**PROJET-SSI | PLAN**

**1. Introduction**

* **Présentation du sujet et de son importance** : Cette section introduira le sujet des cyberattaques, en soulignant leur impact croissant sur les entreprises et les institutions gouvernementales. On expliquera l'importance de la cybersécurité dans un monde de plus en plus numérisé.
* **Pourquoi ce cas a été choisi** : Justification du choix de cette cyberattaque spécifique, que ce soit en raison de son ampleur, de ses conséquences ou de son impact médiatique.
* **Objectifs du rapport** : Expliquer les objectifs du rapport, qui visent à analyser la cyberattaque en question, ses causes, ses conséquences, et à proposer des solutions pour éviter de futures attaques similaires.

**2. Description de la cyberattaque**

* **Présentation de l’incident choisi** :
  + Description précise de l'attaque, de la méthode utilisée (par exemple, phishing, ransomware, malware, etc.).
  + Date et lieu de l'attaque, ainsi que le pays ou la région affectée.
  + Qui étaient les cibles (entreprises, institutions, gouvernements, etc.).
* **Contexte de l'attaque** :
  + Détailler le moment où l'attaque a eu lieu, les acteurs impliqués, et les conditions particulières qui ont facilité l'attaque.
  + Événements antérieurs à l'attaque qui pourraient avoir contribué à la vulnérabilité des systèmes ciblés.

**3. Impact de la cyberattaque**

* **Conséquences sur plusieurs aspects** :
  + **Économique** : Évaluation des pertes financières, des frais de réparation et de récupération, des sanctions possibles, etc.
  + **Social et humain** : Les victimes directes de l'attaque, en particulier les employés ou les clients affectés, ainsi que les répercussions sur la réputation de l'organisation.
* **Liste des parties impliquées** :
  + Les victimes, les attaquants (groupes ou individus), et toute autre partie prenante.
  + Explication des rôles de chaque acteur dans cet incident.

**4. L’organisation affectée**

* **Présentation de l’entreprise ou organisation ciblée** :
  + Détails sur l’organisation, ses activités, et son secteur.
  + Discussion sur la sophistication des systèmes informatiques de l’organisation avant l’attaque.
* **Mesures préexistantes** :
  + L’organisation disposait-elle de systèmes de sécurité pour se protéger contre ce type d'attaque ? Si oui, pourquoi n'ont-ils pas fonctionné ?
  + Méthodes de réponse aux incidents mises en place par l'organisation pendant et après l'attaque.
* **Conséquences sur l'organisation** :
  + Fermeture temporaire, perte de clients, mise à mal de la réputation, ou continuation des activités avec des mesures de sécurité renforcées.

**5. Analyse des attaquants**

* **Qui a revendiqué l’attaque ?**
  + Identification des groupes ou individus responsables. S’il y a plusieurs groupes, détailler chacun d’eux.
* **Motivations des attaquants** :
  + Pourquoi l’attaque a-t-elle eu lieu ? Quels étaient les objectifs des attaquants (financiers, politiques, idéologiques, etc.) ?
  + Quel type de données ont-ils visé ou compromis (informations personnelles, financières, stratégiques, etc.) ?
* **Revendiications ou objectifs** :
  + Si les attaquants ont fait des revendications, les détailler. Par exemple, demande de rançon, diffusion de messages politiques, etc.

**6. Méthodes d’attaque**

* **Technologies et techniques utilisées** :
  + Détail des techniques d’attaque utilisées (phishing, ransomware, malware, etc.).
  + Explication de la vulnérabilité exploitée par les attaquants pour pénétrer le système (par exemple, absence de mise à jour de sécurité, utilisation de mots de passe faibles, etc.).

**7. Aspects critiques**

* **Possibilité de réitération de l'attaque** :
  + Analyser la possibilité que des attaques similaires puissent se reproduire, en tenant compte des failles identifiées.
  + Identifier les menaces persistantes liées à cet incident.

**8. Recommandations**

* **Mesures de prévention et de sécurité** :
  + Quelles actions l'organisation aurait-elle pu prendre pour éviter cette attaque ?
  + Recommandations générales en matière de cybersécurité pour éviter ce type d’incident (mise à jour régulière des systèmes, formation des employés, utilisation d’outils de détection avancée, etc.).
* **Stratégies de réponse en cas d'attaque** :
  + Quelles sont les meilleures pratiques en termes de gestion des incidents et de communication pendant une attaque ?
  + Conseils pour minimiser l'impact d'une cyberattaque et restaurer rapidement les opérations.

NOTES: :  
Sonje plan pa pafè, yon moun ka toujou ajoute, modifye oswa retire yon bagay nan plan si l wè oswa panse ke sa merite fèt, lè w fè l, jis pataje sa ak nou menm nan gwoup lan yon fason pou nou te ka o kouran, epi aprè chak kou, plan ta dwe modifye. Tankou pou moman nou pako fè parèt nan plan nosyon ke nou te wè nan dènye kou an.