MYRA

THREAT FACT SHEET BOT-ATTACKEN

Alles, was Sie über automatisierte Bedrohungen wissen müssen

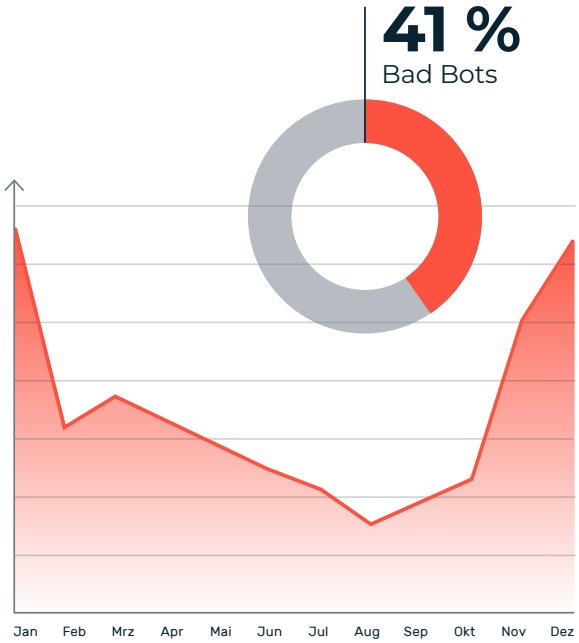
Heutzutage entfällt etwa die Hälfte aller Website-Zugriffe auf Bots, also autonom im Internet agierende Programme. 41 Prozent der Bot-Zugriffe gelten als potenziell gefährlich. Denn neben gutartigen Bots wie Suchmaschinen-Crawlern gibt es auch bösartige Bots. Cyberkriminelle setzen diese Bad Bots als autonome Angriffswerkzeuge ein, um beispielsweise Online-Anwendungen nach ausnutzbaren Schwachstellen zu scannen, unerlaubt Inhalte zu kopieren, Passwörter zu knacken und Nutzerkonten zu kompromittieren. Diese unerwünschten Seitenzugriffe können erhebliche Auswirkungen auf die Leistung, Sicherheit und Integrität von Webplattformen haben. Darunter leidet wiederum das Nutzererlebnis und letztlich Ihr Business. Bei der Betrachtung primär Bot-spezifischer Zugriffsversuche zeigen Untersuchungen aus dem Myra Security Operations Center (SOC) vor allem zum Jahresbeginn sowie zum Jahresende 2023 eine hohe Aktivität.

In diesem Threat Fact Sheet erfahren Sie alles Wissenswerte über Bot-basierte Attacken, deren Auswirkungen und wirksame Gegenmaßnahmen zum Schutz Ihrer Organisation vor automatisierten Angriffen.

Was ist eigentlich ein Bot?

Ein Bot (kurz für „Robot“) ist ein Computer-progamm, das automatisiert und autonom – also ohne menschliches Zutun – vordefinierte, meist repetitive Aufgaben ausführt. Bots kommen unter anderem zum Einsatz, um das Internet für Suchmaschinen zu indexieren, um bestimmte Informationen auf Social Media bereitzustellen oder um via E-Mail bzw. Chat Kundenanfragen zu beantworten. Außer solchen gutartigen Bots gibt es auch schädliche Bots, die Cyberkriminelle für automatisierte Angriffe wie Überlastungsattacken, Phishing und Kontenübernahme nutzen. Oft sind Bad Bots Teil eines Botnetzes, das aus zusammengeschlossenen internetfähigen Geräten wie IP-Kameras, Netzwerkdruckern und Smart-TVs besteht und über zentrale Command-and-Control Server (C&C bzw. C2-Server) gesteuert wird.

Bot-Aktivität 2023



Inhalt

Motivation der Angreifer

Die Motivation hinter Bot-basierten Attacken kann vielfältig sein und hängt von den jeweiligen Bedrohungsakteuren ab. Cyberkriminelle aus dem Kreis der Organisierten Kriminalität verfolgen in der Regel finanzielle Interessen und sind auf schnelles Geld aus. Sie setzen Bots unter anderem dazu ein, betrügerische Klicks auf Anzeigen zu generieren, zuvor gestohlene Kreditkartendaten auf ihre Validität zu testen oder Zugriff auf Nutzerkonten zu erhalten, um wertvolle Daten zu stehlen und anschließend weiterzuverkaufen. Ebenso nutzen Cybercrime-Gruppen Botnetze für Überlastungsangriffe, um Webseiten lahmzulegen und die jeweiligen betroffenen Organisationen zu erpressen.

Insbesondere im E-Commerce-Umfeld verwenden Angreifer Bots, um sich einen Wettbewerbsvorteil zu verschaffen. Unseriöse Mitbewerber kopieren automatisiert ganze Webseiten, Produktinformationen, Preisstrukturen oder andere geschäftsrelevante Daten. Außerdem manipulieren die Angreifer Web-Analysedaten durch gezielte Bot-Anfragen, um unliebsamen Konkurrenten zu schaden.

Eine weitere Gruppe von Bedrohungsakteuren sind politisch oder ideologisch motivierte Angreifer. Diese – häufig staatlich unterstützte – Gruppe verwendet Bots etwa für Desinformationskampagnen oder für Distributed-Denial-of-Service-Attacken (DDoS). Ziel der Angriffe sind meist Websites von Regierungen oder Behörden.

Darüber hinaus gibt es staatliche Akteure wie Geheimdienste, die mittels Bots automatisiert Systemschwachstellen aufspüren, um vertrauliche Informationen zu sammeln oder geistiges Eigentum zu stehlen. Diese Art der Spionage kann sich sowohl gegen staatliche Einrichtungen als auch gegen Unternehmen richten. Eine weitere Bedrohung in diesem Umfeld ist die Sabotage kritischer Infrastrukturen durch Bot-basierte DDoS-Angriffe, die letztlich auf eine Destabilisierung der gesellschaftlichen Ordnung abzielt.

Ein Blick auf die Motivation der Angreifer kann Organisationen helfen, ihr individuelles Risiko besser einzuschätzen und ihre Sicherheitsmaßnahmen an die jeweiligen Bedrohungen anzupassen.

Arten von Bot-basierten Angriffen

Cyberkriminelle setzen Bots und ganze Botnetze für diverse Angriffsaktivitäten ein. Sie zielen unter anderem darauf ab, Webseiten lahmzulegen, Daten zu manipulieren bzw. zu stehlen oder Geschäftsgeheimnisse auszuspionieren. Dadurch schaden Bots den Geschäftsprozessen, den Kunden und der Wettbewerbsfähigkeit des betroffenen Unternehmens. Organisationen mit geschäftskritischen Onlineprozessen sollten sich daher vor folgenden automatisierten Bedrohungen schützen:

Web Scraping / Content Scraping

Mithilfe von Bots können Kriminelle in Sekundenschnelle einzelne Seiteninhalte oder ganze Webseiten kopieren. Solche Kopien werden häufig dazu genutzt, Phishing-Seiten zu erstellen und darüber Anmeldedaten abzugreifen.

Price Grabbing

Bots erlauben es unseriösen Wettbewerbern, Preisinformationen eines konkurrierenden Online-Händlers automatisiert auszulesen, um diesen gezielt zu unterbieten.

Credential Stuffing

Bots können in kürzester Zeit unzählige Nutzernamen/Passwort-Kombinationen systematisch testen, um unautorisierten Zugriff auf ein Konto zu erhalten. Treffer zu aktiven Accounts verkaufen die Bot-Betreiber anschließend oder nutzen sie für Datendiebstahl und weiterführende Angriffe.

(Formular) Spam / Phishing

Über Kontaktformulare bombardieren Bots Organisationen mit unerwünschten Botschaften wie Werbung. Per Online-Formular übermittelte Nachrichten können auch Links zu Phishing-Seiten enthalten oder sogar mit Schadsoftware verseuchte Anhänge. Kriminellen dient diese Phishing-Methode als Ausgangspunkt für weiterführende Angriffe.

Klickbetrug / Ad Fraud

Angreifer setzen Bots dazu ein, auf Websites enthaltene Werbeanzeigen oder Affiliate-Links automatisiert anzuklicken, um auf Kosten der Werbetreibenden Einnahmen zu generieren.

Warenkorb-Manipulation

Beim Cart Abandonment oder Inventory Hoarding füllen Bots automatisch Warenkörbe, ohne den Kaufprozess abzuschließen. Reguläre Kunden und Kundinnen können die Artikel somit vorübergehend nicht mehr kaufen, was geschäftsschädigende Folgen hat.

Scalping

Per Hype Sale Bots sichern sich Betrüger begehrte Waren und verkaufen sie anschließend mit hohem Gewinn weiter. Das sorgt für frustrierte Kundschaft und Imageschäden.

Account Creation & Takeover

Bots können massenhaft gefälschte Nutzerkonten erstellen oder bestehende Accounts übernehmen. Kriminelle nutzen diese anschließend für weitere Angriffe oder Betrugsversuche.

Skewing

Angreifer manipulieren mittels automatisierten Anfragen gezielt Web-Analysedaten, um Unternehmen zu falschen strategischen Entscheidungen zu verleiten und dadurch zu schaden.

Kreditkartentests

Carding-Bots testen in kurzer Zeit und im großen Stil gestohlene Kreditkartendaten auf ihre Validität, etwa durch Online-Käufe oder Reservierungen von Mietwagen und Hotels. So finden Kriminelle schnell heraus, welche Kartendaten funktionieren und sich für die eigene Verwendung oder zum Weiterverkauf eignen.

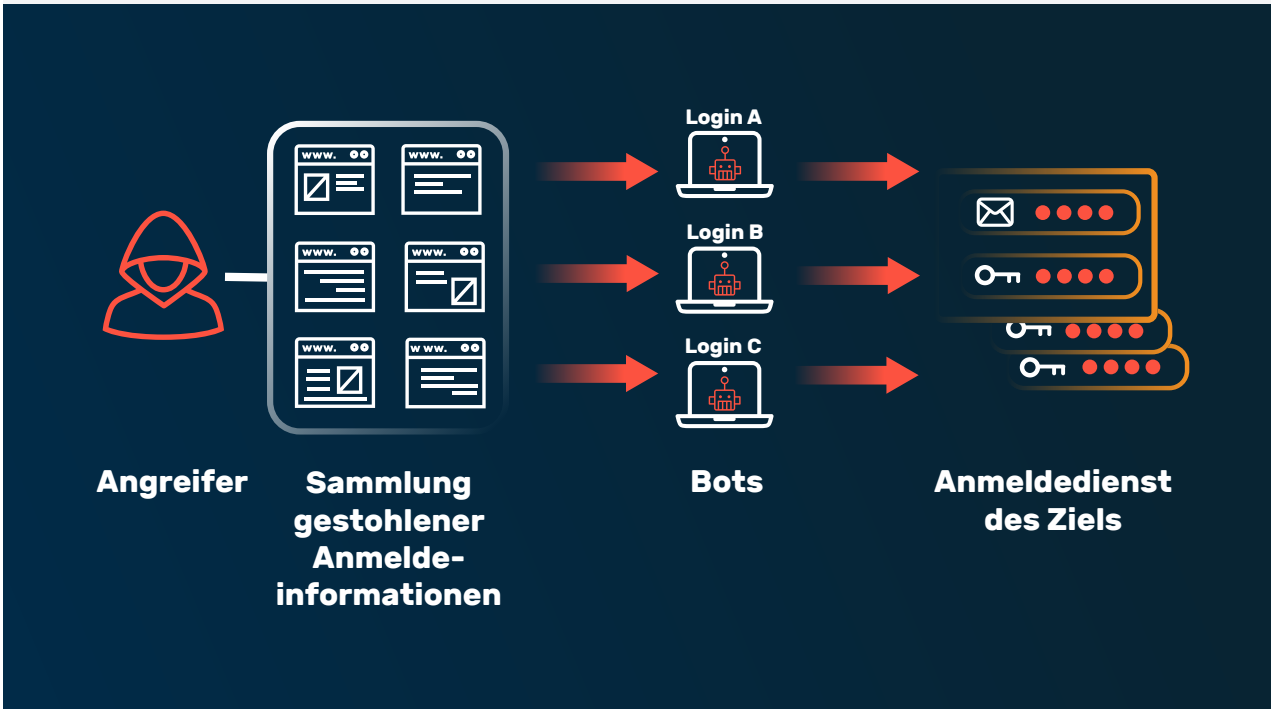
Botnet-basierte Überlastungsangriffe (DDoS)

Ein von Angreifern kontrolliertes Botnetz kann eine Flut automatisierter Anfragen an einen Webserver senden, um diesen zu überlasten und die darauf gehosteten Seiten oder Dienste lahmzulegen.

Threat Spotlight
Credential Stuffing

Bot-basiertes Credential Stuffing ist eine Angriffstechnik, bei der Cyberkriminelle gestohlene Benutzernamen und Passwörter automatisiert auf ihre Validität testen. Dabei machen sich Angreifer die Bequemlichkeit vieler Menschen zunutze, die entgegen der Empfehlung von Sicherheitsfachleuten dieselben Zugangsdaten für mehrere Konten verwenden. Die Vorgehensweise beim Credential Stuffing umfasst mehrere Schritte:

1. **Sammlung von Zugangsdaten:** Durch Datenlecks, Phishing-Angriffe oder den Kauf gestohlener Account-Informationen im Darknet erlangen Angreifer Nutzernamen und Passwörter zum Aufbau eines großen Datenpools.
2. **Automatisierte Überprüfung:** Speziell programmierte Bots testen die zuvor gesammelten Zugangsdaten auf vielen verschiedenen Websites und Plattformen, indem sie Nutzernamen und Passwörter automatisiert in Anmeldemasken eingeben. Auf diese Weise können Angreifer innerhalb kurzer Zeit Millionen Nutzername/Passwort-Kombinationen überprüfen.
3. **Erfolgreicher Kontozugriff:** Stellen sich getestete Zugangsdaten als gültig heraus, erhalten Angreifer vollen Zugriff auf aktive Accounts – falls diese nicht durch eine Multi-Faktor-Authentifizierung zusätzlich abgesichert sind.
4. **Weiterer Missbrauch:** Nach erfolgreicher Anmeldung können Angreifer kompromittierte Konten für betrügerische Aktivitäten nutzen (z.B. Phishing oder Identitätsdiebstahl), im Account gespeicherte Daten manipulieren oder abschöpfen und je nach Dienst auch Online-Käufe oder Finanztransaktionen durchführen. Ebenso werden gültige Anmeldedaten mit Gewinn an andere Kriminelle weiterverkauft.



Auswirkungen Bot-basierter Angriffe

Bots beeinflussen auf vielfältige Weise die Performance und Zuverlässigkeit von Online-Plattformen. Beides sind wichtige Parameter für die Kundenzufriedenheit und damit den geschäftlichen Erfolg. Gerade im E-Commerce können lange Seitenladezeiten oder Totalausfälle zu hohen Umsatzeinbußen führen – insbesondere an Aktionstagen wie Black Friday oder Cyber Monday. Generell sind Dienstausfälle und Betriebsstörungen durch Botnetz-basierte Überlastungsangriffe besonders kritisch. Wenn sie zusätzlich noch mit Erpressungsversuchen einhergehen, müssen Betroffene mit hohen finanziellen Schäden rechnen.

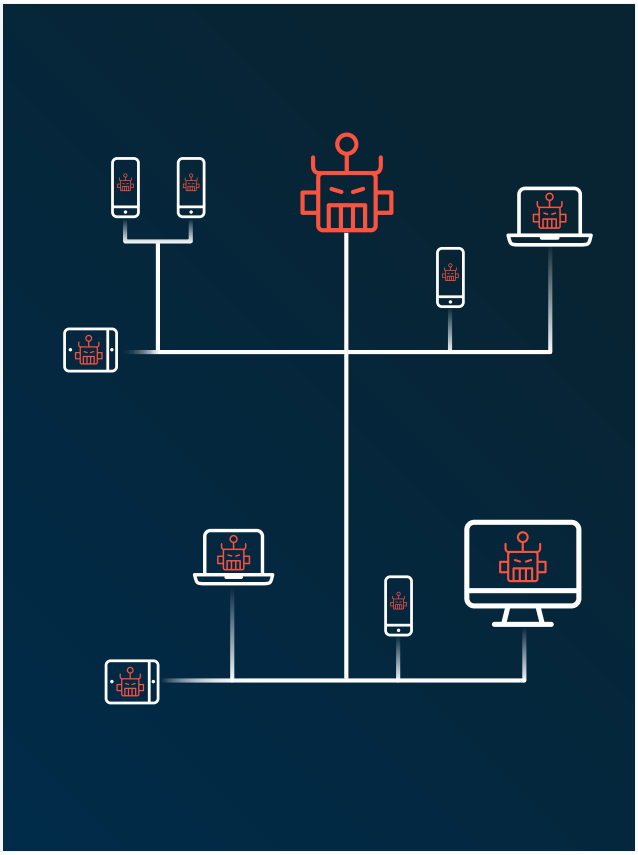
Gelingt es nicht, solche Attacken zeitnah abzuwehren, drohen außerdem langfristige Reputationsschäden: Das Kundenvertrauen in die eigene Marke sinkt, was wiederum den Geschäftserfolg nachhaltig gefährdet. Gleiches geschieht, wenn es zu Datenverlusten kommt, etwa weil Angreifer mittels Bots Nutzerkonten übernommen und anschließend sensible Daten ausgelesen haben. Handelt es sich dabei um personenbezogene Informationen, die schlimmstenfalls sogar veröffentlicht wurden, liegt eine Datenschutzverletzung vor. Die Datenschutz-Grundverordnung (DSGVO) sieht bei Verstößen Bußgelder in Höhe von bis zu 20 Millionen Euro oder bis zu 4 Prozent des weltweit erzielten Jahresumsatzes vor – je nachdem, welcher Betrag höher ausfällt.

Andere regulatorische und gesetzliche Regelungen wie die NIS-2-Richtlinie oder die DORA-Verordnung (Digital Operational Resilience Act) im Finanzsektor sehen sogar direkte rechtliche Konsequenzen für Führungskräfte vor, wenn sie ihre Sorgfaltspflicht hinsichtlich der Cybersicherheit ihres Unternehmens verletzt haben. Laut NIS-2 kann das Management im Sinne der Organhaftung persönlich für Verstöße gegen die Richtlinie haftbar gemacht werden (Artikel 20). Unter anderem sind Mitglieder der Geschäftsführung für die Umsetzung angemessener Sicherheitsmaßnahmen in ihren Einrichtungen verantwortlich.

Fest steht, dass Bot-basierte Angriffe zahlreiche negative Konsequenzen nach sich ziehen können – von finanziellen Verlusten über Imageschäden bis hin zur persönlichen Haftung des Managements. Daher empfiehlt sich die proaktive Implementierung geeigneter Schutzmaßnahmen zur Erkennung und Abwehr von Bot-Attacken, die in den folgenden Abschnitten näher erläutert werden.

Threat Spotlight
Mirai-Botnetz

Mirai gilt seit 2016 als eines der aktivsten Botnetze. Der gleichnamige Computerwurm zielt auf eine breite Palette öffentlich zugänglicher IoT-Geräte ab, um sie als ferngesteuerte Bots für illegale Aktivitäten zu nutzen – von Spam und Phishing über Credential Stuffing bis hin zu DDoS-Angriffen. Unsichere Konfigurationen und Standardpasswörter machen es Kriminellen häufig leicht, IoT-Geräte zu übernehmen und in Botnetze einzubinden. Unter anderem kam das Mirai-Botnetz bereits für Angriffe auf Server des Online-Spiels Minecraft, auf den DNS-Serviceanbieter Dyn oder auf Router der Deutschen Telekom zum Einsatz. Anfang 2022 nutzten Mirai-Derivate gezielt eine Schwachstelle in der Java-Bibliothek Log4J aus, um anfällige IoT-Geräte als DDoS-Angriffswerkzeuge oder Cryptominer zu missbrauchen. Ende 2023 wurden erneut Router und andere IoT-Geräte über zwei Zero-Day-Lücken infiziert und in ein Mirai-Botnetz für DDoS-Angriffe integriert.



The Good, the Bad and the Ugly: Identifikation von Bot-Aktivitäten

Schädliche Bot-Requests von harmlosen Anfragen seitens gutartiger Bots oder menschlicher Nutzerinnen und Nutzern zu unterscheiden, stellt eine der größten Herausforderungen beim Bot Management dar. Bad Bots greifen mit verschiedenen IP-Adressen und aus unterschiedlichen Netzwerken auf Webseiten zu. Die automatisierten Programme geben vor, ein normaler Browser zu sein und fälschen weitere Informationen wie Autonomous System Number (ASN) oder Geräte-ID, um den Anschein regulärer Nutzung zu erwecken. Das erschwert eine zuverlässige Erkennung. Durch eine Kombination folgender Maßnahmen ist eine eindeutige Identifikation aber dennoch möglich:

Verhaltensanalyse / Mustererkennung

Eine fortlaufende Überwachung des Nutzerverhaltens hilft dabei, ungewöhnliche Aktivitäten oder Zugriffsmuster zu erkennen, die vom Standard-nutzerverhalten (z. B. bei Seitenaufrufen oder Eingabegeschwindigkeit) abweichen und somit auf Bot-Aktivitäten hinweisen. Diese Mustererkennung erfolgt automatisiert per Algorithmen, um charakteristische Verhaltensweisen von Bots zu identifizieren. Dadurch lassen sich nicht nur Menschen von Bots unterscheiden, sondern auch vertrauenswürdige von schädlichen Bots.

IP-Adressüberwachung

Die Überwachung von IP-Adressen ermöglicht die Erkennung verdächtiger Aktivitäten, die von einer einzelnen IP-Adresse oder einem bestimmten IP-Adressbereich ausgehen. Dazu zählen sich häufig wiederholende Anfragen oder ungewöhnlich hoher Datenverkehr aus einer Quelle.

CAPTCHAs

Der Einsatz von CAPTCHAs und anderen Human Interaction Challenges kann ebenfalls dabei helfen, zwischen menschlichem und Bot-artigem Verhalten zu unterscheiden. Die kleinen Bild- oder Worträtsel sind für Menschen einfach zu meistern, bereiten Computern aber Probleme. Solche CAPTCHA-Prüfungen dienen etwa der Absicherung von Online-Formularen, aber auch der Vermeidung von False Positives, also fälschlicherweise als nicht vertrauenswürdig eingestuften Anfragen. Nachteile von CAPTCHAs sind allerdings, dass sie je nach Schwierigkeitsgrad relativ leicht umgangen werden können und bei exzessivem Gebrauch menschliche User schnell frustrieren.

JavaScript Challenges

Mittels JavaScript Challenges lässt sich bestimmen, ob Anfragen von einem herkömmlichen Webbrowser stammen. Dabei schickt der Webserver in einer Webseite eingebetteten JavaScript-Code an jeden anfragenden Client, um zu prüfen, ob JavaScript unterstützt wird oder z. B. bestimmte Schriftarten vorhanden sind. Scheitert der Test, handelt es sich höchstwahrscheinlich nicht um einen menschlichen User, sondern um einen Bot. Ähnlich wie CAPTCHAs können aber auch JavaScript Challenges von Bots umgangen werden und ermöglichen allein keine eindeutige Identifikation.

Fingerprinting

Fingerprinting zählt zu den komplexesten Methoden zur Erkennung von Bot-Aktivitäten. Dabei wird bei jedem Zugriff auf die überwachte Webseite anhand dutzender Attribute ein digitaler Fingerabdruck zur eindeutigen Identifikation der verwendeten Software erzeugt. Beispielsweise werden dazu Traffic- und Verhaltensmuster, Hardware-Merkmale (z. B. Gerätetyp, CPU-Informationen, Bildschirmauflösung), Software-Informationen (z. B. Betriebssystem, Browserversion, Plug-ins) sowie Netzwerkdaten (z. B. IP-Adresse, Zeitzone) analysiert und kombiniert ausgewertet. Auf diese Weise lassen sich selbst Bots identifizieren, die ihre IP-Adresse oder andere Daten fälschen, um ihren Ursprung zu verschleiern und den Anschein regulärer Nutzung zu erzeugen. Sobald der Fingerprint eines Bots vorliegt, lässt sich dieser Bot beim nächsten Zugriff sofort wiedererkennen und entsprechend behandeln.

Keine Chance für Bad Bots: Schutzmaßnahmen gegen Bot-Angriffe

Nach der eindeutigen Identifizierung von Bot-Anfragen, können verschiedene Schutzmaßnahmen aktiviert werden, um unerwünschte Requests zu blocken oder anderweitig zu kontrollieren bzw. umzuleiten. Alle automatisierten Anfragen generell zu blockieren, ist keine gute Strategie. Denn damit würden auch hilfreiche Bots ausgesperrt. Suchmaschinen-Crawler sollten etwa stets Zugriff auf alle benötigten Seiteninformationen haben, die dazu beitragen, das Suchmaschinen-Ranking und SEO-Scoring einer Website zu verbessern. Ebenso muss aber sichergestellt sein, dass unerwünschte Bot-Zugriffe gesperrt werden, welche die Leistung oder Verfügbarkeit der Website beeinträchtigen und durch erhöhte Last die Server-Kosten in die Höhe treiben können. Letztlich kommt es auf eine abgestufte Abwehr an, die für jede Anfrage die passende Antwort liefert. Dies gelingt durch eine geschickte Kombination folgender Schutzmaßnahmen:

IP-Blocklisting

Eine der einfachsten Möglichkeiten, unerwünschte Bot-Requests proaktiv abzuwehren, ist die Verwendung einer IP-Blockliste. Mit dieser Methode lassen sich Anfragen von bekannten schädlichen Ursprungs-IP-Adressen oder -Adressbereichen verwerfen, noch bevor sie die Website oder das Netzwerk beeinträchtigen können. Dadurch wird unter Umständen aber auch legitimer Traffic blockiert. Außerdem können fortschrittliche Bots ihre IP-Adresse fälschen (IP-Spoofing) oder andere Verschleierungstaktiken nutzen, um Blocklisten zu umgehen. IP-Blocklisting ist somit nur ein Teil einer umfassenderen Bot-Abwehr.

Rate Limiting

Mittels Rate Limiting lässt sich die Zahl der Requests pro Zeiteinheit begrenzen. Diese Methode hilft nicht nur gegen Bad Bots, sondern auch gegen gutartige Bots, die viel Last erzeugen und dadurch die Website-Performance schwächen. Indem einem Bot nur eine begrenzte Zahl an Anfragen pro Minute, Stunde oder Tag erlaubt wird, bleibt die verursachte Traffic-Last gering – das sichert wiederum eine einwandfreie Performance der Website.

Honeypot

Ein probates Mittel, um Bots wie Price Grabber abzuwehren, ist ein sogenannter Honeypot. Dabei handelt es sich im Prinzip um eine zweite Version der Ziel-Website, die dem Bot suggeriert, sie sei das Original. Tatsächlich enthält sie aber vollkommen andere Informationen, etwa niedrigere oder höhere Preise als auf der Originalseite. Mithilfe solcher Honeypots lassen sich Bots anlocken, um sie zu identifizieren und anschließend zu blockieren.

Multifaktor-Authentifizierung (MFA)

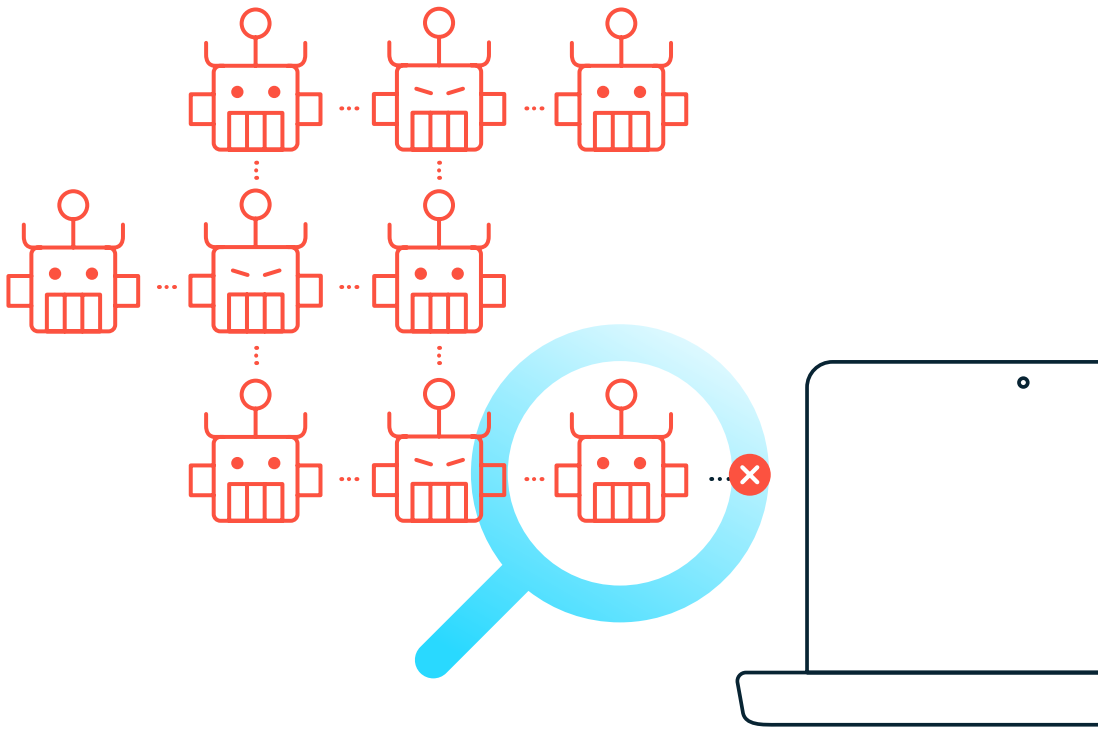
Die Verwendung einer Multifaktor-Authentifizierung ist grundsätzlich empfehlenswert, um Accounts gegen unautorisierten Zugriff abzusichern. Sie kann auch verhindern, dass Bot-Angriffe wie Credential Stuffing letztlich erfolgreich sind. Selbst wenn Angreifer mithilfe von Bots eine korrekte Nutzername/Passwort-Kombination herausgefunden haben, können sie bei aktivierter MFA ohne weitere Authentifizierung nicht auf die Inhalte des geknackten Kontos zugreifen.

Web Application Firewall (WAF)

Eine Web Application Firewall schützt Webanwendungen vor Angriffen über das Hypertext Transfer Protocol (HTTP/S). Anders als klassische Firewalls und Intrusion-Detection-Systeme (IDS) überwacht eine WAF die Kommunikation direkt auf der Anwendungsebene. Mit granularen WAF-Regeln können Bot-Anfragen automatisch blockiert, umgeleitet oder anderweitig kontrolliert werden.

Dediziertes Bot Management

Ein dediziertes Bot Management ermöglicht eine effektive Steuerung aller Bot-Aktivitäten – von der Erkennung über die Prävention bis hin zur Reaktion. Dazu werden die zuvor genannten Techniken in einer einzigen Lösung kombiniert und idealerweise um manuelle Analysen von Sicherheitsfachleuten eines Security Operations Center (SOC) ergänzt.
Ein sauber aufgesetztes Bot Management identifiziert vertrauenswürdige Bots, indem es die Bot-Reputation erkennt, die Ursprungs-IP-Adressen auswertet und das Verhalten von Bots beobachtet. Vertrauenswürdige Bots werden einer Allowlist hinzugefügt und können weiterhin auf die Webseite zugreifen, während unseriösen und schädlichen Bots der Zugriff verweigert wird. Auf diese Weise schützt ein dediziertes Bot Management Websites, Webapplikationen und Online-Schnittstellen (APIs) vor Bot-basierten Angriffen und trägt zugleich zu einer optimalen Website-Performance für menschliche User und gutartige Bots bei.



Cloud-basiertes Bot Management: effektiver Schutz vor automatisierten Bedrohungen

In unserer digitalisierten Welt sind Unternehmen und Organisationen allgegenwärtig mit IT-Sicherheitsbedrohungen konfrontiert. Cyberattacken stellen laut dem aktuellen Allianz Risk Barometer das größte Risiko für Unternehmen in Deutschland und weltweit dar. Angriffe auf die digitalen Systeme deutscher Firmen haben dem Digitalverband Bitkom zufolge im Jahr 2023 Schäden in Höhe von 206 Milliarden Euro verursacht. Angesichts der anhaltend angespannten Bedrohungslage sehen mehr als die Hälfte aller Organisationen ihre Existenz gefährdet.

Die Frage ist nicht, ob, sondern wann die eigene Organisation selbst zum Ziel einer Cyberattacke wird. Zumal Angreifer immer professioneller organisiert sind und ihre Methoden stetig weiterentwickeln, etwa durch Verwendung generativer KI-Modelle. Auch Cybercrime-as-a-Service trägt zur Verschärfung der Bedrohungslage bei: Selbst technisch unversierte Akteure können heutzutage über das Internet bereitgestellte Angriffswerkzeuge wie Botnetze für kleines Geld als Dienstleistung nutzen, um ernsthafte Attacken wie Distributed Denial of Service durchzuführen und schwere Schäden anzurichten.

Vor diesem Hintergrund sollten Unternehmen und Behörden auf einen holistischen Schutz ihrer IT-Infrastrukturen und Webapplikationen setzen. Das schließt auch eine präventive Abwehr von Bot-Angriffen ein, idealerweise in Form eines dedizierten Bot Managements. Der Inhouse-Betrieb einer solchen Bot Management Solution ist jedoch mit hohem zeitlichem und finanziellem Aufwand verbunden. Zudem wird dafür Fachpersonal mit entsprechender Security-Expertise benötigt, das angesichts des Fachkräftemangels im IT-Umfeld nur schwer zu finden sein dürfte.

Als kosteneffiziente und effektive Alternative bietet sich ein Cloud-basiertes Bot Management an, das keine zusätzlichen Investitionen in Hardware, Software oder Fachpersonal erfordert. Ein solcher Service lässt sich deutlich schneller und einfacher implementieren als eine vergleichbare On-Premises-Lösung. Einrichtung, Konfiguration und Betrieb erfolgen in enger Abstimmung mit dem Expertenteam des Dienstleisters. Ein weiterer entscheidender Vorteil: Ein Cloud-basiertes Bot Management ist besser skalierbar und passt sich durch kontinuierliche Aktualisierungen stets an die sich verändernde Bot-Landschaft an. So können Organisationen immer angemessen auf akute Bedrohungen reagieren und sich proaktiv gegen zukünftige Risiken absichern.

Schnell, zuverlässig, skalierbar: Deep Bot Management von Myra Security

Der deutsche Technologiehersteller Myra Security bietet ein dediziertes Bot Management an, das alle eingehenden Anfragen an Webseiten, Online-Anwendungen und APIs unterteilt, klassifiziert und analysiert. Basierend auf dem Ergebnis der Analyse wird für jeden Request die passende Reaktion ausgeliefert. Unerwünschte oder schädliche Anfragen verwirft oder blockiert Myra, noch bevor sie Ihre Server erreichen und diese belasten.

Als Security-as-a-Service-Lösung ist das Deep Bot Management schnell und einfach implementierbar. Zusätzliche Software oder Hardware ist für den Betrieb nicht erforderlich. Myra schützt mit seinen BSI-zertifizierten Security- und Performance-Diensten 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

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 Demo anfordern →

Myra Security GmbH

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