Notion de risques : TP 3 : Audit Interne : Compléments physique

vendredi 23 février 2024 10:44

Objectifs :

- Se poser des questions pour remplir les sujets
- Remplir chacun des sujets / Compléter le rapport 1er draft en appliquant les consignes du cours

Contexte :

- Les éléments de l'architecture N1 et N2 sont dans une salle de l'Université (Type salle de cours) avec un accès sécurisé par badge, l'architecture N1 est dans un Rack et l'architecture dans un autre Rack.
- Architecture N1 : Un serveur Web de développement Web (Linux - Apache - MySql) dite N1
  - Un serveur Web LAMP avec du développement de programmes en PHP pour gérer la communication d'une société
- Architecture N2 : 2 serveurs Web d'intégration/tests Web (Linux - Apache - MySql) dite N2
  - Un serveur Web Applicatif Linux - Apache avec les programmes en PHP pour gérer la communication d'une société
  - Un serveur Web Linux - MySql stockant les données

Prérequis :

- Déterminer les cibles et les éléments à auditer

NB : Ne pas oublier de référencer les outils ou utilitaires utilisables pour chaque sujet

TP3 : Audit de Sécurité : Approche Audit Interne (Eléments physique)

Pour l'architecture N1 comprenant un serveur Web (Apache/Linux/PHP/MySQL) :

1. **Identification des éléments :**

- Serveur Web (Apache)
- Système d'exploitation (Linux)
- Langage de programmation (PHP)
- Système de gestion de base de données (MySQL)

=> Compléter pour N1

5. **Sécurité physique et environnementale :**

- Mettre en place des mesures de sécurité physiques pour protéger le serveur contre les accès non autorisés et les dommages environnementaux.

Quelques éléments que vous pourriez vérifier :

1. **Localisation du serveur** :
   - Est-ce que le serveur est situé dans une zone sécurisée et restreinte, comme une salle serveur verrouillée ou un centre de données sécurisé ?

2. **Contrôle d'accès physique** :
   - Y a-t-il des mesures de contrôle d'accès physique en place pour limiter l'accès au serveur, telles que des serrures, des cartes d'accès ou des systèmes de reconnaissance biométrique ?

3. **Surveillance vidéo** :
  - Est-ce que la zone où se trouve le serveur est surveillée par des caméras de sécurité pour détecter toute activité suspecte ou non autorisée ?

4. **Alimentation électrique et climatisation** :
  - Le serveur est-il connecté à une alimentation électrique sécurisée et redondante pour éviter les pannes de courant ? Y a-t-il des systèmes de climatisation en place pour maintenir des conditions de température et d'humidité optimales ?

5. **Protection contre les incendies et les dégâts d'eau** :
  - Des systèmes de détection et de suppression d'incendie sont-ils installés dans la zone du serveur pour protéger contre les incendies ? Y a-t-il des mesures en place pour protéger le serveur contre les dégâts d'eau en cas de fuite ou d'inondation ?

6. **Sauvegarde et stockage sécurisé des données** :
  - Les données stockées sur le serveur sont-elles régulièrement sauvegardées et les sauvegardes sont-elles stockées de manière sécurisée, de préférence dans un lieu distant ?

7. **Politiques de sécurité physiques** :
  - Existe-t-il des politiques et des procédures documentées concernant la sécurité physique du serveur, y compris les mesures de protection à mettre en œuvre et les responsabilités des employés ?

7. **Accès aux systèmes et aux données :**

  - Définir des politiques d'accès pour contrôler qui peut accéder au serveur et aux données qu'il contient.

Evaluer comment les politiques d'accès sont définies pour contrôler l'accès au serveur et aux données qu'il contient, voici les étapes que vous pourriez suivre :

1. **Examen des documents de politique et de sécurité** :
  - Demandez à examiner les documents de politique de sécurité de l'entreprise, tels que les politiques d'accès, les directives de sécurité et les procédures opérationnelles standard (SOP), pour comprendre comment l'accès au serveur et aux données est réglementé.

2. **Analyse des rôles et des responsabilités** :
  - Identifiez les différents rôles et responsabilités au sein de l'organisation qui ont besoin d'accéder au serveur et aux données, tels que les administrateurs système, les développeurs, les utilisateurs finaux, etc.

6. **Contrôles d'accès physique et logique** :
  - Évaluez les contrôles d'accès physiques et logiques mis en place pour protéger le serveur contre les accès non autorisés, tels que les serrures, les cartes d'accès, les pare-feu, les listes de contrôle d'accès (ACL), etc.

14. **Gestion des changements :**

  - Établir des procédures pour planifier, autoriser, mettre en œuvre et évaluer les modifications apportées à l'architecture du serveur Web afin de minimiser les risques et d'optimiser les avantages.

Evaluer la gestion des changements et les procédures mises en place pour planifier, autoriser, mettre en œuvre et évaluer les modifications apportées à l'architecture du serveur Web.

1. **Processus de gestion des changements** :
  - Assurez-vous qu'un processus formel de gestion des changements est en place, décrivant les

étapes à suivre pour proposer, évaluer, autoriser et mettre en œuvre les modifications sur le serveur Web. Ce processus devrait inclure des exigences de documentation claires pour chaque étape du processus.

2. **Évaluation des risques et impact** :
   - Vérifiez que les changements proposés sont évalués pour leur impact potentiel sur la sécurité, la performance et la disponibilité du serveur Web. Assurez-vous qu'une analyse des risques est effectuée pour identifier les menaces potentielles et les mesures d'atténuation appropriées.

3. **Autorisation des changements** :
   - Assurez-vous qu'un processus d'autorisation formel est en place pour approuver les changements avant leur mise en œuvre. Les changements devraient être autorisés par des parties prenantes appropriées, en fonction de leur impact et de leur criticité.

4. **Planification et test des changements** :
   - Vérifiez que les changements sont planifiés et testés avant leur mise en œuvre pour s'assurer qu'ils fonctionnent comme prévu et qu'ils ne causent pas de perturbations indésirables sur le serveur Web. Les changements critiques devraient être testés dans un environnement de test avant d'être déployés en production.

5. **Documentation des changements** :
   - Assurez-vous que tous les changements apportés à l'architecture du serveur Web sont correctement documentés, y compris les détails des modifications, les raisons du changement, les autorisations accordées et les résultats des tests. Cette documentation est essentielle pour assurer la traçabilité et la transparence des changements.

6. **Évaluation post-implémentation** :
   - Après la mise en œuvre des changements, effectuez une évaluation post-implémentation pour évaluer l'efficacité des changements, identifier les problèmes potentiels et recueillir des leçons apprises pour améliorer les processus de gestion des changements à l'avenir.