aDvens

Security for the greater good

Déni de Service Distribué (DDOS)

Méthodologie de réponse à incident

IRM-04 | 2022-11-30 | **TLP-CLEAR** | CERT aDvens - CSIRT
Advens - 16 Quai de la Mégisserie - 75001 Paris

Sommaire

Introduction

Cette méthodologie de réponse à incident est une feuille de route dédiée aux gestionnaires et aux cellules de crise menant une investigation sur un problème de sécurité précis.

→ La fiche IRM s'adresse aux personnes ou fonctions suivantes :
- Les **RSSI et leurs adjoints**
- Le **CERT**
- Le **SOC**
- Les **administrateurs**

Dans le cas d'un incident : Lire l'IRM et prendre des notes.
Rester calme et contacter immédiatement l'équipe de réponse à incident du secteur d'activité ou un CERT si nécessaire.

Étapes de traitement des incidents

6 étapes sont définies pour gérer les incidents de sécurité :

1. **Préparation** : Se préparer à gérer l'incident,
2. **Identification** : Détecter l'incident,
3. **Confinement** : Limiter l'impact de l'incident,
4. **Remédiation** : Supprimer la menace,
5. **Récupération** : Revenir à un état normal,
6. **Capitalisation et apprentissage** : Élaborer et améliorer les processus.

Cette IRM fournit des informations détaillées pour chaque étape. Les étapes sont issues du NIST.

Cette fiche est issue du travail collaboratif avec le **CERT-SG** de modification et de mise à jour de leurs fiches de méthodologie de réponse à incident.

Références

→ IRM CERT-SG
→ IRM CERT-aDvens

1. Préparation

Objectif : Établir des contacts, définir des procédures, recueillir des informations et se familiariser avec les outils de détection d'intrusion pour gagner du temps lors d'une attaque.

1.1. Prise en charge du fournisseur d'accès Internet

- Contacter votre FAI pour comprendre les services d'atténuation DDoS qu'il propose (gratuits et payants) et la procédure à suivre,
- Si possible, souscrire à une connexion Internet redondante et à un service Anti-DDoS,
- Établir une liste des contacts avec votre FAI et les forces de l'ordre. S'assurer qu'il y a la possibilité d'utiliser un canal de communication tiers (ex. : téléphone),
- S'assurer que le FAI et le service d'atténuation DDoS disposent d'une assistance téléphonique 24h/24 et 7j/7.

1.2. Inventaire

- Créer une liste autorisée des adresses IP et des protocoles, si il y a une priorisation du trafic à réaliser lors d'une attaque,
- Documenter en détails l'infrastructure informatique, y compris les référents métiers, les adresses IP et les ID de réseau, les paramètres de routage (AS, etc.),
  - Préparer une cartographie de la topologie de réseau et un inventaire des actifs.

1.3. Infrastructure de réseau

- Concevoir une bonne infrastructure réseau sans point de défaillance unique ni goulot d'étranglement,
- Déployer un pare-feu applicatif Web (WAF) pour se protéger contre les attaques DDoS au niveau de la couche application,
- Distribuer les serveurs DNS et autres services critiques (SMTP, etc.) via différents AS,
- Renforcer la configuration du réseau, du système d'exploitation et des composants d'application susceptibles d'être ciblés par les attaques DDoS,
- Connaître les performances de l'infrastructure actuelle afin d'identifier une attaque plus rapidement et avec plus de précision,
- Si le business dépend d'Internet, acheter des produits ou services spécialisés d'atténuation des attaques DDoS,
- Confirmer les paramètres DNS de durée de vie (TTL) pour les systèmes susceptibles d'être attaqués. Réduire les TTL, si nécessaire, pour faciliter la redirection DNS si les adresses IP d'origine sont attaquées. 600 est une bonne valeur TTL,
- En fonction de la criticité des services, mettre en place une sauvegarde activable en cas de problème.

1.4. Interlocuteurs internes

- Établir une liste des contacts pour les équipes IDS, pare-feu, systèmes et réseau,
- Collaborer avec les métiers pour comprendre les implications commerciales (par exemple, la perte d'argent) des scénarios d'attaque DDoS probables,
- Impliquer l'équipe de planification BCP/DR sur les incidents DDoS,

2. Identification

Objectif : Détecter l'incident, déterminer son ampleur et impliquer les acteurs appropriés.

2.1. Communication

- → Préparer un modèle de communication interne et externe sur les incidents DDoS,
- → Identifier le canal de communication en cas de DDoS,
- → La phase de « préparation » doit être considérée comme l'élément le plus important d'une réponse réussie à un incident DDoS.

2.2. Analyser l'attaque

- → Garder à l'esprit que l'attaque DDoS pourrait être un écran de fumée cachant une attaque plus sophistiquée et ciblée,
- → Consulter l'analyse du service anti-DDoS et les rapports du centre de nettoyage :
  - Comprendre le flux logique de l'attaque DDoS et identifier les composants de l'infrastructure affectés par celle-ci,
  - Comprendre si le site était la cible de l'attaque ou une victime collatérale.
- → Examiner les fichiers de charge et les journaux des serveurs, routeurs, pare-feu, applications et autres infrastructures concernées,
- → Identifier les aspects du trafic DDoS qui le différencient du trafic légitime :
  - Adresses IP sources, AS, etc,
  - Ports de destination,
  - URL,
  - Indicateurs de protocoles.

Des outils d'analyse de réseau peuvent être utilisés pour examiner le trafic :

- → **Tcpdump, Tshark, Snort, Netflow, Ntop, MRTG, Cacti, Nagios.**

Si possible, créer une signature NIDS pour se concentrer sur la différenciation entre le trafic légitime et le trafic malveillant,

Impliquer les acteurs internes et externes

- → Contacter les équipes internes pour savoir ce qu'ils voient de l'attaque,
- → Contacter le FAI pour lui demander de l'aide. Être précis sur le contrôle du trafic souhaité :
  - Blocs de réseau impliqués,
  - Adresses IP sources,
  - Protocoles.

- → Informer les équipes exécutives et juridiques de l'entreprise,

Vérifier les antécédents

- → Découvrir si l'entreprise a reçu une demande d'extorsion de l'attaquant,
  - Vérifier les e-mails dans la passerelle de messagerie de sécurité en fonction d'une liste de mots clés.
  - Certains pirates envoient des demandes d'extorsion directement aux adresses e-mail figurant dans les enregistrements WHOIS du site Web ciblé.
- → Rechercher des revendications de l'attaque sur les réseaux sociaux,
- → Rechercher si quelqu'un aurait intérêt à menacer l'entreprise :
  - Concurrents,
  - Groupes à motivation idéologique (hacktivistes),
  - Anciens employés.

3. Confinement

Objectif : Atténuer les effets de l'attaque sur l'environnement ciblé.

- Si le goulot d'étranglement est une fonctionnalité particulière d'une application, désactiver temporairement cette fonctionnalité,
- Essayer de limiter ou de bloquer le trafic DDoS aussi près que possible du réseau "cloud" via un routeur, un pare-feu, un équilibreur de charge, un appareil spécialisé, etc.,
- Mettre fin aux connexions ou aux processus indésirables sur les serveurs et les routeurs, et régler leurs paramètres TCP/IP,
- Si possible, passer à d'autres sites ou réseaux utilisant DNS ou un autre mécanisme. Mettre en place un Blackhole DDoS ciblant les adresses IP d'origine,
- Mettre en place un canal de communication alternatif entre l'entreprise et ses clients,
- Si possible, acheminer le trafic via un service ou un produit de nettoyage du trafic via DNS ou des modifications de routage (par exemple : sinkhole),
- Configurer des filtres de sortie pour bloquer le trafic que les systèmes peuvent envoyer en réponse au trafic DDoS (par exemple : backsquatter), afin d'éviter d'ajouter des paquets inutiles au réseau,
- En cas de tentative d'extorsion, essayer de gagner du temps avec le fraudeur. Par exemple, expliquer avoir besoin de plus de temps pour obtenir l'approbation de la direction.

Si le goulot d'étranglement se situe du côté du FAI ou du service anti-DDoS, lui seul peut prendre des mesures efficaces.
Dans ce cas, travailler en étroite collaboration avec le FAI et/ou le fournisseur anti-DDoS et s'assurer de partager efficacement les informations.

4. Remédiation

Objectif : Prendre des mesures pour arrêter l'attaque.

→ Contacter le FAI et/ou le fournisseur anti-DDoS et s'assurer qu'ils appliquent les mesures correctives. Pour information, voici quelques-unes des mesures possibles :
- Filtrage (si possible au niveau Tier 1 ou 2),
- Nettoyage de trafic / Sinkhole / Clean-pipe,
- Équilibrage des IP publics / division / commutation,
- Routage sinkhole.

Les actions de correction technique peuvent principalement être appliquées par le FAI et/ou le fournisseur anti-DDoS.

Si l'attaque a eu un impact majeur, signaler l'incident à l'ANSSI et/ou le régulateur.
Si les attaquants ont été identifiés, envisager d'impliquer les forces de l'ordre.
Cela devrait être effectué par la direction et les équipes juridiques de l'entreprise.

5. Récupération

Objectif : Restaurer le fonctionnement normal du système.

Évaluer la fin de l'incident DDoS

→ S'assurer que les services concernés sont à nouveau joignables,
→ S'assurer que les performances de l'infrastructure sont de retour aux anciens niveaux.

Annuler les mesures d'atténuation

→ Rebasculer le trafic vers votre réseau d'origine,
→ Redémarrer les services arrêtés.

6. Capitalisation et apprentissage

Objectif : Documenter les détails de l'incident, discuter des leçons apprises et ajuster/améliorer les dispositifs et stratégies de défense.

Le rapport d'incident

Il doit être rédigé et mis à la disposition de toutes les parties prenantes.

Le retour d'expérience

Les thèmes du retour d'expérience doivent être décrits avec les éléments suivants :

→ Cause initiale de l'infection,
→ Actions et chronologies de chaque événement important,
→ Ce qui s'est bien passé,
→ Ce qui ne s'est pas bien passé,
→ Coût de l'incident,
→ Indicateurs de compromission.

La capitalisation

Des actions d'amélioration des processus de détection des logiciels malveillants et des intrusions sur le réseau doivent être définies pour capitaliser sur cette expérience.