DDoS : Cyberattaques Comprendre les faits

Neuf mythes concernant les attaques par déni de service distribué (DDoS)

Mythe no 1 : Mon secteur d'activité n'est pas visé par ce type d'attaque

Bien que certains secteurs d'activité soient plus susceptibles d'être victime d'une telle attaque, n'importe quel secteur peut être visé. La facilité d'accès et le faible coût d'exécution des attaques font en sorte que les pirates informatiques peuvent très facilement lancer des attaques contre n'importe quelle entreprise ou personne, dans n'importe quel secteur d'activité.

Mythe no 2 : Mon dispositif de protection contre les attaques DDoS est suffisant

Ces dispositifs peuvent assurer une protection, mais leur capacité de traitement a toujours une limite. La taille des attaques DDoS augmente de façon importante et celles-ci peuvent rapidement déborder la capacité de traitement d'un dispositif, laissant ainsi votre infrastructure vulnérable.

Mythe no 3 : J'ai seulement besoin d'augmenter ma largeur de bande

Le nombre croissant d'attaques, l'augmentation exponentielle de leur taille et la banalisation d'outils d'attaque signifient qu'il est facile de lancer des attaques qui peuvent dépasser la capacité de n'importe quel système. L'approvisionnement d'une largeur de bande additionnelle aura un effet très limité, car les nouvelles attaques consommeront rapidement toutes les ressources disponibles. Selon des recherches indépendantes, la saturation de la liaison Internet est le point de défaillance qui cause 36 % du temps d'arrêt causé par les attaques DDoS.

Mythe no 4 : J'ai seulement besoin d'obtenir plus d'adresses IP

Lorsqu'un dispositif se connecte à un réseau, sa nouvelle adresse IP devient connue en quelques minutes. Le passage à une nouvelle adresse IP ne fournira qu'un répit de courte durée jusqu'au moment où la nouvelle adresse IP est détectée. Si les attaques visent un domaine, alors le changement d'adresse IP n'aura aucun effet.

Mythe no 5 : Mon coupe-feu fournit une protection suffisante

Les coupe-feu ne peuvent pas protéger contre les attaques DDoS, car les pirates informatiques peuvent utiliser des méthodes qui exploitent des fonctions de messagerie ou des ports qui ont été conçus initialement à des fins légitimes. Comme l'indiquent des recherches indépendantes, les dispositifs comme les coupe-feu, les systèmes de détection d'intrusion (IDS) et les systèmes de prévention d'intrusion (IPS) sont des points de défaillance qui sont à l'origine de 31 % du temps d'arrêt causé par des attaques DDoS.

Mythe no 6 : Les attaques DDoS sont seulement des attaques massives

Bien que le nombre d'attaques massives au niveau de la couche réseau soit plus élevé, le nombre d'attaques au niveau de la couche application est aussi en augmentation. Les attaques utilisant plusieurs vecteurs deviennent de plus en plus courantes. Ces attaques combinent des attaques massives au niveau de la couche réseau avec des attaques sophistiquées au niveau de la couche application.

Mythe no 7 : Les attaques DDoS ne toucheront que mon site Web

N'importe quelle partie de votre infrastructure qui fait face à Internet peut être touchée : la chaîne d'approvisionnement, les points de vente, le traitement des transactions, les dossiers des patients et le service à la clientèle, pour ne nommer que ceux-là. Tous les systèmes communiquant avec l'extérieur doivent être protégés, peu importe où ils sont gérés. L'accès à vos systèmes en ligne peut même être bloqué si vos serveurs de noms de domaine (DNS) sont attaqués.

Mythe no 8 : Les solutions DDoS ne valent pas le prix demandé

Selon une étude récente, le temps d'arrêt moyen de systèmes de centre de données qui a été causé par une attaque DDoS est de neuf heures, représentant un coût moyen de 350 000 $. Une étude commandée par Bell a montré que 60 % des attaques coûtent entre 10 000 $ et 1 000 000 $. Les attaques sont de plus en plus nombreuses et gagnent en ampleur, de sorte que leur impact ne peut que croître.

Mythe no 9 : Mon organisation est trop petite, on ne l'attaquera pas

Les attaques DDoS peuvent frapper n'importe quelle entreprise. Une des plus grandes attaques jamais vues a été perpétrée contre une personne. Avec l'émergence d'attaques DDoS avec demande de rançon (RDDoS), les entreprises plus petites deviennent des proies plus faciles, car elles n'ont que des ressources informatiques limitées pour contrer ces attaques.

Si vous avez besoin de plus amples informations sur les attaques DDoS ou pour en savoir plus sur nos solutions de sécurité, veuillez visiter bell.ca/solutionssecurite.

Bell