Qu'est-ce qu'une attaque DDoS et comment s'en prémunir ?

Les TPE et PME sont de plus en plus nombreuses à utiliser internet pour communiquer avec leurs clients et prospects. Il est impensable aujourd'hui - dans cet environnement très concurrentiel - de se faire connaître et de fidéliser sa clientèle sans passer par une communication online. Les petites structures sont ainsi nombreuses à créer leurs sites internet mais aussi leurs boutiques en ligne.

Mais, l'accroissement de l'activité en ligne des petites entreprises attire l'attention des hackers, qui les voient comme des cibles faciles. Parmi les attaques les plus populaires du moment : l'attaque DDoS (Distributed Denial of Service), aussi appelée attaque par déni de service. Relativement simple à orchestrer, ces attaques sont le fait de cyber-criminels, et peuvent même être achetées au sein du Darkweb - partie anonyme et difficile d'accès du web régie par les cybercriminels.

Indisponibilité du site web ou de la boutique en ligne pendant plusieurs jours, perte de commandes, clients mécontents, etc... les conséquences en termes d'image et de chiffres d'affaires peuvent être désastreuses.

Mais qu'est-ce qu'une attaque DDoS ?

L'attaque DDoS vise à envoyer un grand nombre de requêtes à un équipement (hébergeur, serveur, application web, etc...) afin de provoquer à distance un déni de service, c'est à dire un arrêt total du service attaqué. Pour se faire, une « armée de robots » est chargée de lancer automatiquement une multitude de requêtes.

Deux types d'attaques existent :
- Les attaques « applicatives » sont très difficiles à repérer car elles ne nécessitent que peu de bande passante. Elles visent à épuiser les ressources serveur en les submergeant de demandes.
- Les attaques « volumiques » tentent de saturer les liens permettant la connexion à un service ou à un FAI en envoyant un très grand nombre de requêtes nécessitant beaucoup de bande passante. Dans ce cas de figure, le fournisseur d'accès peut facilement aider ses clients à se prémunir de ce type d'attaques.

C'est donc les attaques applicatives qui sont les plus dangereuses pour les petites entreprises, et elles sont plus difficiles à éviter.

Comment s'en prémunir ?

Malheureusement, de très nombreuses entreprises - et à fortiori les PME ne disposant pas de service informatique en interne - ne renforcent pas leur sécurité de manière proactive, en pensant qu'une fois l'attaque arrivée, ils pourront toujours la contrer. Pourtant, c'est en amont que les entreprises devraient concentrer leurs efforts si elles ne souhaitent pas en payer les conséquences.

De la même manière, certaines entreprises pensent être protégées, mais elles restent pourtant vulnérables aux attaques DDoS. En effet, la mise en place d'un pare-feu réseau - méthode de protection la plus connue - n'est pas destinée à arrêter le spam, et n'est pas non plus conçu pour stopper les attaques des applications web - ce qui le rend par définition perméable aux attaques par déni de service. Avec ce type de méprise, les applications web sont donc exposées à des risques. Un pare-feu pour applications web est bien plus adapté au combat contre les attaques par déni de service.

Plusieurs solutions de protection contre les attaques DDoS existent, certaines sont basées sur le cloud et d'autres sur site. Les solutions Cloud sont particulièrement adaptées aux PME, ces dernières demandent en effet moins de maintenance et de connaissances techniques. En règle générale, les services Cloud redirigent d'abord l'intégralité du trafic entrant vers le Cloud, le nettoie avant de le retransmettre au serveur cible. Cela permet de différencier les requêtes réelles - provenant d'internautes légitimes - et les requêtes malicieuses - provenant de robots et visant à inonder le serveur.

Enfin, une autre solution - la plus facile à mettre en place - est l'utilisation d'astuces anti-robots, comme les tests CAPTCHA. En cas d'attaques DDoS, ces derniers s'avèrent salvateurs puisqu'ils protègeront le serveur des requêtes malicieuses.

Aujourd'hui, l'important pour les PME est de comprendre l'environnement numérique dans lequel elles évoluent et les menaces qui pèsent sur leurs épaules. Ainsi, il est plus simple de comprendre les différentes techniques de protection et de se tourner vers un acteur du marché de la cyber-sécurité, avec une demande claire et la possibilité d'avoir un échange instructif avec les experts mis à leur disposition.