeutlichen.

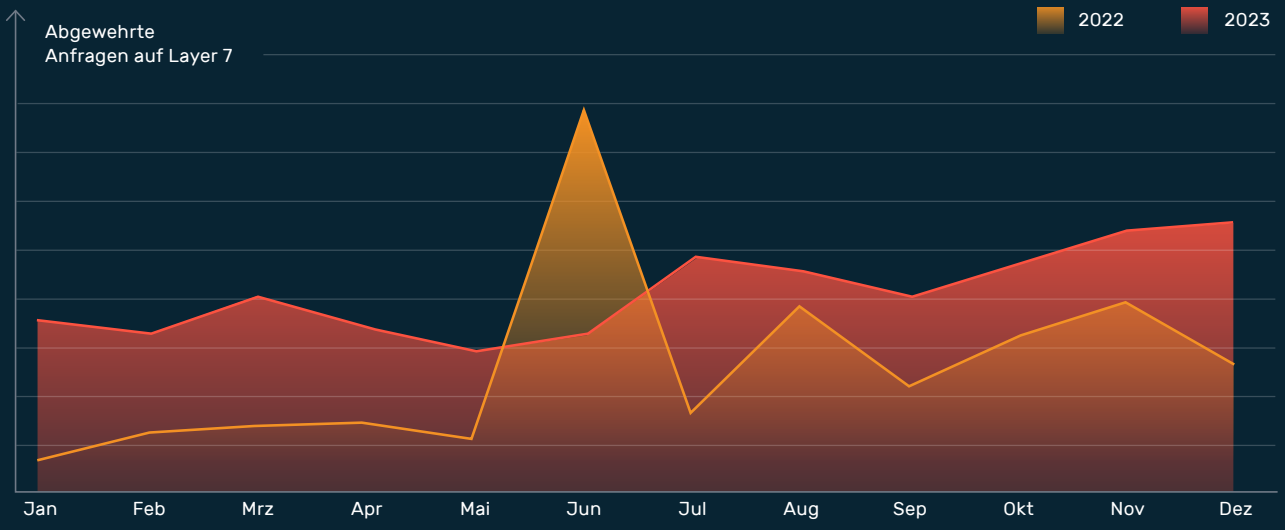
5 Allianz Risk Barometer 2024
6 BKA Cybercrime Bundeslagebild 2022

Myra Threat Intelligence: Zahl der Angriffe steigt

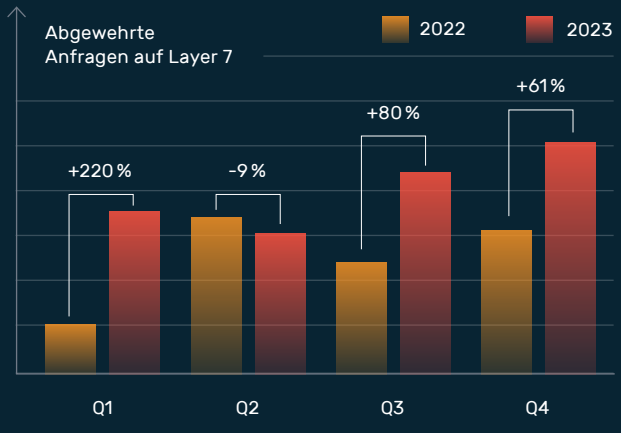
Angriffsaktivität 2023



Jahresvergleich



Quartalsvergleich



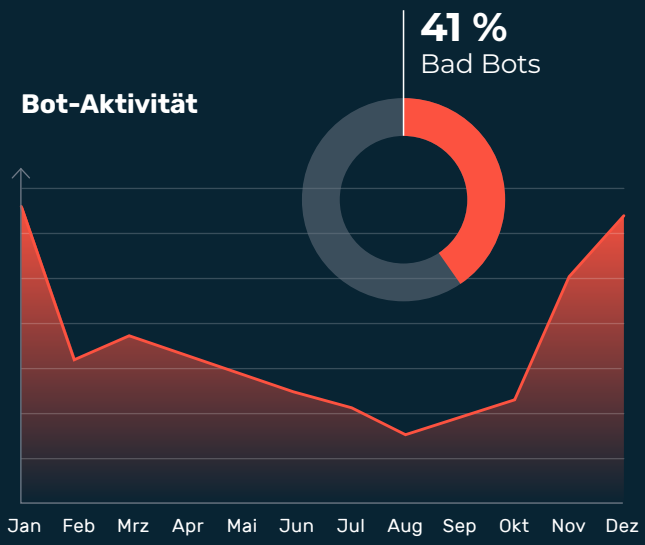
Die Mitigationsdaten aus dem Myra SOC belegen einen eindeutigen Trend: Angriffe auf Webapplikationen hatten im Jahr 2023 Hochkonjunktur – die Bedrohungslage verschärfte sich massiv. Insbesondere im ersten Quartal 2023 stieg die Anzahl schädlicher Anfragen, die durch Myra abgewehrt wurden, um 219 Prozent im Vergleich zum Vorjahr an.

Insgesamt konnte ein Zuwachs von 59 Prozent über den gesamten Jahresverlauf beobachtet werden. Im Gegensatz zu 2022, in dem zur Jahreshälfte kurzzeitig ein enormer Ausschlag der Angriffsaktivität zu verzeichnen war, blieb die Intensität 2023 über den gesamten Jahresverlauf hoch und steigerte sich tendenziell bis zum Jahresende weiter.

Wie schon im Vorjahr konzentrierten sich die Angriffe 2023 primär auf Einrichtungen aus dem Bereich der öffentlichen Verwaltung. Betroffen waren über den gesamten Sektor hinweg Behörden auf Bundes-, Landes- und Kommunalebene. Auch Polizeibehörden standen im Fokus der Cyberkriminellen, die mit ihren Attacken meist geopolitische Ziele verfolgten.

Bad Bots auf dem Vormarsch

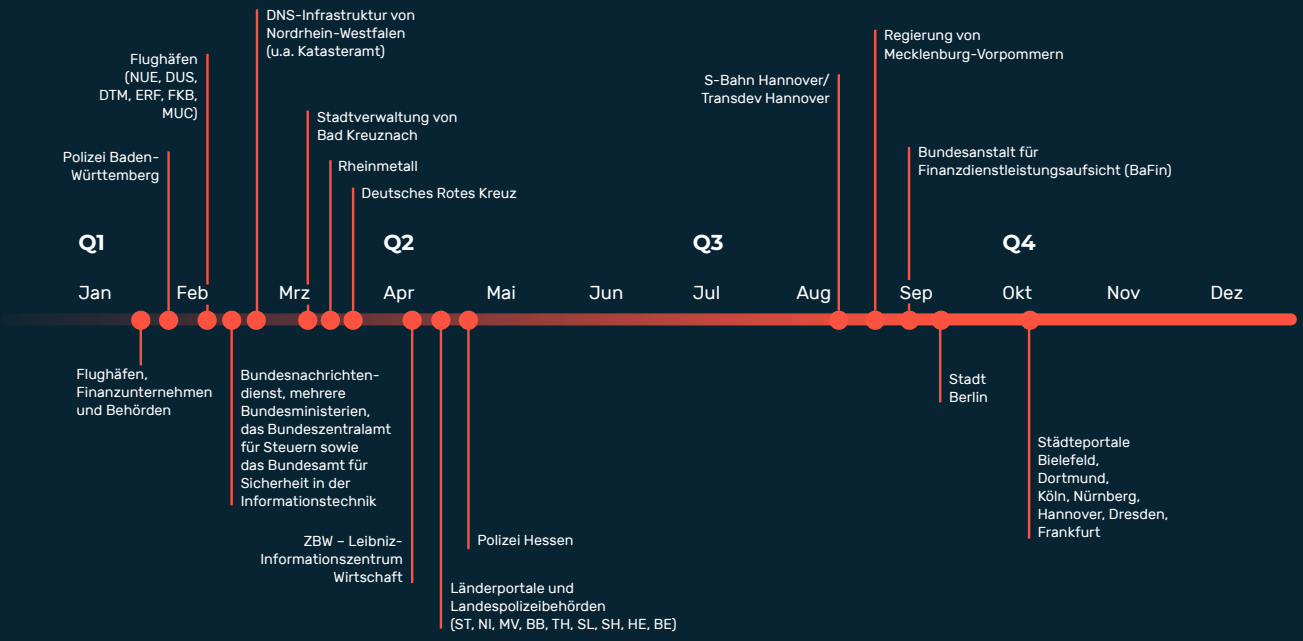
Heutzutage entfällt etwa die Hälfte aller Website-Zugriffe auf Bots, also autonom im Internet agierende Programme. 41 Prozent der Bot-Zugriffe gelten als potenziell gefährlich. Denn neben gutartigen Bots wie Suchmaschinen-Crawlern gibt es auch bösartige Bots. Cyberkriminelle setzen diese Bad Bots als autonome Angriffswerkzeuge ein, um beispielsweise Online-Anwendungen nach ausnutzbaren Schwachstellen zu scannen, Passwörter zu knacken und Nutzerkonten zu kompromittieren. Bei der dedizierten Betrachtung primär Bot-spezifischer Zugriffsversuche zeigen die Untersuchungen aus dem Myra SOC vor allem zum Jahresbeginn sowie zum Jahresende eine hohe Aktivität. Die Myra-Schutzsysteme verhinderten in diesen Zeiträumen besonders viele schädliche Bot-Anfragen.



Behörden im Visier von Cyberkriminellen

Der Trend zu Angriffen auf Ministerien und Behörden kann auch abseits der Mitigationsdaten aus dem Myra SOC beobachtet werden. Anhand von öffentlich kommunizierten Vorfällen aus der Presse und der Berichterstattung betroffener Organisationen lässt sich ein Lagebild der Angriffsaktivität im deutschen Raum zeichnen. Vor allem im Frühjahr und im Herbst 2023 sorgten demnach größere DDoS-Angriffswellen für Ausfälle. So standen im Januar neben Webseiten der öffentlichen Verwaltung auch die Internetportale von diversen Flughäfen, Verkehrsverbänden und Banken unter Beschuss der Cyberkriminellen. Wie das BSI in seinem Lagebericht 2023 zu dieser Thematik feststellt, dürfte das Ziel der Angreifer darin bestanden haben, „gesellschaftliche Verunsicherung zu schüren und das Vertrauen in die Fähigkeiten des Staates zum Schutz und zur Versorgung der Bevölkerung zu beschädigen."

DDoS-Zeitstrahl 2023

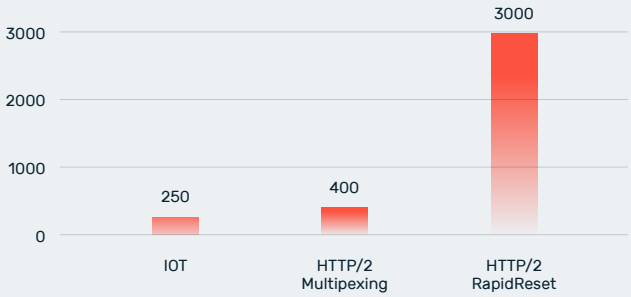


Im Oktober erfolgte eine weitere Serie orchestrierter Angriffe auf die Verwaltungsportale verschiedener Städte. Von den Attacken betroffen waren mitunter die Webseiten der Städte Bielefeld, Dortmund, Dresden, Frankfurt am Main, Hannover, Köln und Nürnberg. Manche der angegriffenen Verwaltungsportale konnten nach wenigen Stunden wieder online gehen, andere mussten aufgrund anhaltender Attacken mehrere Tage abgeschaltet bleiben.

DDoS-Insights von zeroBS: So schlagkräftig ist HTTP/2 RapidReset

Im Sommer 2023 trat mit HTTP/2 RapidReset ein neuer Angriffsvektor auf der Applikationsschicht in Erscheinung. Die Angriffsmethode macht sich eine Zero-Day-Sicherheitslücke (CVE-2023-44487) zunutze, um mit überschaubaren Ressourcen enorm schlagkräftige DDoS-Attacken mit immensen Paketraten auszuführen. Das National Institute of Standards and Technology (NIST) wertet die Kritikalität von CVE-2023-44487 als hoch.

RPS pro Bot

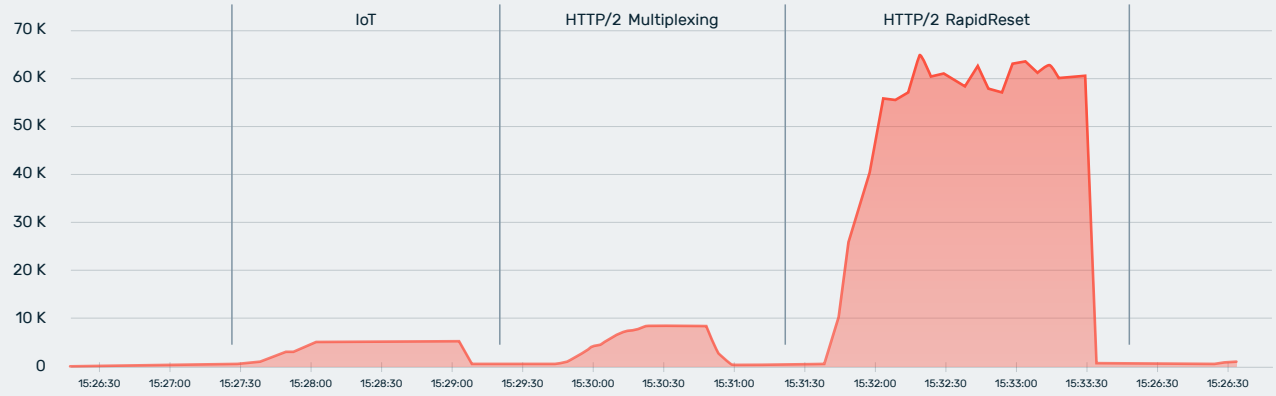


Wie bei standardmäßigen HTTP/2-Attacken auf Basis von Multiplexing werden auch bei einem HTTP/2-Rapid-Reset-Angriff zunächst eine Vielzahl von Anfragen an den anvisierten Webserver gesendet. Anstatt jedoch eine Antwort vom Server abzuwarten, werden diese Streams direkt abgebrochen. Die Verbindung bleibt dabei offen. Der betroffene Server startet zunächst mit der Verarbeitung, stoppt im Anschluss jedoch die weitere Ausführung, ohne die Anfrage zum üblichen Limit von 100 Streams pro Verbindung zu zählen. So sind unzählige Anfragen hintereinander möglich und der Server wird überlastet.

Die DDoS-Analysten von zeroBS haben das Angriffspotenzial der neuen RapidReset-Attacke gemessen und mit der Schlagkraft (RPS, Requests pro Sekunde) von IoT-Bots und herkömmlichen Multiplexing-Angriffen verglichen. Dabei nutzten die Analysten die zu Audit-Zwecken betriebene DDoS-Angriffsinfrastruktur Avydos sowie hauseigene zeroBS-Testserver.

Die geordneten Angriffsraten, Threads usw. wurden während des Tests beibehalten. Wie in den Diagrammen deutlich zu sehen ist, fällt die Angriffsrate von HTTP/2 RapidReset weitaus höher aus als reine Botnet-/IoT-Angriffe oder herkömmliches HTTP/2 Multiplexing. Während das verwendete Botnet den Testserver mit 250 RPS pro Bot belastete, konnten die DDoS-Fachleute durch den RapidReset-Angriff 3.000 RPS pro Bot aussenden. Das entspricht einer um den Faktor 12 gesteigerten Angriffsrate.

RPS



> *Die HTTP/2-RapidReset-Angriffe, die im Herbst des letzten Jahres erstmalig beobachtet wurden, stellen in zweierlei Hinsicht ein Novum in der Landschaft der DDoS-Angriffe dar. Einerseits, weil ein Threat Actor aus dem Botnetz-Umfeld Zeit und Energie in Forschung und Entwicklung eines komplett neuartigen Angriffs investiert hat; andererseits, weil damit die Stack-Angriffe endgültig als dritte Säule neben Volumen und Applikationsangriffen etabliert wurden.*
>
> Markus Manzke, CTO zeroBS

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.

Deshalb entscheiden sich CISOs für Myra

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 hochregulierte Sektoren

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

CANCOM | DSV IT Service | ITSG | flatex DEGIRO

Myra Security GmbH | **Tel. +49 89 414141 – 345** | **www.myrasecurity.com** | **info@myrasecurity.com**