CSC

L'avantage d'un service DNS secondaire

Stratégies de sécurité renforcées pour protéger vos actifs en ligne

Cela peut vous arriver aussi

Le 21 octobre 2016, un prestataire de services DNS très connu a subi une attaque par déni de service distribué (DDoS) massive. Celle-ci a non seulement suspendu la disponibilité et les services du prestataire, mais des dommages collatéraux se sont également propagés à plusieurs marques célèbres dont les sites et les applications Web ont subi des pannes intermittentes.

Suite à ce piratage, la triste réalité s'est imposée : personne n'est à l'abri d'attaques DDoS, notamment celles qui visent le DNS. Une autre source de préoccupation a été la conviction unanimement partagée que les entreprises touchées n'avaient commis aucune erreur. Elles avaient suivi les conseils de nombreux consultants à l'époque et fait appel à un service de gestion du DNS. Leur erreur fatale résidait dans l'absence de solution alternative.

L'attaque du 21 octobre a en outre marqué un changement fondamental dans l'organisation des attaques DDoS. Cette attaque-là avait été lancée à l'aide du botnet (réseau de machines zombies) Mirai, constitué d'une série de périphériques atypiques connectés à Internet (caméras de sécurité, magnétoscopes et routeurs domestiques par exemple). Une fois reliés entre eux, ces appareils piratés se sont transformés en une arme dangereusement puissante. Le botnet Mirai a ainsi permis de lancer une attaque DDoS dévastatrice d'une ampleur inégalée. Et du fait de son efficacité, ce botnet a préfiguré la dangerosité des futures attaques.

Mais plus important encore, cette attaque a permis de tirer de précieux enseignements sur les nouvelles exigences qui devraient s'appliquer à l'infrastructure DNS. En particulier, le fait qu'une entreprise ne devrait pas confier la gestion de l'ensemble de sa présence en ligne à un seul service DNS. Les organisations ayant recours à un seul prestataire de services DNS ont subi de plein fouet les conséquences d'une dépendance à un point unique dès lors que celui-ci a été touché. Si ces entreprises avaient réparti leur DNS entre plusieurs services, leurs sites, leurs applications et leurs actifs en ligne auraient offert une surface de vulnérabilité réduite, et ce même au plus fort de l'attaque.

Le rythme actuel de la cybercriminalité constitue un autre facteur aggravant. Une stratégie solide pour limiter les cyberattaques peut en effet devenir obsolète en moins de six mois. C'est particulièrement vrai dans le cas des attaques DNS, au cours desquelles les criminels profitent des vulnérabilités du DNS pour causer le maximum de dommages.

Ce document s'inspire de la publication « The Case for a Secondary DNS Service » de Neustar®.

Les organisations peuvent actualiser efficacement leur stratégie de sécurité DNS pour un minimum d'efforts et de frais, en incorporant les nouvelles technologies et en réexaminant leurs pratiques de sécurité actuelles.

Analyser en détail le dilemme du DNS

À l'ère d'Internet, la sécurité des entreprises s'est principalement axée sur la protection du périmètre en ligne (c'est-à-dire les limites du réseau). La logique était que si vous pouviez empêcher des malwares et des agents malveillants de pénétrer dans le réseau, alors vous pouviez protéger vos données et vos activités. Cependant, les cybercriminels persistent et s'adaptent. Si une porte se ferme, ils cherchent une fenêtre ouverte. Et il a donc fallu peu de temps avant que les cybercriminels ne découvrent qu'ils pouvaient impacter et désorganiser des entreprises en attaquant le protocole qui gère leur présence en ligne, à savoir le DNS.

Malgré son importance, le DNS a été considéré comme un élément annexe de la sécurité pendant de nombreuses années. Vu d'emblée comme un protocole public permettant de router les requêtes, il n'a jamais été perçu comme une faille de sécurité. Toutes ces certitudes ont volé en éclats avec les attaques DoS, puis DDoS. En inondant un serveur DNS de requêtes, les cybercriminels peuvent entraîner une panne d'une durée indéterminée du site et des applications Web d'une entreprise. Et comme la disponibilité du site et des applications Web est inextricablement liée au DNS, la sécurité de celui-ci est rapidement devenue une priorité.

Pour attaquer un serveur DNS, vous avez d'abord besoin d'une adresse physique. Héberger votre propre système de noms de domaine peut permettre à tout utilisateur d'Internet un peu expérimenté de découvrir son adresse. Un bon utilisateur d'Internet peut ainsi trouver une adresse DNS non protégée en moins de 30 secondes. C'est pourquoi les consultants de sécurité ont commencé à conseiller aux organisations de faire appel à un prestataire de services DNS externe pour gérer leurs requêtes DNS de manière plus sécurisée et efficace.

La bonne stratégie de sécurité pour le DNS faisant autorité

L'initiative la plus importante que les organisations peuvent prendre pour protéger leur service DNS faisant autorité est l'implémentation d'une solution DNS primaire et secondaire. Depuis l'attaque du botnet Mirai, les analystes sectoriels (Gartner, par ex.) recommandent aux organisations de disposer d'un service DNS secondaire pour améliorer les performances et la sécurité.

Un service DNS secondaire ne doit pas être confondu avec un service DNS redondant. Il ne s'agit pas de disposer d'un plan B au cas où votre plan A échouait. Il s'agit d'avoir un plan A plus intelligent qui permet de répartir efficacement votre trafic DNS sur deux réseaux de confiance. Cette stratégie ne vise pas uniquement à protéger votre marque contre une attaque DDoS : elle améliore la redondance de votre DNS en équilibrant la charge entre deux réseaux.

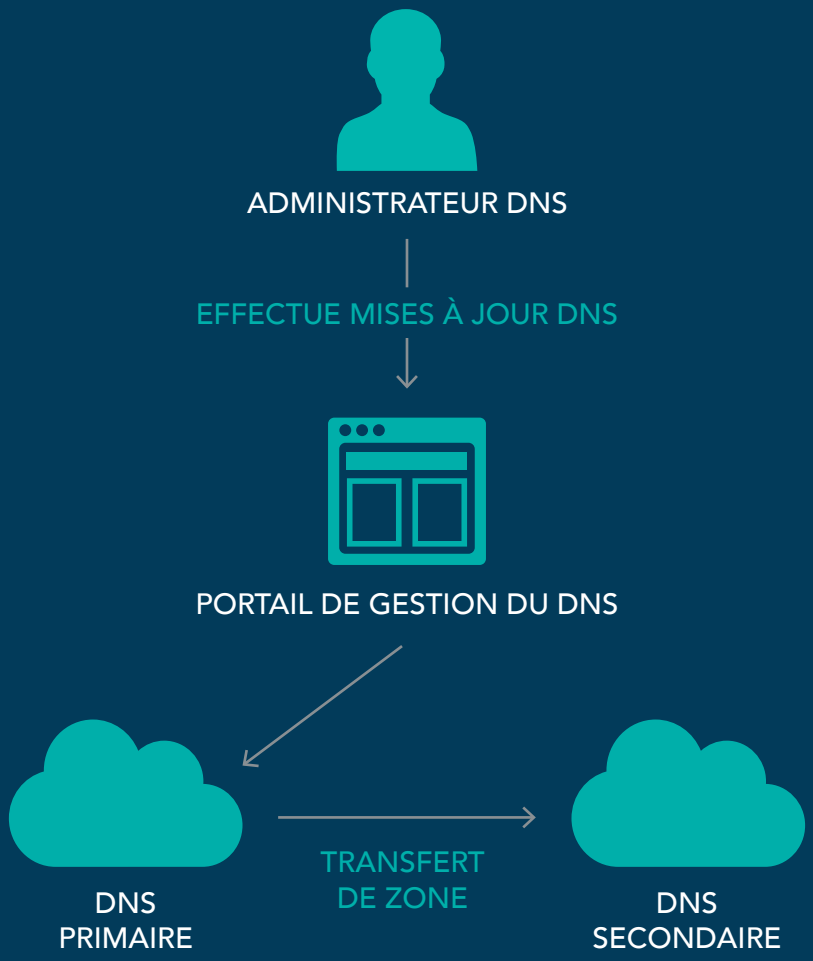
Trouver un service DNS secondaire géré est la première chose à faire pour renforcer la sécurité de votre DNS. Il vous faut ensuite choisir un prestataire de services DNS qui propose un service interne dédié de mitigation de DDoS pour ses réseaux de serveurs DNS. À mesure que davantage de périphériques se connectent à Internet, augmentant le risque d'avoir des armées de botnets plus étendues, prévoir une couche supplémentaire de protection contre les attaques DDoS est une excellente initiative pour les entreprises. Mieux encore, si vous pouvez « masquer » votre DNS sur Internet à l'aide d'une machine air gap, vous pouvez réduire de façon drastique le nombre d'attaques contre celui-ci.

Une stratégie de sécurité renforcée pour un DNS faisant autorité inclut :

- Un service DNS géré primaire et secondaire
- Un prestataire de services DNS qui propose un service dédié de mitigation de DDoS pour son réseau DNS
- La capacité d'empêcher que vos systèmes DNS ne soient directement exposés sur Internet

FONCTIONNEMENT D'UN DNS PRIMAIRE ET SECONDAIRE

1. L'administrateur DNS se connecte au portail de gestion du DNS.
2. L'administrateur DNS met à jour des données DNS.
3. Le changement se propage à tout le réseau DNS.
4. Le DNS secondaire est notifié de la mise à jour et exécute un transfert de zone pour recevoir les nouvelles données.



Mieux protégé contre les attaques DNS avec des partenaires sécurisés de confiance

La sécurité de votre réseau est équivalente à celle de son maillon le plus faible. Choisissez des prestataires qui vous offrent toute la sécurité dont votre entreprise a besoin. CSC est aujourd'hui le prestataire de services de gestion de noms de domaine, de DNS et de certificats numériques le plus conscient des exigences de sécurité. Nous appliquons nos politiques de sécurité pour garantir que nos systèmes sont sécurisés et que notre personnel est correctement formé – et informé – pour réagir aux menaces, afin de protéger les actifs numériques de nos clients 24h/24, 7j/7, 365j/an. Une partie importante de notre stratégie de sécurité consiste à sélectionner et à collaborer avec les bons partenaires.

CSC a choisi Neustar, parce que Neustar est un prestataire de services aux entreprises capable de fournir la disponibilité, la évolutivité et la sécurité requises pour optimiser les infrastructures DNS dans l'environnement numérique d'aujourd'hui. Neustar a investi massivement pour construire des solutions avancées de sécurité DNS qui protègent les organisations contre tous types de menaces. Grâce à ce partenariat, ainsi qu'aux services de gestion de noms de domaine et de certificats numériques combinés au CSC Security Center℠, CSC est en mesure d'aider ses clients à gérer de manière sécurisée tous leurs actifs numériques situés hors du pare-feu, qui sont susceptibles d'être visés par diverses attaques : empoisonnement de cache DNS, piratage de nom de domaine ou de DNS, domain-shadowing, mais également attaques DDoS, logiciels malveillants et phishing.

Demandez plus d'informations sur la manière dont CSC Security Center et nos services DNS peuvent vous aider à atténuer les cybermenaces.

CSC soutient les entreprises qui font d'importants investissements dans la sécurité en identifiant les failles de sécurité dans leurs actifs immatériels tels que les noms de domaine, le DNS et les certificats numériques. Les solutions de sécurité CSC protègent les entreprises des cybermenaces qui pèsent sur leurs actifs numériques, et les aident à éviter les pertes de revenus, les atteintes à la réputation de leur marque ou les pénalités financières pouvant résulter d'une non-conformité aux réglementations de type RGPD. Outre les actifs numériques, les solutions CSC permettent de sécuriser les marques en ligne face aux sites Web contrefaits, à la fraude et aux violations des droits de propriété intellectuelle. Les solutions CSC surveillent et contrent ce type d'attaques, et offrent des services de conseil et d'action en contrefaçon. Plus d'infos sur cscdigitalbrand.services.

cscdigitalbrand.services