Exercice:

Élaboration d'une Politique de Sécurité

KOUASSI GLOHNDY

CONTEXTE:

En tant que responsable de la sécurité des systèmes d'information, votre mission est de créer une politique de sécurité pour la nouvelle infrastructure de l'entreprise.

QUESTIONS ET REPONSES

1. Identification de cinq risques liés à la sécurité de l’infrastructure

-Intrusions externes (cyberattaques, exploitation de vulnérabilités) : piratage de serveurs, applications ou postes de travail.

-Menaces internes : erreurs humaines, comportements malveillants d’employés ou mauvaise gestion des accès.

-Perte ou fuite de données sensibles : exfiltration de données clients, financières ou stratégiques.

-Pannes et indisponibilités : attaque DDoS, défaillances matérielles ou logicielles entraînant une interruption de service.

-Malwares et ransomwares : infections compromettant l’intégrité et la disponibilité des données.

---

2. Bonnes pratiques pour sécuriser l’infrastructure

Gestion des accès et identités (IAM) :

-Mise en place du principe du moindre privilège.

-Authentification multifacteur (MFA).

-Révocation rapide des droits lors des départs d’employés.

Sécurisation du réseau et des systèmes :

-Segmentation réseau (zones DMZ, VLAN).

-Pare-feu nouvelle génération (NGFW), systèmes de prévention d’intrusion (IPS).

-Chiffrement des communications (TLS, VPN).

Protection des données :

-Sauvegardes régulières, testées et stockées hors site.

-Chiffrement des données au repos et en transit.

-Classification et gestion des données sensibles.

Hygiène de sécurité :

-Mise à jour et correctifs réguliers (patch management).

-Formation continue des utilisateurs (sensibilisation phishing, bonnes pratiques).

-Gestion des journaux et traçabilité (SIEM).

Plan de continuité et de reprise d’activité (PCA/PRA) :

-Redondance des services critiques.
-Plans de restauration testés régulièrement.

---

3. Mesures de conformité réglementaire

L’entreprise doit respecter les normes et réglementations applicables, notamment :

-RGPD (Règlement Général sur la Protection des Données) : protection et confidentialité des données personnelles des clients et employés.

-ISO 27001 (système de management de la sécurité de l’information) : cadre de référence pour la gestion des risques.

-NIS2 (Directive européenne sur la sécurité des réseaux et de l’information) pour les opérateurs de services essentiels (si applicable).

-Obligations légales nationales : conservation des journaux, notification d’incidents aux autorités compétentes (CNIL, ANSSI en France).

---

4. Stratégie de protection, détection et réponse aux incidents

Protection :

-Mise en place de solutions EDR (Endpoint Detection & Response).

-Sécurisation des applications via des audits réguliers (tests d’intrusion, pentests).

-Cloisonnement des environnements (dev/test/prod).

Détection :

-Déploiement d’une solution SIEM pour corrélation et alerte en temps réel.
-Supervision réseau et surveillance des logs système/applicatifs.

-Mise en place de honeypots pour détecter des comportements suspects.

Réponse aux incidents :

-Élaboration d’un plan de réponse aux incidents (PRI).

-Équipe dédiée (CSIRT interne ou prestataire MSSP).

-Procédures d’escalade claires (notification, confinement, éradication, restauration).

-Retour d’expérience (REX) après chaque incident pour améliorer les défenses.