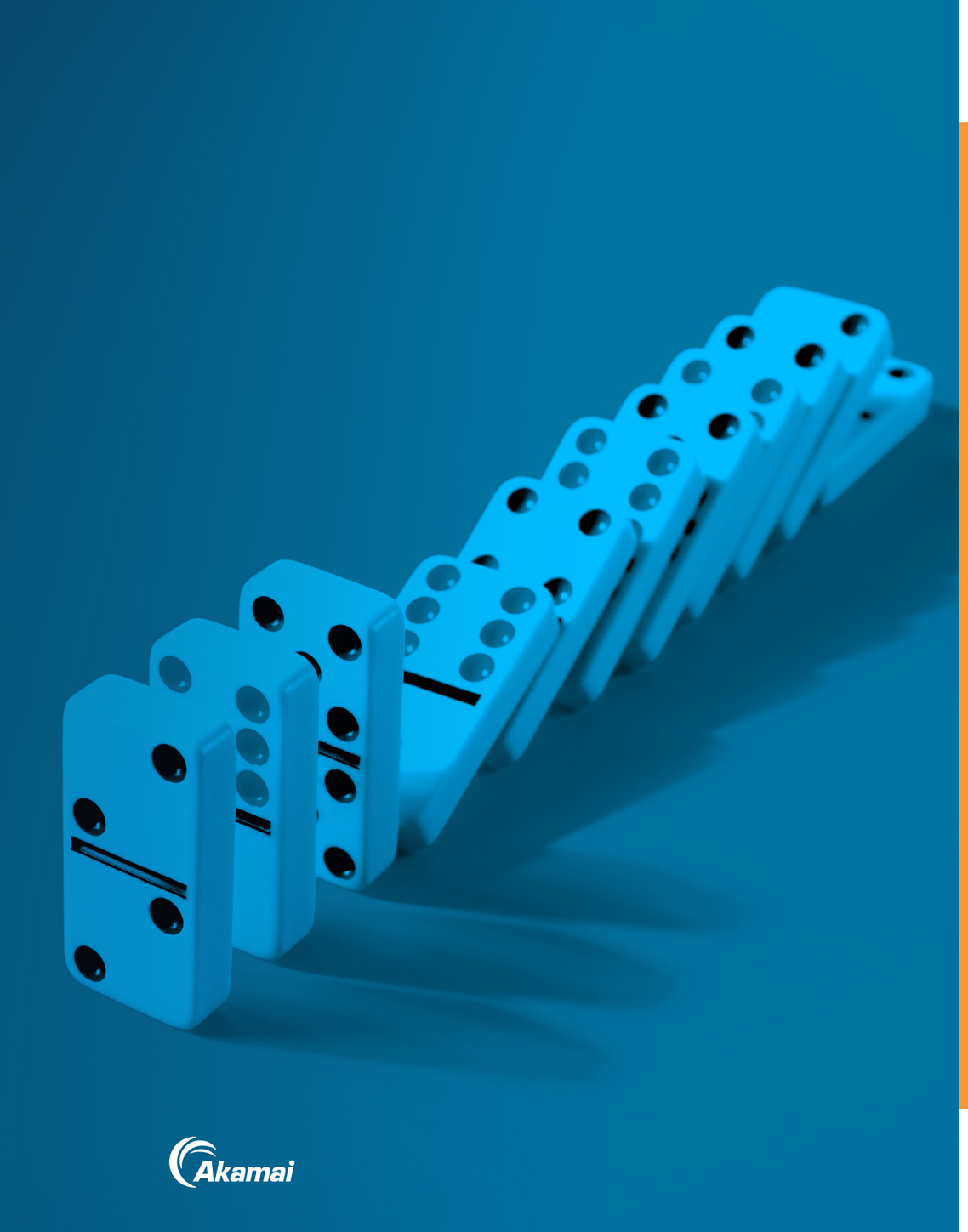
Jeder Tag kann zum Feiertag werden

Tipps, die Sie bei der Vorbereitung auf geschäftliche Spitzenzeiten unterstützen

E-Book



Inhaltsverzeichnis

Einführung

Die drei großen amerikanischen Shopping-Feiertage – Thanksgiving, Black Friday und Cyber Monday – sind nicht die einzigen Spitzenzeiten für Handelsunternehmen wie Einzelhändler, Reiseanbieter oder das Gastgewerbe. Je nach Geschäft oder Branche kann jeder Tag zu einem Spitzenereignis werden. Zum Beispiel ist der Valentinstag der größte Tag des Jahres für Floristen, während die Sommerferien für das Reise- und Gastgewerbe äußerst wichtig sind. Ein Krankenversicherungsunternehmen wird während der Einschreibungsfrist einen Besucheransturm verzeichnen, während ein Einzelhändler einen Ansturm erlebt, wenn ein neues Produkt auf den Markt kommt oder die Schule wieder beginnt. Und abseits der USA können Spitzenzeiten auch durch die Olympischen Spiele, die Fußballweltmeisterschaft oder Feiertage wie Diwali, das Mondneujahrsfest und das Oktoberfest entstehen.

Die Lektionen, die wir bei der Bewältigung von Performanceanforderungen und Sicherheitsrisiken an traditionellen Spitzentagen gelernt haben, lassen sich auf jede Spitzenzeit und jedes Event mit hohem Besucheraufkommen anwenden. In jedem Fall müssen Sie an solchen Tagen deutlich mehr Traffic bewältigen und Risiken managen, als es normalerweise der Fall ist. Und in jedem Fall steht viel auf dem Spiel: Gelingt es Ihnen nicht, diese Momente erfolgreich zu bewältigen, kann das zu Umsatzeinbußen und Rufschädigung führen. Wenn Sie diese Ereignisse jedoch erfolgreich managen, bedeutet das höhere Umsätze und zufriedene Kunden.

Zur Vorbereitung auf Spitzenzeiten müssen Sie die Performance Ihrer Plattform optimieren, sich auf Worst-Case-Szenarien vorbereiten, Ihre Sicherheitsvorkehrungen aktualisieren und eine abschließende Prüfung durchführen, um zu gewährleisten, dass Ihr nächstes Spitzenereignis reibungslos verläuft.

In den folgenden vier Kapiteln stellen wir Ihnen 15 Best Practices vor, mit denen Sie sich auf jedes Spitzenereignis vorbereiten können – egal, wann und wie oft diese Ereignisse eintreten.

INFORMATION: Spitzenereignisse ändern sich. Deshalb muss sich auch Ihre Strategie für diese Ereignisse ändern.

Kunden erwarten heute, dass die Feiertagszeit früher beginnt und länger dauert – Wochen oder Monate statt Tage. Und angesichts von Veränderungen bei Konsumausgaben, Wahlen und immer neuen politischen Ereignissen und anderen makroökonomischen Kräften bringt die Zukunft zahlreiche Unbekannte mit sich. Das bedeutet, dass Ihr Handelsunternehmen die Vorbereitung auf Spitzenereignisse nicht mehr als Vorbereitung auf ein einziges großes Ereignis betrachten kann. Anhaltende Spitzenereignisse erfordern nachhaltige Betriebsprozesse, mit denen Ihr Unternehmen nahezu umgehend auf verschiedene Spitzenereignisse reagieren kann, ohne dass Kunden oder Betrieb beeinträchtigt werden.

Kapitel 1:

Der Entwicklung voraus

Vorausschauende Planung ist der Schlüssel, um die Performance Ihrer Website bei überdurchschnittlich hohem Trafficaufkommen zu steigern. Es versteht sich von selbst, dass ein gutes Netzwerk zur Inhaltsbereitstellung (CDN) ein wesentlicher Bestandteil Ihrer Strategie ist. Aber Sie müssen auch planen, wie Sie sicherstellen können, dass Ihre Website gut funktioniert, wenn mehr Besucher mit ihr interagieren – und wie Sie reagieren können, wenn Ihr System unter Stress Hilfe braucht. Es gibt drei Inhaltstypen, die hierbei relevant sind und die unterschiedlich behandelt werden sollten, um die Performance zu maximieren und die Entlastung zu erhöhen:

Die HTML-Seitenstruktur, die den Basisinhalt Ihrer Website ausmacht (die angestrebte Entlastung sollte 50 % betragen)

Andere statische Inhalte wie JavaScript, CSS, Bilder und Videos (die angestrebte Entlastung sollte mindestens 80 % betragen, wir empfehlen jedoch mindestens 90 %)

API-Verkehr wie mobile Apps, Preisanfragen, Anmeldungen und Kaufabschlüsse (die optimale Entlastung hängt von der Art der API-Aufrufe und den abgerufenen Daten ab)

Im Folgenden finden Sie fünf Best Practices, mit denen Sie sicherstellen können, dass die Performance Ihres Systems optimiert und auf Spitzenzeiten abgestimmt ist.

Tipp 1: Vorab Caching-Einstellungen prüfen

Bewerten Sie, was wo zwischengespeichert wird, um sicherzustellen, dass Ihre Caching-Strategie optimal für alltägliche Zwecke funktioniert, bevor Sie überhaupt an Spitzenereignisse denken. Ziel ist es, den Look-and-Feel Ihrer Website zu optimieren und das gewünschte Weberlebnis bereitzustellen – so schnell wie möglich und mit maximaler Personalisierung. Cache-Einstellungen gelten in erster Linie für statische Inhalte und Assets, die so weit wie möglich gemäß Ihren Geschäftsanforderungen zwischengespeichert werden sollten. Es ist besser, ein Bild auf Ihrem Load Balancer am Ursprung oder in Ihrem CDN zwischenzuspeichern – oder es sogar auf das Gerät Ihres Nutzers zu übertragen –, als es von Ihrem Webserver abzurufen.

Bei HTML gibt es viel mehr zwischenspeicherbare Inhalte als auf den ersten Blick ersichtlich. Es ist möglich, Ihre Website zu strukturieren und den Inhalt zu fragmentieren, um eine höhere HTML-Entlastung zu erzielen. Wenn beispielsweise Nutzer auf der Website nicht angemeldet sind (d. h., eine dynamische Personalisierung der Inhalte ist nicht möglich), können die Inhalte zwischengespeichert und für diese Gruppe wiederverwendet werden. Das Ergebnis: Wenn ein großer Prozentsatz der Nutzer nicht angemeldet ist, sollten Sie die Inhalte für diese Nutzer im Cache speichern. Für andere Arten von statischen Inhalten sollten Sie eine Entlastung von 90 % und mehr anstreben. Wir sind uns darüber im Klaren, dass Sie wahrscheinlich bereits viel Aufwand für die Optimierung dieser Art von Website-Inhalten betreiben – aber überprüfen Sie am besten noch einmal, ob Sie Ihre Ziele erreichen. Damit kommen wir zu den APIs: Hier sind zwar einige Daten so dynamisch, dass sie nicht zwischengespeichert werden können, doch Sie sollten sich überlegen, welche API-Aufrufe gespeichert werden können, z. B. Versandangebote, Filialstandorte oder Preise. Wenn der Bestand alle 60 Sekunden aktualisiert wird, warum nicht 30 Sekunden lang zwischenspeichern? Wenn die Preise einmal am Tag um Mitternacht aktualisiert werden, können Sie alle API-Aufrufe alle 12 Stunden zwischenspeichern. In Spitzenzeiten – wenn jeder Euro zählt – erhöht jede Sekunde, die zwischengespeichert werden kann, die Entlastung, wenn es am wichtigsten ist.

Tipp 2: Entlastung während des Ereignisses erhöhen

Suchen Sie als Nächstes nach Vorteilen, die Sie durch das Zwischenspeichern bestimmter Inhalte nur während des Events erzielen können. Wenn Sie z. B. die Antworten auf Preis- oder Versandanfragen einige Minuten lang zwischenspeichern, können Sie Ihre Server entlasten, sodass Sie zu geringeren Kosten die Skalierung steigern können. Weitere Ideen sind das Zwischenspeichern von Weiterleitungen wie dynamische Seitenzusammenstellung, Pre-Rendering und Bildoptimierung – und Sie sollten Weiterleitungen an der Edge zwischenspeichern. Während des Ereignisses und auch danach kann es viele Dinge geben, die Sie auslagern können, darunter Geschäftslogik, Nutzererlebnis, Weiterleitungen, SEO-Optimierungen und Bot-Management.

Tipp 3: Bilder und Videos optimieren

Bei Bildern und Videos handelt es sich zwar um statische Inhalte, aber Sie können eine Menge tun, um sie Ihren Kunden auf vereinfachte *und intelligente* Weise bereitzustellen. Für ein optimales Nutzererlebnis sollten Sie unbedingt vor dem Spitzenereignis an der Optimierung von Bildern und Videos arbeiten. Höchstwahrscheinlich müssen Sie mit einem Bildoptimierungsanbieter zusammenarbeiten, um sicherzustellen, dass Sie jedem Kunden zur richtigen Zeit die richtige Größe, das richtige Format und den richtigen Blickwinkel auf Ihre Bild- oder Videoinhalte anbieten. Dieser Prozess erfordert auch, dass Sie alle Kombinationen von Geräten, Browsern, Betriebssystemen und sogar Netzwerkverbindungen berücksichtigen, die Ihre Kunden verwenden. Durch die Optimierung Ihrer Bilder und Videos können Sie Folgendes erreichen:

- Geringere Seitengröße und schnelleres Laden (weniger Bytes ohne Qualitätseinbußen)
- Verbesserte Ladezeit und Reaktionsfähigkeit
- Optimiertes Asset-Management, um den Arbeitsaufwand für Kreativ- und Designteams zu reduzieren

Tipp 4: Bots identifizieren und managen

Studien haben ergeben, dass Bots fast 50 % des gesamten Internetverkehrs ausmachen. Das heißt, dass die Hälfte aller Anfragen einfach nur Ihr System belastet. Es ist wichtig, eine Strategie für Bots zu haben, um Überraschungen bei Spitzenereignissen zu vermeiden. Wenn Sie Bots während eines Spitzenereignisses bedienen, verringert sich Ihre Kapazität für zahlende Kunden – und das zu einem Zeitpunkt, an dem Sie diese Kapazität am dringendsten brauchen. Mithilfe von Toolsets können Sie feststellen, welche Art von Nutzer eine Anfrage stellt und welche Absicht mit der Transaktion verfolgt wird. So können Sie bestimmte Bot-Interaktionen priorisieren und andere hintanstellen. Eine Strategie zur Verringerung der Bot-Belastung besteht darin, Bots vorgerenderte und zwischengespeicherte Inhalte von einem anderen Ursprung bereitzustellen. Eine andere Strategie lautet, während Spitzenzeiten alle Website-Crawler abzuschalten und die kurzfristigen SEO-Folgen in Kauf zu nehmen, um den Umsatz zu maximieren. Innerhalb der Bot-Population sollten Sie in der Lage sein, detailliertere Entscheidungen darüber zu treffen, wie Sie während Spitzenzeiten mit den verschiedenen Arten von Bots umgehen – insbesondere wenn Sie nicht dafür bezahlen wollen, sie zu bedienen.

Tipp 5: „Graceful Degradation“ einsetzen

Sie sollten in der Lage sein, einen Teil Ihrer Funktionalität zu verlieren, ohne dass hierdurch Ihre Website offline geht. In der Tat läuft die Seite wahrscheinlich nie ohne Funktionseinbußen – sie befindet sich in einem Zustand namens „Graceful Degradation“ (zu Deutsch etwa „würdevolle Verschlechterung“), einem Konzept aus der Welt komplexer Systeme. Sie können Ihr System so gestalten, dass es bei Spitzenbelastungen strategisch in einem „verschlechterten“ Zustand läuft, um eine bessere Performance zu erzielen. Ein Beispiel dafür ist ein großer Online-Händler, der seine Empfehlungsfunktion während der Haupteinkaufszeiten aussetzt, weil der Geschäftsnutzen dieser Funktion die Belastung des Systems nicht wert ist.

Kapitel 2:

Vorbereitung auf das Schlimmste

Nachdem Sie Ihr System nun so konzipiert haben, dass es die erwartete Belastung während Spitzenereignissen erfolgreich bewältigen kann, sollten Sie sich überlegen, was Sie tun wollen, wenn sich Ihre Erfolgserwartungen nicht erfüllen.

Bei Verkehrsspitzen werden Ihre betrieblichen Einschränkungen und Schwachstellen besonders deutlich, weil Ihr System ohnehin schon belastet ist. Unter dem Druck eines Spitzenereignisses haben Sie möglicherweise keine Zeit, Probleme zu erkennen – geschweige denn, darauf zu reagieren –, bevor es zu spät ist. Deshalb ist es wichtig, dass Sie sich auf potenzielle Probleme vorbereiten, bevor sie sich auf Ihre Kunden oder Ihren Umsatz auswirken. Nehmen Sie sich vor dem Ereignis Zeit, um sich ein umfassendes Bild von der voraussichtlichen Last und ihren möglichen Auswirkungen auf Sicherheit, Performance und Zuverlässigkeit zu machen. Verifizieren Sie die Bereiche, von denen Sie glauben, dass sie dem Ereignis standhalten können, und erstellen Sie Notfallpläne für Bereiche, die es nicht können.

Im Folgenden finden Sie vier Best Practices, mit denen Sie sicherstellen können, dass Sie auf alle Eventualitäten vorbereitet sind.

Tipp 6: Stress- und Belastungstests durchführen

Der erste Schritt in diesem Prozess besteht darin, festzustellen, was ein inakzeptables Ergebnis ist. Ziel ist es hierbei, zu ermitteln, was außerhalb der akzeptablen Grenzen liegt, und einen Plan für den Fall zu entwickeln, dass diese Grenzen überschritten werden. Stress- und Lasttests helfen Ihnen, diese Grenzen zu bestimmen und zu verstehen, was erwartet wird. Führen Sie in den Monaten vor einem Spitzenereignis mehrmals Stresstests durch – in der Erwartung, dass Ihr System anfangs ausfallen wird. So haben Sie Zeit, Probleme zu beheben, und gewinnen immer mehr Vertrauen in Ihre Fähigkeit, die erforderliche Last zu bewältigen.

Tipp 7: Warteraum bereitstellen

Ihre Seite muss in der Lage sein, den Traffic bei Bedarf zu drosseln. Mit einem Wartezimmer können Sie den Kaufprozess während Spitzenzeiten aufrechterhalten und das Nutzererlebnis bei unerwarteten Problemen managen, die diesen Prozess beeinträchtigen könnten. Mit diesem Tool können Sie auch Graceful Degradation einsetzen, z. B. durch zeitversetzten Zugriff oder frühzeitigen exklusiven Zugang. Ein weiterer wichtiger Vorteil eines Warteraums ist, dass er als Ausfallsicherung fungieren kann, wenn etwas schiefläuft. Erfahren Sie mehr über Strategien zur Bewältigung von Spitzenereignissen oder Verkehrsspitzen, mit denen Sie gleichzeitig die Kundentreue steigern können.

INFORMATION: Was bedeutet eine erhöhte Belastung?

Eine erhöhte Belastung Ihres Systems kann verschiedene Formen annehmen: ein kleiner Schub durch einen Feiertag oder auch ein massiver Sprung aufgrund eines gesellschaftsweiten Events. So beobachtete Akamai im April 2020, als die Coronapandemie viele Menschen dazu zwang, zu Hause zu bleiben und online zu gehen, einen Anstieg des weltweiten Internetverkehrs um 30 %. Das entspricht dem Wachstum eines ganzen Jahres in nur wenigen Wochen.

Tipp 8: Notfallwiederherstellung planen

Die Notfallwiederherstellung (oder Disaster Recovery) ist darauf ausgelegt, auf eine größere Natur-, Cyber- oder Unternehmenskatastrophe zu reagieren. Die Wiederherstellung kann oft Tage oder Wochen dauern. Aber was, wenn diese Katastrophe mitten während des Spitzenereignisses eintritt? Wenn Sie beispielsweise vier Tage für den Failover brauchen, das Ereignis aber nur vier Stunden dauert, haben Sie keinen effektiven Disaster-Recovery-Plan. Gehen Sie bei Ihrer Disaster-Recovery-Planung und Ihren -Übungen davon aus, dass Sie sie wahrscheinlich brauchen werden. Stellen Sie also unbedingt sicher, dass Sie in der Lage sind, den Plan schnell genug umzusetzen. Letztendlich kann eine Umstellung auf einen Aktiv/Aktiv-Ansatz statt des Disaster-Recovery-Ansatzes dazu beitragen, dass keine einzige Katastrophe Ihren Betrieb beeinträchtigt.

Tipp 9: Beobachtbarkeit maximieren

Durch Überwachung können Sie feststellen, wie Ihr System während eines Spitzenereignisses funktioniert. Es ist wichtig, sowohl technische als auch geschäftliche Maßnahmen zu überwachen. Vielleicht ist die Hälfte Ihres Dashboards für technische Messwerte wie CPU, Durchsatz und Seitenladezeit vorgesehen, während die andere Hälfte geschäftliche Messwerte wie Klickraten, Warenkorbabbrüche und Konversionen verfolgt. Und Sie brauchen beides – denn die technischen Metriken verraten Ihnen vielleicht, warum etwas nicht funktioniert, aber nicht, wie sich das Problem auf Ihre Nutzer auswirkt. Hierfür benötigen Sie die entsprechenden Geschäftskennzahlen. Indem Sie die Beobachtbarkeit dieser Messgrößen maximieren, können Sie Anomalien erkennen, die automatisierte Aktionen zur Schadensbehebung auslösen können.

Kapitel 3:

Stärkung Ihres Sicherheits-Frameworks

Sicherheit wird immer unter dem Aspekt des Risikos diskutiert: Risikoidentifizierung, Risikominderung, Risikoauswirkung, Risikowahrscheinlichkeit. Und es ist von entscheidender Bedeutung, wie Sie auf dieses Risiko reagieren. Es ist im Wesentlichen ein Balanceakt: Sie könnten sich beispielsweise dafür entscheiden, bei Spitzenereignissen aggressiver gegen potenzielle Risiken vorzugehen, aber das könnte sich auf die Nutzerfreundlichkeit auswirken. Zu den Best Practices für Sicherheit gehört es, sicherzustellen, dass Ihre Plattform über gut abgestimmte Kontrollen verfügt; Schwellenwerte für den Traffic festzulegen; zu bestimmen, wie Warnmeldungen verarbeitet werden sollen; und einen Plan dafür zu definieren, wie Sie im Falle von Problemen vorgehen wollen.

Sehen Sie sich diese sechs Best Practices an.

Tipp 10: Ihr Runbook prüfen

Ihr Runbook sollte alle relevanten Informationen zu Mitarbeitern, Prozessen und Voraussetzungen für Ihre Sicherheitsstrategie enthalten. Für Mitarbeiter sollten Sie Schichtpläne, Wissensstand und -lücken sowie die erforderlichen Schulungen auflisten. Beim Prozess sollten Sie ein Protokoll oder ein Flussdiagramm erstellen, damit alle wissen, was zu tun ist und an wen sie sich in den verschiedenen Fällen wenden müssen. Bei den Voraussetzungen sollten Sie die Abhängigkeiten und Kommunikationsanforderungen für Sicherheitseskalationen beschreiben. Das Runbook sollte auch Notfallprotokolle enthalten, um den Ursprung bestmöglich zu schützen.

Tipp 11: Optimal auf DDoS-Angriffe vorbereiten

Um DDoS-Angriffe abzuwehren, sollten Sie sicherstellen, dass Ihre Plattform über eine gut abgestimmte Ratensteuerung verfügt. Verweigern Sie Traffic oberhalb bestimmter Schwellenwerte und senden Sie ordnungsgemäße HTML-Antworten, um Bots zu täuschen. Caching ist eine wirksame Waffe gegen DDoS-Angriffe, also speichern Sie so viel zwischen wie möglich. Führen Sie eine theoretische Übung durch, um blinde Flecken oder Ineffizienzen in Ihren Reaktionsprozessen zu finden. Arbeiten Sie mit einem Sicherheitsanbieter zusammen, der Ihre Umgebung und die Art Ihrer Webanwendungen kennt, um die wirksamsten Schutzmaßnahmen zu ergreifen.

Tipp 12: Kunden nicht vergessen

Angesichts der Zunahme von Web-Skimming-, Supply-Chain- und Magecart-Angriffen ist es entscheidend (und mit PCI DSS 4.0 auch vorgeschrieben), dass Sie das gesamte JavaScript-Ausführungsverhalten in Ihren Webanwendungen verwalten und überwachen, um sich vor clientseitigen Angriffen zu schützen – während Spitzenereignissen *und darüber hinaus*. Gerade die Feiertage sind die beste Zeit für Betrüger, Ihre Marke zu imitieren, indem sie gefälschte Websites und Social-Media-Konten erstellen, um Anmeldedaten und Kreditkarteninformationen zu stehlen oder gefälschte Waren oder Reservierungen zu verkaufen. Stellen Sie im Rahmen Ihrer Strategie sicher, dass Sie über ein Überwachungstool verfügen – und über einen Plan dafür, wie Sie reagieren, wenn eine gefälschte Website oder ein Missbrauch entdeckt wird –, um die Treue und das Vertrauen Ihrer Kunden zu schützen.

INFORMATION: DDoS-Angriffe brechen Rekorde

DDoS-Angriffe haben erheblich an Umfang und Raffinesse gewonnen. Tatsächlich fanden acht der zehn größten DDoS-Angriffe, die Akamai je abgewehrt hat, zwischen Mitte 2022 und Ende 2023 statt. Im Februar 2023 schützte Akamai einen Kunden vor einem großen DDoS-Angriff, der einen Höchstwert von 900,1 Gigabit pro Sekunde (Gbit/s) und 158,2 Millionen Paketen pro Sekunde (Mpps) erreichte.

Tipp 13: API-Angriffsfläche verstehen

Die Ausbreitung von APIs ist für jedes Unternehmen eine Herausforderung, besonders aber für den Handel. Richten Sie einen Bestandsaufnahme-Prozess für APIs ein und führen Sie den Audit durch. Ihr Sicherheitsteam ist möglicherweise nicht mit den neueren APIs vertraut, die Ihr Anwendungsteam über die Plattform ausführt. Deshalb ist es wichtig, diese neuen APIs bei der Plattform zu registrieren und einen akkuraten Bestand zu gewährleisten. Wenn Ihr Sicherheitsteam eine API nicht kennt, kann es sie blockieren – wenn die APIs jedoch registriert sind, kann das Team sie schützen. Eine weitere Best Practice besteht darin, zu gewährleisten, dass Ihre Web Application Firewall auf dem neuesten Stand ist und sich im automatischen Modus befindet.

Tipp 14: Warnungen konfigurieren, um unnötige Alarme zu reduzieren

Zwar ist es wichtig, alles zu überwachen, doch hierdurch besteht auch die Gefahr, dass zu viel Rauschen entsteht: Denn zu viele Warnungen bedeuten im Grunde keine Warnungen, weil Ihr Team nicht erkennen kann, welche Warnungen wichtig sind. Die Optimierung dieser Warnungen hilft Ihnen, das Rauschen zu reduzieren und besser zu reagieren. Führen Sie diesen Schritt rechtzeitig vor einem Spitzenereignis durch, nicht erst in letzter Minute. Außerdem ist es wichtig, einen Weiterleitungsplan für Warnungen zu erstellen, der die wichtigsten Informationen übermittelt, damit die richtigen Personen reagieren können.

Tipp 15: Verteidigung gegen schädliche Bots verbessern

Bestimmte Arten von Bots können gutartig sein – andere können verwendet werden, um DDoS-Angriffe zu starten, Inhalte oder Bestände zu durchsuchen, gefälschte Konten zu erstellen, Credential-Stuffing-Angriffe durchzuführen oder noch Schlimmeres zu tun. Und selbst gute Bots können Ihre Website während wichtigen Ereignissen verlangsamen, sodass Nutzer nur noch inakzeptable Geschwindigkeiten erhalten. Stellen Sie sicher, dass Ihre Bot-Strategie es Ihnen ermöglicht, so aggressiv wie nötig vorzugehen, um bösartige Bots auszuschalten. Konzentrieren Sie sich hierbei auf Notfallprotokolle, die definieren, was zu tun ist, wie es zu tun ist und mit wem Sie zusammenarbeiten, um Bots zu neutralisieren. Mithilfe von Tools können Sie Bots separat verfolgen und die Auswirkungen von Angriffen berücksichtigen, die zu kompromittierten Konten, Ausfällen und sogar zu Datenschutzverletzungen führen können.

Kapitel 4:

Zusammenfassung der gewonnenen Erkenntnisse

Bei der Vorbereitung und Bewältigung von Spitzenereignissen gewinnen Sie zahlreiche technische und geschäftliche Informationen. Deshalb ist es von entscheidender Bedeutung, die gewonnenen Erkenntnisse zu erfassen, um Ihr Team bei der Verbesserung zu unterstützen. Es kann jedoch schwierig sein, die Zeit und Energie für eine formelle Überprüfung aufzubringen – insbesondere in der Zeit nach den Feiertagen am Ende des Jahres. Für Unternehmen, die regelmäßig oder häufig Spitzenereignisse erleben, kann es schwierig sein, dazwischen eine Überprüfung einzuschieben. Unserer Meinung nach ist es jedoch eine wichtige Best Practice, die anschließende Überprüfung in den Kalender einzutragen, damit sie mit größerer Wahrscheinlichkeit stattfindet.

Um Sie genau hierbei zu unterstützen, geben wir Ihnen einen zusätzlichen Tipp.

Bonustipp 16: Formelle Überprüfung durchführen

Führen Sie die Nachbereitung durch, solange das Ereignis noch in den Köpfen der Mitarbeiter ist. Wenn sie sich noch gut an das Ereignis erinnern, kann Ihr Team die wertvollen Daten, die es währenddessen gesammelt hat, besser interpretieren und die Prioritäten für das nächste Mal festlegen.

- Haben Sie die richtigen Dinge gemessen?
- Gab es Lücken in Ihren Messwerten oder Prozessen, die Sie vor dem nächsten Ereignis schließen wollen?

Wenn Sie sich rechtzeitig auf eine formelle Überprüfung der technischen und geschäftlichen Performance nach dem Ereignis vorbereiten, können Sie das Gelernte und die gesammelten Daten optimal nutzen.

Transformieren Sie Ihren Ansatz für Spitzenzeiten

Wenn jeder Tag ein Spitzentag sein kann, sollte Ihr Ziel darin bestehen, Spitzenereignisse weniger als Ausnahme zu sehen, sondern eher als Standardereignis, auf das Sie jederzeit vorbereitet sind. Genau hier kommen wir ins Spiel: Die Unterstützung durch einen Experten wie Akamai kann den gesamten Prozess erheblich vereinfachen. Und während Sie immer weiter dazulernen, können Sie Ihre Vorbereitungen nach und nach in Ihre technische Architektur, Ihre Prozesse und Ihre Kultur integrieren, bis sie letztlich zur Gewohnheit werden. Dann kann jeder Tag ein Feiertag sein – und Ihr Team ist jederzeit gut vorbereitet.

Sind Sie bereit, die Performance Ihres Unternehmens bei Spitzenereignissen zu steigern?

Erfahren Sie mehr über die Einblicke und Lösungen von Akamai für den Einzelhandel sowie das Reise- und Gastgewerbe oder wenden Sie sich an einen Akamai-Experten.

Akamai schützt Ihr Kundenerlebnis, Ihre Mitarbeiter, Systeme und Daten und integriert Sicherheit in alle von Ihnen erstellten Inhalte – überall dort, wo Sie sie erstellen und bereitstellen. Dank der Einblicke unserer Plattform in globale Bedrohungen können Sie Ihre Sicherheitsstrategie anpassen und weiterentwickeln, um Zero Trust zu implementieren, Ransomware zu stoppen, Anwendungen und APIs zu schützen oder DDoS-Angriffe abzuwehren. Das gibt Ihnen das nötige Vertrauen, um kontinuierlich Innovationen zu entwickeln, zu expandieren und alles zu transformieren, was möglich ist. Möchten Sie mehr über die Cloud-Computing-, Sicherheits- und Bereitstellungslösungen von Akamai erfahren? Dann besuchen Sie uns unter akamai.com und akamai.com/blog oder folgen Sie Akamai Technologies auf X (ehemals Twitter) und LinkedIn.