TP 2 : Audit de conformité et gestion d'incident

Vous travaillez au sein de l'ANSSI, et vous êtes missionnés pour réaliser un audit de conformité dans une entreprise du secteur des transports ferroviaires afin d'évaluer son respect des exigences en cybersécurité imposées par la loi de programmation militaire (LPM) et NIS 2.

Cette mission intervient après la survenue d'un incident critique : une intrusion malveillante dans le système de gestion des signaux ferroviaires, qui a causé des retards massifs et plusieurs incidents de sécurité. L'entreprise, RailHotte, exploitant les trains à grande vitesse, doit démontrer qu'elle est en conformité avec la réglementation et qu'elle a bien pris les mesures nécessaires pour sécuriser son infrastructure.

Informations sur l'entreprise et l'incident

- RailHotte exploite un réseau de trains interconnecté à travers l'Europe.
- Ses infrastructures incluent :
    - Système de gestion des signaux ferroviaires (permet le bon fonctionnement des feux et aiguillages).
    - Réseau de télécommunication interne.
    - Systèmes de billetterie et gestion des passagers.
    - Infrastructure IT et cloud stockant les données de maintenance et exploitation.

Incident récent :

- Une attaque par malware a permis une prise de contrôle temporaire sur le système de signalisation.
- Plusieurs trains ont été arrêtés en urgence pour éviter des collisions.
- La compromission des bases de données a mené à une exposition de données sensibles.

Entreprise : RailHotte

Secteur : Transport ferroviaire à grande vitesse
Statut : Entreprise privée sous contrat avec l'État
Taille : 18 000 employés
Budget annuel : 3,8 milliards d'euros
Sites principaux :

- Siège social : Lyon
- 5 centres de maintenance répartis en France
- 1 centre de supervision ferroviaire en Île-de-France
- 1 datacenter principal à Bordeaux, un secondaire à Lille

Infrastructure informatique et systèmes critiques

Système	Description	Criticité
Système de gestion des signaux ferroviaires	Contrôle l'état des feux, aiguillages, limitations de vitesse	**Élevée**
Système de supervision des trains (TMS)	Communication en temps réel avec les conducteurs, gestion des horaires	**Élevée**
Système de billetterie et clients	Réservation, gestion des abonnés, paiements	**Moyenne**
Infrastructure IT et stockage	Bases de données contenant les plans de maintenance et logs	**Moyenne**
Système de vidéo-surveillance des gares et trains	Enregistrement des flux vidéo pour la sécurité	**Faible**

Détails sur l'incident cyber

- Type d'attaque : Malware sophistiqué (probablement un ransomware)
- Périmètre impacté :
    - Système de gestion des signaux compromis pendant 45 minutes → Retards massifs et arrêt de plusieurs trains
    - Bases de données des horaires et plans de maintenance corrompues
    - Fuite potentielle de données sur les abonnés premium et les membres du personnel
- Hypothèses sur l'origine de l'attaque :
    - Exploitation d'une faille non corrigée dans le serveur de supervision
    - Phishing réussi sur un employé du centre de supervision

- Conséquences :
    - Risque d’accidents ferroviaires si attaque plus grave à l’avenir
    - Perte de confiance des usagers et impact sur la réputation de RailHotte
    - Sanctions potentielles si non-conformité à NIS2 et LPM

Contexte réglementaire

- RailHotte est classée comme OIV, donc doit respecter les obligations de la loi de programmation militaire (LPM) et de la directive NIS2.
- L’ANSSI peut réaliser des audits et contrôles pour vérifier la conformité.
- L’entreprise doit prouver qu’elle a mis en place des mécanismes de gestion des incidents.

Travail à faire :

1. **Audit de conformité et analyse des failles**
    - Analyser les obligations réglementaires applicables à RailHotte selon la LPM et NIS 2.
    - Vérifier si l'entreprise respecte les mesures de sécurité obligatoires (gouvernance, contrôle, gestion des incidents, audits).
    - Identifier les failles techniques et organisationnelles ayant permis l'incident.
2. **Plan de réponse à incident**
    - Décrire les actions à mettre en œuvre immédiatement pour limiter l'impact de l'incident.
    - Définir un plan de communication interne et externe en cas d'attaque.
    - Proposer des améliorations à long terme pour éviter une récidive.
3. **Présentation de recommandations à la direction de RailHotte**
    - Rédiger un rapport incluant l'évaluation des failles et recommandations.
    - Préparer une présentation orale simulant un rapport d'audit devant la direction de RailHotte et l'ANSSI.

- Rapport écrit détaillé,
- Présentation orale : simulation de présentation devant la direction de RailHotte.