RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

LES ESSENTIELS

Dénis de service distribués (DDoS *)

1/ CONSTRUIRE ET PROTÉGER

➔ **Acquérir et mettre en œuvre un service de protection anti-DDoS dédié à cette seule fonction** :

- auprès de votre hébergeur en cas d'hébergement externe, celui-ci pouvant déjà intégrer une prestation anti-DDoS, en fonction de l'offre d'hébergement souscrite ;
- et/ou auprès d'un fournisseur d'accès à Internet (trou noir, dépollution des flux **) ;
- et/ou auprès d'un fournisseur de service professionnel (déroutement, dépollution des flux **).

Dans tous les cas, sa mise en œuvre nécessite une prise en main préalable, un paramétrage adapté au trafic de l'entité et aux applications exposées et des tests réguliers de la solution pour s'assurer de son bon fonctionnement et de l'absence d'effet de bord.

➔ **Protéger son site Web avec un CDN (*Content Delivery Network*) pour la répartition de charge.** Les CDN permettent la répartition de ressources sur un grand nombre de serveurs, ce qui peut contribuer à améliorer la résistance aux attaques DDoS. **Une attention doit être portée au fait qu'une partie de ces ressources peut être hébergée à l'étranger (impact potentiel en confidentialité).**

➔ **Configurer les pare-feux en coupure d'Internet** :

- activer uniquement un filtrage au niveau réseau et transport (niveaux 3 et 4 du modèle OSI) et désactiver les fonctions de filtrage applicatif (niveaux 5 et plus) ;
- réduire les flux UDP entrants au strict nécessaire.

➔ **Restreindre au strict besoin opérationnel les services exposés à Internet.**

➔ **Concevoir les services exposés à Internet de façon à ce qu'une attaque DDoS sur un service n'ait pas d'impact sur la disponibilité des autres services** (chaînes d'accès Internet distinctes, segmentation des plans d'adressage réseau, hébergeurs distincts, etc.).

➔ **Concevoir les architectures de telle sorte qu'un service exposé à Internet qui subit une attaque DDoS puisse continuer à être administré malgré cette attaque** (réseau d'administration physiquement dédié, cloisonnement réseau des flux de supervision, etc.).

(*) L'acronyme anglais DDoS pour *Distributed Denial of Service* est le plus couramment utilisé.
(**) Par exemple, la dépollution des flux peut faire intervenir des critères de géolocalisation, de conformité protocolaire, d'inspection de paquets et de volumétrie par protocole susceptible d'être utilisé dans les DDoS (ex. : DNS en UDP, NTP, CHARGEN).

RÉPUBLIQUE
FRANÇAISE
Liberté
Égalité
Fraternité

2/ ANTICIPER ET RÉAGIR

- **Mettre en place un dispositif de supervision et détection des attaques DDoS**, afin de détecter au plus tôt une attaque :
  - utiliser un dispositif de centralisation des journaux afin de faciliter le diagnostic d'un incident DDoS *a posteriori* ;
  - rédiger et tester régulièrement une procédure définissant la marche à suivre en cas d'attaque.
- **Prévoir un mode dégradé pour les activités critiques en cas d'attaque DDoS**, le temps de la remédiation. Intégrer le fait que votre fournisseur d'accès à Internet peut aussi imposer un mode dégradé en cas d'attaque DDoS sur sa propre infrastructure, même si cette attaque ne cible pas directement votre entité.
- **Faire régulièrement l'inventaire des services ouverts sur Internet** afin d'adapter la procédure de réponse à des attaques DDoS.
- **Mettre en place un dispositif de gestion des crises**, en lien avec vos prestataires de protection DDoS.

Pour aller plus loin : https://cyber.gouv.fr/guide-ddos