Titre : *Étude de cas cybersécurité – Attaque DDoS & réponse dans une entreprise multimédia selon le NIST CSF*

Nom & rôle : *Lyncold Stephensky CHERY – Analyste cybersécurité*

Date : Le 24 avr. 2025

Ce document présente la réponse complète à un scénario réaliste d'attaque DDoS subie par une entreprise. Il démontre l'application concrète du NIST Cybersecurity Framework (CSF) dans un contexte professionnel.

Titre : *Sommaire*

1. Identifier
2. Protéger
3. Détecter
4. Répondre
5. Récupérer

Titre : *Contexte de l'incident*

L’entreprise a été victime d’une attaque DDoS qui a compromis le réseau interne pendant deux heures. Lors de cette attaque, les services réseau ont été brusquement interrompus en raison d’un flot massif de paquets ICMP, rendant le trafic interne totalement dysfonctionnel.

1. Identifier

L’équipe de cybersécurité a mené une enquête approfondie pour identifier l’origine de l’incident. Elle a découvert qu’un acteur malveillant avait lancé une attaque par inondation ICMP (Ping Flood), en exploitant un pare-feu mal configuré. Cette faille a permis au cyberattaquant de submerger le réseau interne en envoyant un grand volume de paquets ICMP.

Des audits futurs réguliers des pare-feux, des systèmes réseau, et des privilèges d’accès sont désormais planifiés pour prévenir de telles vulnérabilités.

2. Protéger

Afin de renforcer la protection du réseau, l’équipe a mis en place les mesures suivantes :

- **Mise en place de règles de limitation du taux ICMP** sur le pare-feu (rate-limiting).
- **Vérification des adresses IP sources** pour identifier les paquets ICMP usurpés (IP spoofing).
- **Déploiement d’un outil de surveillance réseau** pour détecter les comportements anormaux.
- **Mise en œuvre d’un système IDS/IPS** pour analyser et filtrer les paquets ICMP suspects.

Des politiques de sécurité renforcées et des procédures de configuration sécurisée des équipements réseau ont également été instaurées.

3. Détecter

Pour améliorer les capacités de détection d’incidents similaires à l’avenir, l’entreprise a :

- Activé les **logs de pare-feu** pour surveiller en temps réel les connexions entrantes.
- Intégré un **système IDS** pour surveiller le trafic provenant d’Internet.
- Implémenté une solution **SIEM** (Security Information and Event Management) pour corréler les événements et identifier les menaces potentielles plus rapidement.

4. Répondre

Lors de l’incident, l’équipe a rapidement :

- **Bloqué tous les paquets ICMP entrants** via les équipements réseau.
- **Arrêté les services non critiques** pour réduire la charge.
- **Rétabli les services critiques** une fois la menace contenue.

Une communication a été initiée avec les parties prenantes pour les informer de l’incident et des mesures prises.

5. Récupérer

Une fois l’attaque neutralisée, l’équipe a :

- **Relancé tous les services réseau** de manière contrôlée.
- **Effectué une vérification d’intégrité** des systèmes critiques.
- **Informé l’ensemble du personnel que le réseau était de nouveau opérationnel et sécurisé.**