DS B3

jeudi 27 novembre 2025 10:11

Partie 1:

1) Un système d'information: c'est l'ensemble de ressource qui permet de traite des données dans une entreprise
   Exemple de 3 actifs:
- Employé
- Client
- PC

2) Les 5 catégorie d'actifs sont:
- Actif humain exemple: client
- Actif matériel exemple: serveur
- Actif immatériel exemple: réputation
- Actif logiciel exemple: antivirus
- Actif informationnel: données client

3) La criticité c'est l'importance d'un actifs
   Les 3 critères sont:
- l'importance
- Vulnérabilité
- l'impact

Triade CIA

1) Confidentialité c'est une donnée qui ne soit pas accessible à tout le monde
   Intégrité c'est une donnée qui ne soit pas modifier volontairement ou involontairement
   Disponibilité c'est une donnée qui est tout le temps accessible

2)

Scénario	Pilier(s) compromis	Justification
Ransomware chiffre les serveurs de fichiers	Disponibilité et intégrité	Le serveurs de fichiers est chiffré donc le serveur n'est plus disponible et il a était modifier
Interception de mots de passe en transit	Confidentialité	Les mots de passes sont accessible par une personne qui ne devait pas avoir
Modification non autorisée des prix en base	Intégrité	Les prix en base sont modifier sans autorisation
Panne électrique longue durée	Disponibilité	La panne électrique fait que le site n'est plus accessible

Menace, vulnérabilité, incident, risque

1) Menace c'est quelque chose qui peut exploité une vulnérabilité
   Vulnérabilité c'est une faiblisse d'un actifs exploité par une menace
   Incident c'est que la menace à exploité une vulnérabilité et qu'il y a un impact sur l'entreprise

Risque c'est la probabilité qu'un évènement se produit et la probabilité de son impact

2)

Mesures de sécurité

1) 3 mesures techniques contre le phishing sont:
   - Vérificateur
   - Authentification à multi facteur
   - Bloquer les spam

2) 3 mesures humaine sont :
   - Gérer les droits
   - Sensibilisation

3) 3 mesures physique sont:
   - Sauvegarder avec la règle 3-2-1
   - Pas de pc extérieur

Propriétés complémentaires de sécurité

1) Authenticité: vérifier l'identité de la personne qui fait les changements
   Preuve: démontrer que quelque chose s'est passé

Typologie des menaces

- Employé qui envoie par erreur un document confidentiel à un mauvais destinataire
  Humaine non intentionnelle car c'est un employé qui a envoyé un document et il a fait par erreur

- Groupe de hacker ciblant un secteur industriel
  Humaine intentionnelle car c'est un groupe de hacker et ils cible

- Inondation dans la salle serveurs
  Environnementale car c'est une inondation

- CNIL constate une non-conformité RGPD
  Légale car le CNIL c'est une organisation de l'état

- Ransomware via phishing
  Humaine non intentionnelle + technique car c'est un virus est c'est un employé qui cliqué sur le mail

- Configuration par défaut exposée sur une base de données
  Technique car c'est une configuration par défaut

- Tremblement de terre impactant le datacenter
  Environnementale car c'est un tremblement de terre

- Utilisation d'un logiciel sans licence
  Technique car c'est un logiciel

QCM

1) La disponibilité protège contre: (B) car disponibilité c'est le fait qu'une donnée soit accessible tout

le temps

2) Un ransomware compromet d'abord: (B) car il a accès au donner sensible
3) Un log centralisé sert principalement à: (B) car les log sert à voir qui a fait quoi
4)
5) Une configuration par défaut exposée est une: (B) car elle peut être exploité par une menace

Partie 2:

Étape 0:

1)

Étape 1:

1) Les 5 actifs de la société sont:
   - Matériel (PC, serveur, réseau)
   - Humaine (client, employé)

2)

1- Serveur car c'est là où tous les données sensible sont stocké (critique)
2- Réseau car si il tombe en panne plus personne peut aller sur le site et personne peut travail (critique)
3- Pc car si il y a pas de pc personne peut travail (élever)
4- Client (moyenne)
5- Employé (faible)

Étape 2:

n°	Scénario	Pilier(s) compromis	Mesure prioritaire
1	Phishing sur comptable, vol d'identifiants	Confidentialité	Changer d'identifiants et mot de passe, sensibilisation au phishing
2	DDoS sur le site e-commerce	Disponibilité	Anti-DDoS et Surdimensionner le réseau
3	Injection SQL sur formulaire de login	Confidentialité intégrité	Protéger sont formulaire et changer tous les login
4	Sauvegardes hors service pendant 3 semaines	Disponibilité	Réparer les sauvegardes
5	Employé mécontent exfiltre des données	Confidentialité intégrité	Retiré tous les droit

Étape 3:

Élément	Catégorie	Justification
Version obsolète d'Apache	Vulnérabilité	
Absence de MFA sur VPN	Vulnérabilité	Car si il a une attaque il vont facilement rentré
Groupe APT ciblant le secteur	Menace	Car il peuvent attaque à tout moment
Chiffrement réussi de la	Incident	Car la menace à exploité une

base client		vulnérabilité et donc la base client est chiffré
Probabilité élevée de fuite de données sensible	Risque	Car c'est une probabilité d'une vulnérabilité

Étape 4:

Étape 5:

- Ransomware sur serveur de fichiers

Impacts financiers: payer une rançon où payer quelqu'un pour déchiffré les donnes
Impacts juridiques: amende

Étape 6:

1) Phishing:
   - Envoie un mail ou message etc…
   - Personne clique sur le liens et rentre ses mot de passe
   - Récupère de mot de passe
   - Se connecte

DDoS:

- Envoie plient de paquet au serveur
- Le serveur tombe
- Les gens rentre

Injection SQL:

- Repérer un formulaire peut protéger
- Requête SQL à la place de login
- Récupération d'information