Quels dégâts après une attaque DDoS ?

Quels dégâts après une attaque DDoS ?

Selon les résultats d'une étude réalisée par Kaspersky Lab et B2B International, une attaque DDoS contre les ressources en ligne d'une entreprise pourrait causer un préjudice considérable, se chiffrant en moyenne entre 52 000 et 444 000 dollars selon la taille de l'entreprise. Pour de nombreuses entreprises, ce coût a un sérieux impact sur leur bilan ainsi que sur leur réputation en raison de la perte d'accès aux ressources en ligne pour leurs partenaires et leurs clients.

Ce coût total reflète plusieurs problèmes. Selon l'étude, 61 % des victimes d'une attaque DDoS ont temporairement perdu l'accès à des informations critiques ; 38 % ont été dans l'incapacité de poursuivre leur activité principale ; 33 % font état de pertes d'opportunités et de contrats. En outre, dans 29 % des cas, le succès d'une attaque DDoS a eu un impact négatif sur la cote de crédit de l'entreprise et, dans 26 % des cas, a entraîné une augmentation de ses primes d'assurance.
Les experts incluent dans le calcul des coûts moyens la réparation des conséquences d'un incident. Par exemple, 65 % des entreprises ont consulté des spécialistes en sécurité informatique, 49 % ont payé pour faire modifier leur infrastructure informatique, 46 % ont eu recours à leurs avocats et 41 % ont fait appel à des gestionnaires de risque. Et il ne s'agit là que des frais les plus courants.
Les informations sur les attaques DDoS et les perturbations qui en résultent pour l'entreprise sont souvent rendues publiques, ce qui accentue encore les risques. 72 % des victimes ont divulgué des informations relatives à une attaque DDoS contre leurs ressources. En particulier, 43 % des responsables interrogés ont informé leurs clients d'un incident, 36 % l'ont signalé aux autorités et 26 % en ont parlé aux médias. 38 % des entreprises ont subi une atteinte à leur réputation à la suite d'une attaque DDoS et près d'une sur trois a dû demander l'aide de conseillers en image.
« Une attaque DDoS qui fait mouche peut compromettre des services critiques, avec des conséquences graves pour l'entreprise. Par exemple, les récentes attaques contre des banques scandinaves (en particulier OP Pohjola Group en Finlande) a interrompu pendant quelques jours les services en ligne ainsi que le traitement des transactions par carte, un problème fréquent en pareil cas. C'est pourquoi les entreprises doivent aujourd'hui considérer la protection DDoS comme faisant partie intégrante de leur politique globale de sécurité informatique. Cet aspect est tout aussi important que la protection contre les malwares, les attaques ciblées, les fuites de données et autres », commente Tanguy de Coatpont, Directeur Général chez Kaspersky Lab France.
La technologie de Kaspersky Lab assure la continuité d'accès aux ressources en ligne de ses clients, y compris pendant les attaques DDoS complexes, prolongées ou d'un type jusque-là inconnu. Kaspersky DDoS Protection détourne le trafic client vers les centres de nettoyage de Kaspersky Lab pendant la durée de l'attaque, filtrant le trafic malveillant de sorte que le client ne reçoive que les requêtes légitimes et que ses infrastructures et services ne soient pas saturés.

Après cette lecture, quel est votre avis ?
Cliquez et laissez-nous un commentaire…

Source : http://www.globalsecuritymag.fr/Kaspersky-Lab-et-B2B-International,20150128,50328.html par Kaspersky