Akamai

LIVRE BLANC

11 idées reçues qui persistent sur les attaques DDoS

Ces dernières années, les attaques par déni de service distribué (DDoS) ont considérablement augmenté et ont parfois atteint des records en termes de taille, d'échelle, de distribution et de sophistication. Malheureusement, de nombreuses organisations s'accrochent encore à une pensée dépassée sur la façon de se défendre : en supposant que leurs défenses sont suffisantes, ou pire, qu'elles sont peu susceptibles d'être une cible. La vérité est tout autre : les victimes de ces attaques couvrent tous les secteurs clés, des services financiers au commerce électronique en passant par les jeux en ligne. En fait, les attaques contre des infrastructures publiques essentielles, notamment les services et équipement liés à la santé, l'éducation, l'énergie et les transports, ont été particulièrement préoccupantes. En 2023, Akamai a protégé un client de la région Asie-Pacifique contre une attaque massive de 900 Gbit/s (Gigabits par seconde). Plus tard dans la même année, Akamai a empêché une attaque de 634 Gbit/s et 55 Mpps (millions de paquets par seconde) qui comportait une combinaison complexe de vecteurs d'attaque ; l'une des plus importantes attaques jamais perpétrées contre un client américain du secteur financier. Celle-ci s'ajoute à la plus grande attaque DDoS qu'Akamai a atténuée à ce jour : une attaque distribuée à 1,44 Tbit/s et 385 Mpps qui a duré près de deux heures. Ces événements montrent clairement que les cybercriminels continuent de cibler des piliers essentiels de l'économie.

L'ampleur de ces attaques peut amener certaines petites entreprises à penser que le risque de devenir la cible d'une attaque DDoS est faible. Mais, en réalité, les services et applications stratégiques dans tous les secteurs sont des cibles faciles. La montée en puissance des hacktivistes motivés par des raisons politiques et idéologiques, et le coût relativement faible des DDoS en tant que service offert par des groupes cybercriminels, tels que Killnet et Anonymous Sudan, ont fait de presque tout le monde une cible potentielle. De plus, ce n'est pas seulement l'attaque initiale dont les organisations doivent s'inquiéter. Les attaques DDoS sont de plus en plus utilisées comme écran de fumée pour détourner l'attention des ressources réseau et de sécurité tandis que les attaquants tentent des attaques DDoS par ransomware simultanées (RDDoS) ou d'autres exploits néfastes comme des campagnes d'extorsion triples. Enfin, l'utilisation croissante et alarmante d'outils d'intelligence artificielle pour orchestrer des attaques DDoS hautement sophistiquées et distribuées crée un défi défensif majeur pour les entreprises et les institutions publiques qui doivent garantir une disponibilité et des performances constantes.

Alors que les menaces deviennent de plus en plus complexes et évoluent presque chaque jour, les idées reçues sur la protection contre les attaques DDoS sont malheureusement nombreuses à subsister, certaines d'entre elles étant même mises en avant par des fournisseurs de solutions de sécurité. La protection contre les attaques DDoS doit être un principe clé de toute stratégie de sécurité. Il est donc essentiel de comprendre le danger que représentent ces fausses vérités pour élaborer votre défense contre ces attaques.

IDÉE REÇUE N°1

La capacité totale indique l'étendue totale des ressources disponibles en matière d'atténuation

Bien que la capacité totale soit importante, un simple chiffre de capacité réseau peut induire en erreur en omettant des détails majeurs. Les entreprises qui évaluent des solutions technologiques de protection contre les attaques DDoS doivent se poser les questions suivantes :

- Quelle est la capacité réseau dédiée à la consommation du trafic des attaques ?
- Quelle proportion des ressources du système d'atténuation est **formellement consacrée** à stopper les attaques ?
- Quelle proportion des ressources réseau et système est disponible pour fournir un trafic propre à toutes les origines des clients sur cette plateforme ?

Ces questions sont cruciales car si la capacité totale du réseau inclut d'autres exigences, telles que la diffusion de contenu, la capacité réelle de défense contre les attaques DDoS ne représente peut-être qu'une fraction de ce que le fournisseur prétend.

La capacité de défense DDoS ne se limite pas non plus à la technologie. À un moment donné, si la technologie cesse de fonctionner efficacement, y aura-t-il des ressources humaines dédiées aux escalades, à la réponse aux incidents et à l'optimisation des mesures d'atténuation ? L'atténuation la plus robuste combine l'automatisation et l'intelligence des machines avec l'expertise humaine pour offrir une protection approfondie.

Conseil

Examinez plus en détail les écarts entre la capacité totale du réseau fournisseur et la stabilité de sa plateforme, ainsi que la capacité dédiée à l'atténuation des attaques et à la diffusion de trafic propre. Ils doivent être considérés comme des segments uniques. Par exemple, la capacité doit être répartie par objectif, comme le routage réseau du trafic d'attaque, l'arrêt ou l'atténuation du trafic d'attaque et la diffusion d'un trafic propre au centre de données.

IDÉE REÇUE N°2

La protection DDoS des fournisseurs de services Internet et/ou des fournisseurs de services cloud est suffisante

Malheureusement, de nombreuses organisations pensent encore que la protection offerte par leur fournisseur d'accès à Internet (FAI) est tout ce dont elles ont besoin. La vérité est tout autre : en général, les FAI ne fournissent qu'une protection DDoS prête à l'emploi, redimensionnée à des fins commerciales et avec une bande passante limitée. Leur matériel est partagé entre leur propre infrastructure et la vôtre, ce qui se traduit par des contraintes de capacité et de cycles CPU. Les attaques DDoS sont aujourd'hui si massives qu'elles les submergent toutes les deux, et les FAI vont rediriger votre trafic vers un « trou noir » (ou blackhole) afin d'éviter les dommages collatéraux sur d'autres ressources de production. Lorsque le « blackholing » est déclenché, les entreprises perdent le trafic et les services légitimes des utilisateurs finaux, rendant ainsi l'attaque réussie en mettant l'entreprise hors ligne à toutes fins pratiques.

En outre, comme les fournisseurs de services cloud (CSP) permettent souvent aux clients de définir leurs propres contrôles et de maintenir la souveraineté sur leur posture de sécurité au sein de l'environnement cloud du CSP, la plupart des CSP eux-mêmes rejettent généralement toute responsabilité et finissent par facturer les clients pour le trafic DDoS illégitime. Cela peut entraîner des dépassements importants pour les victimes, compte tenu de l'ampleur et de la taille des attaques DDoS actuelles.

Conseil

Vérifiez attentivement et négociez les clauses de protection DDoS avec votre FAI ou CSP. En outre, déterminez si votre FAI utilise un matériel de protection DDoS robuste sur site avec une sauvegarde dans le cloud afin que les attaques DDoS petites mais rapides soient atténuées sur site tandis que les attaques volumétriques de grande envergure puissent être correctement atténuées par un service de protection DDoS dans le cloud.

IDÉE REÇUE N°3

Tous les accords de niveau de service (SLA) de temps d'atténuation sont égaux

Parfois, les chiffres peuvent être trompeurs. Le temps d'atténuation (TTM) est un nombre souvent utilisé comme argument commercial par les fournisseurs de sécurité. Le TTM définit la rapidité avec laquelle un trafic DDoS malveillant est bloqué ou arrêté, sans affecter le trafic et les utilisateurs légitimes. Or, cela laisse une large place à l'interprétation. Par exemple, un fournisseur peut ne pas considérer une augmentation du trafic comme une attaque DDoS tant qu'elle n'a pas duré au moins cinq minutes consécutives. Il est donc possible que le compteur SLA ne démarre pas dans les cinq premières minutes de l'attaque. La durée moyenne des attaques étant inférieure à cinq minutes, vous pouvez voir à quel point cela est problématique. En d'autres termes, un temps annoncé de 10 secondes pour atténuer une attaque pourrait être en fait de plus de cinq minutes.

D'autres fournisseurs définissent le temps d'atténuation comme la vitesse à laquelle une règle d'atténuation peut être déployée. Il ne reflète pas l'arrêt de l'attaque, ni la qualité ou la cohérence avec laquelle ce contrôle est activé. En fin de compte, ce qui vous importe, c'est le temps nécessaire pour sécuriser et rétablir les ressources Internet, **avec le moins d'impact possible sur les utilisateurs ou les services légitimes.** Veillez à lire attentivement les petites lignes du SLA de votre fournisseur.

Conseil

Examinez soigneusement les détails relatifs au temps d'atténuation indiqués dans un SLA. Il doit représenter l'équation : Le temps réel qui compte = temps de détection des attaques + temps d'application des contrôles d'atténuation + temps de blocage/arrêt des attaques + qualité/cohérence des mesures d'atténuation. Sélectionnez un fournisseur qui offre un **véritable SLA zéro seconde** pour atténuer les attaques DDoS sans affecter les utilisateurs légitimes.

IDÉE REÇUE N°4

Le routage vers une interface nulle ou « blackholing », et la limitation du débit sont des défenses acceptables

Le routage nul (ou blackholing) est une réponse défensive commune et plutôt primitive de certains fournisseurs de protection contre les attaques DDoS. Lorsqu'une ressource est attaquée et met en danger d'autres clients ou services, le fournisseur peut essayer d'éviter les dommages collatéraux en faisant disparaître le trafic de cette ressource dans un trou noir virtuel. Cette solution est-elle réellement efficace ? Du point de vue d'un attaquant, le blackholing signifie que la mission est accomplie : la ressource ciblée est effectivement hors ligne. Selon l'infrastructure du fournisseur, d'autres clients peuvent également être déconnectés ou subir une dégradation de leurs performances.

Une autre réponse primitive de défense contre les attaques DDoS proposée par de nombreux fournisseurs de sécurité consiste à imposer des limites de débit au trafic client comme contre-mesure dans les environnements partagés. Cependant, une baisse de 20 à 40 % du trafic légitime pour donner l'impression que la ressource ou le service est toujours opérationnel n'est pas un résultat satisfaisant pour le client attaqué. La limitation de débit est efficace comme contre-mesure secondaire ou tertiaire lors de la gestion d'attaques DDoS au niveau des couches 3, 4 et 5. Lorsque vous êtes confronté à des attaques DDoS de couche 7, la limitation du débit peut être un contrôle initial plus efficace, mais vous devez toujours vous fier en premier lieu à l'atténuation des signatures. Vous méritez une protection de votre infrastructure numérique efficace à 100 % contre les attaques DDoS, quelle que soit la couche du modèle d'interconnexion des systèmes ouverts qu'elles affectent, et certainement pas seulement 60 % ou moins.

Conseil

Demandez à votre fournisseur à quelle fréquence il active des trous noirs ou des limites de trafic, en période normale et lors d'une attaque. Déterminez dans quelles circonstances un fournisseur fera disparaître du trafic dans un trou noir et quels critères vous devrez remplir pour que vos services soient restaurés.

IDÉE REÇUE N°5

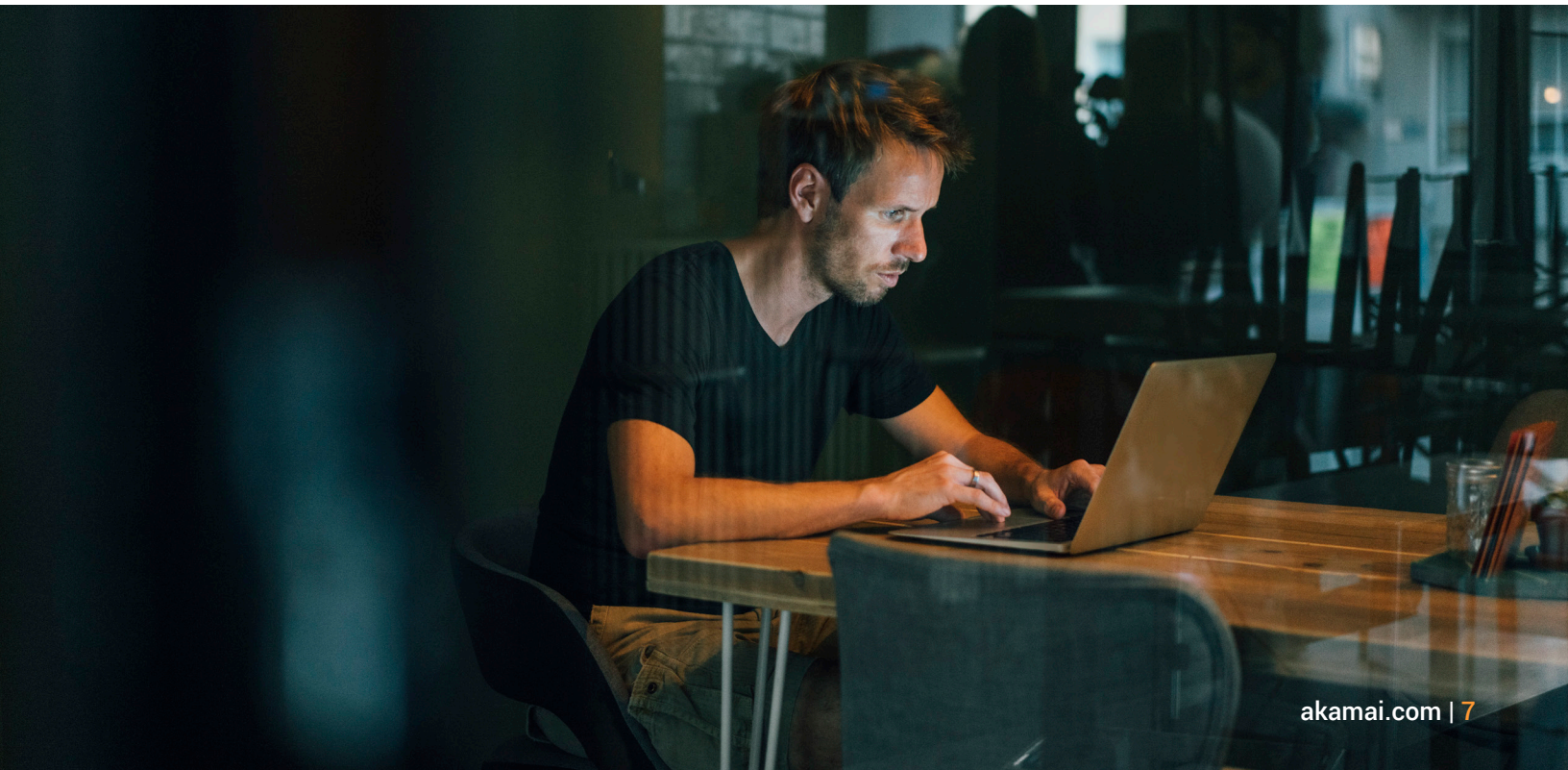
Peu importe qui partage la plateforme cloud

Chaque entreprise a besoin de sécurité. Les entreprises controversées qui attirent des attaques fréquentes, comme celles du marché gris telles que les sites de jeux d'argent ou pornographiques, ont aussi besoin de défenses de sécurité contre les attaques DDoS. Même les entreprises qui font la promotion d'activités criminelles et d'attaques terroristes se dotent d'une cybersécurité auprès de fournisseurs de cloud légitimes.

Vous pensez sans doute que cela ne vous concerne pas. Toutefois, si votre entreprise partage une plateforme de sécurité dans le cloud avec une entreprise illégale ou qui est cible d'attaques fréquentes, le risque de dommages collatéraux est élevé. Les ressources du fournisseur peuvent être impactées, voir submergées, laissant votre entreprise exposée.

Conseil

Lisez attentivement la politique d'utilisation acceptable d'un fournisseur de solutions de sécurité dans le cloud, pour vous assurer que vous ne partagerez pas les ressources de la plateforme de sécurité avec des cibles à haut risque. Consultez également les conseils donnés à la suite des idées reçues N°1 et 2 concernant la capacité et les règles d'application.



IDÉE REÇUE N°6

Un pare-feu d'application Web est suffisant pour la protection contre les attaques DDoS

Les pare-feux d'applications Web (WAF), qui font souvent partie du groupe plus large de solutions de protection des applications Web et des API (WAAP), offrent une protection efficace contre les attaques DDoS de la couche applicative (couche 7). Bien qu'ils puissent fournir une protection de base de la couche réseau (couche 3) ou de la couche transport (couche 4), il ne suffit pas de couvrir tous les IP, ports et protocoles de manière exhaustive.

Les attaques DDoS se déclinent en différentes versions et formats, et peuvent cibler les couches d'infrastructure (couches 3 et 4), les couches applicatives HTTP (couche 7) et l'infrastructure DNS. De plus, les attaquants basculent souvent les attaques de façon dynamique et pourraient, par exemple, commencer par l'infrastructure DNS, puis ensuite s'étendre à d'autres couches ou protocoles. La véritable protection DDoS s'appuie sur une stratégie de défense en profondeur qui adopte une plateforme de solutions robustes dotées de forces et de capacités spécifiques pour offrir une protection aux couches 3, 4, 7 et DNS. Une seule solution ne suffit pas toujours à protéger toutes les bases, et peut rendre votre organisation vulnérable aux attaques et aux niveaux de risque plus élevés en cas d'atténuation excessive du trafic ou des services légitimes.

Conseil

Assurez-vous que votre solution de protection contre les attaques DDoS n'est pas orientée vers un type particulier d'attaque DDoS ou de conception d'implémentation. La meilleure défense provient d'un fournisseur unique, capable de fournir plusieurs fonctionnalités de protection DDoS dédiées qui maintiennent l'interopérabilité et sont prises en charge par une équipe unifiée de services de sécurité à réponse rapide pour protéger vos ressources de production. La situation devient complexe lorsque ces ressources sont déployées sur des réseaux hybrides et des environnements hébergés dans le cloud. Les services de protection doivent être indépendants du réseau ou du modèle de déploiement.

IDÉE REÇUE N°7

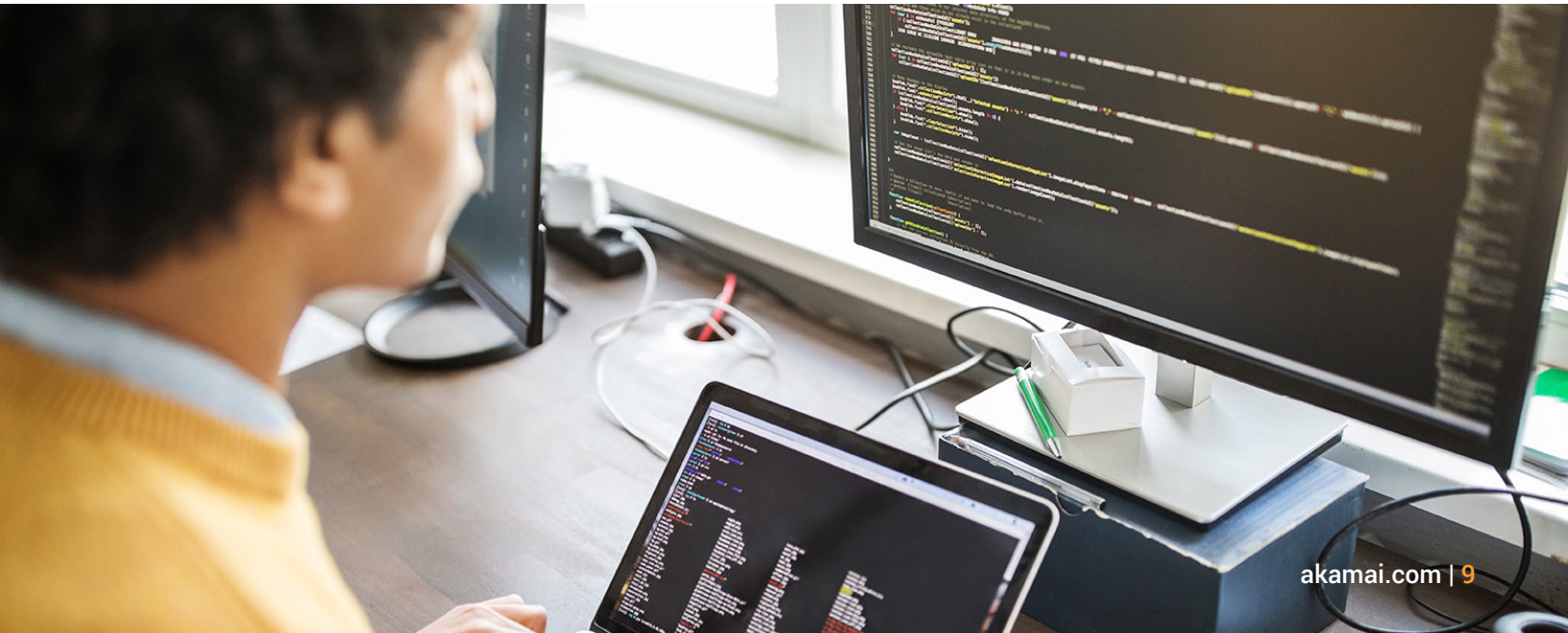
Une plateforme de sécurité tout-en-un garantit une meilleure expérience de sécurité

Certains fournisseurs proposent une variété de services empilés sur une plateforme cloud unique. Cela pourrait réduire la complexité technique du déploiement et de l'intégration des contrôles de sécurité à court terme. Mais plusieurs services qui partagent la même infrastructure back-end et les mêmes réseaux sont vulnérables aux pannes de plateforme, aux dommages collatéraux et aux problèmes de résilience si d'autres parties de l'environnement sont perturbées. Souvent, les fournisseurs de guichet unique préfèrent sacrifier la fonctionnalité en raison des limites de leur approche à plateforme unique.

Un maillage transparent de plateformes ou de solutions fabriquées sur mesure de réseau de diffusion de contenu (CDN), de DNS et de protection contre les attaques DDoS, conçu pour résoudre des problèmes techniques et de sécurité spécifiques, permet d'améliorer la qualité des mesures d'atténuation et des performances à grande échelle et d'optimiser les postures défensives.

Conseil

Gardez à l'esprit que vous n'avez pas besoin de partager la même infrastructure pour obtenir une expérience de sécurité unifiée. Une approche de défense basée sur la diversité utilise des architectures sous-jacentes qui peuvent offrir une expérience utilisateur ininterrompue ainsi que de hautes performances en termes de sécurité et d'atténuation.



IDÉE REÇUE N°8

La protection DDoS n'est pas nécessaire pour IPv6

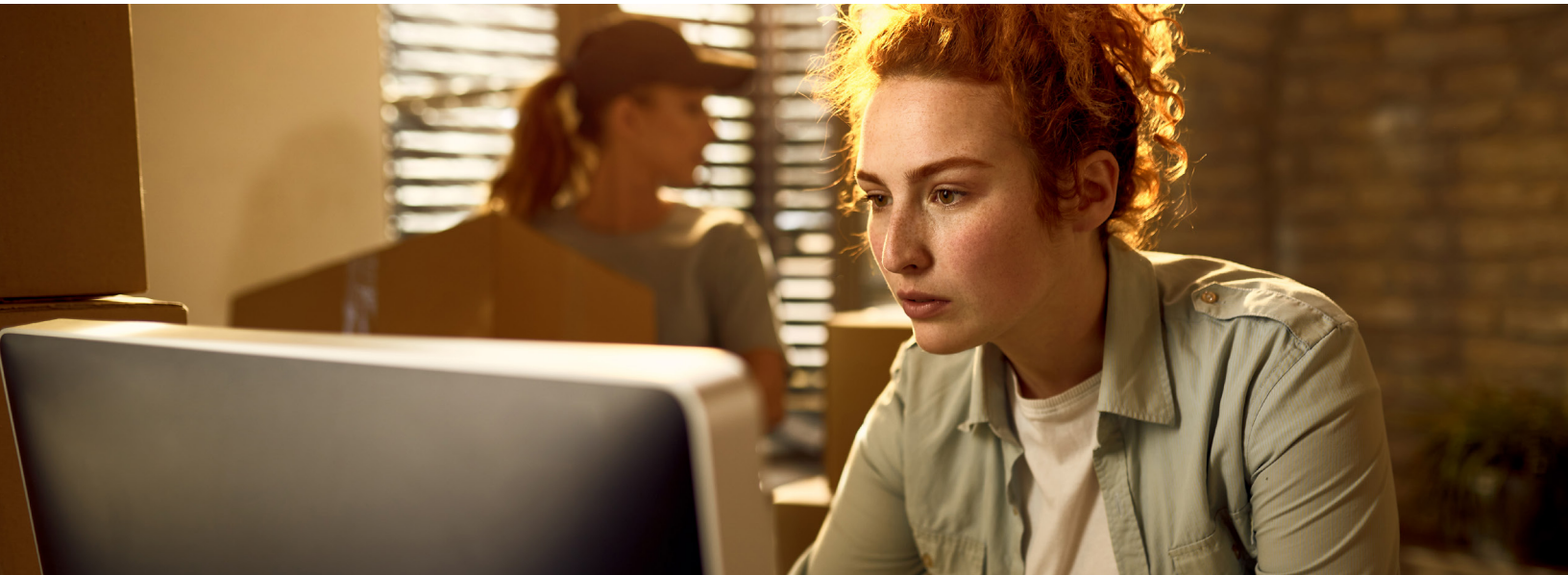
Selon Google, environ 45 % du trafic Internet provient de terminaux compatibles IPv6. En termes d'attaques DDoS, IPv6 introduit quelques améliorations par rapport à IPv4, telles qu'un espace d'adressage plus grand et des fonctionnalités de sécurité intégrées comme IPsec, mais il ne protège pas intrinsèquement contre ces types d'attaques.

Les attaques DDoS peuvent cibler à la fois les réseaux IPv4 et IPv6 en les submergeant d'un volume important de trafic, en exploitant des vulnérabilités ou en utilisant divers vecteurs d'attaque indépendants de la version IP. Les cybercriminels utilisent déjà l'espace IP considérablement élargi d'IPv6 pour créer des attaques DDoS volumétriques encore plus importantes. Dans certains cas, les attaquants ont envoyé du trafic à des adresses aléatoires dans un réseau, créant une tempête de diffusion sur la couche réseau physique, et bloquant et épuisant les ressources du routeur ou du réseau.

La fragmentation actuelle entre IPv4 et IPv6 ajoute de nouvelles complexités, car les environnements IPv6 propres ne peuvent généralement pas être pris en charge.

Conseil

La protection DDoS pour IPv6 nécessite des stratégies et des technologies similaires à celles pour IPv4, y compris la surveillance du réseau, le filtrage du trafic, la limitation du débit et l'utilisation de services spécialisés d'atténuation des attaques DDoS.



IDÉE REÇUE N°9

Vous n'avez pas besoin de plusieurs couches de défense

La plupart des organisations n'y croient pas, mais certaines construisent parfois leur stratégie de défense comme si c'était vrai. Lorsque vous sécurisez votre maison, le fait de verrouiller votre porte d'entrée ne signifie pas que vous pouvez laisser la porte arrière et vos fenêtres ouvertes. Une véritable défense DDoS est obtenue en construisant des couches de sécurité qui fonctionnent ensemble de manière homogène pour empêcher les attaquants d'atteindre leur objectif en un seul coup.

Une défense DDoS de classe mondiale commence par un pare-feu cloud réseau qui réduit la charge de vos pare-feux à la bordure de l'Internet de votre réseau. Ensuite, un modèle de protection contre les attaques DDoS hybrides inclura une protection sur site basée sur des configurations matérielles contre les attaques DDoS courtes mais précises, et reviendra à une protection dédiée basée sur le cloud pour les attaques DDoS de grande envergure, complexes et volumétriques. Votre infrastructure DNS doit également être protégée par une stratégie similaire en couches qui inclut l'utilisation d'un service proxy capable de mettre en œuvre de manière dynamique des stratégies de sécurité à la bordure de l'Internet de votre réseau et qui se superpose également avec une solution DNS faisant autorité, en mode primaire ou secondaire. Enfin, vous devez protéger toutes vos applications et API avec une solution WAAP robuste qui inclut la fonctionnalité WAF.

Conseil

Superposez des technologies et des solutions de pointe avec des forces différentes et dédiées pour construire une stratégie complète de défense en profondeur qui rend la tâche extrêmement difficile pour les cybercriminels de réussir leur attaque.

IDÉE REÇUE N°10

Chaque centre d'opérations de sécurité offre le même niveau de support

De nombreux fournisseurs annoncent la prise en charge des centres d'opérations de sécurité (SOC). Mais la disponibilité d'un SOC 24 h/24 et 7 j/7 n'est pas ce qui importe le plus. Ce qui est important, c'est le niveau de service et d'expertise auquel vous pouvez prétendre lorsque vos ressources sont attaquées. Lorsque vous évaluez des fournisseurs de protection contre les attaques DDoS, vous devez prendre en compte les points suivants :

- Quel type d'assistance et d'analyse recevrez-vous avant, pendant et après une attaque ?
- Comment sont constituées les équipes du SOC qui assurent la continuité de la défense ?
- Si vous contactez le SOC, la personne que vous appelez est-elle l'analyste en charge des mesures d'atténuation, ou simplement le point de contact de remontée ?
- Votre fournisseur dispose-t-il de professionnels de la sécurité formés à l'atténuation, ou bien s'agit-il simplement de « gendarmes du trafic » qui acheminent le trafic vers des dispositifs d'atténuation prêts à l'emploi ?
- Propose-t-il un runbook personnalisé ?

Le centre d'opérations de sécurité (SOC) de votre fournisseur de sécurité doit servir de prolongement à votre équipe de réponse aux incidents pour générer une valeur réelle.

Conseil

Évaluez la qualité d'assistance que vous pouvez attendre du centre d'opérations de sécurité (SOC) du fournisseur de services. Outre la détection et l'atténuation des attaques, déterminez s'il offre des services d'intégration et de test, de dépannage des incidents, d'analyse post-hoc (leçons apprises) et d'un support de conception pour réduire la surface d'attaque.

IDÉE REÇUE N°11

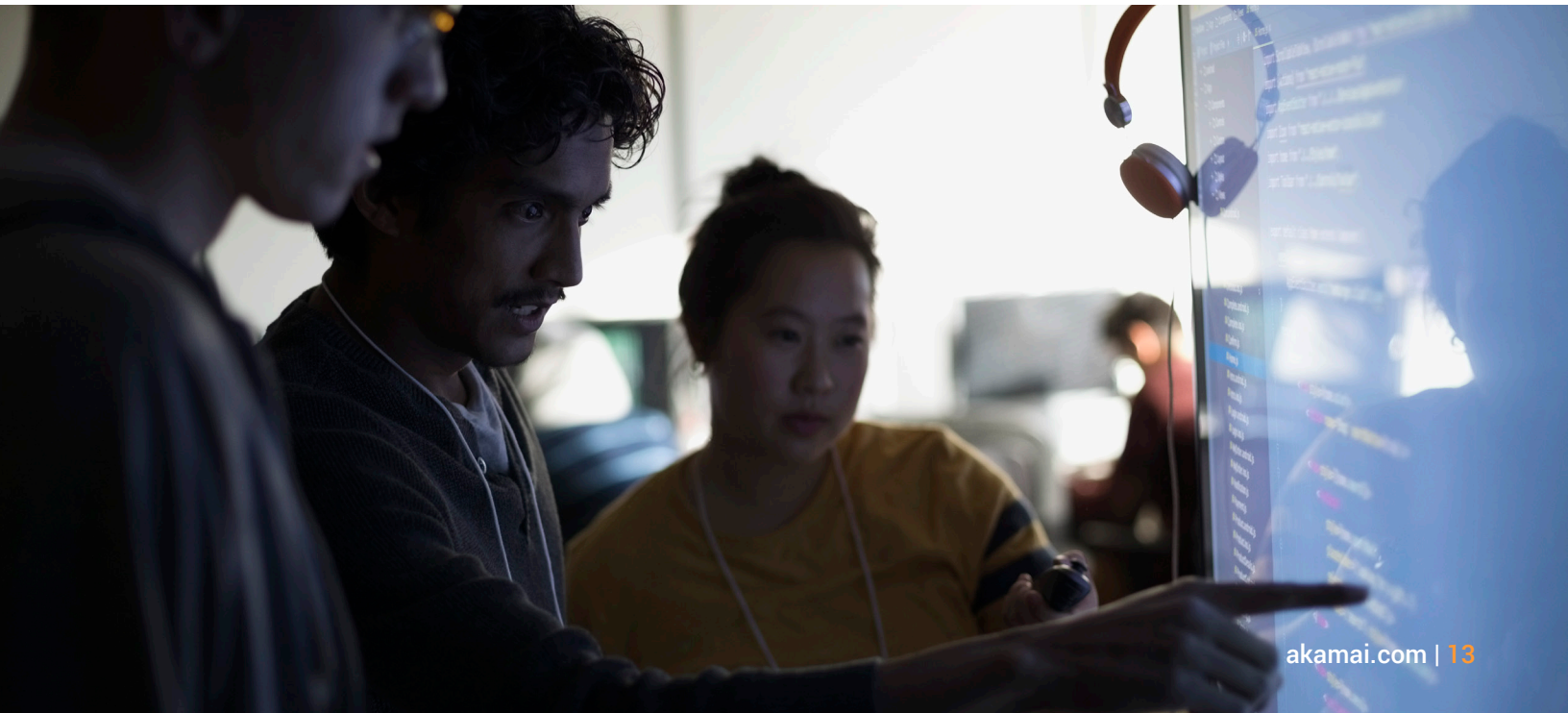
La protection contre les attaques DDoS est un produit ancien, donc la solution la moins chère suffira

La maxime « rien n'est jamais gratuit » est probablement la plus pertinente dans la protection contre les attaques DDoS. Même si un prix inférieur peut sembler attractif, il peut y avoir des coûts cachés.

Certains fournisseurs proposent un prix bas, mais limitent le nombre ou la taille des attaques qu'ils atténueront. Si vous êtes visé par un grand nombre d'attaques ou par une attaque trop importante, ils vous demanderont d'opter pour un niveau de service plus élevé (et plus coûteux) avant d'arrêter l'attaque, et ce, tandis que vous essayez de remettre votre entreprise en ligne. Les fournisseurs de sécurité DDoS chevronnés offrent aux clients la flexibilité de choisir entre une protection DDoS « toujours active » et « à la demande », et de passer de l'une à l'autre en toute transparence, afin de maintenir des coûts d'exploitation bas tout en offrant la meilleure protection de sa catégorie. Lorsque vous comparez les fournisseurs et les prix, assurez-vous de comprendre ce que cela implique en termes de fonctionnalités et d'impacts sur votre posture de sécurité contre les attaques DDoS.

Conseil

Sachez ce qui est inclus dans le prix qui vous est proposé avant de signer.



La sécurité DDoS est complexe et nécessite beaucoup de temps et de ressources dans le contexte actuel en rapide évolution. Ce qui a fonctionné hier pourrait ne pas fonctionner aujourd'hui ou demain. Rester connecté aux utilisateurs finaux et à vos salariés est la base de votre activité. Il n'y a pas de place pour l'erreur ici. Et il est inutile de supporter un coût élevé en tentant de faire cavalier seul. En tant que plateforme de protection DDoS la plus complète, la plus flexible et la plus fiable, Akamai peut vous aider.

En savoir plus à propos des solutions de sécurité DDoS d'Akamai.

À propos d'Akamai Security

Akamai Security protège les applications qui stimulent votre activité à chaque point d'interaction, sans compromettre les performances ou l'expérience client. En tirant parti de l'envergure de notre plateforme mondiale et de la visibilité qu'elle offre sur les menaces, nous travaillons avec vous pour prévenir, détecter et atténuer les menaces, afin de vous permettre de renforcer la confiance en votre marque et de concrétiser votre vision. Pour en savoir plus sur les solutions de Cloud Computing, de sécurité et de diffusion de contenu d'Akamai, rendez-vous sur akamai.com et akamai.com/blog, ou abonnez-vous à Akamai Technologies sur X (anciennement Twitter) et LinkedIn. Publication : 10/24.