Notion de risques : TP 5 bis : Audit Interne : Compléments

vendredi 23 février 2024 10:44

Objectifs :

- **Complète le TP5** en se posant les questions sur les sujets non traités jusqu'à présent

TP5 : Audit de Sécurité : Approche Audit Interne

- Prérequis : Architecture N1, N2, N3 définie
- Compléter vos précédents travaux avec les sujets :
    - 4. **Sécurité des ressources humaines** :
    - 5. **Sécurité physique et environnementale => déjà traité précédemment
    - 6. **Gestion des configurations** :
    - 7. **Accès aux systèmes et aux données => déjà traité précédemment
    - 8. **Cryptographie** :
    - 9. **Gestion des opérations** :
    - 10. **Contrôle d'accès** :
    - 11. **Sécurité des systèmes d'information** :
    - 12. **Gestion des incidents de sécurité** :
    - 14. **Gestion des changements => déjà traité précédemment

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

1. **Identification des éléments :**

- Architecture N1
    - Serveur Web (Apache)
    - Système d'exploitation (Linux)
    - Langage de programmation (PHP)
    - Système de gestion de base de données (MySQL)
- Architecture N2 et N3 : A compléter

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 :**

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

Evaluer le niveau de connaissances et de sensibilisation des différents profils concernant les bonnes pratiques de sécurité et la gestion des incidents liés à la sécurité informatique :

Profil Administrateur :

1. Pouvez-vous expliquer les principales mesures de sécurité que vous avez mises en place sur le serveur pour protéger les données et les applications ?

2. Comment gérez-vous les mises à jour de sécurité sur le serveur et les applications hébergées ?

3. Quels sont les processus que vous suivez pour surveiller les journaux d'activité du serveur et détecter les anomalies ou les activités suspectes ?

4. En cas d'incident de sécurité, quelle est la procédure que vous suivez pour enquêter, répondre et remédier à la situation ?

Profil Développeur :

1. Pouvez-vous expliquer comment vous assurez-vous que les applications que vous développez intègrent des mesures de sécurité telles que la validation des entrées utilisateur et la protection contre les attaques de type injection SQL ?

2. Comment gérez-vous les dépendances et les bibliothèques tierces dans vos projets de développement afin de garantir qu'elles sont à jour et sécurisées ?

3. Avez-vous déjà réalisé des tests de sécurité des applications que vous avez développées ? Si oui, pouvez-vous décrire le processus et les outils utilisés ?

Profil Utilisateur :

1. Quelles sont les mesures que vous prenez pour protéger vos mots de passe et vos identifiants lors de la connexion aux systèmes informatiques de l'entreprise ?

2. Avez-vous reçu une formation sur la reconnaissance des attaques de phishing et les étapes à suivre en cas de réception d'un e-mail suspect ?

3. En cas de soupçon d'activité malveillante ou d'incident de sécurité, savez-vous vers qui vous tourner et comment signaler l'incident à l'équipe 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.

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 ?

6. **Gestion des configurations :**

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

S'assurer du contrôle des modifications apportées aux logiciels et aux configurations du serveur Web

1. **Identification des changements autorisés** :
   - Établissez-vous une liste des changements autorisés/appliqués sur les logiciels et sur les configurations du serveur Web ?

2. **Gestion des demandes de changement** :
   - Avez-vous mis en place un processus formel de gestion des demandes de changement (GDC) pour enregistrer, évaluer et approuver les modifications proposées aux logiciels et aux configurations du serveur Web ?

3. **Validation des changements** :
   - Avant d'implémenter un changement, avez-vous un processus de validation par les personnes appropriées, comme les administrateurs système et les responsables de la sécurité, qui s'assurent qu'il est conforme aux politiques et aux normes de l'entreprise ?

4. **Journalisation des modifications** :
   - Consignez-vous toutes les modifications apportées aux logiciels et aux configurations du serveur Web. Sont-elles consignées dans un journal (log/logiciel/tableur), y compris des informations telles que la date et l'heure de la modification, la nature de la modification et l'identité de la personne ayant apporté la modification ?

5. **Contrôle des versions** :
   - Utilisez-vous un système de contrôle de version pour suivre les versions des logiciels et des configurations du serveur Web, qui permettrait de revenir à des versions précédentes en cas de besoin et de suivre les changements au fil du temps ?

6. **Tests et validation post-changement** :
   - Après l'implémentation d'un changement, effectuez-vous des tests pour vous assurer que le serveur Web fonctionne correctement ? Que les modifications n'ont pas introduit de vulnérabilités de sécurité ou de dysfonctionnements ? Avez-vous un protocole de tests ?

7. **Gestion des exceptions** :
   - Avez-vous établi un processus pour gérer les exceptions aux procédures de contrôle des changements, notamment pour les changements d'urgence ou critiques qui doivent être mis en œuvre rapidement ?

8. **Surveillance continue** :
   - Avez-vous mis en place des mécanismes de surveillance continue pour détecter et signaler les changements non autorisés ou les violations des politiques de configuration 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.

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.

3. **Définition des droits d'accès** :
   - Vérifiez comment les droits d'accès sont définis pour chaque groupe d'utilisateurs, en fonction de leurs besoins opérationnels. Cela peut inclure des droits d'accès spécifiques aux fichiers, aux répertoires ou aux fonctionnalités du serveur.

4. **Mécanismes d'authentification et d'autorisation** :
   - Évaluez les mécanismes d'authentification et d'autorisation utilisés pour contrôler l'accès au serveur, tels que l'authentification par mot de passe, l'authentification à deux facteurs, l'accès basé sur les rôles, etc.

5. **Gestion des comptes utilisateurs** :
   - Examinez les politiques et les procédures de gestion des comptes utilisateurs, y compris la création, la modification et la suppression des comptes, pour garantir que seules les personnes autorisées ont accès aux ressources appropriées.

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.

7. **Surveillance et audit des accès** :
   - Vérifiez comment les accès au serveur sont surveillés et audités pour détecter et prévenir les accès non autorisés. Cela peut inclure la journalisation des événements, les journaux d'audit et les alertes de sécurité.

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.

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

1. **Chiffrement des communications entre le serveur Web et les clients** :
   - Vérifiez si le serveur Web utilise des protocoles de communication sécurisés tels que HTTPS (HTTP Secure) pour chiffrer les données échangées entre le serveur et les navigateurs des clients. Assurez-vous que des certificats SSL/TLS valides sont utilisés pour garantir l'authenticité du serveur et protéger la confidentialité et l'intégrité des données transitant sur le réseau.

2. **Paramètres de chiffrement TLS** :
   - Examinez les paramètres de chiffrement TLS (Transport Layer Security) utilisés pour sécuriser les communications HTTPS, tels que les versions de TLS autorisées, les algorithmes de chiffrement (comme AES, RSA, etc.) et les paramètres de clé (longueur de clé, etc.). Assurez-vous que des paramètres de chiffrement sécurisés et conformes aux normes actuelles sont utilisés pour éviter les vulnérabilités connues.

3. **Chiffrement des données stockées dans la base de données** :
   - Vérifiez si les données stockées dans la base de données sont chiffrées pour protéger leur confidentialité en cas de compromission du stockage. Assurez-vous que les données sensibles, telles que les informations personnelles des utilisateurs ou les données financières, sont chiffrées à l'aide d'algorithmes de chiffrement robustes avant d'être stockées dans la base de données. Ou non !

4. **Gestion des clés de chiffrement** :
   - Examinez les pratiques de gestion des clés de chiffrement pour vous assurer que les clés de chiffrement sont générées de manière sécurisée, stockées de manière protégée et gérées de manière appropriée tout au long de leur cycle de vie. Assurez-vous également qu'un processus de rotation régulière des clés est en place pour renforcer la sécurité du chiffrement.

5. **Audits de sécurité et conformité** :
   - Vérifiez si des audits de sécurité sont réalisés régulièrement pour évaluer l'efficacité des mesures de chiffrement mises en œuvre et pour garantir la conformité aux normes de sécurité et aux meilleures pratiques de l'industrie, telles que les normes PCI DSS (Payment Card Industry Data Security Standard).

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.

Evaluer la gestion des opérations liées au serveur Web, y compris la surveillance des activités, la protection contre les logiciels malveillants, les sauvegardes régulières des données et la gestion des incidents de sécurité.

1. **Surveillance des activités du serveur Web** :
   - Vérifiez si des outils de surveillance des activités du serveur Web sont en place pour suivre les performances, la disponibilité et l'utilisation des ressources du serveur. Cela peut inclure des outils de surveillance des journaux d'accès, des performances du serveur, et des alertes en cas d'anomalies ou d'activités suspectes.

2. **Protection contre les logiciels malveillants** :

- Examinez les mesures de protection mises en place pour prévenir les logiciels malveillants sur le serveur Web, tels que l'installation et la mise à jour régulière d'un logiciel antivirus, la configuration de pare-feu et de filtres anti-malware, et la limitation des droits d'accès aux fichiers sensibles.

3. **Sauvegardes régulières des données** :
   - Vérifiez si des politiques et des procédures de sauvegarde régulières sont en place pour protéger les données stockées sur le serveur Web contre la perte de données accidentelle, la corruption des données ou les attaques de ransomware. Assurez-vous que les sauvegardes sont effectuées régulièrement, que les données sauvegardées sont chiffrées et stockées de manière sécurisée, et que des tests de restauration sont effectués périodiquement pour garantir l'intégrité des sauvegardes.

4. **Gestion des incidents de sécurité** :
   - Examinez les procédures de gestion des incidents de sécurité pour savoir comment les incidents de sécurité sont détectés, signalés, évalués et traités sur le serveur Web. Assurez-vous qu'une équipe de réponse aux incidents est en place, avec des procédures claires pour enquêter sur les incidents, prendre des mesures correctives et préventives, et communiquer avec les parties prenantes concernées.

5. **Formation et sensibilisation du personnel** :
   - Vérifiez si le personnel est formé et sensibilisé aux procédures de gestion des opérations liées au serveur Web, y compris la surveillance des activités, la protection contre les logiciels malveillants, les sauvegardes des données et la gestion des incidents de sécurité. Assurez-vous que le personnel sait comment reconnaître et signaler les incidents de sécurité potentiels et comment réagir en cas d'urgence.

10. **Contrôle d'accès :**

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

Evaluer les mécanismes d'authentification et d'autorisation :

1. **Authentification** :
   - Assurez-vous que des mécanismes d'authentification robustes sont mis en place pour accéder aux ressources du serveur, tels que l'authentification par mot de passe sécurisé ou l'authentification à deux facteurs si nécessaire.

2. **Gestion des utilisateurs** :
   - Vérifiez que seuls les utilisateurs autorisés disposent de comptes sur le serveur. Désactivez ou supprimez les comptes inactifs ou non nécessaires pour réduire les risques.

3. **Contrôles d'accès aux fichiers et répertoires** :
   - Utilisez les permissions Linux pour contrôler l'accès aux fichiers et répertoires. Limitez les autorisations d'accès aux données sensibles uniquement aux utilisateurs nécessaires.

4. **Authentification MySQL** :
   - Configurez l'authentification MySQL de manière sécurisée en utilisant des mots de passe forts pour les utilisateurs MySQL et en limitant l'accès aux bases de données selon le principe du moindre privilège.

5. **Surveillance des journaux** :
   - Activez la journalisation des événements pour surveiller les activités du serveur, y compris les tentatives d'accès non autorisées ou les activités suspectes.

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.

Ce qu'il faut examiner :

1. **Mise à jour et patch management** :
   - Assurez-vous que le système d'exploitation Linux ainsi que les logiciels serveur tels qu'Apache, PHP et MySQL sont régulièrement mis à jour avec les derniers correctifs de sécurité pour corriger les vulnérabilités connues.

2. **Configuration sécurisée des services** :
   - Vérifiez que les services Apache, PHP et MySQL sont configurés de manière sécurisée en désactivant les fonctionnalités non nécessaires, en limitant les privilèges d'accès et en utilisant des paramètres de sécurité recommandés.

3. **Protection contre les attaques par injection SQL** :
   - Mettez en place des mesures de prévention contre les attaques par injection SQL en utilisant des requêtes paramétrées ou en appliquant des méthodes de filtrage et de validation des données d'entrée dans les applications PHP.

4. **Sécurisation des fichiers et répertoires** :
   - Utilisez les permissions Linux pour limiter l'accès aux fichiers et répertoires du serveur Web uniquement aux utilisateurs nécessaires. Assurez-vous que les fichiers sensibles, tels que les fichiers de configuration, sont protégés contre les accès non autorisés.

5. **Utilisation d'un pare-feu** :
   - Déployez un pare-feu sur le serveur pour surveiller et contrôler le trafic réseau entrant et sortant. Configurez des règles de pare-feu pour limiter l'accès aux services autorisés et bloquer le trafic suspect.

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

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

Evaluer la gestion des incidents de sécurité et les processus mis en place pour détecter, signaler, enquêter et répondre aux incidents de manière efficace et opportune.

1. **Détection des incidents** :
   - Vérifiez si des outils de détection des incidents sont en place pour surveiller les activités du serveur Web et des bases de données, ainsi que le trafic réseau, afin de détecter les comportements malveillants ou anormaux.

2. **Signalement des incidents** :
   - Assurez-vous qu'il existe des procédures claires pour signaler les incidents de sécurité dès qu'ils sont détectés. Identifiez les canaux de communication internes et externes pour signaler les incidents aux parties concernées.

3. **Enquête sur les incidents** :
   - Vérifiez s'il existe des protocoles établis pour enquêter sur les incidents de sécurité une fois qu'ils ont été signalés. Assurez-vous que des équipes dédiées sont en place pour mener des enquêtes approfondies sur les incidents, en recueillant des preuves, en analysant les causes sous-jacentes et en identifiant les actions correctives nécessaires.

4. **Réponse aux incidents** :

- Assurez-vous que des plans de réponse aux incidents sont en place pour prendre des mesures immédiates pour contenir et atténuer les incidents dès qu'ils sont détectés. Identifiez les étapes à suivre pour restaurer les services, remédier aux vulnérabilités et minimiser l'impact sur les activités de l'entreprise.

5. **Coordination et communication** :
- Vérifiez s'il existe des protocoles de coordination et de communication pour travailler avec les équipes internes et externes, y compris les fournisseurs de services de sécurité, les autorités réglementaires et les parties prenantes concernées, lors de la gestion des incidents de sécurité.

6. **Analyse post-incident** :
- Assurez-vous que des processus sont en place pour mener une analyse post-incident afin d'évaluer la réponse aux incidents, d'identifier les leçons apprises et d'apporter des améliorations aux processus de gestion des incidents pour l'avenir.

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.

Evaluer la gestion de la continuité des activités avec un seul serveur Linux/Apache/PHP/MySQL :

1. **Redondance au niveau du matériel et de l'infrastructure** :
- Assurez-vous que le matériel du serveur est doté de composants redondants (par exemple, disques durs en RAID, alimentations redondantes) pour réduire les risques de défaillance matérielle.

2. **Sauvegardes régulières des données** :
- Vérifiez que des sauvegardes régulières de la base de données MySQL et des fichiers du serveur Web sont effectuées. Assurez-vous que ces sauvegardes sont stockées sur un périphérique de stockage externe sécurisé et testées régulièrement pour garantir leur intégrité.

3. **Scripts de sauvegarde automatisés** :
- Mettez en place des scripts de sauvegarde automatisés pour faciliter le processus de sauvegarde et minimiser les erreurs humaines. Ces scripts devraient être planifiés pour s'exécuter régulièrement selon un calendrier défini.

4. **Plan de reprise d'Activités (**PRA**) ou Plan de reprise après sinistre (PRS) simplifié** :
- Élaborez un plan de reprise après sinistre (PRS) simple mais efficace, décrivant les étapes à suivre pour restaurer le serveur Web en cas de panne majeure. Ce plan devrait inclure des instructions détaillées sur la restauration des données à partir des sauvegardes et la reconstruction de l'environnement de serveur.

5. **Tests de restauration** :
- Effectuez régulièrement des tests de restauration à partir des sauvegardes pour vous assurer que les données peuvent être récupérées avec succès en cas de besoin. Identifiez et corrigez les problèmes éventuels rencontrés lors de ces tests.

6. **Surveillance proactive** :
- Mettez en place un système de surveillance proactive pour détecter les signes de défaillance potentielle du serveur, tels que des alertes sur l'utilisation des ressources, les erreurs système, etc. Cela permettra d'intervenir rapidement pour éviter les incidents majeurs.

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.