

TP GESTION RISQUES

Bonjour,

Vous trouverez ci-joint l'énoncé de ce que vous devez préparer pour le prochain cours afin que nous puissions échanger.

Je vous rappelle que l'architecture Web, définie ci-après, est supposée :
« être installée dans la salle où nous avons cours. (Salle avec badge, rack, switch, etc...) ».

Bonne réflexion.

- -----

Prérequis :

- Déterminer les cibles à auditer
- Exemple : Une architecture Web (Linux - Apache - MySQL) dite N1
 - Un serveur Web LAMP avec du développement sous PHP pour gérer la communication d'une société

Objectifs : Remplir chacun des sujets

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

TP1 : Audit de Sécurité : Approche Audit Interne

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)

2. ****Gestion des actifs**** :

- Identifier, classer et gérer les logiciels et les composants matériels associés à chaque élément de l'architecture.

3. ****Conformité**** :

- S'assurer que les configurations et les politiques de sécurité sont conformes aux normes de sécurité et aux meilleures pratiques.

4. ****Sécurité des ressources humaines**** :

- Former le personnel sur les bonnes pratiques de sécurité et la gestion des incidents liés à la sécurité informatique.

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.

6. ****Gestion des configurations**** :

- Établir une procédure pour contrôler les modifications apportées aux logiciels et aux configurations du serveur Web.

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.

8. ****Cryptographie**** :

- Mettre en œuvre le chiffrement pour sécuriser les communications entre le serveur Web et les clients, ainsi que les données stockées dans la base de données.

9. ****Gestion des opérations**** :

- Surveiller les activités du serveur Web, mettre en place des mesures de protection contre les logiciels malveillants, assurer des sauvegardes régulières des données et gérer les incidents de sécurité.

10. ****Contrôle d'accès**** :

- Mettre en place des mécanismes d'authentification et d'autorisation pour contrôler l'accès aux ressources du serveur.

11. ****Sécurité des systèmes d'information**** :

- Mettre en place des mesures de sécurité techniques pour détecter et prévenir les failles de sécurité et les attaques informatiques sur le serveur Web et les bases de données.

12. ****Gestion des incidents de sécurité**** :

- Établir un processus pour détecter, signaler, enquêter et répondre aux incidents de sécurité de manière efficace et opportune.

13. **Gestion de la continuité d'activité** :

- Planifier et préparer des mesures pour garantir la disponibilité continue du serveur Web en cas d'incident majeur ou de catastrophe.

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.