MYRA

THREAT FACT SHEET DDOS

Alles, was Sie über DDoS-Attacken wissen müssen

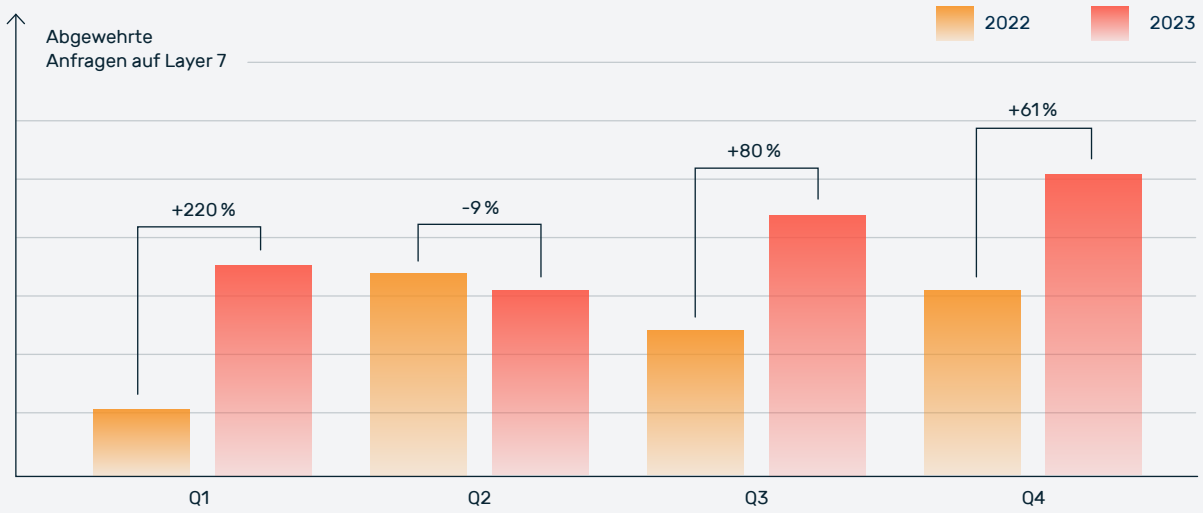
DDoS-Attacken (Distributed Denial of Service) zählen zu den größten digitalen Bedrohungen für Unternehmen und Organisationen. Laut einer aktuellen Umfrage von Lünendonk & KPMG halten es 7 von 10 IT-Führungskräfte für sehr wahrscheinlich, dass ihr Unternehmen in naher Zukunft einen schwerwiegenden DDoS-Angriff erleiden wird. Untersuchungen aus dem Security Operations Center (SOC) von Myra haben allein für das Jahr 2023 eine Zunahme von schädlichen Anfragen um rund 60 Prozent festgestellt.

Cyberkriminelle verfolgen mit DDoS-Attacken das Ziel, die Ressourcen eines Servers, Onlinedienstes oder Netzwerks zu überlasten, indem sie eine große Menge künstlichen Datenverkehr erzeugen. Diese Mehrbelastung kann dazu führen, dass die betroffenen Prozesse nur noch eingeschränkt oder überhaupt nicht mehr für legitime Benutzer zur Verfügung stehen. Solche Komplettausfälle ziehen erhebliche finanzielle und operationelle Konsequenzen nach sich – von direkten operativen Kosten über Reputationsschäden bis hin zu Bußgeldern.

DDoS-Attacken können in verschiedenen Formen auftreten, etwa als volumenbasierte Angriffe, als Angriffe auf der Anwendungseben oder als verdeckte Angriffe, die kaum von legitimem Traffic zu unterscheiden und damit nur schwer abzuwehren sind. Je nach Art und Angreifer sind seitens der betroffenen Organisationen unterschiedliche Präventions- und Abwehrmaßnahmen erforderlich.

In diesem Threat Fact Sheet erfahren Sie, wie DDoS-Attacken funktionieren, welche Gefahren von ihnen ausgehen und wie Sie Ihre Organisation effektiv vor Schäden schützen können.

Schädlicher DDoS-Traffic auf der Überholspur



Im SOC von Myra konnte im vergangenen Jahr eine Zunahme von Angriffen um 59 Prozent festgestellt werden. Der stärkste Zuwachs erfolgte im ersten Quartal 2023, als sich die Angriffsaktivität gegenüber dem Vergleichszeitraum des Vorjahres mehr als verdreifachte.

Inhalt

Funktionsweise von DDoS-Attacken

Grundsätzlich unterscheiden IT-Sicherheitsfachleute DDoS-Attacken anhand der OSI-Netzwerkschicht (Open Systems Interconnection), auf der die jeweilige Attacke ausgeführt wird. DDoS-Attacken belasten die Ziele entweder auf der Vermittlungs- und Transportschicht (Layer 3/4) oder auf der Anwendungsschicht (Layer 7).

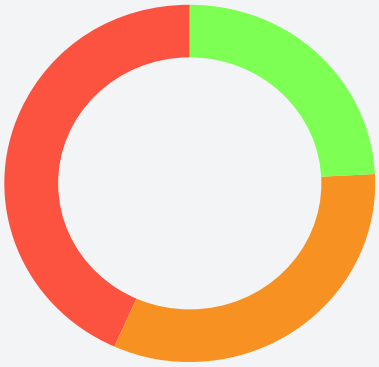
Layer-7-Attacken

Durch die fortdauernde Migration von lokalen Diensten in die Cloud verändert sich die digitale Bedrohungslandschaft grundlegend. Cyberkriminelle fokussieren ihre Attacken zunehmend auf die äußerste Netzwerkschicht (Layer 7) und nehmen die dort befindlichen Webanwendungen, Internetseiten und Online-Schnittstellen (APIs) ins Visier. In der Praxis lässt sich beobachten, dass Unternehmen bei der Mitigation von Layer-7-Angriffen die meisten Schwierigkeiten haben. Aus diesem Grund attackieren versierte Akteure bevorzugt diese Netzwerkschicht.

DDoS-Attacken auf Webanwendungen basieren in der Regel auf bereits aufgebauten Verbindungen von Diensten wie HTTP, HTTPS, FTP oder SMTP und sind daher nur schwer von legitimem Traffic zu unterscheiden. Zu den typischen DDoS-Angriffen auf Layer 7 zählen etwa HTTP Floods, die sich wiederum in HTTP GET Floods und HTTP POST Floods unterteilen. Bei Attacken mittels HTTP GET Flood überhäufen Angreifer einen Webserver mit HTTP-Anfragen, die gezielt Webseiten mit großem Ladevolumen aufrufen. Dadurch wird der Webserver letztlich überlastet und kann keine legitimen Anfragen mehr verarbeiten.

Bei einer HTTP-POST-Flood-Attacke werden hingegen wiederholt Daten an den Webserver gesendet, die dieser verarbeiten muss. Mit jeder Anfrage wird der Ressourcenaufwand auf Serverseite bis zur maximalen Auslastung erhöht. In der Praxis nutzen Cyberkriminelle meist Botnetze für ihre Flood-Attacken, um das Volumen der Anfragen und damit den Ressourcenaufwand auf der Serverseite zu steigern.

3 von 4 Firmen scheitern bei der Abwehr von Layer-7-Attacken



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

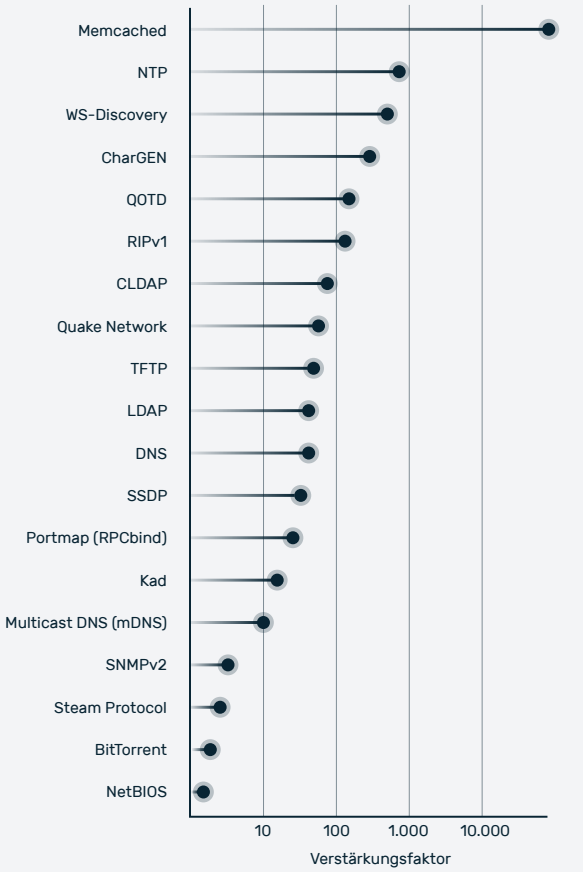
Quelle: zeroBS, 2023

Weitere gängige Attacken auf der Applikationsebene sind Low-and-Slow-Angriffe, Slowloris-Attacken, SSL Negotiation/Garbage Flood, R.U.D.Y. („R U Dead Yet?"), HTTP/S Bombing, Outbound Pipe Saturation und HALO-Angriffe. Prinzipiell bedienen sich alle Varianten unterschiedlicher Formen der oben beschriebenen HTTP-Flood-Angriffe – allerdings werden dabei verschiedene Angriffswerkzeuge eingesetzt und andere Strategien verfolgt, die darauf abzielen, die Zielserver zu überlasten.

Threat Spotlight
DRDoS: Angriffe über Bande

Aus technischer Sicht handelt es sich bei einer DRDoS-Attacke um eine Sonderform von DDoS. Hier stammen die schädlichen Anfragen nicht direkt vom Angreifer selbst oder einem dafür aufgesetzten Botnet, sondern von regulären Internetdiensten. Diese funktionieren Cyberkriminelle zur Waffe um, indem sie diverse Internetprotokolle missbrauchen. So können Angreifer beispielsweise per IP-Spoofing (dem Versenden von IP-Paketen mit verfälschter IP-Absenderadresse) Internetdienste manipulieren, um den Traffic auf ein bestimmtes Ziel umzuleiten. Durch dieses Vorgehen verschleiern die Angreifer den eigentlichen Ursprung der DDoS-Attacke und sorgen gleichzeitig für eine massive Steigerung der abgefeuerten Bandbreite.

DRDoS-Attacken erfolgen in der Regel über hoch verstärkende Reflektoren wie DNS-Dienste, welche die kurzen Anfragen der Angreifer mit großen Datenpaketen beantworten. Auf diese Weise steigern solche Reflection-Attacken die Schlagkraft der Angriffe um ein Vielfaches. Weitere gängige Typen von Reflektoren sind etwa die Protokolle NTP, TFTP oder Memcached – über Letzteres lässt sich die Bandbreite von Attacken maximal um das 51.000-fache verstärken.



Quelle: https://us-cert.cisa.gov/ncas/alerts/TA14-017A

Layer-3/4-Attacken

Zu den häufigsten DDoS-Attacken auf der Vermittlungs- und Transportschicht (Layer 3/4) zählen TCP SYN Floods und DRDoS-Angriffe auf UDP-Basis. Weitere typische Angriffsvarianten sind ICMP-Flood, UDP-Fragmentation, UDP-Amplification via DNS, NTP, rpcbind, SSDP, ACK-Flood und RST-Flood. Alle diese Angriffe belasten das Ziel entweder mit sehr hohen Bandbreiten oder immensen Paketraten. Legitime Zugriffe finden so keinen Datenkanal mehr, um eine Kommunikation zu etablieren.

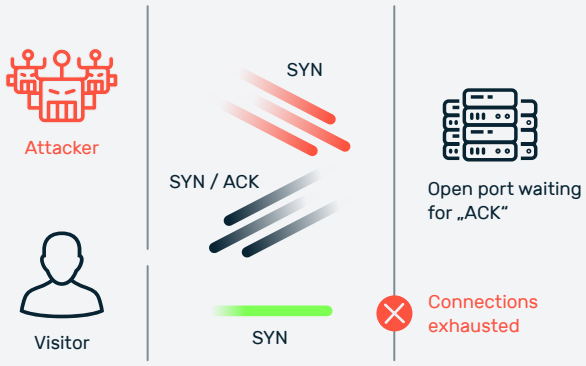
Diese DDoS-Angriffsarten gefährden Ihre Infrastruktur

Das Spektrum möglicher Angriffsarten ist auf Layer 3/4 sehr groß und erfordert entsprechend effektive Schutztechnologien und performante Schutzinfrastruktur:

- ACK Attack or ACK-PUSH Flood
- DNS Amplified (Reflective)
- DNS Flood
- Fake Session Attack
- Fraggle Attack
- Fragmented ACK Flood
- ICMP Flood
- ICMP Fragmentation Flood
- IP NULL
- Memcached Attack
- Non-Spoofed UDP Flood
- NTP Amplified (Reflective)
- NTP Flood
- Other Amplified Attacks (Reflective)
- Ping Flood
- RST/FIN Flood
- Same Source/Dest Flood (LAND Attack)
- Slow Read Attack
- Slow Session Attack
- Smurf Attack
- SSDP Amplified (Reflective)
- SYN Flood
- SYN-ACK Flood
- TCP Null
- TOS Flood
- UDP Flood
- UDP Fragmentation

Threat Spotlight
SYN/ACK

Bei einer SYN/ACK-Attacke (oder SYN- und ACK-Floods) bombardiert ein von Angreifern ferngesteuertes Botnetz einen Server mit SYN-Paketen. Diese sind normalerweise Teil des sogenannten Three-Way-Handshake (Drei-Wege-Handschlag), der beim Aufbau einer TCP-Verbindung zwischen Client und Server erfolgt. Eine SYN/ACK-Attacke provoziert massenhaft halboffene Verbindungen, indem sie viele SYN-, aber keine zum vollständigen Verbindungsaufbau benötigten ACK-Pakete sendet. Die Folge: Es können keine neuen Verbindungen mehr hergestellt werden, und die Website ist nicht mehr erreichbar.



DDoS-Attacken: Ausfälle und Auswirkungen

Je nach Angriffsart, Stärke und betroffenen Diensten unterscheiden sich die durch DDoS-Attacken provozierten Ausfälle massiv voneinander. Während einige Attacken nur einen geringen Impact auf die anvisierten Server hervorrufen und diese für kurze Zeit belasten, können orchestrierte Angriffskampagnen auch mehrtägige Ausfälle provozieren.

Dies zeigte sich etwa Anfang 2023 als staatlich unterstützte Cybergruppierungen Angriffe auf die Webpräsenzen deutscher Städte, Verwaltungsbehörden und der Polizei starteten – manche der angegriffenen Dienste konnten nach wenigen Stunden wieder online gehen, andere blieben aufgrund anhaltender Attacken mehrere Tage abgeschaltet.

Schäden für Unternehmen

Für die betroffenen Unternehmen und Organisationen haben DDoS-Attacken meist schwerwiegende Auswirkungen. Laut einer Analyse der Allianz verursachen externe Ereignisse wie DDoS-Attacken 85 Prozent der globalen Cyberversicherungsschäden. Insbesondere Firmen, deren operatives Geschäft direkt mit den ausgefallenen Webprozessen verknüpft ist, müssen mit hohen Ausfallkosten im Angriffsfall rechnen. Hierzu zählen etwa Direktbanken, Direktversicherer, Online-Broker, Cloud-Service-Dienstleister, E-Commerce-Unternehmen oder Online-Apotheken.

Neben operativen Schäden verursachen DDoS-Angriffe auch weiterführende Kosten wie Reputationsschäden und Imageverluste, erhöhte Betriebskosten aufgrund von teurem Traffic oder – im Fall unzureichender Absicherung – Bußgelder aufgrund regulatorischer Verfehlungen.

Massive Schäden verzeichnen auch Einrichtungen des öffentlichen Sektors bei Ausfällen ihrer Verwaltungsportale. Digitale Bürgerleistungen müssen in diesem Fall manuell abgearbeitet werden, was zu erheblichen Verzögerungen führt – lange Schlangen vor den Behörden und verärgerte Bürgerinnen und Bürger sind die Folge.

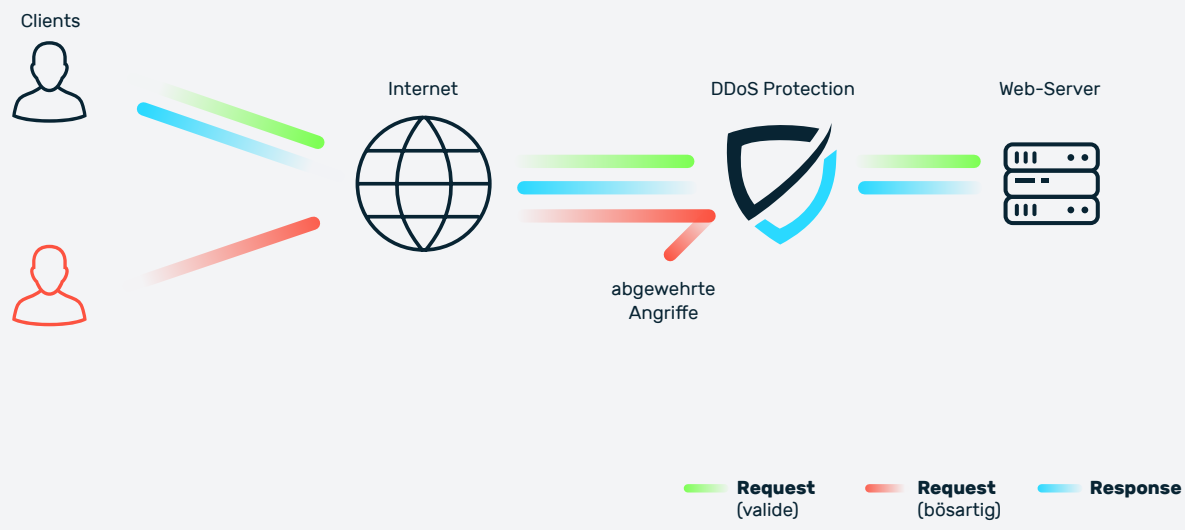
Prävention und Abwehr von DDoS-Attacken

Grundsätzlich lassen sich DDoS-Attacken zwar auch im akuten Angriffsfall durch die Hilfe spezialisierter Schutzdienstleister abwehren. Allerdings ist bei solchen Notfallaufschaltungen zu beachten, dass bereits Schaden durch überlastete Server und ausgefallene Dienste entstanden ist. Zu diesem Zeitpunkt kann nur noch Schadensminimierung betrieben werden. Verlässlicher Schutz vor DDoS-Angriffen ist daher ausschließlich über eine präventive Absicherung auf allen relevanten Netzwerkschichten (Layer 3/4 und 7) möglich.

Dedizierter Applikationsschutz gegen DDoS

Oftmals erliegen Organisationen dem Fehlglauben, dass eine DDoS-Absicherung durch den eingesetzten Hoster oder Rechenzentrumsbetreiber bereits ausreicht, um vor DDoS-Attacken sicher zu sein. Das ist aber nicht der Fall, wenn die Angreifer direkt auf der Anwendungsebene agieren. Für Schutzsysteme auf Layer 3/4 sind Attacken auf Layer 7 nicht von herkömmlichen Traffic zu unterscheiden. Hier sind weiterführende Filtermethoden erforderlich, um schädliche Anfragen als solche zu identifizieren. Per Fingerprinting, Blocklisting, Request Limiting und zusätzlichen Filter- und Bearbeitungsmethoden lässt sich bösartiger Traffic zielgenau erkennen und abwehren. Dedizierte Lösungen für Applikationsschutz umfassen solche granularen Filtermethoden.

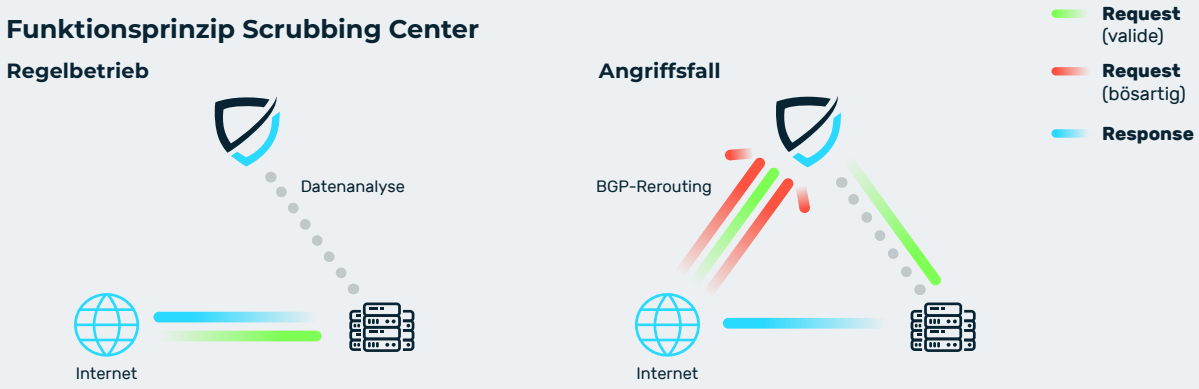
Funktionsprinzip von Cloud-basierten DDoS-Schutz (Layer 7)



Scrubbing Center

Für DDoS-Angriffe auf der Vermittlungs- und Transportschicht (Layer 3/4) haben sich Scrubbing Center zur Bereinigung des Traffics als probates Mittel erwiesen. Als Scrubbing Center werden zentralisierte Datenreinigungsstationen bezeichnet, in denen der Datenverkehr analysiert und bösartiger Traffic, wie er bei DDoS-Angriffen entsteht, herausgefiltert wird. In der Regel betreiben große Organisationen wie Internet Service Provider (ISPs), Cloud Provider oder spezialisierte Schutzdienstleister eigene Scrubbing Center – meist direkt an großen Internetknoten, um auch großvolumige Angriffe verarbeiten zu können. Für herkömmliche Unternehmen ist der Einsatz eigener Scrubbing Center nur bedingt sinnvoll, da die Anbindung des Firmen-Rechenzentrums an das Internet der limitierende Faktor ist. Sobald das Angriffsvolumen die Anbindungskapazitäten überschreitet, ist keine Abwehr mehr möglich.

Funktionsprinzip Scrubbing Center

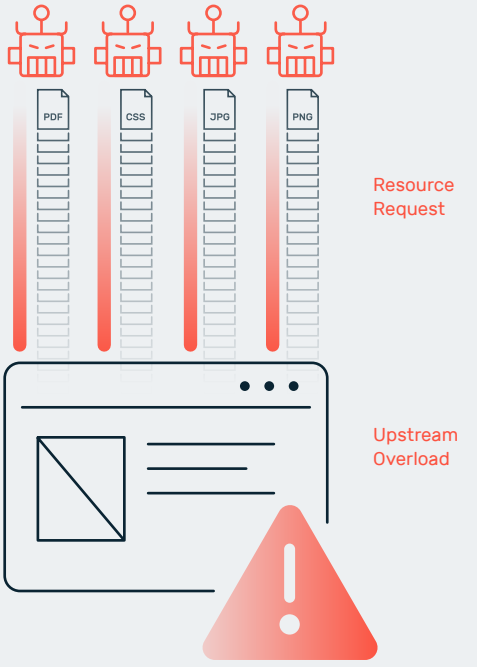


Im Regelbetrieb verläuft der Traffic standardmäßig zwischen der Kunden-Infrastruktur und dem Internet. Kommt es im Angriffsfall zur Überschreitung der definierten Schwellenwerte, wird der komplette eingehende Traffic mittels BGP-Rerouting auf die Scrubbing Center des Schutzdienstleisters gelenkt. Dort wird der Angriffs-Traffic verworfen und der verbleibende saubere Traffic über eine vorher vereinbarte Verbindung dem Kunden wieder zugeleitet.

Threat Spotlight

HALO Attack: der Upstream-Blocker

Beim HALO-Angriff handelt es sich um eine Reverse HTTP Amplification, die 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. Bedrohungssimulationen der DDoS-Analysten von zeroBS haben dabei gezeigt, dass beim Einsatz eines Botnetzes mit 5.000 Bots und 1 RPS (Requests Per Second) mit Dateien von durchschnittlich 1 MByte Größe ein Upstream-Traffic von 70 GBit/s generiert werden kann. Dank der relativ niedrigen RPS-Rate können Angreifer mit der HALO-Attacke gängige WAF- und Bot-Management-Lösungen umgehen, während die schädliche Bandbreite den Upstream vollständig auslastet und den Datenkanal blockiert.



Bereitstellung per Schutzsoftware, -Hardware oder Cloud

Ein DDoS-Schutz kann entweder inhouse als selbst verwaltete Software oder Hardware-Appliance betrieben oder von einem Service-Betreiber zugeliefert werden. Der Betrieb in Eigenregie bietet zwar ein Maximum an Kontrolle, erfordert aber im Gegenzug großen Aufwand für Implementierung, Betrieb und Wartung. Die Leistungsfähigkeit einer DDoS Protection hängt maßgeblich von der korrekten Konfiguration ab, die es laufend an aktuelle Bedrohungen anzupassen und zu aktualisieren gilt. Eine fehlerhaft konfigurierte Lösung bietet Angreifern Schlupflöcher für Attacken und kann die Funktionalität und Performance der Webapplikationen einschränken.

Entsprechend muss für den Inhouse-Betrieb das erforderliche Fachpersonal entweder verfügbar sein oder eingestellt werden, was aufgrund des angespannten Arbeitsmarktes mit hohen Kosten verbunden ist und die Inbetriebnahme erheblich verzögern kann. Laut Bitkom sind in Deutschland 149.000 Stellen für IT-Fachleute quer durch alle Branchen unbesetzt (Stand Dez. 2023). Im Schnitt dauert es fast acht Monate, bis geeignete Fachkräfte für offene Stellen gefunden sind. Wird der DDoS-Schutz hingegen von einem Dienstleister bereitgestellt, entfallen solche Verzögerungen sowie zusätzliche Aufwendungen für Personal, Software oder Hardware. Hier fallen nur die vereinbarte Service-Pauschale sowie etwaige Kosten für das initiale Aufsetzen individueller Regelsätze an.

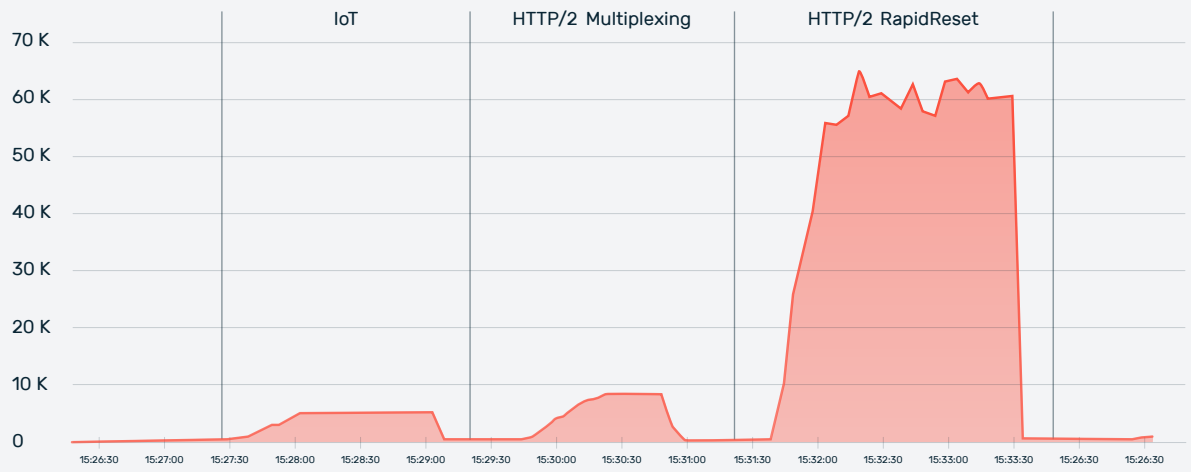
Threat Spotlight

HTTP/2 RapidReset: Fataler Zero-Day-Angriff

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.

Bei HTTP/2 RapidReset senden Angreifer über ein Botnet eine Vielzahl von Anfragen an den anvisierten Webserver. Anstatt jedoch eine Antwort vom Server abzuwarten, werden diese Streams direkt wieder abgebrochen. Die Verbindung bleibt dabei offen. Der betroffene Webserver startet zunächst mit der Verarbeitung, bricht im Anschluss allerdings die weitere Ausführung ab, ohne die Anfrage zum üblichen Limit von 100 Streams pro Verbindung zu zählen. So sind unzählige Anfragen hintereinander möglich und der Server wird überlastet.

RapidReset ermöglicht massive Paketraten



Rechtliche Aspekte und Compliance

Je nach Unternehmensgröße und Branche gelten für Organisationen unterschiedliche nationale sowie internationale Compliance-Anforderungen an Informationssicherheit und Datenschutz. Der folgende Abschnitt soll eine kompakte Übersicht über die regulatorische Landschaft im Bereich der Informationssicherheit liefern und dabei die wichtigsten Regelwerke vorstellen.

Beispielsweise fordert die NIS-2-Richtlinie von Unternehmen ab einer Größe von 50 Mitarbeitern die Umsetzung technisch-organisatorischer Maßnahmen (TOMs) zur Absicherung von IT und Prozessen, um dadurch Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit sicherzustellen – dies schließt eine Absicherung gegen DDoS-Angriffe in vielen Fällen mit ein.

Verstoßen Organisationen gegen die Vorgaben aus NIS-2 drohen empfindliche Bußgelder. Das deutsche Umsetzungsgesetz der Richtlinie sieht laut Referentenentwurf Strafen bis zu 20 Mio. Euro vor. Darüber hinaus umfasst die Richtlinie eine persönliche Haftung für das verantwortliche Management. Die ordnungsgemäße Umsetzung der Vorgaben soll durch die verantwortlichen Aufsichtsbehörden laufend kontrolliert werden.

Aktuelle EU-Verordnungen und Richtlinien

Datenschutz-Grundverordnung (DSGVO)	BSI-Gesetz (BSIG)
Cyber Resilience Act (CRA)	KRITIS-Verordnung (KRITISV)
KI-Haftungsrichtilinie	IT-Sicherheitsgesetz 2.0 (IT-SIG 2.0)
Artificial Intelligence Act (AI Act)	NIS-2 Richtlinie (NIS2UmsuCG)

Überblick der zentralen regulatorischen Regelwerke für den Bereich der Informationssicherheit (Auswahl)

Neben NIS-2 verlangen auch andere regulatorische Vorgaben wie etwa die DORA-Richtlinie (Geltung im Finanz- und Versicherungsumfeld) eine Absicherung digitaler Systeme nach dem Stand der Technik – und das auch von angeschlossenen IKT-Dienstleistern. Zudem müssen Organisationen die Datenschutz-Grundverordnung (DSGVO) beachten, was insbesondere die Zusammenarbeit mit Dienstleistern außerhalb des Europäischen Wirtschaftsraums (EWR) erschwert. Einfacher und langfristiger lässt sich hier die Rechtssicherheit über lokale Service-Anbieter realisieren.

Round-up: Risiken erkennen, Maßnahmen ableiten, Cyberresilienz ausbauen

DDoS-Attacken stellen eine akute Bedrohung für Organisationen aus Wirtschaft, Industrie, öffentlicher Verwaltung und Wissenschaft dar. In den vergangenen Jahren hat sich die Bedrohungslage kontinuierlich verschärft – allein für das Jahr 2023 belegen die Mitigationsdaten aus dem Myra SOC einen Anstieg schädlicher Anfragen auf Webseiten, Internetportalen und Online-APIs um 59 Prozent. Gleichzeitig sorgen komplexere Angriffsmethoden und die zunehmende Professionalisierung der Cyberkriminellen für einen erheblichen Mehraufwand bei der Abwehr. So werden etwa gezielt Sicherheitslücken in Protokollen und Software missbraucht, um die Schlagkraft von DDoS-Attacken zu maximieren. Mittels „Cybercrime as a Service" lassen sich DDoS-Angriffe im Darknet schon für geringe Summen buchen. Diese Angriffe sind meist nicht mit den Attacken einschlägiger Gruppierungen wie Fancy Bear, Lazarus Group oder NoName057 vergleichbar, Webserver ohne dedizierte Schutzsysteme bringen Sie aber dennoch an die Belastungsgrenzen.

Diese Entwicklung wurde auch von den verantwortlichen Aufsichtsbehörden und dem Gesetzgeber wahrgenommen. Straffere regulatorische Vorgaben und Gesetze, die den Aufbau einer effizienten und holistischen Informationssicherheit in allen Organisationen fordern, sind die Antwort darauf. Eine effektive Absicherung kritischer Geschäftsprozesse im Internet vor Überlastungsangriffen ist daher für viele Firmen allein schon aus Compliance-Sicht erforderlich. Unternehmen, die den Vorgaben nicht nachkommen, riskieren hohe Bußgelder – inklusive Managerhaftung.

Durch die fortlaufende Digitalisierung und anhaltende Cloud-Migration wächst die virtuelle Angriffsfläche zusehends. In Deutschland nutzen laut Angaben des Bitkom 9 von 10 Unternehmen Cloud Computing. All diese Unternehmen müssen sich um die Absicherung ihrer Systeme und Prozesse in der Cloud kümmern. So verwundert es kaum, dass IT-Verantwortliche die größten Hürden bei der Umsetzung von Cloud-Projekten in den Bereichen Sicherheit und Fachkräftemangel sehen.

In dieser dynamischen Gemengelage aus verschärfter Cyberbedrohung, straffer Regulatorik und wachsender Angriffsfläche sind Unternehmen auf effiziente, skalierbare und flexible Strategien zur Absicherung ihrer IT angewiesen. Eine solche Absicherung lässt sich am einfachsten über Security-as-a-Service-Lösungen realisieren. Durch die Zusammenarbeit mit spezialisierten Schutzdienstleistern profitieren Unternehmen von einem beschleunigten Deployment neuer Sicherheitslösungen, ohne dabei auf zusätzliche Hardware, Software oder Fachkräfte angewiesen zu sein. Wer bei der Auswahl des passenden Dienstleisters auf einen hochzertifizierten Anbieter mit Branchenerfahrung setzt, bewältigt dadurch auch regulatorische Hindernisse.

Schnell, zuverlässig, skalierbar: DDoS-Schutz von Myra Security

Der deutsche Technologiehersteller Myra Security bietet ein vollautomatisches DDoS-Schutzsystem für Webseiten, Online-Anwendungen, APIs und Webinfrastrukturen. Die Lösung erkennt Angriffe in Echtzeit, blockiert bösartige Zugriffe, bevor diese Ihre Server erreichen und sorgt für einen reibungslosen Ablauf Ihrer Geschäftsprozesse im Web.

Als Security-as-a-Service-Plattform ist Myra in kurzer Zeit integriert und konfiguriert. Zusätzliche Software oder Hardware sind für den Betrieb nicht erforderlich. Myra ist langjähriger Service-Partner des Bundesministeriums für Gesundheit und versorgt mit seinen BSI-zertifizierten Schutz- und Performancediensten Bundes-, Landes- und Kommunalbehörden, namhafte Banken und Versicherungen sowie Betreiber kritischer Infrastrukturen (KRITIS).

ISO 27001 BSI zertifiziert auf der Basis von IT-Grundschutz Zertifikat Nr.: BSI-IGZ-0479-2021 | PCI DSS Certified | BSIG KRITIS-qualifiziert | 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 (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

Akuter DDoS-Notfall? Das müssen Sie wissen

Steht Ihr Unternehmen unter einem DDoS-Angriff, zählt jede Minute. Umgehendes und entschiedenes Handeln ist hier essenziell. Im akuten Angriffsfall hilft Myra Security schnell, unkompliziert und diskret per Notfallaufschaltung, um weiteren Schaden abzuwenden und die Verfügbarkeit Ihrer Webressourcen sicherzustellen. Sie müssen lediglich Kontakt mit uns aufnehmen und einige grundlegende Informationen bereitstellen – wir kümmern uns um den Rest.

Verhalten im DDoS-Notfall

1. Myra-Notfallteam kontaktieren 	**24 / 7-Notfallnummer:** +49 89 414141-333 **Notfallformular:** myrasecurity.com/notfallkontakt **VIP-Telefonnummer für Bestandskunden** (optional)
2. Informationen für Notfall-Setup übermitteln 	• Kontaktdaten (Name, E-Mail, Telefonnummer, Mobilfunknummer) • Name des Unternehmens / der Organisation • Betroffene Domain, Autonomous System Number (ASN) und IPv4- oder IPv6-Netze • Traffic pro Monat / durchschnittliche Bandbreite • Peak-Bandbreite • Detailinformationen zum Angriff oder zum Erpresserschreiben • Beschreibung der Auswirkungen, falls die Attacke bereits erfolgt ist
3. Für Rückfragen bereithalten	Unser Expertenteam wird in enger Abstimmung mit Ihrer Technikabteilung die Notfallaufschaltung binnen weniger Stunden abschließen.

Made in Germany

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

Sie wollen mehr darüber erfahren, wie Sie mit unseren Lösungen Ihren Umsatz steigern, Ihre Kosten minimieren und Ihre Anwendungen vor bösartigen Angriffen schützen? Unser Expertenteam berät Sie gerne individuell und erarbeitet eine maßgeschneiderte Lösung für Ihr Unternehmen. Vereinbaren Sie am besten noch heute ein unverbindliches Beratungsgespräch.

Kostenlose Schutzberatung anfordern →

Myra Security GmbH

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