Akamai

LIVRE BLANC

9 mythes sur la défense contre les attaques DDoS

Au cours des deux dernières années, la taille des attaques par déni de service distribué (DDoS) a doublé et le nombre et les combinaisons de vecteurs d'attaque ont considérablement augmenté. En 2020, une attaque de 809 millions de paquets par seconde (Mpps) a frappé une entreprise, faisant de cet événement la plus grande attaque en nombre de paquets par seconde jamais enregistrée. Bien que certaines entreprises puissent penser qu'elles sont des cibles à faible risque d'attaque DDoS, les services et applications stratégiques de tous les secteurs sont des proies de choix et toute entreprise peut être exposée à des temps d'arrêt et à une baisse de performance si l'infrastructure n'est pas protégée.

La protection contre les attaques DDoS doit être un élément clé de votre stratégie de sécurité globale, il est donc essentiel que vous ayez connaissance des principaux mythes pour déterminer au mieux votre position défensive face aux attaques DDoS.

Il existe de nombreux mythes autour de la protection contre les attaques DDoS, dont certains sont alimentés par des fournisseurs de sécurité eux-mêmes.

Mythe 1. La capacité totale indique les ressources d'atténuation disponibles

Un simple chiffre de capacité réseau ne suffit pas à fournir toutes les informations importantes. Il convient notamment de répondre aux questions suivantes : Quelle est la capacité réseau dédiée à la consommation du trafic des attaques ? Quelle proportion des ressources du système d'atténuation est 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 ? Et la capacité ne se limite pas qu'à la technologie. À un certain point, si les technologies ne fonctionnent pas efficacement ou n'optimisent pas les mesures d'atténuation, quelle est la capacité humaine dédiée disponible pour traiter les problèmes remontés, gérer les interventions en cas d'incident et affiner les mesures d'atténuation ?

Conseil : examinez plus en détail les écarts entre la capacité totale du réseau et la stabilité de la plateforme d'un fournisseur, la capacité disponible pour l'atténuation des attaques et l'utilisation de la distribution de trafic propre.

Mythe 2. Tous les SLA de temps d'atténuation sont égaux

Le temps d'atténuation signifie la rapidité avec laquelle le trafic 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. Il est donc possible que le compteur SLA ne démarre pas dans les cinq premières minutes de l'attaque. En d'autres termes, une période annoncée de 10 secondes pour atténuer une attaque pourrait être en fait de cinq minutes ou plus. D'autres fournisseurs définissent le temps d'atténuation comme la vitesse à laquelle une règle d'atténuation peut être déployée. En fin de compte, ce qui vous intéresse, c'est le temps nécessaire au rétablissement du bon fonctionnement de vos ressources Internet. Veillez à lire attentivement les petites lignes de l'accord de niveau de service (SLA) de votre fournisseur.

Conseil : examinez soigneusement les détails relatifs au temps d'atténuation indiqués dans un SLA. Il doit représenter l'équation : temps de détection de l'attaque + temps d'application des contrôles d'atténuation + temps de blocage de l'attaque + qualité de l'atténuation = temps réel pour stopper l'attaque.

Mythe 3. Le blackholing et la limitation du débit sont des défenses acceptables

L'utilisation de trous noirs, ou « blackholing », est une réponse défensive courante de certains fournisseurs de protection contre les attaques DDoS. Lorsqu'une ressource est attaquée et met en danger d'autres clients, 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 de nombreux fournisseurs consiste à limiter le trafic client à titre de 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 positif pour le client attaqué.

Conseil : demandez à votre fournisseur à quelle fréquence il crée des trous noirs ou limite le 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.

Mythe 4. 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. 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. Il est facile de penser que cela ne vous concerne pas. Toutefois, si votre entreprise partage une plateforme de sécurité dans le cloud avec une entreprise illégale ou cible d'attaques fréquentes, le risque de dommages collatéraux est élevé. Les ressources du fournisseur peuvent être sous tension, voir submergées, laissant votre entreprise exposée.

Si votre entreprise partage une plateforme de sécurité dans le cloud avec une entreprise illégale ou cible d'attaques fréquentes, le risque de dommages collatéraux est élevé.

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.

Mythe 5. Une plateforme de sécurité tout-en-un implique une meilleure expérience de sécurité

Certains fournisseurs offrent une variété de services empilés sur une plateforme cloud unique, ce qui peut réduire la complexité technique pour le déploiement et l'intégration de contrôles de sécurité à court terme. Toutefois, lorsque plusieurs services partagent la même infrastructure back-end et les mêmes réseaux, ils sont vulnérables aux pannes de la plateforme, aux dommages collatéraux et aux problèmes de résilience lorsque d'autres parties de l'environnement sont perturbées. Il n'est pas rare que les fournisseurs de tout-en-un sacrifient des fonctionnalités en raison des limites de la conception d'une approche à plateforme unique. Un maillage transparent de clouds de réseau de diffusion de contenu (CDN), de DNS et de nettoyage DDoS dédiés, 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. Diverses architectures sous-jacentes peuvent fournir une expérience utilisateur fluide et une protection hautement performante.

Mythe 6. Une solution sur site offre davantage de contrôle

Bien qu'une solution sur site permette aux entreprises d'actionner elles-mêmes les commandes, le contrôle peut être illusoire. Le maillon le plus faible de toute solution sur site est souvent la taille de la liaison Internet. Les attaques DDoS sont de plus en plus nombreuses et complexes (multivectorielles), et même une attaque type de moins de 4 Gbit/s peut saturer la liaison Internet et entraîner un déni de service, y compris pour les centres de données qui bénéficient du meilleur matériel sur site. Pour les déploiements sur site, vous achetez essentiellement des minutes pour déplacer l'atténuation des attaques vers le cloud. Avec des compétences en matière de sécurité limitées et un personnel sous tension, les entreprises externalisent la protection contre les attaques DDoS vers des plateformes dans le cloud plutôt que de développer une expertise interne dans ce domaine.

Conseil : vous ne pouvez pas maîtriser les événements si votre réseau, votre service informatique et votre équipe de réponse aux incidents sont dépassés. Le DDoS est un vecteur d'attaque qui sera mieux géré par des experts en atténuation. Doublez vos capacités de réaction en interne en faisant appel à des experts en externe.

Mythe 7. 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. Prenons l'exemple d'une approche hybride. Une entreprise qui cherche à renforcer sa solution de sécurité sur site peut effectuer une mise à niveau en ajoutant une solution basée sur le cloud du même fournisseur. Se doter d'une solution tout-en-un peut être pratique, mais n'assure pas nécessairement une défense en profondeur. Si plusieurs couches de défense sont construites sur la même technologie sous-jacente, ces couches auront les mêmes lacunes et faiblesses, vous laissant tout aussi exposé.

Conseil : prévoyez des couches de technologies de pointe présentant des points forts et des points faibles différents, de sorte que les faiblesses d'une couche soient couvertes par la défense d'une autre couche.

Mythe 8. Chaque centre d'opérations de sécurité (SOC) offre le même niveau d'assistance

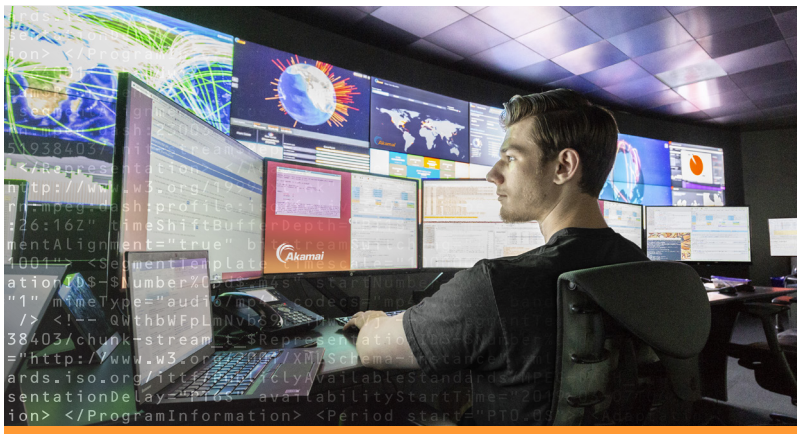
De nombreux fournisseurs annoncent sur leurs fiches techniques l'assistance d'un centre d'opérations de sécurité (SOC). Mais la disponibilité d'un SOC 24 h/24 et 7 j/7 n'est pas ce qui importe le plus. Ce qui est important, c'est le niveau de service et d'expertise auquel vous pouvez prétendre lorsque 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 remontée ? Votre fournisseur dispose-t-il de professionnels de la sécurité formés à l'atténuation, ou bien s'agit-il 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.

Mythe 9. La protection contre les attaques DDoS est exhaustive

Même si un prix inférieur peut sembler attractif, il peut y avoir des coûts cachés. Certains fournisseurs offrent 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 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. Lorsque vous comparez les fournisseurs et les prix, assurez-vous de comprendre ce que cela implique en termes de fonctionnalités et l'impact sur votre profil de risque.

Conseil : sachez ce qui est inclus dans le prix qui vous est proposé avant de signer.



Si vous êtes visé par un grand nombre d'attaques ou une attaque trop importante, certains fournisseurs 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.

La protection contre les attaques DDoS est complexe, chronophage et en constante évolution. Rester connecté aux consommateurs, à vos clients et à vos salariés est la base de votre activité. Il n'y a pas de place à l'erreur ici. Et il est inutile de supporter le coût élevé d'une tentative de faire cavalier seul. Akamai propose la plateforme de diffusion dans le cloud la plus importante et la plus fiable pour votre sécurité Web. Pour en savoir plus, rendez-vous sur www.akamai.com/secureapps.