LINK11

WHITEPAPER

State of Bot Management

www.link11.com

Inhalt

Einführung

Zusammensetzung des Webverkehrs
Ein robustes Bot-Management ist in der heutigen, sich ständig verändernden Bedrohungslandschaft wichtiger denn je. Im Jahr 2024 hat der automatisierte Bot-Verkehr erstmals seit über zehn Jahren den von Menschen erzeugten Internetverkehr übertroffen und machte 51 % aller Webaktivitäten aus.

Large Language Models beschleunigen Bot-Angriffe
Die Zunahme bösartiger Bot-Aktivitäten steht in direktem Zusammenhang mit der Verbreitung generativer KI und großer Sprachmodelle (LLMs) wie ChatGPT, Gemini, Claude und Perplexity AI. Diese Tools ermöglichen es selbst unerfahrenen Angreifern, Bots in großem Umfang und mit hoher Frequenz einzusetzen. Durch das Aufkommen eines wachsenden „Bots-as-a-Service"-Ökosystems sind die Einstiegshürden sogar noch weiter gesunken, sodass technisch nicht versierte Akteure mit minimalem Aufwand automatisierte Angriffe starten können.

Aus technischer Sicht nutzen Angreifer KI nun, um fehlgeschlagene Angriffe zu analysieren und ihre Methoden kontinuierlich zu verfeinern. Dadurch entstehen immer raffiniertere, ausweichende Bots, die für herkömmliche Sicherheitssysteme schwerer zu erkennen sind.

Ein robustes Bot-Management ist heute für die Web-Sicherheit unerlässlich. Im Durchschnitt der verschiedenen Branchen stammen nur 38 Prozent der eingehenden Anfragen von menschlichen Nutzern. Die restlichen 62 Prozent haben einen automatisierten Ursprung.

Nicht alle Bots sind schädlich. Einige (z. B. Suchmaschinen-Spider) sind auf Websites sogar willkommen, während andere (z. B. Content-Aggregatoren) nicht offensichtlich feindselig sind. Dennoch stammen fast 40 Prozent der eingehenden Anfragen von bösartigen Bots (siehe Grafik).

Folgen eines unzureichenden Schutzes
Bedrohungsakteure nutzen Bots, um eine Vielzahl von Webangriffen durchzuführen. Tatsächlich sind an fast allen Angriffen auf die eine oder andere Weise Bots beteiligt. Werden feindliche Bots nicht identifiziert und blockiert, können sie für Unternehmen mit bedeutenden Webressourcen (Websites und Webanwendungen, Microservices und mobile/native API-Endpunkte) eine Vielzahl von Problemen verursachen.

Einige der potenziellen Probleme sind:

Ausfall von Websites,
wenn DDoS-Angriffe die Ressourcen von Anwendungen oder Servern erschöpfen.

Datendiebstahl
durch Scraping.

Eindringen in die Website
durch Bots, die Schwachstellen aufspüren.

Umsatzeinbußen
durch das Horten von Beständen.

Schlechte Geschäftsentscheidungen
durch verzerrte Analysen.

Kontodiebstahl
durch Ausfüllen von Anmeldeinformationen.

Probleme mit Händlerkonten
aufgrund von Kreditkartentests

Beeinträchtigung der Kundenerfahrung
durch Bandbreiten- und Ressourcenverluste

Die Bedrohungslandschaften

Unterschiedliche Branchen, unterschiedliche Bot-Bedrohungen
Nicht jeder feindliche Bot-Traffic sieht gleich aus. Unterschiedliche Branchen sind unterschiedlichen Arten von Angriffen ausgesetzt. Der Grund dafür ist, dass Angreifer es auf die wertvollen Daten eines bestimmten Sektors abgesehen haben. So kann beispielsweise die Website einer Fluggesellschaft von Bots überschwemmt werden, die versuchen, Flugpreise abzugreifen, während die Website eines E-Commerce-Unternehmens von Bots überschwemmt wird, die begrenzte Warenbestände horten.

Um diese Bedrohungen besser zu verstehen und darauf zu reagieren, ist es hilfreich, eine einfache, aber wichtige Frage zu stellen: „Wer ist der Nutznießer?" Dieses Prinzip, abgekürzt WSTG (Who stands to gain?), kann Unternehmen dabei helfen, mögliche Angreifer und ihre Motive zu identifizieren. Ähnlich wie Detektive in Krimiserien „dem Geld folgen", können Cybersicherheitsexperten oft die Absicht eines Bot-Angriffs bestimmen, indem sie sich ansehen, wer davon profitiert. Die häufigsten Arten von Bot-Bedrohungen sind im Folgenden aufgeführt und werden in den nächsten Abschnitten näher erläutert.

Distributed Denial of Service (DDoS):
Systeme flächendeckend lahmlegen

Kreditkartenbetrug:
Automatisierung als Kernelement

Zugangsdaten
in großem Maßstab stehlen

Automatisierte Hamsterkäufe
verhindern echten Zugriff

Scraping und Datendiebstahl:
Geräuschlose, skalierbare Extraktion

Schwachstellenscans
ebnen den Weg für gezielte Angriffe

Automatisierte Klicks
verzerren Kampagnen und schmälern Einnahmen

Bots nutzen Schwachstellen
in APIs systematisch aus

Distributed Denial of Service (DDoS):
Systeme flächendeckend lahmlegen

Distributed-Denial-of-Service-Angriffe (DDoS) zählen zu den aggressivsten und lästigsten botbasierten Bedrohungen. Angreifer nutzen große Bot-Netzwerke, um Webanwendungen oder APIs mit einer Flut von Daten zu überlasten, sodass sie für legitime Benutzer nicht mehr verfügbar sind. Wenn der Angriffsverkehr nicht wirksam gefiltert werden kann, dann kann die Störung unbegrenzt andauern – ganz nach den Bedingungen der Angreifer.

Im Gegensatz zu anderen Arten von Angriffen, die manuell durchgeführt werden können (z. B. das Scannen von Sicherheitslücken), sind DDoS-Angriffe von Natur aus automatisiert und verteilt. Die beteiligten Bots sind unterschiedlich komplex und reichen von mit Malware infizierten PCs bis hin zu gekaperten IoT-Geräten.

Timing und Strategie

DDoS-Angriffe sind oft sorgfältig getaktet. Bei Online-Spielen können sie beispielsweise kurz vor einem großen Ereignis stattfinden, um die Nutzer zu konkurrierenden Plattformen zu treiben. Im E-Commerce zielen die Angreifer oft auf die Haupteinkaufszeiten ab und nutzen Ausfallzeiten als Druckmittel für Erpressungsforderungen.

Wer profitiert davon?

- **Cyberkriminelle:** Sie nutzen DDoS für Lösegeldforderungen (DDoS-for-hire oder Erpressung).
- **Konkurrenten:** Sie versuchen, den Betrieb zu stören und Nutzer abzulenken.
- **Hacktivisten:** Sie starten Angriffe als Vergeltungsmaßnahme oder aus Protest.
- **Staatliche Akteure:** Sie unterdrücken abweichende Meinungen, indem sie Nichtregierungsorganisationen, die Medien und Oppositionsgruppen ins Visier nehmen.

Die Folgen:

Die Auswirkungen gehen über reine Ausfallzeiten hinaus. Unternehmen können Umsatzeinbußen erleiden sowie ihren Ruf und das Vertrauen ihrer Kunden verlieren. In schwerwiegenden oder wiederholten Fällen kann sich zudem die Platzierung in Suchmaschinen verschlechtern, was sich wiederum auf die Sichtbarkeit und die Besucherzahlen auswirkt.

Kreditkartenbetrug:
Automatisierung als Kernelement

Bots spielen beim modernen Kreditkartenbetrug eine zentrale Rolle. Kriminelle nutzen sie, um Kartennummern zu stehlen, zu testen und auszunutzen, was zu finanziellen Verlusten, Rückbuchungen und Rufschädigungen für Händler führt.

Eine gängige Methode ist das Scannen von Schwachstellen, bei dem Bots nach Schwachstellen in Websites für die Zahlungsabwicklung suchen, z. B. in E-Commerce-Plattformen oder Serviceportalen. Sobald eine Schwachstelle gefunden ist, dringen die Angreifer in das System ein und extrahieren große Mengen an Kartendaten, wobei sie oft Tausende von gültigen Nummern in einem einzigen Angriff stehlen.

Die gestohlenen Kartennummern werden dann mithilfe von Bots validiert. Diese Bots übermitteln die Daten an Online-Formulare, um zu sehen, ob die Nummern akzeptiert oder abgelehnt wird. Die Angreifer verwenden auch eine Brute-Force-Methode namens „Kartenaufzählung“, bei der die Bots so lange Zahlenkombinationen durchgehen, bis sie gültige finden. Diese Methode ist zwar grob, aber effektiv und vollständig automatisiert.

Ein wichtiger Grund für diesen Trend ist die Zunahme des „Card-not-present“-Betrugs (CNP). Da EMV-Chipkarten den Betrug im persönlichen Umfeld erschweren, haben Cyberkriminelle ihren Schwerpunkt auf das Internet verlagert, wo Bots in großem Umfang und mit minimalem Risiko eingesetzt werden können.

Wer profitiert davon?

Cyberkriminelle: Sie profitieren, indem sie gestohlene Karten im Darknet verkaufen oder sie für betrügerische Einkäufe verwenden.

Die Folgen:

Den Händlern entgehen Einnahmen, wenn Waren versandt und betrügerische Zahlungen rückgängig gemacht werden. Wiederholter Betrug kann zu Geldstrafen und in schweren Fällen zur Kündigung des Händlerkontos durch den Zahlungsanbieter führen.

Jahr	Geschätzte Verluste (in Mrd. USD)
2022	17,5
2023	44,3
2024	48,0
2029	107,0

77%

der Einzelhändler in den USA sind online tätig.

77%

der Internetnutzer in der EU kauften 2024 online ein.

84%

der Bevölkerung in den nordischen Ländern kaufen online ein.

Zugangsdaten
in großem Maßstab stehlen

Benutzerdaten wie Logins und Passwörter sind das Hauptziel von Cyberkriminellen. Bots werden routinemäßig für Brute-Force-Angriffe eingesetzt, bei denen unzählige Zeichenkombinationen getestet werden, bis der Zugang gewährt wird. Alternativ dazu erbeuten Angreifer Anmeldedaten durch groß angelegte Datenpannen und -lecks.

Sobald gültige Zugangsdaten erlangt wurden, können diese für weitere Angriffe verwendet oder auf Dark-Web-Marktplätzen verkauft werden. Eine gängige Taktik ist das „Credential Stuffing", bei dem Bots gestohlene Zugangsdaten auf mehreren Websites testen. Dabei wird ausgenutzt, dass viele Benutzer dieselben Anmeldedaten wiederverwenden. Dies führt nach nur einem Einbruch oft zu mehreren erfolgreichen Kontoübernahmen.

Eine weitere wachsende Bedrohung ist die automatische Erstellung oder Übernahme von Konten. Dabei erstellen Bots gefälschte Konten für Missbrauch (z. B. Werbebetrug oder Spam) oder übernehmen die Kontrolle über echte Benutzerkonten, um diese auszubeuten oder zu stehlen.

Wer profitiert davon?

Cyberkriminelle: Sie profitieren, indem sie gestohlene Zugangsdaten weiterverkaufen oder sie für den Zugriff auf sensible Systeme und Dienste verwenden.

Die Folgen:

Kompromittierte Konten führen zu Betrug, Datenpreisgabe und Rufschädigung. Betroffene Unternehmen müssen mit öffentlichen Reaktionen, dem Verlust des Kundenvertrauens und möglicherweise mit Geldstrafen rechnen – insbesondere in Branchen, die mit persönlichen oder finanziellen Daten umgehen.

84%

der Nutzer weltweit verwenden ihre **Passwörter für mehr als eine Website** oder Anwendung.

Automatisierte Hamsterkäufe
verhindern echten Zugriff

Webanwendungen, die Einkäufe oder Reservierungen erleichtern, sind ein bevorzugtes Ziel für „Inventory Hoarding". Dabei handelt es sich um eine von Bots gesteuerte Taktik, die legitime Kunden am Zugriff auf verfügbare Bestände hindert. Bots überschwemmen Einzelhandels- oder Buchungsplattformen, indem sie Produkte oder Reservierungen in Warenkörbe legen, ohne den Kauf abzuschließen. Dadurch werden Bestände blockiert und es entsteht eine künstliche Verknappung.

Die Reisebranche ist besonders anfällig. Bots nutzen das 15-minütige Zeitfenster „Zeit bis zum Checkout" aus, indem sie Buchungen kontinuierlich durchlaufen, ohne einen Kauf abzuschließen. Dadurch wird verhindert, dass echte Nutzer Tickets oder Reservierungen sichern können.

Der finanzielle Schaden kann über entgangene Umsätze hinausgehen. Viele Reise-Websites verlassen sich bei Flugdaten auf Aggregatoren von Drittanbietern. Jede Benutzersuche kann eine Gebühr für die Datenabfrage auslösen, die unabhängig davon berechnet wird, ob ein Kauf zustande kommt. Da Bots ein hohes Volumen an nicht konvertierendem Traffic generieren, können diese Gebühren schnell zu einer großen Kostenstelle werden, die nicht durch Einnahmen ausgeglichen werd

Wer profitiert davon?

Konkurrenten nutzen Bots, um den Geschäftsbetrieb zu stören und Ressourcen zu verschwenden.

Die Folgen:

Das Horten von Beständen wirkt wie ein Denial-of-Service-Angriff auf der Anwendungsebene und führt zu:

- verlorenen Einnahmen durch blockierte Käufe,
- unverkaufte Bestände (z. B. Veranstaltungstickets, Flüge),
- steigende Betriebskosten (z. B. Gebühren für Aggregatoren),
- beschädigtes Kundenvertrauen aufgrund schlechter Nutzererfahrung.

59%

des E-Commerce-Verkehrs **stammen von Bots**, von denen ein erheblicher Teil zum Horten von Beständen genutzt wird.

Scraping und Datendiebstahl:
Geräuschlose, skalierbare Extraktion

Scraping-Bots sind darauf ausgelegt, wertvolle Daten aus Websites und Webanwendungen zu extrahieren – und das oft, ohne dabei entdeckt zu werden. Sie zielen auf Branchen ab, die auf geschützte Daten oder Inhalte angewiesen sind, darunter Aggregatoren, Versicherungsplattformen und Online-Händler. Für datengesteuerte Unternehmen stellt Scraping eine direkte Bedrohung ihrer wichtigsten Umsatzmodelle dar.

Im Einzelhandel sammeln Bots beispielsweise Produktdetails, Preise und Bestandsdaten. Konkurrenten können diese Informationen nutzen, um Preise zu unterbieten, Angebote zu kopieren oder nutzergenerierte Inhalte wie Bewertungen zu replizieren. Das schadet der Markendifferenzierung und der Verkaufsleistung.

Fortschrittlichere Scraping-Bots verwenden automatisierte, hochfrequente Abfragen, um ganze Datensätze zu rekonstruieren, die nicht über eine einzelne Webseite oder einen API-Aufruf zugänglich sind. So können beispielsweise Tools zur Erstellung von Versicherungsangeboten ausgenutzt werden, indem tausende Angebotsanfragen mit unterschiedlichen Parametern gestellt werden, wodurch nach und nach vollständige Preismodelle offengelegt werden.

Wer profitiert davon?

- **Wettbewerber** nutzen gescrapte Daten, um sich unlautere Vorteile zu verschaffen, beispielsweise niedrigere Preise, geklonte Inhalte oder eine schnellere Markteinführung.
- **Kriminelle** verkaufen gestohlene Daten an Dritte oder nutzen sie für betrügerische Zwecke.

Die Folgen:

Der Schaden ist vielschichtig:

- Verlust des Wettbewerbsvorteils durch Preisgestaltung und Diebstahl von Inhalten,
- geringere Sichtbarkeit in Suchmaschinen aufgrund von doppelten Inhalten,
- Markenerosion, wenn Nutzer an anderer Stelle auf veraltete, kopierte oder missbrauchte Informationen stoßen.

Bis 2025 werden KI-gestützte Scraping-Tools zum Standard gehören.
Sie werden Anti-Bot-Maßnahmen erkennen und umgehen, CAPTCHAs lösen und sich an dynamische Websites anpassen.

Im Jahr 2024 waren **neun von zehn Websites** Ziel von Bot-Angriffen, einschließlich Scraping.

Schwachstellenscans
ebnen den Weg für gezielte Angriffe

Cyberkriminelle nutzen Bots, um eine große Anzahl von Systemen auf bekannte Schwachstellen zu scannen. Diese automatisierten Scans dienen oft als Ausgangspunkt für schwerwiegendere Angriffe. Sobald eine Schwachstelle identifiziert wurde, handeln die Angreifer schnell. Entweder sofort oder indem sie die Grundlage für zukünftige Angriffe schaffen.

Welche Taktik sie dabei anwenden, hängt von der jeweiligen Schwachstelle ab. In einigen Fällen lösen die Bots innerhalb weniger Minuten Datendiebstahl, Malware oder eine Ransomware-Verschlüsselung aus. In anderen Fällen installieren die Angreifer Hintertüren, um sich langfristigen Zugang zu verschaffen und nach und nach tiefer in das System einzudringen. Dieser Ansatz ist üblich, wenn komplexe Umgebungen mit hochwertigen Daten angegriffen werden.

Ein berüchtigtes Beispiel ist der Einbruch bei Equifax, bei dem eine ungepatchte Apache-Struts-Schwachstelle ausgenutzt wurde. Der Angriff begann mit einem automatischen Scan und führte schließlich zu einem massiven Datenverlust, von dem Millionen Menschen betroffen waren.

Wer profitiert davon?

- **Cyberkriminelle** nutzen Scans als Einfallstor für umfassendere Angriffe, oft als Teil größerer Kampagnen.

Die Folgen:

Unmittelbare Risiken:

- Datenexfiltration,
- Malware-Infektionen,
- Einsatz von Ransomware.

Langfristige Risiken:

- hartnäckige Hintertüren, Netzwerkkompromittierung und Rufschädigung.

Die Folgen für die Gesetzgebung können Untersuchungen, Strafen und Versagen bei der Einhaltung von Vorschriften nach groß angelegten Datenschutzverletzungen sein.

60 % der Datenschutzverletzungen werden durch nicht gepatchte Sicherheitslücken verursacht.

In großen Unternehmen bleiben **45,4 %** der Sicherheitslücken länger als 12 Monate ungepatcht, insbesondere im Netzwerkbereich.

Automatisierte Klicks
verzerren Kampagnen und schmälern Einnahmen

Klickbetrug ist eine der am meisten unterschätzten Formen des botgesteuerten Missbrauchs. Bots erzeugen gefälschte Klicks auf Anzeigen. Dadurch werden die Traffic-Metriken aufgebläht und Werbekampagnen sabotiert. Auch wenn Klickbetrug weniger aggressiv erscheint als andere Angriffsarten, kann er erhebliche finanzielle Auswirkungen haben.

Werbetreibende sind die unmittelbaren Opfer, da sie ihr Budget für gefälschtes Engagement verschwenden und schlechte Ergebnisse erzielen. Aber auch die Herausgeber, also die Websites, die die Anzeigen hosten, sind betroffen. Bleibt Bot-Verkehr unentdeckt, setzen Werbenetzwerke die Website oft auf eine schwarze Liste, was die künftige Monetarisierung der Website verhindert.

Werbenetzwerke überwachen den ungültigen Datenverkehr daher sehr genau. Entdecken sie übermäßige betrügerische Klicks, machen sie bereits bezahlte Einnahmen rückgängig, was zu direkten Einkommensverlusten für den Publisher führt. Noch schlimmer ist, dass diese Impressionen nicht mehr monetarisiert werden können, da der Traffic nicht mehr vorhanden ist.

Wer profitiert davon?

- **Cyberkriminelle v**erdienen Affiliate-Einnahmen durch betrügerische Klicks auf ihren eigenen werbefinanzierten Seiten.
- **Konkurrenten** setzen Bots ein, um die Werbebudgets von Konkurrenten abzuschöpfen oder deren Ruf bei Netzwerken zu schädigen.

Die Folgen:

- Einnahmeverluste durch Zahlungsrückbuchungen und Strafen für ungültigen Traffic,
- langfristiger Schaden, da sich Werbenetzwerke weigern, künftiges Inventar bereitzustellen,
- schlechte Kampagnenleistung für Werbetreibende, die geschäftliche oder politische Ziele verfolgen.

Laut dem „Ad Fraud Report 2025" sind fast **12 %** aller **Klicks auf bezahlte Anzeigen ungültig**, d. h. sie stammen von Bots, Wettbewerbern oder betrügerischen Quellen.

Bots nutzen Schwachstellen
in APIs systematisch aus

Diese Kategorie umfasst eine breite Palette botgesteuerter Angriffe, die die einzigartigen Funktionen einer Webanwendung oder ihrer APIs ausnutzen. Im Gegensatz zu anderen Bedrohungsarten ist diese Kategorie nicht an eine einzige Taktik gebunden. Sie reicht von SMS-Spam über Telekom-APIs bis hin zum unbefugten Zugriff auf die Anwendungslogik.

Da API-Endpunkte zentrale Funktionen und Daten offenlegen, haben es Angreifer zunehmend auf sie abgesehen. Viele der oben genannten Angriffe – wie beispielsweise Credential Stuffing, Scraping und das Horten von Beständen – können direkt über APIs ausgeführt werden. Einige Bots sind speziell für das Reverse Engineering undokumentierter APIs konzipiert, um versteckte Methoden oder Schwachstellen zu identifizieren, die sich in großem Umfang ausnutzen lassen.

Die Eindämmung des Anwendungsmissbrauchs erfordert eine mehrschichtige Verteidigung:

- Verhinderung von API-Entdeckung und Reverse Engineering,
- Erzwingen von Schema-Validierung und angemessener Ratenbegrenzung,
- Erkennung abnormaler Nutzungsmuster, die für jede Anwendung oder jeden Dienst einzigartig sind.

Dies macht den Anwendungsmissbrauch zu einer der dynamischsten und am schwierigsten zu handhabenden Bot-Bedrohungen.

Wer profitiert davon?

- **Cyberkriminelle:** Ausnutzung der offengelegten Funktionen für Betrug, Spam oder Ressourcendiebstahl.
- **Konkurrenten:** Beeinträchtigung von Diensten oder Extraktion geschützter Daten.

Die Folgen:

Der Missbrauch von Anwendungen kann zu einer Vielzahl von Problemen führen, darunter:

- DDoS-Angriffe auf APIs,
- Angriffe auf Anmeldeinformationen,
- Horten von Beständen oder Verweigerung,
- Scraping und Datendiebstahl,
- betrügerische Aktivitäten oder Massen-Spamming.

Die Wahrscheinlichkeit eines jeden Angriffs hängt davon ab, wie stark die Anwendung oder API exponiert ist und wie gut sie geschützt ist.

Laut Statista werden sich die weltweiten Verluste durch Cyberkriminalität im Jahr 2029 auf rund 15,6 Billionen US-Dollar belaufen – **ein Anstieg von fast 70 %** im Vergleich zu 2024.

Traditionelle Erkennungsmethoden

In der Vergangenheit stützte sich die Bot-Erkennung auf nur wenige Kerntechniken:

Rate Limiting:
Bei dem Nutzer gesperrt werden, die bestimmte Anforderungsschwellen überschreiten.

IP-Blacklisting:
Verweigerung des Datenverkehrs von bekanntermaßen bösartigen oder verdächtigen IP-Adressen.

Erkennung der Traffic-Umgebung:
Verwendung von JavaScript-Challenges oder Cookie-Tests zur Erkennung von Nicht-Browser-Umgebungen.

Signaturabgleich:
Identifizierung bekannter Bot-Muster in Anfrage-Headern oder im Verhalten.

CAPTCHA:
Bilder und Rätsel, um Menschen von Bots zu unterscheiden.

Diese Methoden sind gegen einfache oder veraltete Bots wirksam, gegen die modernen Bedrohungen von heute sind sie jedoch unwirksam. Viele moderne Bots, insbesondere solche, die von KI gesteuert werden oder menschliches Verhalten nachahmen, können diese Schutzmaßnahmen vollständig umgehen.

Das Problem liegt nicht in den Methoden selbst, sondern darin, dass man sich auf sie allein verlässt. Leider machen viele Intrusion-Detection-Systeme (IDS) zur Erkennung von Eindringlingen und zur Eindämmung von Bots immer noch genau das, wodurch Unternehmen den immer raffinierteren Bot-Angriffen ausgesetzt sind.

Warum herkömmliche Abwehrmaßnahmen gegen moderne Bots versagen

Veraltete Bot-Erkennungstechniken sind nicht mehr ausreichend. Da die Angreifer immer raffinierter werden und die künstliche Intelligenz die Einstiegshürde immer weiter senkt, sind moderne Bots darauf ausgelegt, herkömmliche Abwehrmaßnahmen zu umgehen.

Hier sind die Gründe, warum diese Methoden versagen:

- **Rate Limiting** wird umgangen, indem IP-Adressen rotieren und Anfragen gedrosselt werden, um innerhalb akzeptabler Grenzen zu bleiben.
- **IP-Blacklists** sind gegen große Botnets und Proxy-Netzwerke, die zahllose IP-Adressen durchlaufen, unwirksam.
- **Die Erkennung von Signaturen** kann leicht umgangen werden, indem Header wie User-Agent-Strings gefälscht werden, um legitimen Datenverkehr zu imitieren.
- **Headless-Browser** können von der Umgebungserkennung nicht zuverlässig gestoppt werden, da sie mittlerweile die Ausführung von JavaScript, die Handhabung von Cookies und menschenähnliche Interaktionsmuster unterstützen.
- **Headless-Browser** werden immer fortschrittlicher und sind zunehmend schwer von echten Benutzern zu unterscheiden, zumal sie häufig für legitime Automatisierungen und Tests verwendet werden.

Diese Fortschritte haben herkömmliche Erkennungstechniken weitgehend überflüssig gemacht. Eine wirksame Bot-Abwehr erfordert heute einen anpassungsfähigeren, verhaltensorientierten Ansatz, der echte Benutzer in Echtzeit von ausgeklügelten Automatisierungen unterscheiden kann.

CAPTCHA-Lösungen zwischen Sicherheit und Benutzerfreundlichkeit

CAPTCHA ist eine gängige Methode, um zwischen menschlichen Benutzern und Bots unterscheiden zu können. Bei verdächtigem Datenverkehr werden diese Aufgaben gestellt, die so konzipiert sind, dass sie von Menschen gelöst werden können, automatisierten Systemen jedoch Schwierigkeiten bereiten.

CAPTCHA-Systeme werden häufig eingesetzt, um zwischen menschlichen Benutzern und Bots zu unterscheiden. Diese Systeme führen Challenge-Response-Tests durch, die von einfachen Aufforderungen zum Ankreuzen von Kästchen bis hin zu Bilderkennungsaufgaben reichen. Sie zielen darauf ab, bösartigen Datenverkehr zu blockieren, ohne legitime Benutzer zu stark zu belasten.

Im Laufe der Zeit hat sich die Bot-Landschaft jedoch erheblich weiterentwickelt. Viele moderne Bots, die von KI, Headless-Browsern oder CAPTCHA-Lösungsdiensten angetrieben werden, können herkömmliche Aufgaben umgehen. Dies hat zu einem stetigen Kreislauf immer komplexerer CAPTCHA-Mechanismen geführt, welche das Nutzererlebnis beeinträchtigen können.

Lösungen wie reCAPTCHA v3 versuchen, die sichtbaren Aufgaben zu umgehen, indem sie das Benutzerverhalten im Hintergrund analysieren. Dies verringert die Reibungsverluste zwar, wirft aber auch Fragen auf hinsichtlich der Erkennungsgenauigkeit, der Auswirkungen auf den Datenschutz aufgrund der tiefen Integration in Browser-Cookies sowie der Kostenstruktur für Websites mit hohem Aufkommen.

Trotz dieser Fortschritte kann keine CAPTCHA-Lösung das Risiko des Bot-Missbrauchs vollständig ausschalten, ohne Kompromisse einzugehen.

- KI-gestützte Bots können Text- und Bild-CAPTCHAs präzise lösen.
- Automatisierte CAPTCHA-Lösungsdienste ermöglichen eine groß angelegte Umgehung.
- Herkömmliche CAPTCHAs blockieren einfache Bots, sind aber weniger wirksam gegen fortschrittlichere Bedrohungen.
- Behavioral CAPTCHAs erkennen Bots auf unauffällige Weise und verbessern die Benutzerfreundlichkeit.

Daher erforschen viele Unternehmen ergänzende oder alternative Ansätze zur Bot-Abwehr wie Verhaltensanalyse, Fingerprinting und serverseitige Validierung, um den Schutz zu verstärken und sich nicht ausschließlich auf aufgabenbasierte Abwehrmaßnahmen zu verlassen.

CAPTCHA ist zwar nach wie vor eine weitverbreitete Sicherheitsebene, aber am effektivsten, wenn es mit umfassenderen Bot-Management-Strategien kombiniert wird, die sich mit den heutigen adaptiven und unbekannten Bedrohungen befassen.

Im Durchschnitt braucht eine Person **32 Sekunden**, um eine CAPTCHA-Aufgabe zu lösen.

Die zunehmende Irrelevanz von IP und Geolokalisierung

Herkömmliche Methoden zum Aufspüren von Angreifern beruhen auf IP-Adressen. Allerdings sind Systeme zur Erkennung von Eindringlingen, die sich stark auf die IP-Adresse stützen, heutzutage weitgehend unwirksam.

Sich auf IP-Adressen zu verlassen, um Angreifer zu identifizieren, ist nicht mehr effektiv. Moderne Benutzer – sowohl legitime als auch böswillige – ändern ständig ihre IP-Adressen, wenn sie zwischen mobilen Netzwerken, virtuellen privaten Netzwerken (VPNs) und öffentlichen WLAN-Netzwerken wechseln. Ein einzelnes Gerät kann in einer einzigen Sitzung mehrere Adressen durchlaufen und ein öffentlicher Hotspot kann an einem Tag tausende Benutzer bedienen. Die Sperrung einer IP-Adresse wegen eines einzigen böswilligen Benutzers könnte viele legitime Kunden ausschließen.

Angreifer machen sich diese Fluktuation zunutze. Bot-Betreiber wechseln bei jeder Anfrage die IP-Adressen, missbrauchen mobile Gateways und kapern IoT-Geräte oder Browser-Erweiterungen, um sich hinter riesigen Adresspools zu verstecken. Bei groß angelegten Angriffen werden routinemäßig zehntausende Anfragen pro Minute gestellt, wobei jede Anfrage von einer einzigartigen IP-Adresse stammt, die von jedem Ort auf dem ganzen Globus kommen kann. Keine einzige Adresse taucht zweimal auf, was die Erstellung von Schwarzen Listen unwirksam macht.

Die Geolokalisierung ist ebenso unzuverlässig. Da IP-Adressen so schnell wechseln, ändern sich die Standortdaten von Anfrage zu Anfrage und geben kaum Aufschluss über die Absicht.

IP- und Geolokalisierung haben zwar immer noch einen begrenzten Wert gegen einfache Bedrohungen, die ihre Adressen nicht wechseln. Sie erkennen jedoch nur noch einen schrumpfenden Prozentsatz des feindlichen Datenverkehrs. Für eine wirksame Verteidigung sind tiefergehende, verhaltensbasierte Signale erforderlich statt der Annahme, dass es sich um „gute" oder „schlechte" IPs handelt.

Bis 2025 werden über **60 % der Bots rotierende Proxys und IP-Wechsel nutzen**, um Blockaden zu umgehen.

Die Herausforderung des API-Schutzes

Traditionelle Bot-Erkennungsmethoden wurden in erster Linie für den Webverkehr entwickelt. Heutzutage machen bei vielen Unternehmen mobile Anwendungen und Microservices jedoch einen erheblichen Teil der Netzwerkaktivität aus. Bedrohungsakteure nutzen häufig Reverse Engineering von Anwendungsprogrammierschnittstellen (APIs), indem sie die Kommunikation von mobilen Anwendungen analysieren, um Bots zu programmieren, die das Verhalten legitimer Anwendungen imitieren.

Diese Bots zielen auf anfällige Funktionen wie die Kreditkartenvalidierung, das Ausfüllen von Anmeldedaten, Brute-Force-Anmeldeversuche sowie den Missbrauch von Geschenkkarten und Gutscheincodes ab. Da jede Aktion, die ein legitimer API-Benutzer durchführen kann, auch von Bots automatisiert werden kann, geht der potenzielle finanzielle Schaden pro Monat in die Millionen.

Erschwerend kommt hinzu, dass viele herkömmliche Verfahren zur Bot-Erkennung auf der Überprüfung browserbasierter Umgebungen beruhen, was bei APIs nicht möglich ist. Dies macht herkömmliche Methoden für die Sicherung von API-Endpunkten gegen ausgeklügelte automatisierte Angriffe weitgehend unwirksam.

Leider sind viele der herkömmlichen Methoden zur Bot-Erkennung für den API-Schutz nicht geeignet. So hat ein API-Benutzer beispielsweise keine Webbrowser-Umgebung, die überprüft werden könnte.

57 % der Unternehmen haben in den letzten zwei Jahren **mindestens einen** API-bezogenen Sicherheitsvorfall erlebt.

Fazit

Ältere Bots machen zwar nach wie vor einen beträchtlichen Teil des automatisierten Datenverkehrs aus und können mit herkömmlichen Methoden wirksam aufgespürt werden, doch bleiben diese Ansätze aufgrund ihrer Effizienz und der geringen Rechenkosten ein Kernbestandteil vieler Bot-Management-Lösungen. Da jedoch immer raffiniertere Bots sowohl auf Webanwendungen als auch auf APIs abzielen, reicht es nicht mehr aus, sich ausschließlich auf diese Verfahren zu verlassen. Um diese hochentwickelten Bedrohungen wirksam zu bekämpfen, sind moderne, fortschrittliche Erkennungsmethoden unerlässlich.

Was heute funktioniert

Moderne Bot-Erkennungslösungen verbessern herkömmliche Methoden, indem sie fortschrittliche, proaktive Techniken einsetzen. Während sich klassische Ansätze oft auf passive Metriken wie die Überwachung des Ressourcenverbrauchs und die Beobachtung des Benutzerverhaltens stützen, überprüfen effektivere Lösungen aktiv die Authentizität und Absicht jeder Anfrage.

Diese Techniken ergänzen sich gegenseitig und sollten kombiniert werden, um die Erkennungsgenauigkeit zu maximieren. Link11 nutzt diese Methoden in Kombination mit zusätzlichen proprietären Technologien, um einen umfassenden Schutz zu bieten.

Client-Zertifizierung

Durch die weitverbreitete Verfügbarkeit von Serverzertifikaten von Drittanbietern können Clients überprüfen, ob ihre Verbindung mit einem legitimen Endpunkt besteht. Der nächste Schritt ist die gegenseitige Authentifizierung, bei der die Clients Zertifikate vorlegen, um ihre Identität zu bestätigen. Während dies in Branchen wie FinTech üblich ist, ist die Client-Zertifizierung anderswo noch selten. Link11 bietet eine entsprechende Funktion an und ermutigt zu deren Einsatz, um die Sicherheit zu erhöhen.

Andere Methoden der Kundenauthentifizierung

Zusätzlich zu den Zertifikaten können Kunden auch über native oder mobile Anwendungen mit integrierten Verifizierungsmechanismen authentifiziert werden. Link11 bietet ein SDK für Android und iOS an, das Kunden in ihre eigenen Anwendungen integrieren können. Das SDK signiert die Anwendung, authentifiziert das Gerät und verifiziert die Identität des Benutzers. Die gesamte Kommunikation wird über TLS gesichert und umfasst eine HMAC-Signatur.

Dabei handelt es sich um einen eindeutigen kryptografischen Nachweis pro Sitzung oder Anfrage, der auf mehreren Faktoren wie Zeit, Standort und Umgebung basiert. Dieser Ansatz stellt sicher, dass der Datenverkehr von legitimen Benutzern und nicht von Emulatoren oder Bots stammt. Darüber hinaus profitieren Anwendungen, die das Link11-SDK verwenden, von fortschrittlichen Authentifizierungsmethoden wie der biometrischen Verhaltensprofilierung.

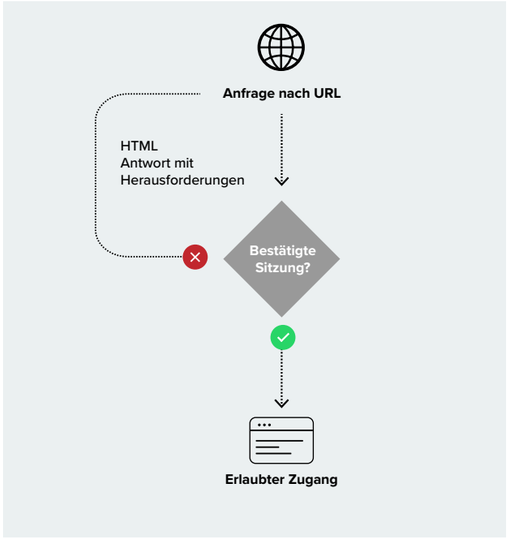
Erweiterte Browser-Verifizierung

Traditionelle Methoden zur Überprüfung von Browserumgebungen sind unwirksam geworden, da moderne Headless-Browser JavaScript vollständig unterstützen. Einfache JavaScript-(JS)-Überprüfungen können Bots nicht mehr zuverlässig von echten Benutzern unterscheiden.

Fortschrittliche Sicherheitslösungen gehen dieses Problem an, indem sie strengere Anforderungen stellen. So kann eine Web Application Firewall (WAF) beispielsweise einen JavaScript-basierten Rechentest durchführen und Browser, die diesen nicht lösen, als „Headless" kennzeichnen. Andere Techniken umfassen die Überprüfung der Fähigkeit des Browsers, Audio oder Bilder darzustellen.

Link11 erweitert diesen Ansatz mit einer Reihe proprietärer Umgebungserkennungsmethoden, die JavaScript-basierte und alternative Techniken kombinieren, um eine zuverlässige Browserüberprüfung zu gewährleisten.

Wie bereits gesehen, sind die traditionellen Methoden zur Überprüfung von Browser-Umgebungen veraltet. Die erste Generation von Headless-Browsern konnte beispielsweise kein JavaScript ausführen. Heute sind die meisten automatisierten Umgebungen jedoch dazu in der Lage. Eine einfache Überprüfung von JavaScript (JS) ist daher nicht mehr effektiv.



UEBA: User and Entity Behavioral Analytics

UEBA steht für „User and Entity Behavior Analytics" (Analyse des Benutzer- und Entitätsverhaltens).
Bei diesem Prozess werden Daten über das Benutzerverhalten in Intrusion-Detection-Systeme (IDS) eingespeist, um Grundlinien für normale Aktivitäten zu erstellen. Das nachfolgende Benutzerverhalten wird dann mit diesen Grundlinien verglichen, um potenzielle Bedrohungen zu identifizieren. UEBA ist kein einzelnes Verfahren, sondern ein breit angelegter Ansatz, dessen Umsetzung zwischen den verschiedenen Sicherheitslösungen stark variiert – von nicht vorhanden über einfach bis hin zu hochentwickelt.

1. Grundlegende UEBA

Auf der grundlegendsten Ebene überwacht UEBA einfache Metriken wie die Tippgeschwindigkeit und Interaktionsmuster. So variieren beispielsweise die Geschwindigkeit und der Rhythmus des menschlichen Tippens, während Bots dazu neigen, lange Zeichenfolgen schnell und mechanisch einzugeben. Auch das mehrmalige Anklicken desselben Bildschirmpixels ohne typische Mausbewegungen kann auf Automatisierung hindeuten.

2. Biometrisches Verhaltensprofiling und maschinelles Lernen

Moderne Bots können menschliches Verhalten mittlerweile sehr gut imitieren und somit einfache UEBA-Systeme umgehen. Um diese fortschrittlichen Bedrohungen abzuwehren, verwendet eine ausgereiftere UEBA maschinelles Lernen, um detaillierte Verhaltensprofile auf Grundlage biometrischer Daten oder messbarer menschlicher Merkmale zu erstellen. Bei diesem Ansatz werden umfassende Datensätze jeder geschützten Anwendungsprogrammierschnittstelle (API) analysiert, darunter:

- Geräte- und Softwaredetails (z. B. Hardware, Bildschirmauflösung, Akkustand, Erweiterungen usw.),
- Benutzerinteraktionen (z. B. Mausbewegungen, Klicks, Bildläufe, Tippgeschwindigkeit),
- Sitzungsmetriken (Anfragemuster, IP-Nutzung, Timing),
- Verbrauchsanalysen (angezeigte Seiten und Verweildauer),
- Anwendungsspezifische Ereignisse und vieles mehr.

Durch die Verarbeitung von Milliarden Anfragen pro Tag identifiziert ML subtile Muster und Beziehungen, die menschlichen Analysten möglicherweise entgehen. Anstatt starre Regeln zu verwenden, weist das System jedem Anfragestellen gewichtete Verhaltenswerte zu. Wenn diese Werte einen Schwellenwert überschreiten, wird der Anfragende markiert und blockiert.

Der Schwerpunkt von UEBA auf der Erkennung von Anomalien unterscheidet sie von herkömmlichen, statischen sowie regelbasierten WAFs. Deshalb haben viele ältere Sicherheitsprodukte diese Funktion nicht.

3. Granulare Profilerstellung

Eine wirksame Verhaltensprofilierung sollte nicht nur ganze Anwendungen, sondern auch einzelne Seiten oder Bildschirme analysieren. Wenn beispielsweise die meisten Benutzer beim ersten Öffnen einer mobilen Anwendung eine Karte vergrößern, könnten Benutzer, die nie zoomen, als verdächtig markiert werden. In ähnlicher Weise könnten Besucher von Einzelhandelsgeschäften als verdächtig eingestuft werden, die typische Seiteninteraktionen überspringen wie z. B. das Scrollen, um Garantien anzuzeigen.

Bei diesen Verhaltensweisen handelt es sich um gewichtete Faktoren, nicht um strenge Regeln. Auf diese Weise kann das System Indikatoren akkumulieren und eine sehr genaue Bot-Erkennung erreichen. Die granulare Profilerstellung erhöht die Robustheit gegenüber Angreifern, da sie sich auf private Analysemuster stützt, die von Bedrohungsakteuren nicht ohne Weiteres nachgeahmt oder nachgebaut werden können.

Des Weiteren deckt maschinelles Lernen (ML) komplexe, nicht offensichtliche Verhaltensmuster auf und verbessert die Erkennung über das hinaus, was eine menschliche Analyse allein erreichen könnte.

Dieser vielschichtige, datengestützte Ansatz macht UEBA zu einem der effektivsten Werkzeuge, um Bots von legitimen Nutzern in der heutigen komplexen Bedrohungslandschaft zu unterscheiden.

Der globale UEBA-Markt wird von 2,39 Milliarden US-Dollar im Jahr 2024 auf 3,21 Milliarden US-Dollar im Jahr 2025 wachsen – das entspricht einer jährlichen Wachstumsrate (CAGR) von 34,3 %.

Moderne Bot-Erkennung

Herkömmliche Methoden zur Verfolgung von Anfragern anhand von IP-Adressen und Geolokalisierung sind nicht mehr zuverlässig. Zentrale Grundlage für die Erkennung muss nun die Identität und – noch wichtiger – das Verhalten des Users sein. Die Verhaltensanalyse ist von entscheidender Bedeutung, da selbst verifizierte menschliche Benutzer böswillig handeln können. Allerdings weichen alle feindlichen Akteure, ob Bots oder Menschen, irgendwann von legitimen Verhaltensmustern ab. Die Erstellung von Verhaltensprofilen dient dazu, diese Abweichungen zu erkennen.

Die Grenzen der Bot-Erkennung

Da Bots immer raffinierter werden, müssen Sicherheitslösungen kontinuierlich weiterentwickelt werden. Zu den wichtigsten Bereichen für eine kontinuierliche Verbesserung gehören:

- Optimierung der Leistung,
- Optimierung der Geschäftsergebnisse,
- Integration neuer Datenquellen.

Die Methoden zur Bot-Erkennung haben sich erheblich weiterentwickelt und lassen sich im Allgemeinen in vier Kategorien einteilen:

1. Statische Regeln,
2. Statistische Ansätze,
3. Maschinelles Lernen (ML),
4. Hybride Ansätze, die ML und statistische Analyse kombinieren.

This spectrum ranges from fast, lightweight, and less precise techniques, like static rules, to more complex and resource-intensive methods, like ML. For effective bot detection, an IDS should blend these approaches, using simpler methods for rapid preliminary detection and advanced analytics to ensure high accuracy and reduce false positives.

1. Statische Regeln

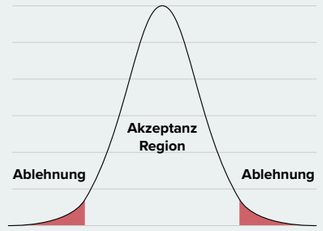
Statische Regelsätze sind die einfachste Form der Bot-Erkennung. Zu ihnen zählen Zugriffskontrolllisten (ACLs), Beschränkungen der Größe oder des Zeitpunkts von Anfragen, IP-Blacklists und ähnliche Maßnahmen. Da nur eine minimale Verarbeitung erforderlich ist, sind statische Regeln schnell und ressourcenschonend. Moderne Bots können diese Kontrollen jedoch leicht umgehen, indem sie beispielsweise IP-Adressen rotieren, die Anfragerate verlangsamen oder andere Taktiken anwenden.

Ein weiterer Nachteil besteht darin, dass zu strenge statische Regeln oft zu sogenannten „False Positives" (FPs) führen und unbeabsichtigt legitime Benutzer blockieren. So kann beispielsweise die Begrenzung der Anzahl von Anfragen pro Sitzung dazu führen, dass Benutzer mit längeren oder aktiveren Sitzungen fälschlicherweise blockiert werden.

Trotz dieser Einschränkungen sind statische Regeln nach wie vor nützlich. Mäßig strenge Regelsätze können eine beträchtliche Anzahl feindlicher Bots abfangen und gleichzeitig die Rate der Falschmeldungen niedrig halten. Bei leicht zu erkennenden Bedrohungen reduziert die Verwendung statischer Regeln als erste Verteidigungslinie den Bedarf an umfangreichen Berechnungen.

2. Statistische Ansätze

Die statistische Analyse des Datenverkehrs ist zwar aufwendiger als die Anwendung statischer Regeln, dennoch ist sie relativ einfach zu handhaben. Gängige statistische Tests wie der t-Test nach Student, der Z-Test und die Varianzanalyse (ANOVA) helfen bei der Unterscheidung zwischen normalem und abnormalem Verhalten. Dazu werden Standardabweichungen berechnet und Schwellenwerte festgelegt.



Statistische Methoden wie der Z-Test bieten klare, gut verstandene Analysemethoden zur Ermittlung von Anomalien innerhalb eines Datensatzes.

In der Regel werden diese Analysen in Echtzeit an aggregierten Daten aus Verkehrsprotokollen und nicht an einzelnen Anfragen durchgeführt. Die Ergebnisse können verwendet werden, um „lokale" oder benutzerdefinierte Regeln zu erstellen, die in Echtzeit ein Intrusion-Detection-System (IDS) neben statischen Regeln durchsetzt. Idealerweise aktualisiert das IDS diese Regeln häufig, um sich mit minimaler Verzögerung an die sich entwickelnden Verkehrsmuster anzupassen.

3. Maschinelles Lernen (ML)

Da Bots immer raffinierter werden, wird die Anwendung von Machine Learning (ML) zur Bot-Erkennung immer notwendiger. Obwohl einige Lösungen noch nicht so weit sind, ist ML unerlässlich, um Bots zu erkennen, die legitimes menschliches Verhalten imitieren und sich der statischen oder statistischen Erkennung entziehen.

Frühere ML-Modelle konzentrierten sich auf die Erkennung von Anomalien und Ausreißern. Dazu wurden Methoden wie RANSAC (Random Sample Consensus) verwendet, die die Modellparameter schätzt und Ausreißer ignoriert. Die heutigen Bots sind jedoch subtiler und erfordern eine komplexere Verhaltensanalyse.

Wie die statistischen Methoden verwendet auch ML aggregierte Daten, um Erkennungsregeln zu entwickeln, die in Echtzeit angewendet werden. ML erfordert jedoch größere Datensätze – etwa zehnmal mehr Beobachtungen pro Merkmal – und ist schwieriger zu konfigurieren. Die Auswahl der richtigen Merkmale und das Verständnis der Datenverteilung erfordern spezielle Fachkenntnisse, was für manche Benutzer eine Herausforderung darstellen kann.

4. Kombination von ML und statistischen Verfahren

Keine Erkennungsmethode ist perfekt oder universell anwendbar. Selbst theoretisch ideale Techniken würden von Angreifern, die neue Umgehungsstrategien entwickeln, schnell umgangen werden.

Daher kombinieren in der Praxis die effektivsten Bot-Erkennungslösungen statische Regeln, statistische Analysen und maschinelles Lernen (ML). Einfache Bots können mit leichtgewichtigen Methoden schnell blockiert werden, während fortschrittlichere Bedrohungen durch tiefergreifende Analysen identifiziert werden. Die größte Herausforderung für IDS-Anbieter besteht darin, flexible Plattformen bereitzustellen, die mehrere Erkennungsmethoden nahtlos integrieren und über benutzerfreundliche Schnittstellen verfügen. Dadurch wird der Bedarf an profunden ML-Kenntnissen minimiert.

Optimierung für Geschäftsergebnisse

Bei der Evaluierung einer Bot-Erkennungslösung ist in der Regel die Genauigkeit das erste Kriterium, das einem in den Sinn kommt. Sie lässt sich einfach berechnen: Man teilt die Anzahl der korrekt identifizierten Anfragen durch die Gesamtzahl der Anfragen. Die Genauigkeit allein ist zwar nützlich, sagt aber noch nicht alles aus.

$$\textit{Genauigkeit} = \frac{(TP + TN)}{(TP + FP + FN + TN)}$$

(Dabei stehen TP und TN für True Positive bzw. True Negative).

Es ist zwar verlockend, einen „perfekten" Erkennungsalgorithmus anzustreben, der in allen Szenarien die höchstmögliche Genauigkeit liefert, doch in der Praxis ist dies nicht umsetzbar. In Wirklichkeit gibt es jedoch keinen solchen universellen Algorithmus. Die Bot-Erkennung ist stark kontextspezifisch. Ein Ansatz, der auf einen bestimmten Anwendungsfall zugeschnitten ist, kann in einem anderen schlecht abschneiden. Was für eine E-Commerce-Plattform gut funktioniert, ist für eine Banken-API vielleicht nicht ideal – und umgekehrt.

Außerdem kann die Genauigkeit allein irreführend sein. Eine hohe Gesamtgenauigkeitsrate kann kritische Fehler verdecken. Besonders wichtig sind zwei Fehlerarten: falsch-positive (FP) und falsch-negative (FN).

- FPs treten auf, wenn legitime Benutzer fälschlicherweise blockiert werden.
- FNs entstehen, wenn böswillige Anfragen fälschlicherweise zugelassen werden.

Beide Fehlerarten sind problematisch, jedoch nicht in gleichem Maße. Ihre Auswirkungen hängen vom jeweiligen Geschäftskontext ab. Im Einzelhandel können FPs beispielsweise direkt zu Umsatzeinbußen führen, wenn Kunden daran gehindert werden, ihre Einkäufe abzuschließen. Im Gegensatz dazu kann ein falsch-negatives Ergebnis in einem stark regulierten Sektor wie dem Finanz- oder Gesundheitswesen zu einer Datenschutzverletzung führen, die Geldstrafen, Gerichtsverfahren oder Rufschädigung nach sich zieht.

Daher hat das effektivste Bot-Erkennungssystem nicht unbedingt die höchste Genauigkeit, sondern es stimmt vielmehr am besten mit der Risikotoleranz und den geschäftlichen Prioritäten des Unternehmens überein. Manchmal ist eine etwas geringere Genauigkeit mit weniger falsch-negativen Ergebnissen vorzuziehen, auch wenn dies bedeutet, dass eine höhere Rate von falsch-positiven Ergebnissen in Kauf genommen werden muss – je nachdem, welcher Fehler die größeren Kosten verursacht.

Um die Ergebnisse zu optimieren, müssen Intrusion-Detection-Systeme (IDS) anpassungsfähig sein. Sie sollten Organisationen in die Lage versetzen,

- Prioritäten bei der Minimierung von falsch-positiven oder falsch-negativen Ergebnissen je nach ihren spezifischen Anforderungen zu setzen,
- Erkennungsstrategien pro Anwendung oder Endpunkt abzustimmen sowie Leistung und Schutz dynamisch auszugleichen.

Leider bieten die meisten älteren Web-Sicherheitsprodukte nur begrenzte Anpassungsmöglichkeiten. Die Feinabstimmung der Erkennung erfordert in der Regel die Offenlegung interner Erkennungsparameter sowie die Darstellung von Leistungsrückmeldungen auf eine benutzerfreundliche Weise, die den Benutzer nicht mit technischer Komplexität überfordert. Die Entwicklung einer solchen Schnittstelle ist zwar eine Herausforderung, aber notwendig. Da sich die Bot-Taktiken weiterentwickeln und der regulatorische und kommerzielle Druck zunimmt, wird die Anpassung von IDS unerlässlich.

Die Herausforderung in der Praxis lautet daher: Wie können Benutzer wissen, ob ihr IDS falsch-positive (FP) oder falsch-negative (FN) Fehler macht? Schließlich kann das IDS selbst nicht immer zwischen richtigen und falschen Entscheidungen unterscheiden. Diese Frage führt uns zu unserem nächsten Thema.

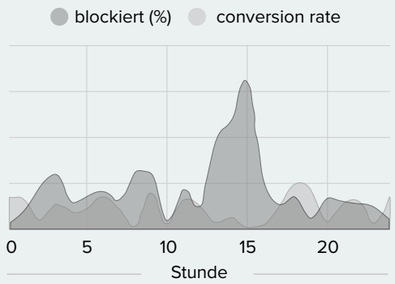
Nutzung neuer Datenquellen

Traditionell konzentriert sich die Bot-Erkennung auf die Analyse des eingehenden Datenverkehrs, indem Anfrage-Header, IP-Adressen, Verhalten und andere technische Signale untersucht werden. Verkehrsdaten sind jedoch nicht die einzige Quelle für wertvolle Erkenntnisse. Vorausschauende Sicherheitsstrategien beziehen zunehmend Metriken der Anwendungsebene, insbesondere die Conversion Rate (CR), in ihren Erkennungs- und Optimierungsprozess ein.

CR bezieht sich auf den Prozentsatz der Besucher oder Anfragen, die zu einem definierten Ziel führen, wie z. B. einen Kauf tätigen, ein Formular ausfüllen, eine Datei herunterladen oder eine andere wichtige Aktion innerhalb der Anwendung ausführen.

Bots führen diese zielgerichteten Verhaltensweisen im Allgemeinen nicht aus. Wenn ein Intrusion Detection System (IDS) Bots korrekt identifiziert und herausfiltert, sollten die Konversionsraten konstant bleiben, da es unwahrscheinlich ist, dass diese Besucher von vornherein konvertieren würden.

Blockierte Anfragen vs. Conversion Rate



Vergleich der blockierten Anfragen mit der Conversion Rate. Bei Stunde 15, als mehr Anfragen blockiert wurden, sank die Konvertierungsrate auf nahezu Null. Dies deutet darauf hin, dass das IDS wahrscheinlich eine hohe Anzahl von FPs erzeugt.

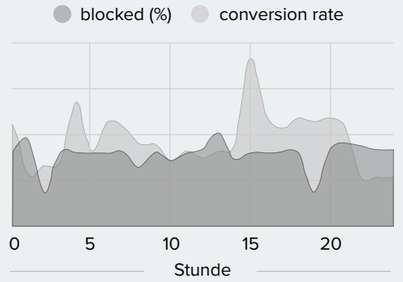
Wenn das IDS jedoch legitime Benutzer blockiert (d. h. Fehlalarme erzeugt), können diese ihre beabsichtigten Aktionen nicht mehr durchführen. Dies führt zu einem Rückgang der Konversionsrate und kann ein Zeichen dafür sein, dass die Erkennungsregeln zu aggressiv sind.

Darin liegt eine Chance. Die Konversionsrate kann als Feedback-Mechanismus für die Anpassung des IDS dienen. Ein Beispiel:

- Wenn neue Erkennungsregeln oder Algorithmus-Updates zu einem Rückgang der Konversionsrate führen, kann dies ein Hinweis auf eine Zunahme von Fehlalarmen sein. Eine sofortige Überprüfung wäre dann angebracht.
- Wird hingegen mehr Datenverkehr blockiert, während die Konversionsrate konstant bleibt (oder sich verbessert), deutet dies darauf hin, dass hauptsächlich nicht konvertierende Bots gefiltert wurden und die Änderungen wirksam waren.

Beachten Sie, dass dies voraussetzt, dass die Conversion Rate anhand aller eingehenden Anfragen berechnet wird, einschließlich derjenigen, die später als Bots gekennzeichnet werden. Einige Systeme berechnen die CR nur für Besucher, die das Bot-Screening bestanden haben. In diesem Fall wirken sich falsch-negative Ergebnisse (Bots, die fälschlicherweise als Menschen identifiziert werden) auf die CR aus und die Feedbackschleife wird komplexer. In jedem Fall liefert das Conversion Tracking verwertbare Erkenntnisse.

Blockierte Anfragen vs. Conversion Rate



Vergleich der blockierten Anfragen mit der Conversion Rate. Es scheint nur eine geringe Korrelation zwischen den blockierten/abgelehnten Anfragen und der CR zu geben. Die Schwankungen der CR sind also eher auf andere Faktoren zurückzuführen (z. B. normale Schwankungen im Käuferverhalten im Laufe des Tages) als auf FPs und FNs.

Neben der Konversionsrate können auch andere Anwendungsanalysen von Nutzen sein. Durch die Integration des IDS mit Analyseplattformen wie Google Analytics ist eine tiefere Korrelation zwischen Erkennungsereignissen und Benutzerverhaltensmustern möglich. Dies wiederum kann dabei helfen, die FP- und FN-Raten genauer einzuschätzen, was das IDS allein nicht immer leisten kann.

Zusammenfassung:

Netzwerkverkehrsprotokolle sind nicht mehr die einzige Informationsquelle für die Bot-Erkennung. Durch die Kombination von Verhaltensprofilen, Konversionsmetriken und umfassenderen Analysen können Unternehmen die Effektivität ihrer Intrusion-Detection-Systeme besser bewerten, Fehlalarme minimieren und somit sowohl die Sicherheit als auch die Unternehmensleistung optimieren.

Fazit

Der Schutz vor bösartigen Bots ist für jedes Unternehmen mit relevanter Online-Präsenz längst keine freiwillige Option mehr, sondern eine strategische Notwendigkeit. Im Durchschnitt bestehen fast 40 % des eingehenden Web-Traffics aus automatisierten, schädlichen Aktivitäten. Die konkreten Bedrohungsszenarien variieren zwar je nach Branche, die Folgen sind jedoch ähnlich: eingeschränkte Performance, verfälschte Analysen, Datenverlust und Umsatzeinbußen.

Trotz der zunehmenden Raffinesse heutiger Angriffe basieren viele Intrusion-Detection-Systeme weiterhin auf veralteten Methoden wie Blacklists, statischem Rate Limiting, regelbasierten Signaturen oder klassischen CAPTCHAs. Diese Herangehensweisen sind modernen Bots oft nicht mehr gewachsen, da sie gezielt umgangen werden.

Um heutigen und künftigen Bedrohungen wirksam zu begegnen, müssen Erkennungsmethoden weiterentwickelt werden. Hier kommen Technologien wie UEBA (User and Entity Behavior Analytics), maschinelles Lernen und biometrisches Verhaltensprofiling ins Spiel. Sie ermöglichen eine hochgranulare Analyse des Nutzerverhaltens bis hinunter auf die Ebene einzelner Sitzungen, Seiten oder Interaktionen und helfen dabei, selbst sehr gut getarnte Bots zuverlässig von echten Nutzern zu unterscheiden.

Diese Technologien sind im Jahr 2025 keine Zukunftsmusik mehr:

- UEBA ist in vielen mittleren und großen Unternehmen fester Bestandteil der Sicherheitsarchitektur, insbesondere in regulierten Branchen wie dem Finanzwesen, der Energiewirtschaft oder bei Behörden.
- Maschinelles Lernen wird von über 70 % der Unternehmen eingesetzt, um in Echtzeit Anomalien, Angriffe und Zero-Day-Bedrohungen zu erkennen – zunehmend auch in Verbindung mit SIEM- und SASE-Systemen.
- Biometrisches Profiling, etwa über das Tippverhalten oder die Mausbewegungen, gewinnt an Bedeutung, um Menschen zuverlässig von Bots zu unterscheiden – insbesondere in sicherheitskritischen Anwendungen wie dem Online-Banking oder dem E-Commerce.

Die effektivsten IDS-Lösungen kombinieren diese Verfahren. Sie haben eine höhere Erkennungsrate, minimieren Fehlalarme und passen sich flexibel an neue Angriffsmuster an. Gleichzeitig müssen sie anpassbar sein, um auf die individuellen Risiken, Geschäftsmodelle und Toleranzgrenzen einer Organisation abgestimmt werden zu können. Dabei kann eine maßgeschneiderte Erkennung, die beispielsweise bewusst eine höhere False-Negative-Rate in Kauf nimmt, wirtschaftlich sinnvoller sein als eine maximal präzise, aber kundenfeindliche Konfiguration.

Wie im vorangehenden Abschnitt erläutert, lassen sich IDS-Strategien heute sogar über Business-KPIs wie Conversion Rates (CR) steuern. Eine sinkende CR kann ein Indikator für zu viele FPs sein und somit einen konkreten Impuls darstellen, um die Detektionslogik gezielt anzupassen. Solche Feedbackschleifen stärken nicht nur die Sicherheit, sondern verbessern auch die Betriebseffizienz.

Link11 geht diesen Weg aktiv mit. Bereits heute integrieren wir die neuesten Technologien in unsere Plattform – mit Fokus auf Benutzerfreundlichkeit, Flexibilität und Echtzeit-Transparenz. Gleichzeitig treiben wir die Erforschung neuer Methoden und Zukunftstrends weiter voran, um der dynamischen Bedrohungslage auch künftig einen Schritt voraus zu sein.

Denn effektiver Bot-Schutz bedeutet heute: verhaltensbasiert, adaptiv und auf konkrete Geschäftsziele ausgerichtet.

Sources

2025 Bad Bot Report | Resource Library
https://cropink.com/ecommerce-fraud-statistics
https://ec.europa.eu/eurostat/web/products-eurostat-news/w/ddn-20250220-3
European e-commerce: Report + 2025 insights - E-commerce Germany News
World Password Day - Global Survey 2025 | Bitwarden
https://www.mind-verse.de/post/ki-fuer-bot-detection-zukunft-cybersicherheit
https://latesthackingnews.com/2025/01/03/data-scraping-in-2025-trends-tools-and-best-practices/
https://hackernoon.com/web-scraping-in-2025-staying-on-track-with-new-rules
https://www.indusface.com/blog/key-cybersecurity-statistics/
https://www.getastra.com/blog/security-audit/cyber-security-vulnerability-statistics/
https://www.helpnetsecurity.com/2025/04/30/edgescan-2025-vulnerability-statistics/
https://www.edgescan.com/stats-report/
https://www.kim-weinand.de/ad-fraud-report-2025/
https://www.statista.com/forecasts/1280009/cost-cybercrime-worldwide
https://prosopo.io/blog/what-is-the-future-of-captcha-and-online-privacy/
Botting in 2025: Why CAPTCHA-Solving Services Are No Longer Optional – Blog
https://clickpatrol.com/does-captcha-stop-bots-the-effectiveness-and-fut/
https://securityboulevard.com/2025/03/captchas-demise-multi-modal-ai-is-breaking-traditional-bot-management/
reCAPTCHA v2 vs v3: Effective Bot Protection? [2025 Update]
http://azapi.ai/blog/best-captcha-solvers/
https://www.cybersecurity-insiders.com/2025-global-state-of-api-security-report-new-data-shows-api-breaches-continue-to-rise-due-to-fraud-bot-attacks-and-genai-risks/
https://www.thebusinessresearchcompany.com/market-insights/user-and-entity-behavior-analytics-market-overview-2025
https://www.thebusinessresearchcompany.com/report/user-and-entity-behavior-analytics-global-market-report

Hauptsitz

Link11
Lindleystr. 12
60314 Frankfurt