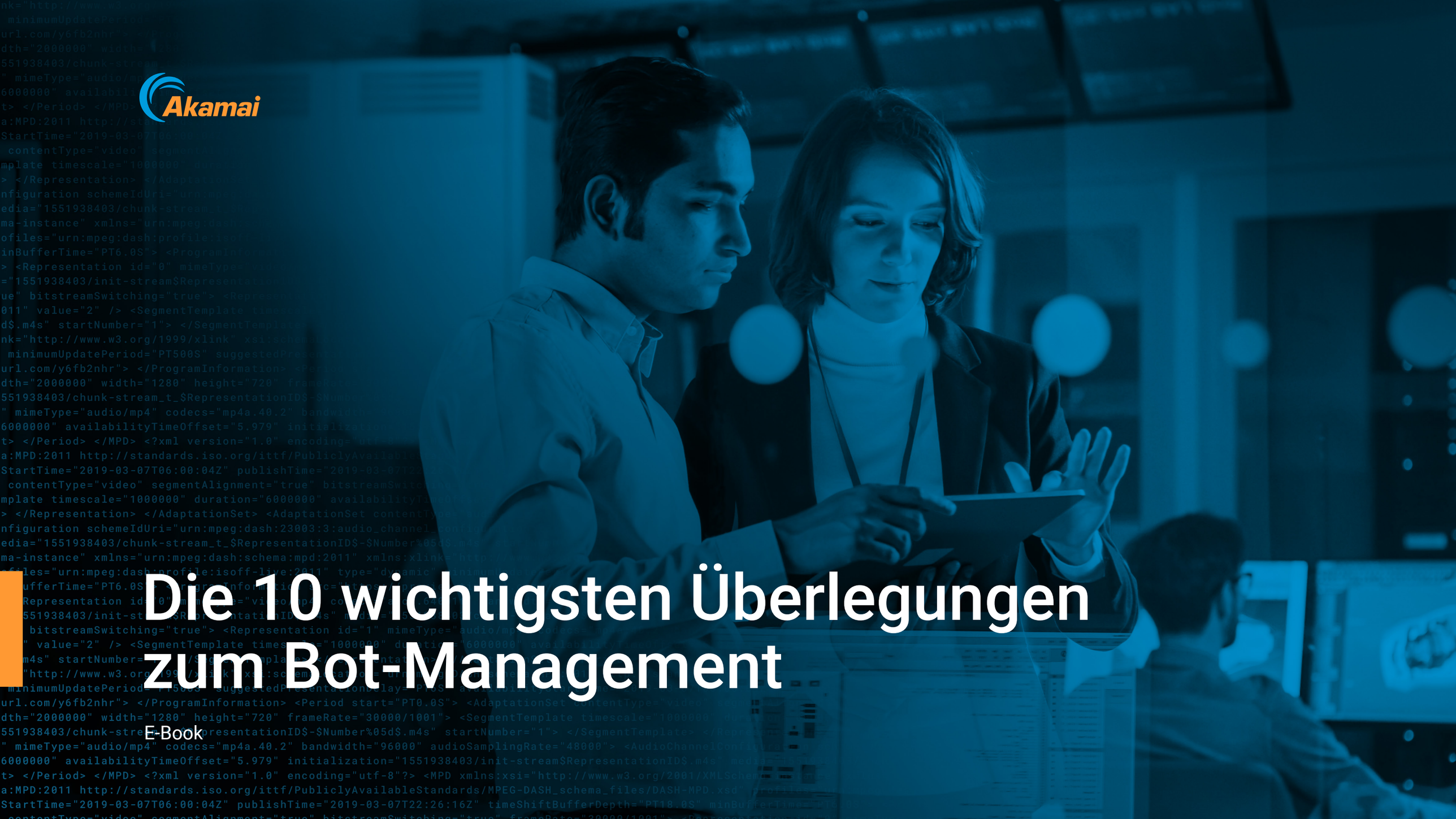

Die 10 wichtigsten Überlegungen zum Bot-Management

E-Book

INHALTSVERZEICHNIS

Einführung

Sie fragen sich, wie groß das Problem mit Bots inzwischen ist? Versuchen Sie mal, ein Ticket für Taylor Swift oder ein neues Paar Air Jordans abzustauben. Und das sind bloß Hype-Events. Bots breiten sich in allen Branchen immer mehr aus und werden immer gefährlicher.

Wer hier nach Antworten sucht, hat zusätzlich das Problem, dass die Spielregeln beim Bot-Management sich geändert haben. In Wahrheit haben sie sich immer schon verändert. Bot-Management wird oft als Rüstungswettlauf oder als Katz-und-Maus-Spiel beschrieben, bei dem Unternehmen Abwehrmechanismen aufbauen und Bot-Entwickler immer neue Wege finden, sie zu umgehen. Aber jetzt sind es nicht mehr nur die Bots selbst, die sich weiterentwickeln. Auch das Umfeld um sie herum entwickelt sich weiter. So haben Unternehmen es nicht mehr nur mit einzelnen Akteuren oder koordinierten Gruppen zu tun. Inzwischen ist jetzt möglich, einen Bot für die Woche zu mieten, als würde man eine Unterkunft bei Airbnb buchen. Ebenso können Sicherheitslösungen Bots nicht einfach in gute und schlechte Bots kategorisieren. Zu viele Bots bewegen sich inzwischen in einer Grauzone.

Diese Entwicklung von Bots und ihrer Umgebung hat die Auswahl von Bot-Management-Software schwieriger denn je gemacht. Es reicht nicht zu wissen, was gegen die Bots von gestern effektiv war. Man muss auch herausfinden, was gegen die Bots von heute und morgen wirkt.

Dieser Leitfaden behandelt einige der wichtigsten Überlegungen für Käufer, die eine Bot-Management-Software suchen. Nutzen Sie ihn, um sich ein klareres Bild zu verschaffen und eine fundierte Kaufentscheidung zu treffen.

1 Umfassende Expertise

Zu den wesentlichen Aufgaben von Bot-Management-Lösungen gehört es, Bots zu erkennen. Mit anderen Worten: Sie suchen nach Anzeichen für Automatisierung und anderen Indikatoren, dass der Anfordernde kein Mensch ist. Doch Bots haben sich weiterentwickelt und sind raffinierter und damit auch spezieller geworden. Bots werden inzwischen gezielt für bestimmte Zwecke konzipiert. Beispiele hierfür sind das Abgreifen von Inhalten Ihrer Website, das Horten von Bestandsartikeln während Hype-Events und das Credential Stuffing für die Übernahme Ihrer Kundenkonten und andere Anwendungsfälle. Erkennungsmethoden für eine bestimmte Art von spezialisierten Bots erkennen häufig die anderen Arten nicht. Sie müssen wissen, ob der Anbieter die spezifischen Bots, mit denen Sie konfrontiert sind, stoppen kann, und nicht nur die einfachen, unspezifischen Bots.

Überlegungen:

- Verfügt der Anbieter über spezielle, auf geschäftlichen Anwendungsfällen basierende Erkennungstechnologien für Bots?
- Kann der Anbieter sein Know-how in Bezug auf Ihr spezifisches Bot-Problem nachweisen?
- Wie viele der anderen Kunden des Anbieters haben dieselben Probleme? Profitieren Sie von dem, was der Anbieter von diesen Kunden gelernt hat?
- Offeriert der Anbieter Berichte, Services oder andere Funktionen, die Ihren Kampf gegen spezialisierte, feindliche Bots weiter unterstützen?

2 Informationsgewinnung

Eine Bot-Management-Lösung ist nur so gut wie ihre Fähigkeit, die Eigenschaften der von ihr überwachten Bots zu erkennen. Zwar behaupten manche Anbieter, 99 % der Bots zu erkennen. Doch es ist unmöglich, Effektivität objektiv zu messen. Bots ändern sich ständig. Ein Bot, den Sie gestern erfasst haben, hat wahrscheinlich heute schon gelernt, wie er dieser Erkennung entgehen kann. Ein besseres Kriterium für die Bewertung von Bot-Management-Tools ist, welche Daten der Anbieter seinen Bot-Erkennungsfunktionen zugrunde legt. Sie benötigen eine Lösung, die die ausgefeiltesten Bots (nicht nur die üblichen Verdächtigen) erkennt und Daten aus dem größten Datensatz bezieht. Beachten Sie, dass viele auf künstlicher Intelligenz (KI) und Machine Learning (ML) beruhende Tools Open-Source-Lösungen sind. Daher werden die Datenmenge, die Sauberkeit der Daten und die Geschwindigkeit, mit der die Lösung die Daten in die Algorithmen speist, bei der Bewertung der KI- oder ML-Qualität der betreffenden Lösung nicht ausreichend berücksichtigt. Die Erkenntnisse sollten domainübergreifend Vertrauensindikatoren und Risikobewertungen für jeden Login beinhalten. Darüber hinaus müssen effektive Lösungen einen mehrgleisigen Ansatz für die Bot-Erkennung verwenden und die neuesten Methoden nutzen.

Überlegungen:

- Bitten Sie den Anbieter um nähere Informationen darüber, wie er seine Bot-Erkennungsfunktionen mit Daten speist. Anbieter mit großen Kunden, die für Angreifer attraktiv sind, werden über mehr Erfahrung und umfassendere Datensätze verfügen, auf denen sie ihre Fähigkeiten aufbauen können. Hier geht es zum Beispiel um die Bewertung der richtigen Risiko- und Vertrauenssignale oder um die Erkennung eine größeren Zahl von Geräteanomalien. Bei mangelnder Transparenz ist Vorsicht geboten.

- Verwendet der Anbieter KI/ML zur Unterstützung der Lösung? Wie ausgefeilt sind diese Modelle? Ebenso wichtig ist: Wie viele Daten fließen in diese Modelle ein? Angreifer setzen definitiv auf KI. Sie sollten es ebenfalls tun.

- KI reicht jedoch nicht aus. Verfügt der Anbieter über ein Team qualifizierter Experten wie Sicherheitsforscher und Analysten für Bedrohungsinformationen, die ständig nach neuartigen Angriffsmethoden suchen und Hacker-Communitys überwachen, um sicherzustellen, dass Sie immer einen Schritt voraus sind?

3 Zuverlässiger Schutz

Wenn Sie einen raffinierten Bot blockieren, verschwindet er nicht dauerhaft. Er kommt immer wieder zurück – in mutierter Form, um Ihrer Erkennung zu entgehen. Viele Bot-Management-Lösungen können die Bots (oder zumindest einige von ihnen) gleich erkennen, wenn sie zum ersten Mal auftauchen. Sie verlieren jedoch ihre Effektivität, sobald die Bots mutieren. Akamai hat Bots beobachtet, die innerhalb weniger Stunden mutieren. Herkömmliche Entwicklungszyklen sind zu langsam, um hier mithalten zu können. Stellen Sie sicher, dass die von Ihnen gewählte Lösung im Laufe der Zeit lernt und sich weiterentwickelt, vorzugsweise mit maschinellem Lernen. Dazu gehört präventiver Schutz gegen Angreifer, die an Informationen gelangen wollen, mit denen sie Ihre Abwehrmaßnahmen umgehen können.

Überlegungen:

- Suchen Sie nach Lösungen mit den fortschrittlichsten Bot-Erkennungstechnologien, wie zum Beispiel die Analyse des Nutzerverhaltens und kundenspezifische Lernmodelle. Solche Lösungen erfüllen länger ihren Zweck, selbst wenn die Bots mutieren.
- Finden Sie heraus, ob die Lösung defensive Taktiken wie JavaScript-Verschleierung umfasst. Solche Lösungen machen es Angreifern schwerer, Bots rückzuentwickeln, die sich an Ihren Abwehrmaßnahmen vorbeischleichen können.
- Fordern Sie Nachweise oder Referenzen von anderen Kunden an, die sich für die entsprechende Lösung entschieden haben. So können Sie herausfinden, ob sie auch nach einiger Zeit noch effektiv funktioniert.

4 False Positives und False Negatives

Wenn eine Bot-Management-Lösung meldet, dass sie einen Bot blockiert hat, wie können Sie sich sicher sein, dass das System keinen legitimen Nutzer blockiert hat? Viele Anbieter gehen leichtfertig mit False Positives um. Wenn es ihnen an einer Lösung fehlt, die Bots anhand jeder Erkennung bewertet, sind sie möglicherweise nicht in der Lage, graue Bots zu erkennen. Das führt zu binären Ja/Nein-Entscheidungen. Diese Anbieter zeigen Kunden gerne, dass sie viele „Bots“ blockiert haben, selbst wenn ihre False-Positive-Rate hoch ist. Das bedeutet, dass sie Bots stoppen, aber auch gültigen Traffic – Menschen oder „gute“ Bots, die für Ihr Unternehmen wertvoll sind. Andererseits klingt eine niedrige False-Negative-Rate gut, bis Sie feststellen, dass die False-Negative-Rate so niedrig ist, weil der Anbieter die Gesamteffektivität der Lösung reduzieren musste, um sicherzustellen, dass sie keine menschlichen Nutzer blockiert. Und dann lässt er Bots durch, die nicht passieren dürfen. Sie sollten bösartige Bots blockieren, ohne Hindernisse für Ihr Geschäft aufzubauen. Gleichzeitig sollten Sie aber auch Ihren Schutz nicht einschränken. Sie müssen Ihrem Technologiepartner vertrauen und darauf bauen können, dass er Wert auf Präzision legt und die Auswirkungen von False Positives und False Negatives versteht und berücksichtigt.

Überlegungen:

- Überlässt der Anbieter die Feineinstellungen der Erkennungsregeln für False Positives/Negatives Ihnen, oder investiert er in Funktionen und Services, um eng mit Ihnen zusammenzuarbeiten?
- Lernt die Lösung aus den Trafficmustern über Websites hinweg und optimiert sie sich automatisch selbst, sodass sich die Belastung für Ihr Team verringert?
- Schlägt der Anbieter statt anderer Challenge-Aktionen die Verwendung eines CAPTCHA vor? Hierbei handelt es sich oft um ein verräterisches Anzeichen. Nutzer mögen sie hassen, doch für den Anbieter ist es deutlich leichter, CAPTCHAS zu verwenden, als die Regeln für die Minimierung von False Positives einzustellen.
- Werden Ihnen Gründe angegeben, warum die Lösung eine Anfrage als Bot-Anfrage kennzeichnet? Oder ist die Lösung eine Blackbox? Entscheiden Sie sich für eine Lösung, mit der Sie die ergriffenen Maßnahmen mit fein abgestufter Transparenz überprüfen können. Die Lösung sollte auch die Möglichkeit bieten, Änderungen an Ihren Einstellungen vor der Umsetzung zu visualisieren.

5 Flexible Maßnahmen

Man sollte denken, es ginge allein darum, schlechte Bots zu blockieren und gute durchzulassen. Aber das Umfeld ist heute sehr viel komplexer geworden. Viele Bot-Betreiber haben gelernt, ihre Risikosignale so weit zu senken, dass sich ihre Bots in einer Grauzone bewegen. Schließlich wissen sie, dass die meisten Unternehmen eher riskieren, einen schlechten Bot einzuschleusen, als einen legitimen Nutzer zu blockieren. Ihre Lösung sollte eine Reihe von intelligenten Aktionen ermöglichen, damit Sie über das Blockieren oder Erlauben hinaus die Option für Challenge-Aktionen wie kryptografische Sicherheitsabfragen und Step-up-MFA haben. Außerdem sollte Ihre Lösung auch Aktionen für den Umgang mit anderen Szenarios wie zum Beispiel guten Bots umfassen. Vielleicht möchten Sie Ihre Partner-Bots in Zeiten mit hohem Traffic verlangsamen und diese Bots in Zeiten mit geringem Traffic sofort durchlassen. Sie können auch verschiedene Aktionen für Bots derselben bekannten Kategorie auswählen. Wenn Sie beispielsweise ein Einzelhändler sind, können Sie die beliebtesten Coupon-Bots Ihre Website überprüfen lassen, während Sie andere blockieren, mit denen Sie keine Geschäfte tätigen möchten. Sie benötigen eine Reihe flexibler Maßnahmen, die Sie je nach Auswirkungen auf Ihr Geschäft und auf die IT für die verschiedenen Bot-Typen anwenden können – insbesondere, wenn diese Auswirkungen abhängig von Standort, Tageszeit oder Saison variieren. Darüber hinaus brauchen Sie eine Lösung, die nicht einfach alle Bots blockiert (und ihnen dadurch beibringt, die Ausweichtaktik zu ändern). Vielmehr muss die Lösung Blockaden aufbauen, die den Angreifern das Leben schwerer und teurer macht.

Überlegungen:

- Können Sie mit der Lösung unterschiedliche Kategorien von Bot-Typen festlegen, oder gibt es nur „gut“ und „schlecht“? Kann sie auch verschiedene Aktionen für Bots in derselben Kategorie erstellen, wie Suchmaschinen oder Finanzaggregatoren?
- Welche Arten von bedingten Aktionen unterstützt die Lösung? Unterstützt sie fortschrittliche Funktionen wie Slow Content oder alternative Inhalte, mit denen Sie Ihren Traffic besser kontrollieren können? Umfasst sie Aktionen wie eine kryptografische Sicherheitsabfrage?
- Wie flexibel ist die Lösung bei der Verwaltung der Vielfalt an Bots? Ist sie nur ein weiterer Hammer im Werkzeugkasten, oder kann sie basierend auf Uhrzeit, Trafficprozentsatz oder URL die nötigen Maßnahmen präzise anwenden?
- Kann die Lösung ressourcenintensive Probleme einbauen, die für den Bot-Betreiber teuer werden und Angriffe mit hohem Anfragevolumen über eine bloße „harte“ 403 hinaus verlangsamen?

6 Bereitstellung

Bei einer jeden Bot-Management-Lösung ist danach zu fragen, wie lange die Einführung der Lösung dauert und wie schnell sie sich modifizieren lässt. Das sind zentrale Aspekte. Käufer sollten bei Lösungen, die Änderungen an ihren vorhandenen Anwendungen erfordern oder die Anwendungsperformance beeinträchtigen, auf der Hut sein. Verzögerungen bei der Bereitstellung können kostspielig sein. Und wenn Sie bei bestimmten geschäftlichen Ereignissen wie zum Beispiel Flash-Verkäufen jedes Mal Änderungen an Ihren Anwendungen vornehmen müssen, erfordert das einfach nur mehr Ressourcen.

Überlegungen:

- Funktioniert die Lösung in Echtzeit, ohne die Performance Ihrer vorhandenen Anwendungen zu beeinträchtigen?
- Müssen Sie für die Lösung Änderungen an Ihren vorhandenen Anwendungen vornehmen?
- Kann sie skaliert werden, um unvorhergesehenen Ereignissen wie volumetrischen Angriffen oder erwarteten Ereignissen wie Flash-Verkäufen gerecht zu werden?

7 Transparenz und Reporting

Jede Bot-Management-Lösung kann allgemeine Statistiken zum Bot-Traffic anzeigen. Das reicht jedoch nicht aus. Für die Infrastrukturplanung oder das Reporting an die Führungsebene haben sich allgemeine Statistiken durchaus bewährt. Sie bieten jedoch nicht die detaillierten Einblicke, die Sie zur Analyse Ihres Bot-Traffics benötigen. Darüber hinaus erhalten Sie keine Beweise für die Richtigkeit der ergriffenen Maßnahmen – Beweise, die nötig sind, damit Sie der Lösung vertrauen können. Denn bei einer Lösung, die Ihre Nutzer blockieren kann, ist eine Blackbox wenig erstrebenswert. Sie benötigen detailliertes Reporting, um Ihr Unternehmen zu unterstützen und besser zu verstehen, wie sich Änderungen an Risikoschwellen auf die Performance auswirken.

Überlegungen:

- Verfügt die Lösung über Berichtsfunktionen, mit denen Sie bestimmte Bots, Botnets oder Bot-Eigenschaften näher untersuchen können? Kann sie Berichte über verschiedene Scoring-Segmente erstellen, aus denen hervorgeht, welche Bots welche Endpunkte angreifen und welche Maßnahmen ergriffen wurden?
- Können Sie Trafficspitzen und einzelne Anfragen untersuchen? Schließlich müssen Sie sich manchmal die Anfragedetails ansehen, bevor Sie wissen, was zu tun ist.
- Kann Ihnen die Lösung zeigen, wie Ihr Bot-Traffic im Vergleich zum Bot-Traffic bei anderen in der Branche abschneidet?
- Inwiefern lässt sich das Reporting in andere Sicherheitslösungen integrieren? Können Sie den Traffic ganzheitlich analysieren oder sind verschiedene Ansichten erforderlich?

8 Schutz von APIs

Die fortschrittlichsten Bot-Erkennungstechnologien verlassen sich heutzutage unabhängig von Anbieter oder Lösung auf die Einschleusung von JavaScript-Code und die Analyse der Clientantwort. Aber was tun, wenn die API-basierten Clients nicht auf JavaScript antworten? Wenn Sie offene APIs für Apps oder Drittanbieter einsetzen, benötigen Sie eine Lösung, mit der Sie die Schnittstellen im selben Maße schützen können wie Ihre Webseiten. Andernfalls wandern Ihre Bots – und auch Ihre Bot-Probleme – einfach von Ihren Webseiten zu Ihren APIs.

Überlegungen:

- Welche Art von Schutz bietet der Anbieter für APIs? Nur Kontingentsverwaltung und Ratenbeschränkung?
- Fragen Sie stattdessen nach einer mobilen Funktion, die die fortschrittlichsten Erkennungstechnologien des jeweiligen Anbieters in Ihre Apps integrieren kann.
- Auch ein reputationsbasierter Ansatz – obwohl nicht so effektiv wie andere Methoden – kann eine gute Option darstellen, um APIs für Drittanbieter zu schützen, die keinen Zugriff auf eine mobile Funktion wie SDK haben.

9 Site oder Seite

Wenn Ihre Website aus mehr als einer Seite besteht, haben Sie wahrscheinlich in verschiedenen Bereichen der Site mit unterschiedlichen Bot-Problemen zu kämpfen: Price Scraping, das Auslesen von Preisen, kann erhebliche Auswirkungen auf Ihre Produktseiten haben. Content Scraping, das Abgreifen von Content, kann den Wert Ihrer digitalen Inhalte beeinträchtigen. Daneben gibt es weiterhin Angriffe auf Ihre Anmeldeseiten, die auf den Missbrauch von Anmeldedaten zielen. Es gibt jedoch einige Bot-Managementlösungen, die nur ein einzelnes Problem angehen können. Stellen Sie sicher, dass die ausgewählte Lösung Ihre Bot-Probleme lösen kann – egal, ob diese nur eine Seite oder die ganze Website betreffen.

Überlegungen:

- Worauf konzentriert sich die Lösung: einzelne Seiten oder die gesamte Website? Wie wird sie bereitgestellt: vor einzelnen Seiten oder vor der gesamten Website?
- Kann die Lösung Sie bei Ihren Bot-Problemen unterstützen, auch bei Missbrauch von Anmeldedaten, Web Scraping und Content Aggregation?

10 Managed Services

Sie müssen Bots managen, um ihre Auswirkung auf Ihr Unternehmen zu kontrollieren. Dieses Bot-Management ist jedoch nicht ganz einfach. Auch wenn Sie über das nötige Fachwissen in Ihrem Unternehmen verfügen, ist manchmal doch Hilfe von außen erforderlich: Sie benötigen Experten, die Ihre Bot-Probleme verstehen. Im Übrigen wird die Besetzung solcher Stellen immer schwieriger. Was passiert, wenn einige Ihrer Fachkräfte das Unternehmen verlassen? Jeder kann sich eine HTTP-Anfrage ansehen und eine Signatur erstellen, um Traffic zu blockieren. Das löst jedoch nicht Ihr Problem. Sie brauchen jemanden, der herausfindet, welche Bots Ihre Hauptprobleme verursachen, und der eine Strategie entwickelt und umsetzt, um diese Probleme zu beheben.

Überlegungen:

- Verfügen Sie über interne Ressourcen mit ausreichend Fachkenntnissen auf dem Gebiet des Bot-Managements, um die Lösung selbst optimieren zu können?
- Bietet der Bot-Management-Anbieter auch Professional Services an oder verkauft er nur Produkte?
- Können Sie im Notfall jederzeit auf proaktive Überwachung und zusätzliche personelle Fachressourcen zugreifen?

Seien Sie proaktiv, nicht reaktiv

Man sollte in das Bot-Management investieren, bevor Bots zu einem Problem werden und bevor die nächste Evolutionswelle bestehende Abwehrsysteme alt aussehen lässt. Berücksichtigen Sie diese Überlegungen, wenn Sie Ihre Optionen ausloten. Akamai Bot Manager kann Ihnen die Sicherheit bieten, die Sie brauchen. Sie möchten gerne mehr erfahren? Fordern Sie eine auf Ihren Fall zugeschnittene Angriffssimulation an.

Weitere Informationen