

Quand n'importe quel jour peut connaître une forte affluence

Conseils pour vous aider à vous préparer aux événements de commerce générant un pic de trafic

Livre numérique

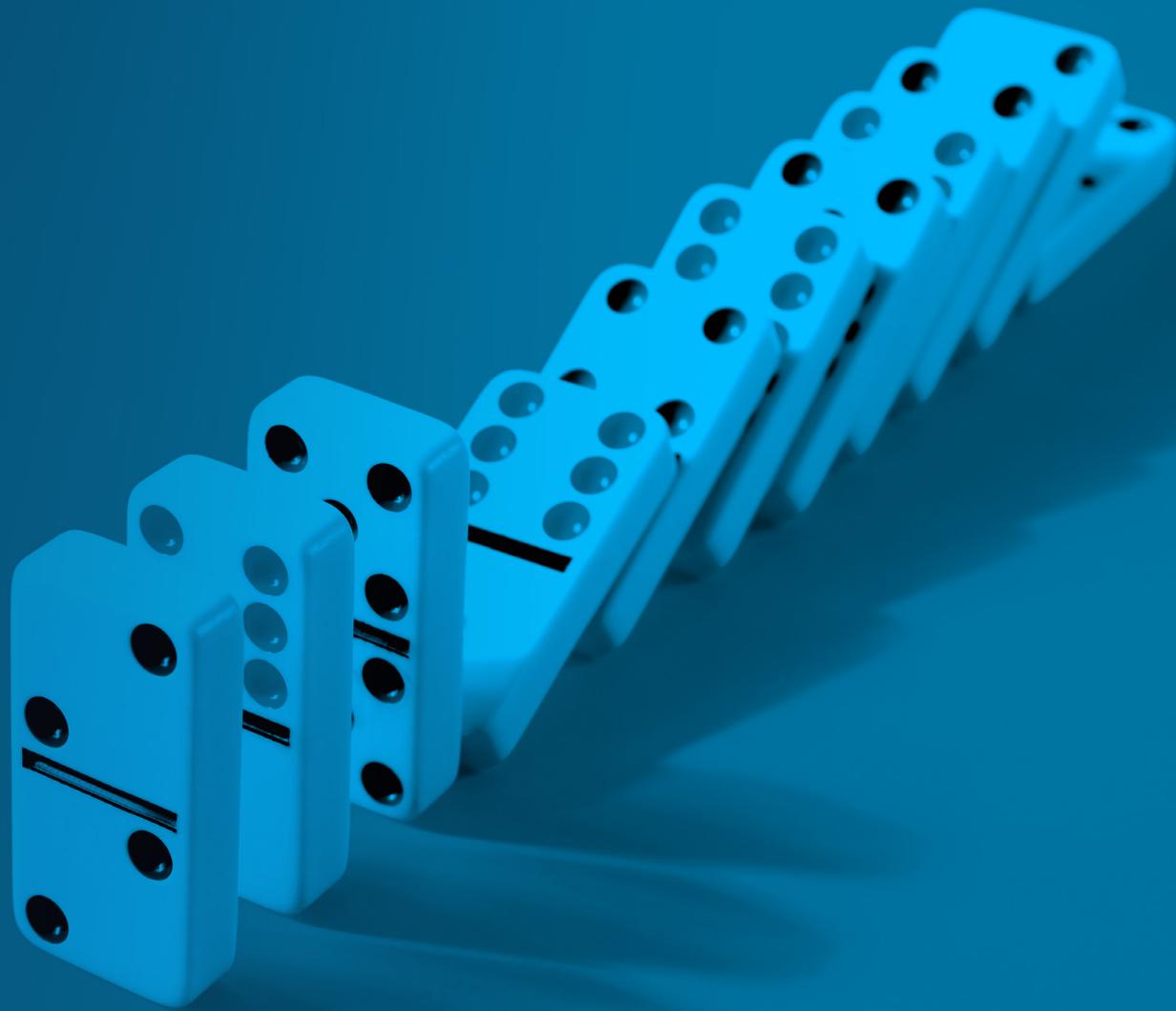


Table des matières

Introduction	03
Chapitre 1 : Prendre une longueur d'avance sur la courbe des performances	04
Conseil n° 1 : Vérifiez au préalable les paramètres de mise en cache	04
Conseil n° 2 : Augmentez le délestage pendant l'événement	04
Conseil n° 3 : Optimisez vos images et vidéos	05
Conseil n° 4 : Identifiez et gérez les bots	05
Conseil n° 5 : Adoptez la « dégradation fluide »	05
Chapitre 2 : Se préparer au pire	06
Conseil n° 6 : Effectuez des tests de contrainte et de charge	06
Conseil n° 7 : Déployez une salle d'attente	06
Conseil n° 8 : Planifiez la reprise après sinistre	07
Conseil n° 9 : Maximisez l'observabilité	07
Chapitre 3 : Renforcer votre infrastructure de sécurité	08
Conseil n° 10 : Passez en revue votre runbook	08
Conseil n° 11 : Ne soyez pas pris de court par des attaques DDoS	08
Conseil n° 12 : N'oubliez pas le client	08
Conseil n° 13 : Comprenez la surface d'attaque de vos API	09
Conseil n° 14 : Réglez les alertes pour réduire le bruit	09
Conseil n° 15 : Renforcez votre défense contre les bots malveillants	09
Chapitre 4 : Enregistrer les leçons apprises	10
Conseil bonus n° 16 : Effectuez un examen formel	10
Transformez votre approche des pics de trafic	11

Introduction

Les trois principales journées commerciales aux États-Unis, à savoir Thanksgiving, Black Friday et Cyber Monday, ne constituent pas les seuls pics de trafic pour les entreprises de commerce, qui incluent les entreprises de vente au détail, du voyage et de l'hôtellerie. Selon votre activité ou secteur, n'importe quel jour peut connaître un pic de trafic. Par exemple, la Saint-Valentin est le jour le plus important pour un fleuriste, tandis que les vacances d'été représentent une grande opportunité pour les entreprises du secteur des voyages et de l'hôtellerie. Une compagnie d'assurance maladie connaîtra un pic d'affluence pendant la période des adhésions, tandis qu'une entreprise de vente au détail verra affluer les clients potentiels chaque fois qu'un nouveau produit devient viral ou au moment des achats des fournitures scolaires. Au-delà des États-Unis, des pics de trafic sont susceptibles de survenir en raison des Jeux olympiques, de la Coupe du monde de football ou de fêtes telles que Divali, le Nouvel an lunaire et l'Oktoberfest.

Les leçons tirées en matière de gestion des besoins en performances et de risques de sécurité lors de pics de trafic traditionnels peuvent s'appliquer à tout pic de trafic d'événements. Dans tous les cas, le niveau de gestion des pics de trafic et des risques est plus élevé que d'ordinaire. Et dans tous les cas, les enjeux sont importants : si vous n'arrivez pas à gérer ces moments, cela peut vous faire perdre des revenus et nuire à votre réputation. Réussir à gérer ces événements se traduit par une augmentation des revenus et des clients satisfaits.

La préparation aux pics de trafic nécessite d'optimiser les performances de votre plateforme, de se préparer aux pires scénarios, de mettre à jour votre posture de sécurité et de mener un examen après action pour savoir comment s'assurer que votre prochain pic de trafic se déroule sans accroc.

Dans les quatre chapitres suivants, nous vous présentons quinze meilleures pratiques qui vous aideront à vous préparer à tout pic de trafic, quels que soient le moment et la fréquence de ces événements.

ANALYSE : Les pics de trafic changent. Votre stratégie en la matière doit également changer.

Les clients d'aujourd'hui s'attendent à ce que [la saison des fêtes commence plus tôt et dure plus longtemps](#) : des semaines ou des mois, au lieu de jours. Et avec les changements dans les dépenses de consommation, les élections et les événements politiques changeants, et d'autres forces macroéconomiques, l'avenir ajoute des inconnues importantes dans l'équation. Cela signifie que votre organisation commerciale ne peut plus aborder la préparation aux événements générant des pics de trafic comme elle le faisait avec un événement unique de grande envergure. Les pics de trafic soutenus exigent une cadence opérationnelle durable qui permette à votre entreprise de réagir presque immédiatement à une série de pics de trafic sans perturber vos clients ou vos opérations.

Chapitre 1 :

Prendre une longueur d'avance sur la courbe des performances

Il est essentiel de planifier à l'avance pour optimiser les performances de votre site Web à des charges de trafic plus élevées que la normale. Il va sans dire qu'un bon réseau de diffusion de contenu (CDN) est un élément essentiel de votre stratégie. Mais vous devez également planifier la manière de vous assurer que votre site fonctionnera bien, que davantage de visiteurs interagiront avec lui et la façon de réagir lorsque votre système aura besoin d'aide en cas de stress. Il existe trois types de contenu qui font partie de cette image et qui doivent être traités différemment pour maximiser les performances et augmenter le délestage :



Structure de page HTML qui compose le contenu de votre site Web de base (le délestage cible doit être de 50 %)



Autres contenus statiques tels que JavaScript, CSS, images et vidéos (le délestage cible doit être d'au moins 80 %, mais nous recommandons de viser 90 % et plus)



Trafic API tel que les applications pour mobile, la tarification, les connexions et les paiements (le délestage optimal varie en fonction de la nature des appels API et des données récupérées)

Voici cinq meilleures pratiques pour vous assurer que les performances de votre système sont optimisées et réglées pour une période de pic de trafic.

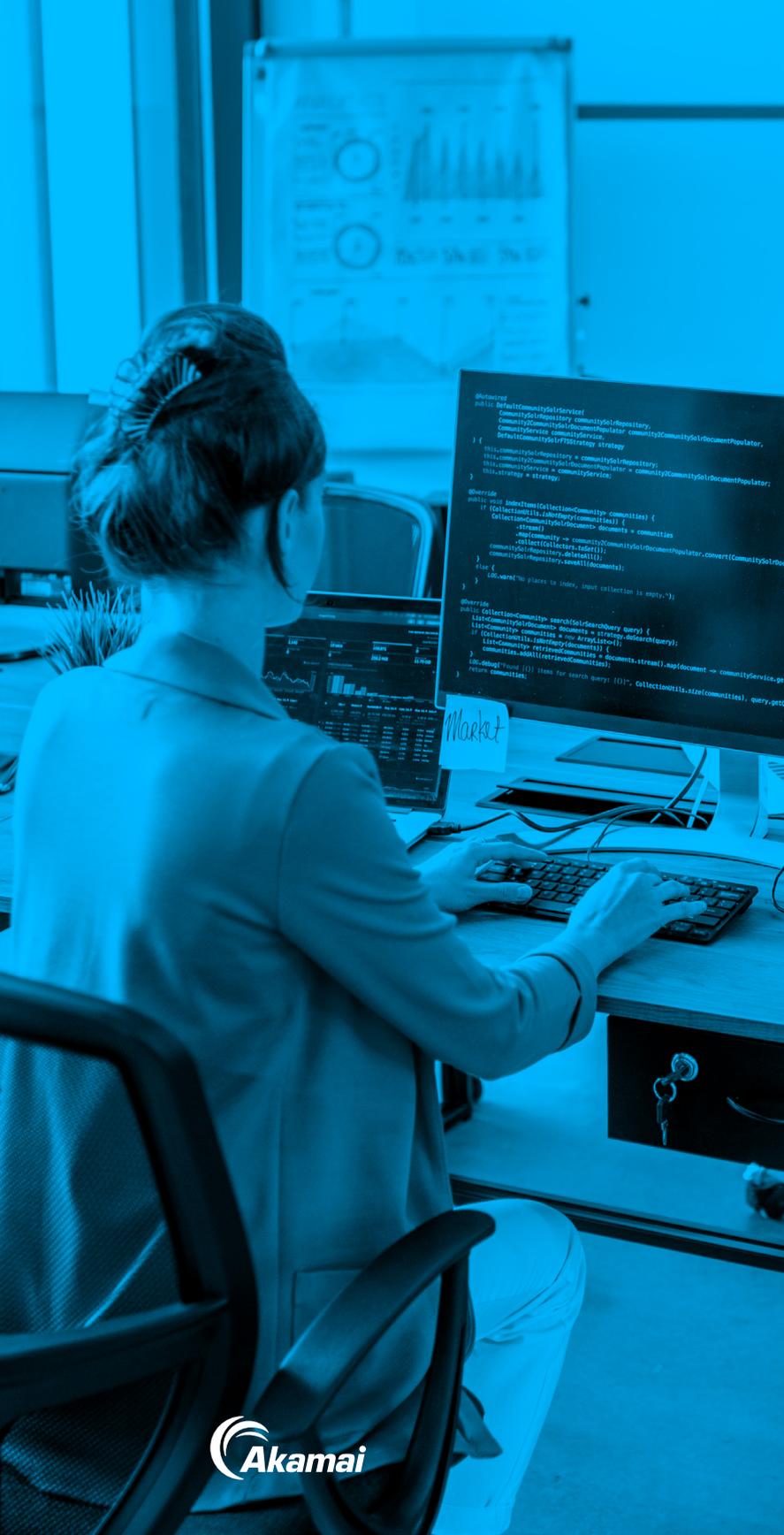
Conseil n° 1 : Vérifiez au préalable les paramètres de mise en cache

Évaluez ce que vous mettez en cache et où, afin de vous assurer que votre stratégie de mise en cache est la meilleure possible pour les besoins quotidiens, avant même d'ajouter un pic de trafic à l'équation. L'objectif est d'optimiser l'apparence de votre site et de fournir l'expérience Web souhaitée aussi rapidement que possible avec une personnalisation maximale. Les paramètres de mise en cache s'appliquent principalement au contenu et aux ressources statiques, qui doivent être mis en cache autant que possible pour répondre aux besoins de votre entreprise. Il est préférable de mettre en cache une image sur votre équilibreur de charge à l'origine ou sur votre CDN – ou même de l'intégrer au terminal de vos utilisateurs – que de l'extraire de votre serveur web.

Avec HTML, il y a beaucoup plus de contenu pouvant être mis en cache qu'à première vue. Il est possible de structurer votre site et de prendre des décisions pour fragmenter le contenu afin d'obtenir un délestage HTML plus élevé. Par exemple, si les utilisateurs du site ne sont pas connectés (c'est-à-dire que la personnalisation dynamique du contenu n'est pas disponible), le contenu peut être mis en cache et réutilisé pour ce groupe. Résultats : si un grand pourcentage d'utilisateurs ne sont pas connectés, mettez-les en cache en conséquence. Pour les autres types de contenu statique, vous devriez vous efforcer de viser un délestage égal à 90 % et plus. Nous reconnaissons que vous consacrez probablement déjà beaucoup d'efforts pour optimiser ce type de contenu de site, mais il suffit de vérifier à nouveau pour vous assurer que vous atteignez vos objectifs. Enfin, pour les API, bien que certaines données soient si dynamiques qu'elles ne peuvent pas être mises en cache, considérez quels appels API pourraient être concernés, comme les devis d'expédition, les localisations de magasins ou les prix. Si l'inventaire est mis à jour toutes les 60 secondes, pourquoi ne pas le mettre en cache pendant 30 secondes ? Si la tarification est mise à jour une fois par jour à minuit, mettez en cache tous les appels API toutes les 12 heures. Lors de votre pic de trafic, alors que chaque dollar compte, chaque seconde qui peut être mise en cache augmentera votre délestage lorsque cela compte le plus.

Conseil n° 2 : Augmentez le délestage pendant l'événement

Ensuite, recherchez les avantages que vous pourriez obtenir en mettant en cache certains contenus uniquement pendant votre événement. Si vous mettez en cache les réponses de tarification ou de devis d'expédition pendant quelques minutes, par exemple, vous pourriez libérer vos serveurs afin de pouvoir évoluer à moindre coût. D'autres idées incluent la mise en cache des redirections comme l'assemblage dynamique de page, le pré-rendu et les optimisations d'image, et vous devriez mettre en cache les redirections en bordure de l'Internet. Pendant l'événement et même après, il peut y avoir beaucoup à délester, y compris la logique métier, l'expérience utilisateur, les redirections, les optimisations SEO et la gestion des bots.



Conseil n° 3 : Optimisez vos images et vidéos

Les images et les vidéos peuvent constituer du contenu statique, mais il y a beaucoup à faire pour aider à les fournir à vos clients de manière simplifiée et *intelligente*. Il est essentiel de travailler sur l'optimisation des images et des vidéos avant votre pic de trafic pour une meilleure expérience utilisateur. Vous devrez probablement travailler avec un fournisseur d'optimisation d'image pour vous assurer que vous fournissez la bonne taille, le bon format et le bon point de vue de vos ressources image ou vidéo au bon moment à chaque client. Ce processus exige également que vous considériez toutes les combinaisons de terminaux, de navigateurs, de systèmes d'exploitation, et même de connexions réseau, que vos clients peuvent utiliser ou avoir. En optimisant vos images et vidéos, vous pouvez :

-  Rendre vos pages plus légères et plus rapides (en réduisant les octets sans affecter la qualité)
-  Améliorer le temps de chargement et la réactivité de votre site
-  Rationaliser la gestion des ressources pour réduire le travail de vos équipes de création et de conception

Conseil n° 4 : Identifiez et gérez les bots

La recherche indique que [les bots représentent près de 50 % de tout le trafic Internet](#), ce qui signifie que la moitié de toutes les demandes mettent votre système à l'épreuve. Il est crucial d'avoir une stratégie concernant les bots afin d'éviter les surprises lors des pics de trafic. Servir des bots pendant une période de pic de trafic diminue votre capacité à servir des clients payants à un moment où vous avez besoin de cette capacité autant que possible. Vous pouvez utiliser des ensembles d'outils pour identifier quel type d'utilisateur fait une demande et l'intention de cette transaction, ce qui peut vous permettre de hiérarchiser certaines interactions de bot et d'en déprioriser d'autres. Une stratégie pour réduire la charge des bots consiste à servir du contenu pré-rendu et mis en cache provenant d'une origine différente. Une autre stratégie consiste à désactiver tous les bots d'indexation pendant les heures de forte affluence et à subir les conséquences SEO à court terme pour maximiser les revenus. Au sein de la population de bots, vous devez être équipé pour prendre des décisions plus granulaires sur la façon de gérer différents types de bots pendant votre pic de trafic, surtout si vous ne voulez pas payer pour les servir.

Conseil n° 5 : Adoptez la « dégradation fluide »

Vous devez être en mesure de perdre une partie de vos fonctionnalités tout en maintenant votre site en fonctionnement. En fait, il vous manquera toujours des fonctionnalités, étant dans un état de « dégradation fluide », concept issu de systèmes complexes. Vous pouvez concevoir votre système pour qu'il fonctionne stratégiquement dans un état « dégradé » pendant les pics de charge afin d'améliorer les performances. Il peut s'agir par exemple d'un grand détaillant en ligne suspendant sa fonction de recommandations pendant les jours de pointe d'achat parce que la valeur commerciale de la fonction ne vaut pas la charge qu'elle applique au système.

Chapitre 2 :

Se préparer au pire

Maintenant que vous avez conçu votre système pour gérer avec succès les charges que vous attendez pendant les périodes de pic de trafic, pensez à ce que vous ferez si la situation tourne mal.

Les périodes de pic de trafic augmentent vos contraintes opérationnelles et vos vulnérabilités. Sous la pression d'un pic de trafic, vous n'aurez peut-être pas le temps d'identifier les problèmes, et encore moins d'y répondre, avant qu'il ne soit trop tard. C'est pourquoi il est essentiel de se préparer aux problèmes potentiels avant qu'ils n'affectent vos clients ou vos revenus. Passez du temps avant votre événement pour acquérir une solide compréhension de votre charge prévue et de son effet possible sur votre sécurité, vos performances et votre fiabilité. Vérifiez où vous pensez pouvoir fonctionner, et créez des contingences au cas où vous ne le pourriez pas.

Voici quatre meilleures pratiques qui peuvent vous aider à vous assurer que vous êtes prêt à faire face à chaque éventualité.

Conseil n° 6 : Effectuez des tests de contrainte et de charge

La première étape de ce processus consiste à identifier ce qui est un résultat inacceptable. Le but est d'identifier ce qui est exactement hors limites et d'avoir un plan pour quand ces limites sont dépassées. Les tests de contrainte et les tests de charge vous aident à établir ces limites et à comprendre ce qui est attendu. Exécutez des tests de contrainte plusieurs fois au cours des mois précédant un pic de trafic, en vous attendant à ce que votre système tombe en panne au début. Vous aurez le temps de corriger les problèmes et, au fil du temps, d'être davantage confiant dans votre capacité à gérer la charge nécessaire.

Conseil n° 7 : Déployez une salle d'attente

Votre site doit avoir la capacité de réguler le trafic à la demande. Une salle d'attente vous permet de maintenir votre flux de paiement pendant les heures de forte affluence et de gérer l'expérience utilisateur lors de problèmes inattendus qui peuvent ralentir ce flux. Cet outillage vous permet également d'utiliser une dégradation fluide, par exemple en décalant dans le temps ou en offrant un accès exclusif anticipé. Et l'un des principaux avantages d'une salle d'attente est qu'elle peut fonctionner comme une solution de repli que vous pouvez employer si les choses tournent mal. Apprenez-en plus sur les [stratégies pour gérer les événements médiatisés ou les pics de trafic](#) tout en favorisant la fidélisation des clients.

ANALYSE : À quoi ressemble une augmentation de la charge ?

L'augmentation de la charge sur votre système peut ressembler à un petit pic d'activité lors d'un jour férié ou d'un saut massif en raison d'un événement à l'échelle de la société. Par exemple, en avril 2020, alors que la pandémie de COVID-19 obligeait de nombreuses personnes à rester chez elles et en ligne, [Akamai a observé](#) une augmentation de 30 % du trafic Internet mondial, soit l'équivalent d'une année entière de croissance en seulement quelques semaines.



Conseil n° 8 : Planifiez la reprise après sinistre

La reprise après sinistre est conçue pour répondre à une catastrophe naturelle, cybernétique ou commerciale majeure, et la reprise peut souvent prendre des jours, voire des semaines. Et si cette catastrophe se produisait au milieu d'un pic de trafic ? Par exemple, si le basculement prend quatre jours, mais que votre événement dure quatre heures, vous ne disposez pas d'un plan de reprise après sinistre efficace. Associez votre planification et vos exercices de reprise après sinistre à la probabilité d'en avoir besoin, et assurez-vous que votre calendrier et votre capacité à exécuter sont compatibles avec cette probabilité. En fin de compte, passer à une approche active-active et abandonner une stratégie de reprise après sinistre peut vous aider à vous assurer qu'aucun sinistre n'endommage vos opérations.

Conseil n° 9 : Maximisez l'observabilité

La surveillance vous permet de savoir comment votre système fonctionne pendant un pic de trafic. Il est important de surveiller les mesures techniques ainsi que les mesures commerciales. La moitié de votre tableau de bord peut être dédiée à des métriques techniques telles que le processeur, le débit et le temps de chargement des pages, tandis que l'autre moitié suit des mesures commerciales telles que les taux de clics, les abandons de panier et les conversions. Vous avez besoin des deux, étant donné que les métriques techniques peuvent vous dire pourquoi quelque chose ne fonctionne pas, mais ne vous diront pas le poids du problème sur les utilisateurs réels. Pour cela, vous avez besoin des métriques métier associées. Maximiser l'observabilité de ces métriques vous aide à détecter les anomalies, ce qui peut déclencher des actions automatisées pour réparer les dommages.

Chapitre 3 :

Renforcer votre infrastructure de sécurité

La sécurité est toujours abordée en termes de risque — identification des risques, atténuation des risques, impact des risques, probabilité des risques — et il est essentiel de décider de la façon dont vous réagirez à ce risque. Il s'agit essentiellement d'équilibrage. Vous pouvez choisir d'être plus agressif contre les risques potentiels lors des pics de trafic, par exemple, mais cela pourrait affecter votre expérience utilisateur. Les meilleures pratiques en matière de sécurité consistent à s'assurer que votre plateforme dispose de contrôles bien ajustés, à définir des seuils de trafic, à déterminer comment consommer les alertes et à établir un plan d'action en cas de problème.

[Découvrez les six meilleures pratiques suivantes.](#)

Conseil n° 10 : Passez en revue votre runbook

Votre runbook doit détailler toutes les informations pertinentes sur les personnes, les processus et les conditions préalables dans votre stratégie de sécurité. Pour les employés, dressez la liste des horaires des quarts de travail, de la base de connaissances et des lacunes, ainsi que de la formation requise. Pour les processus, créez un protocole ou un organigramme afin que tout le monde sache quoi faire et qui contacter pour chaque éventualité. Pour les conditions préalables, décrivez les dépendances et les exigences de communication pour les remontées de sécurité. Le runbook doit également énumérer les protocoles d'urgence visant à protéger l'origine autant que possible.

Conseil n° 11 : Ne soyez pas pris de court par des attaques DDoS

Pour atténuer les attaques DDoS, assurez-vous que votre plateforme dispose de contrôles de débit bien réglés. Refusez le trafic au-dessus de certains seuils et envoyez un retour HTML sain pour tromper le trafic de bot. La mise en cache est une arme efficace contre les attaques DDoS, alors mettez en cache autant que possible. Effectuez un exercice sur table pour identifier les angles morts ou les inefficacités dans vos processus de réponse aux incidents. Pour des contrôles d'atténuation plus efficaces, travaillez avec un fournisseur de sécurité qui comprend votre environnement et la nature de vos applications Web.

Conseil n° 12 : N'oubliez pas le client

Avec le [web skimming](#), [la chaîne logistique et les attaques de type Magecart en hausse](#), il est essentiel (et obligatoire avec PCI DSS 4.0) que vous géiez et surveilliez tous les comportements d'exécution JavaScript sur vos applications Web pour vous défendre contre les [attaques côté client](#) pendant votre pic d'activité et *au-delà*. La saison des fêtes en particulier est également un moment privilégié pour les fraudeurs de détourner votre marque, de [créer de faux sites et comptes de réseaux sociaux](#) conçus pour voler des identifiants et des informations de carte de crédit, ou vendre des marchandises contrefaites ou de fausses réservations. Dans le cadre de votre stratégie, assurez-vous de disposer d'un outil de surveillance en place, et d'un plan pour réagir lorsqu'un faux site ou un abus est détecté, afin de protéger la fidélité et la confiance des clients.

ANALYSE : Les attaques DDoS battent des records

[Les attaques DDoS ont considérablement augmenté](#) en taille et en sophistication. En fait, 8 des 10 plus grandes attaques DDoS atténuées par Akamai ont eu lieu entre la mi-2022 et fin 2023. En février 2023, Akamai a protégé un client contre une attaque DDoS de grande envergure atteignant un pic de 900,1 gigabits par seconde (Gbit/s) et 158,2 millions de paquets par seconde (Mpps).



Conseil n° 13 : Comprenez la surface d'attaque de vos API

La prolifération des API est un défi pour toute organisation et en particulier pour le secteur du commerce. Configurez un processus de découverte d'inventaire pour les API et exécutez l'audit. Votre équipe de sécurité ne connaît peut-être pas les nouvelles API que votre équipe exécute sur la plateforme. Il est donc important d'enregistrer ces nouvelles API sur la plateforme et de s'assurer que l'inventaire est exact. Si votre équipe de sécurité ne reconnaît pas une API, elle peut la bloquer, mais si des API sont enregistrées, l'équipe peut les protéger. Une autre bonne pratique consiste à vous assurer que votre pare-feu d'application Web est à jour et en mode automatique.

Conseil n° 14 : Réglez les alertes pour réduire le bruit

Il est important de tout surveiller, mais créer trop de bruit peut constituer un danger. Un trop grand nombre d'alertes est contre-productif, car votre équipe peut ne pas identifier ce qui est important. Le réglage de vos alertes vous aide à réduire le bruit et à être plus réactif. Effectuez cette étape bien avant un événement de forte affluence, pas à la dernière minute. Et il est important de développer un plan de routage pour les alertes permettant de transmettre les informations clés afin que les bonnes personnes puissent répondre.

Conseil n° 15 : Renforcez votre défense contre les bots malveillants

Certains types de bots peuvent être considérés comme bénins, mais d'autres peuvent être utilisés pour lancer des attaques DDoS, récupérer du contenu ou de l'inventaire, ouvrir de faux comptes, exécuter des attaques par credential stuffing et pire encore. Même les bots bienveillants peuvent ralentir votre site à des vitesses inacceptables lors de votre pic de trafic. Assurez-vous que votre stratégie en matière de bot vous permet d'être aussi agressif que nécessaire pour arrêter les bots malveillants, en vous concentrant sur les protocoles d'urgence pour savoir quoi faire, comment le faire et avec qui travailler pour les neutraliser. Des outils peuvent vous permettre de suivre les bots séparément et de tenir compte avec précision de l'impact d'une attaque qui peut mener à des comptes compromis, des pannes et même des violations de données.

Chapitre 4 :

Enregistrer les leçons apprises

Le processus de préparation et de réalisation des pics de trafic fournit beaucoup d'informations techniques et commerciales, ce qui rend essentiel l'enregistrement des leçons apprises pour aider votre équipe à s'améliorer. Cependant, trouver le temps et l'énergie pour mener un examen officiel peut être difficile, surtout après les vacances de fin d'année. Pour les entreprises qui subissent des pics de trafic réguliers ou fréquents, il peut être difficile de planifier ces examens. Cependant, nous pensons qu'il est nécessaire de mettre votre évaluation post-événement sur le calendrier afin qu'elle soit plus susceptible de se produire.

Pour vous aider à faire cela, nous vous donnons un conseil bonus.

Conseil bonus n° 16 : Effectuez un examen formel

Effectuez votre évaluation peu après l'événement, alors qu'il est encore frais dans l'esprit de tous les membres de votre organisation. Avec un souvenir clair de l'événement, votre équipe est en mesure d'apporter des informations exploitables pour interpréter les données précieuses que vous avez recueillies lors de l'événement et prioriser les activités pour la prochaine fois.



Avez-vous mesuré les bonnes choses ?



Avez-vous identifié des lacunes dans vos indicateurs ou processus que vous souhaitez combler avant le prochain événement ?

Préparer longtemps à l'avance un examen post-événement formel de vos performances techniques et commerciales vous permet de tirer le meilleur parti de ce que vous avez appris et des données que vous avez recueillies.





Transformez votre approche des pics de trafic

Quand n'importe quel jour peut être un jour de forte affluence, votre objectif doit être de faire des pics de trafic moins une exception et plus une occurrence standard pour laquelle vous êtes toujours prêt. C'est là que nous entrons en jeu. Obtenir l'assistance d'un expert tel qu'Akamai permet de faciliter l'ensemble du processus. Et au fur et à mesure que vous apprenez, vous pouvez intégrer progressivement vos préparations dans votre architecture technique, vos processus et votre culture afin qu'elles deviennent une seconde nature. Alors, n'importe quel jour pourrait être un jour de forte affluence, et votre équipe y sera bien préparée.

Êtes-vous prêt à élever les performances de votre entreprise lors des pics de trafic ?

[En savoir plus](#) sur les informations et solutions d'Akamai pour la vente au détail, les voyages et l'hôtellerie, ou [contactez un expert Akamai](#).

Akamai protège votre expérience client, votre personnel, vos systèmes et vos données en vous aidant à intégrer la sécurité dans tout ce que vous créez, dans toutes vos conceptions et diffusions. La visibilité de notre plateforme sur les menaces mondiales nous aide à adapter et à faire évoluer votre stratégie de sécurité (activer le Zero Trust, bloquer les ransomwares, sécuriser les applications et les API, ou lutter contre les attaques DDoS), vous donnant ainsi la confiance nécessaire pour innover, prospérer et ouvrir le champ des possibles. Pour en savoir plus sur les solutions de Cloud Computing, de sécurité et de diffusion de contenu, rendez-vous sur akamai.com et akamai.com/blog, ou abonnez-vous à Akamai Technologies sur [X](#) (anciennement Twitter) et [LinkedIn](#).

