Notion de risques : TP 2 : Rapport de l'Audit

vendredi 23 février 2024 10:44

Objectifs : Remplir chacun des sujets / Rédiger un rapport 1er draft en appliquant les consignes du cours

Contexte :

- 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

TP2 : Audit de Sécurité : Approche Audit Interne

Le rapport doit comprendre les chapitres suivants:

1. Résumé Exécutif (pour la Direction Générale/DSI)
   1. Objectif : Fournir une vue d'ensemble non technique des résultats, des risques principaux, et des recommandations.
   2. Contenu : Un plan inspiré du cours applicable à une direction
      a. Un tableau récapitulatif des risques majeurs, avec une évaluation de l'impact sur l'entreprise.
      b. Matrice des risques majeurs issue du plan d'action
      c. Format : Langage clair, sans jargon technique, axé sur les implications commerciales et les mesures correctives stratégiques.
      d. Résultat de l'exécution du Plan d'Action TP1/N1

2. Description de la Méthodologie (pour le DSI et les Équipes Techniques)
   1. Objectif : Présenter les objectifs et les cibles de l'audit, et de la méthodologie utilisée.
   2. Contenu : Un plan inspiré du cours applicable à un DSI
      a. Matrice des Vulnérabilités
      b. Matrice des risques
      c. Matrice du plan d'action
      d. Périmètre de l'audit : Liste des systèmes, applications, et réseaux testés.(**cf. Annexes : Reprise de la trame du document d'audit TP1/N1**)(voir ci-dessous)
   3. Méthodologie : Description des étapes, des outils utilisés, et des approches (boîte xxx)
   4. Format : Plus technique, incluant des détails spécifiques sur les tests réalisés.

3. Recommandations et Plan d'Action (pour le DSI et les Équipes Techniques)

Pour l'architecture de développement, dite 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)

Pour l'architecture d'intégration/tests, dite N2, un peu plus complexe comprenant un serveur Web (Apache/Linux/PHP), un serveur Linux/MySQL, des cartes réseau publiques et d'administration pour chaque serveur :

1. **Identification des éléments** :

- Serveur Web (Apache)
- Serveur Linux (système d'exploitation)
- Serveur MySQL (base de données)
- Carte réseau publique et carte d'administration pour chaque serveur
- Pare-feu en front-end ?
- Pare-feu entre le serveur Web et le serveur de base de données ?

=> Compléter pour N2

2. **Gestion des actifs** :

- Identifier, classer et gérer les logiciels et les composants matériels associés à chaque serveur, à chaque carte réseau et à chaque pare-feu.

3. **Conformité** :

- S'assurer que les configurations et les politiques de sécurité sont conformes aux normes de sécurité et aux meilleures pratiques pour chaque composant de l'architecture, y compris les pare-feu.

4. **Sécurité des ressources humaines** :

- Former le personnel sur les bonnes pratiques de sécurité et la gestion des incidents liés à la sécurité informatique pour chaque élément de l'architecture.

5. **Sécurité physique et environnementale** :

- Mettre en place des mesures de sécurité physiques pour protéger chaque serveur, chaque carte réseau et chaque pare-feu contre les accès non autorisés et les dommages environnementaux.

6. **Gestion des configurations** :

- Établir une procédure pour contrôler les modifications apportées aux logiciels, aux configurations et aux règles des pare-feu pour chaque composant de l'architecture.

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

- Définir des politiques d'accès pour contrôler qui peut accéder aux serveurs, aux cartes réseau et aux pare-feu, en particulier pour les serveurs contenant des données sensibles.

8. **Cryptographie** :

- Mettre en œuvre le chiffrement pour sécuriser les communications entre les serveurs, les cartes réseau et les pare-feu, ainsi que les données stockées dans la base de données.

9. **Gestion des opérations** :

- Surveiller les activités de chaque serveur, chaque carte réseau et chaque pare-feu, 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 de chaque serveur, chaque carte réseau et chaque pare-feu.

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 chaque serveur, chaque carte réseau et chaque pare-feu.

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

- Établir un processus pour détecter, signaler, enquêter et répondre aux incidents de sécurité de manière efficace et opportune pour chaque composant de l'architecture.

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

- Planifier et préparer des mesures pour garantir la disponibilité continue de chaque serveur, chaque carte réseau et chaque pare-feu 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, y compris les changements de configuration des pare-feu et des règles de filtrage, afin de minimiser les risques et d'optimiser les avantages.