Exercices #1 Chapitre 1

1) Lequel des principes suivants est un principe du DIC qui signifie que les sujets autorisés se voient accorder un accès rapide et ininterrompu aux objets?
   A. Intégralité
   B. Disponibilité
   C. Confidentialité
   D. Intégrité

2) Lequel des éléments suivants n'est pas considéré comme une violation de la confidentialité?
   A. Vol du mot de passe
   B. Écoutes
   C. Destruction matérielle
   D. Ingénierie sociale

3) Une entreprise XYZ avait un programme efficace de gestion des risques qui indique :
   A. Les menaces globales sont minimisées
   B. Les vulnérabilités sont éliminées
   C. Le risque résiduel est minimisé
   D. Le risque global est éliminé.

4) Quel est l'objectif d'attribuer des scores de risque à chaque actif TI?

   Des scores de risque sont attribués pour la priorisation des actifs à être protégés.

5) Expliquez brièvement les différences entre les termes suivants
   A. Identification des risques
   B. Analyse des risques
   C. Évaluer les risques
   D. Traitement des risques

   1. **Identifier les risques:** Déterminer les menaces, les vulnérabilités
   2. **Analyser les risques:** Évaluer la probabilité et l'impact de chaque risque.
   3. **Évaluer les risques:** Prioriser les risques en fonction de leur importance et déterminer les contrôles appropriés.
   4. **Traiter les risques:** Mettre en place des stratégies de réduire les risques.

6) Qu'est-ce que la catégorisation? Qu'est-ce qu'on catégorise? Pourquoi le fait-on ? Et comment?

La catégorisation de l'information est le processus de classer l'info selon le DIC afin de protéger les actifs par des contrôles de sécurité, en fonction des valeurs de la Disponibilité de l'intégrité et de la Confidentialité.
D'abord, les responsables de chaque info classe et autorise l'info dont il est responsable. Et ensuite,

7) Pourquoi est-il important d'avoir des politiques pour une organisation ?

Les politiques sont importantes pour une organisation afin de transmettre les instructions de la haute direction à ceux qui prennent des décisions, entreprennent des actions et exécutent d'autres tâches au nom de l'organisation.

****

Exercices no2

8) Lequel des éléments suivants est lié à la poursuite des opérations commerciales ?
A. Analyse de l'impact sur les entreprises
B. Planification de la continuité des activités
C. Planification de reprise après sinistre
D. Planification de la réponse aux incidents

9) Qu'est-ce que le BIA? A quoi sert-il?
BIA permet d'identifier et prioriser les processus d'affaires et les systèmes dans le but de connaître quels seront ceux que l'entité paiera pour poursuivre ses activités.

10) Comment les entités peuvent s'y prendre pour bâtir le BIA?

Collecte des informations

- **Questionnaires** : Distribuer des questionnaires aux responsables de différentes unités pour recueillir des informations sur les processus clés, les ressources nécessaires, et les impacts potentiels d'une interruption.
- **Interviews** : Conduire des entretiens avec les parties prenantes clés pour obtenir des informations détaillées sur les opérations et leurs dépendances critiques.

  Ateliers collaboratifs : Organiser des ateliers avec plusieurs équipes pour identifier ensemble les fonctions critiques et discuter des impacts potentiels

Ou/et

Gestion des risques de sécurité (DIC) est un point de départ: la classification des systèmes et leur interdépendance ont été établis

11) Qu'est-ce qu'un incident versus un événements? Incident: est un **événement** qui **menace la confidentialité, l'intégrité ou la disponibilité** des systèmes d'information ou des données d'une organisation.
Évenement: activités des utilisateurs et des systèmes liées à la sécurité (ex: accès des administrateurs)

Tous les incidents sont des événements, mais tous les événements ne sont pas des incidents

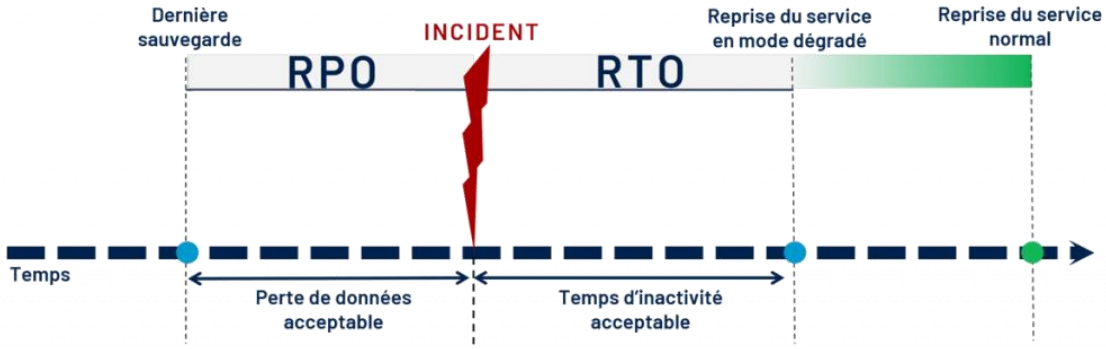
12) Après avoir développé des plans de contingence, qu'est-ce qui est important de faire?

- Tester : Simuler un incident réel pour évaluer la réponse globale de l'organisation.
- Training : informer les usagers sur leur rôles et responsabilités et les préparer pour les tests.
- Maintenance : mis à jour suite à des changements (inventaire, processus, etc.)

13) Qu'est-ce que le RTO et le RPO en gestion des incidents?

- RPO: temps entre les backups. Exemple: si le backup est effectué à tous les jours, donc RPO= 24 hres
- RTO: le temps que le système doit reprendre et être disponible

Réponses du module



1- Qu'est-ce que le RPO ?

Perte de données acceptable lors d'un incident

2- Quelles sont les différentes méthodes de backup?

Méthodes : full, différentiel et incrémental

3- Quelles sont les différentes sortes d'infrastructure que l'entité peut utiliser pour son backup?

NAS, SAN, virtualisation, cloud

4- Si l'entité utilise un backup externe, quelles sont les façons qu'elle peut utiliser pour transférer son backup vers l'externe?

voûte électronique (transfert en mode sécurisé du backup à intervalles réguliers), journaux à distance (transfert en ligne ou en bloc des modifications à la base de données) et transfert en temps réel du backup (miroir)

5- Pourquoi est-il intéressant d'appliquer la rotation des sauvegardes?

Libération d'espace de stockage, Réduction des coûts, Amélioration de la performance, Conformité réglementaire

6- Qu'est-ce que le RTO ?

Temps d'inactivité où les systèmes ne fonctionnent pas.

7- Quel est le lien entre le RTO et les différentes sortes de sites alternatifs?

-hot site :RTO=0, les données doivent être transférées en miroir (en double : site principal et site alternatif), ou appelé « en temps réel »
-warm : prend quelques jours pour l'installation, donc RTO=48 ou 72 heures
-cold : RTO > 72 heures ou comme 2e site alternatif.

8- Qu'est-ce que la redondance?

Équipement de surplus qui si l'équipement principal est brisé, l'autre équipement le remplace sans coupure de fonctionnement des systèmes.

9- Qu'est-ce que le RAID? Est-ce un moyen de redondance?

redondant array of inexpensive disks. Oui mais pas pour le RAID 0.

10- Quelle est la différence entre le RAID 0 et 1?

RAID 1 : Le miroir. Chaque bloc de données est écrit sur deux disques durs distincts. On dit qu'il y a "mirroring" ou "miroir".

11- Qu'est-ce que le RAID 5?

Avec RAID 5, les données et la parité sont réparties sur trois disques ou plus.
Les matrices RAID 5 ne peuvent tolérer qu'une panne de disque d'un seul membre.
Stockage fiable et relativement bon marché

Exercices - Chapitre 4

1) Lequel des éléments suivants traite spécifiquement des types d'attaques contre les systèmes informatiques d'une organisation ?

A. Plan de continuité du soutien
B. Plan de continuité des opérations
C. Plan de continuité des activités
D. Plan de réponse aux incidents

2) Une politique de réponse aux incidents doit contenir :

A. arborescences d'appels mises à jour.
B. processus d'escalade.
C. modèles de communiqués de presse.
D. Inventaire des fichiers de sauvegarde critiques.

Explication:
Les processus d'escalade, indiquant la structure hiérarchique – personne responsable, a respecté selon le niveau de gravité des incidents, doivent être contenus dans une politique de réponse aux incidents. Les arborescences téléphoniques, les modèles de communiqués de presse et les listes de fichiers de sauvegarde critiques sont trop détaillés pour être inclus dans un document de politique.

3) Les informations de compte d'un client ont été piratées. Quelle serait la première étape pour faire face à cette attaque ? Choisissez une option et réorganisez également les autres étapes à suivre.

A. commencer le confinement.
B. aviser la haute direction.
C. confirmer l'incident.
D. avertir les forces de l'ordre.

C →A →B →D

4) Quand le plan IR doit-il être activé?

Lorsqu'un événement est classé comme un incident, le plan IR doit être activé

5) Quel type de test est considéré comme l'étape préliminaire à un test réel. Expliquer.

- Test de la liste de contrôle/Vérification documentaire
- Il faut s'assurer que tout est écrit avant de faire une simulation

6) Expliquez les différences entre les quatre phases du processus de gestion des incidents selon la NIST 800-61 en utilisant un format de tableau ci-dessous.

	Préparation de la phase I	Détection et analyse de phase II	Phase III Confinement, éradication et récupération	Phase IV Activité post-incident
1. la phase relève d'avant, après ou Pendant l'incident ?	Avant	Pendant	Pendant et après	Après
2. Soulignez certaines actions importantes à effectuer ou stratégies à adopter à chaque phase. Cette explication peut également être faite en prenant un exemple d'incident.	-Préparation des politiques, procédures et du plan de réponse aux incidents -Formation et training de l'équipe CSIRT	-Indicateurs -Analyse et prioriser les incidents (faible, moyen et élevé)	-Réponse à l'incident -Éradiquer les logiciels malveillants installés -Restaurer les systèmes infectés	-Lecons apprises - recommandations

7. Quelles sont les activités d'un post-incident (deux réponses)?

- Suivre les métriques
- Éradiquer
- Documenter l'incident
- Compléter un rapport de suivi

****

Exercices- Chapitre 6
Détection et analyse- réponse aux incidents

1. Qu'est-ce que des vecteurs d'attaques?

Un vecteur d'attaque est la méthode ou le chemin qu'un cybercriminel emprunte pour pénétrer dans un système informatique, un réseau ou voler des données

2. Quels sont les principaux types de vecteurs?

Les logiciels malveillants (malware) : Virus, vers, chevaux de Troie, ransomwares, etc. Ils s'introduisent dans les systèmes pour voler des données, crypter des fichiers, ou perturber les opérations.
Les vulnérabilités logicielles: Des failles dans les logiciels, les systèmes d'exploitation ou les applications peuvent être exploitées par les attaquants.
L'ingénierie sociale: Cette technique consiste à manipuler les utilisateurs pour qu'ils divulguent des informations sensibles ou qu'ils exécutent des actions qui compromettent la sécurité.
Les erreurs de configuration: Des erreurs de configuration dans les systèmes ou les réseaux peuvent créer des portes dérobées pour les attaquants.
Les accès physiques: Un attaquant peut accéder physiquement à un système pour le manipuler ou y installer des dispositifs malveillants.

3. Qu'est-ce qu'un IOC?

Événement indésirable en cours. Signes plus directs qu'un incident est en cours.

4. Comment les IOC sont utilisés dans les outils de sécurité?

Systèmes de prévention d'intrusion (IPS) : Les IPS utilisent les IOC pour filtrer le trafic réseau et bloquer les connexions vers des adresses IP, des ports ou des domaines connus pour être malveillants.
Systèmes de détection d'intrusion (IDS) : Les IDS analysent les logs et les événements système pour détecter des activités suspectes correspondant à des IOC connus.
Solutions EDR (Endpoint Detection and Response) : Les EDR surveillent en permanence les terminaux pour identifier les fichiers malveillants, les processus suspects et les comportements anormaux basés sur des IOC.

5. Il est crucial que l'entité implante des alertes pour prévenir les attaques. Quelles sont les différents types d'alerte?

Alertes causés par l'outil IDPS
Alertes causés par l'outil SIEM
Alertes causés par les Antivirus
Alertes causés par les EDR, XDR

6. Qu'est-ce qu'un SIEM?

Outil logiciel puissant qui joue un rôle central dans la surveillance en collectant, grâce à la collecte et à l'analyse (en temps quasi réel et historiques) des événements de sécurité

7. Comment cet outil fonctionne? Quelle différence avec les outils IDPS?

Les SIEM génèrent des alertes basées sur l'analyse des données de journal

- Les journaux de sécurité: Les logs générés par les pare-feu, les serveurs, les systèmes d'exploitation, les applications, etc.
- Les journaux des équipements réseau: Le trafic réseau, les événements de connexion, etc.
- Les journaux des dispositifs de sécurité: Les alertes générées par les antivirus, les IPS, etc.

SIEM : centraliser des journaux. Alors qu'un IDPS est un outil de prévention et de détection qui génère des journaux qui doivent être connectés au SIEM.

8. Pourquoi est-ce important de faire de l'analyse lors d'incidents?

a. de comprendre les causes profondes de l'incident,
b. d'identifier les points faibles de votre système de sécurité et
c. de mettre en place des mesures correctives pour prévenir la récurrence de tels événements.
d. Et ainsi d'évaluer les impacts et la portée de l'incident pour pouvoir la prioriser.

9. Quelles sont les différentes méthodes?

Analyse chronologique: Reconstitution de la séquence des événements dans l'ordre chronologique pour identifier les points de vulnérabilité et les actions de l'attaquant.
Analyse des logs: Examen approfondi des logs système, réseau et applicatifs pour détecter les anomalies, les activités suspectes et les traces de l'intrusion.
Analyse forensique: Utilisation d'outils spécialisés pour collecter, préserver et analyser les preuves numériques. Cela comprend l'analyse des images disque, l'examen des fichiers temporaires, la récupération de données effacées, etc.
Analyse des vulnérabilités: Identification des vulnérabilités exploitées par l'attaquant et évaluation de leur impact sur le système.
Analyse des contre-mesures: Évaluation de l'efficacité des mesures de sécurité mises en place pour prévenir et détecter les incidents.

10.Comment les incidents sont classés ? Et pourquoi?

- Décisions critiques basées sur les facteurs suivants (selon NIST):
  – Impact de l'incident sur les fonctions de l'entité

Impact de l'incident sur le DIC de l'information

  – Récupérabilité de l'incident
- Pour la priorisation : incident mineur est géré par l'équipe IR, alors qu'un incident majeur devra être escaladé à un responsable (processus d'escalade).