M106 — Sécurité des données et gestion des accès

F. Mauron

EPAI

02 décembre 2023

Plan

Plan

Database

Les bases de données sont le coeur de presque toutes les applications modernes, stockant et gérant les informations essentielles à nos systèmes.

Une bonne compréhension de la **gestion des bases de données** n'est pas seulement **cruciale** pour la manipulation des données, mais aussi pour garantir leur **sécurité**, leur **intégrité**, et leur **disponibilité**.

Sujets clés du module

Dans ce cours, nous couvrirons une gamme de sujets clés, y compris mais sans s'y limiter :

- **Sécurité des données** et **Gestion des accès** : Apprenez à élaborer des concepts de sécurité et à gérer les accès pour protéger les données sensibles.
- **Interrogation et manipulation des données** : Maîtrisez les techniques de requête pour extraire et manipuler les données de manière efficace.
- **Sauvegarde et restauration des données** : Comprenez les stratégies essentielles pour la sauvegarde des données et leur restauration en cas de perte.
- **Optimisation de la base de données** Découvrez comment optimiser les performances de la base de données pour un fonctionnement efficace et rapide.

Plan

But

Établir un concept de sécurité dans le cadre d'un système de gestion de base de données (SGBD) implique plusieurs étapes clés pour assurer la protection et l'intégrité des données.

Plan

Analyse des besoins et des risques

- **Évaluation des données** : Identifier la nature et la sensibilité des données gérées par le SGBD.
- **Analyse des risques** : Déterminer les menaces potentielles (accès non autorisé, perte de données, etc.) et leur impact possible.

Évaluation des données

Identifier la nature et la sensibilité des données gérées par un système de gestion de base de données (SGBD) est une étape essentielle pour établir un concept de sécurité efficace.

Classification des données

- **Catégorisation** : Déterminer les différents types de données stockées (personnelles, financières, opérationnelles, etc.).
- **Sensibilité** : Évaluer le degré de sensibilité de chaque catégorie de données (publique, interne, confidentielle, secrète).

Analyse des sources de données

- **Origine des données** : Identifier d'où proviennent les données (internes, externes, tierces parties).
- **Mode de collecte** : Comprendre comment les données sont collectées et intégrées dans le SGBD.

Évaluation de l’utilisation des données

- **Utilisation courante** : Examiner comment et par qui les données sont actuellement utilisées.
- **Accès et partage** : Identifier qui a accès aux données et comment elles sont partagées ou transmises.

Identification des exigences réglementaires

- **Conformité** : Déterminer les réglementations applicables (comme le RGPD pour les données personnelles).
- **Obligations légales** : Prendre en compte les obligations légales liées à la conservation et à la protection des données.

Évaluation des risques associés

- **Risques de perte de données** : Estimer le risque et l'impact de la perte ou de la divulgation non autorisée de données.
- **Conséquences d'une violation** : Analyser les conséquences potentielles d'une violation de données (réputation, financière, juridique).

Audit et revue de sécurité

- **Examen des politiques actuelles** : Vérifier les politiques de sécurité actuelles et leur adéquation avec la nature des données.
- **Évaluation des mesures de protection** : Examiner les mesures de protection en place (chiffrement, contrôle d'accès).

Consultation avec les parties prenantes

- **Discussion avec les utilisateurs** : Dialoguer avec les utilisateurs pour comprendre leurs besoins et préoccupations en matière de données.
- **Collaboration avec les experts en sécurité** : Travailler avec des spécialistes de la sécurité pour évaluer les aspects techniques.

Documentation et mise à jour

- **Documentation des catégories de données** : Tenir à jour une documentation détaillée sur les types de données et leur sensibilité.
- **Révision périodique** : Réévaluer régulièrement la classification des données pour tenir compte des changements dans l'entreprise ou de la réglementation.

Plan

Objectif

Identifier et évaluer les menaces potentielles auxquelles les données et les systèmes de l'entreprise sont exposés, ainsi que l'impact possible de ces menaces.

Menaces potentielles I/V

Accès non autorisé

- **Description :** Intrusion dans les systèmes par des utilisateurs non autorisés.
- **Impact possible :** Fuite de données confidentielles, perturbation des opérations, atteinte à la réputation.

Menaces potentielles II/V

Perte de données

- **Description :** Perte de données due à des erreurs humaines, pannes de système, ou désastres naturels.
- **Impact possible :** Interruption des activités, perte de confiance des clients, coûts élevés de récupération.

Menaces potentielles III/V

Attaques par malware

- **Description :** Infection par des logiciels malveillants comme des virus, ransomware, ou spyware.
- **Impact possible :** Corruption des données, vol d'informations sensibles, perte de productivité.

Menaces potentielles IV/V

Ingénierie sociale

- **Description :** Manipulation des individus pour obtenir un accès non autorisé aux informations.
- **Impact possible :** Fuite d'informations, fraudes, usurpation d'identité.

Menaces potentielles V/V

Failles de sécurité

- **Description :** Vulnérabilités dans les logiciels ou le matériel qui peuvent être exploitées.
- **Impact possible :** Accès non autorisé, perturbation des services, compromission des systèmes.

Évaluation de l'impact I/II

Méthodologie

- **Évaluation des conséquences :** Déterminer l'impact d'une menace sur les opérations, la réputation, et les finances.
- **Probabilité d'ocurrence :** Estimer la fréquence à laquelle une menace peut se réaliser.
- **Priorisation des risques :** Classer les menaces en fonction de leur impact et probabilité pour identifier les risques prioritaires.

Évaluation de l'impact II/II

Exemple d'évaluation

- **Accès non autorisé :**
  - *Impact :* Élevé (fuite de données sensibles).
  - *Probabilité :* Moyenne.
  - *Priorité :* Haute.
- **Perte de données :**
  - *Impact :* Très élevé (interruption des activités).
  - *Probabilité :* Faible à moyenne.
  - *Priorité :* Haute.

Planification de la Réponse

Stratégies

- **Prévention :** Mettre en place des mesures pour prévenir les menaces (formations, sécurité physique et logique).
- **Détection :** Systèmes de surveillance pour détecter rapidement les incidents.
- **Réponse :** Procédures d'intervention en cas d'incident pour minimiser l'impact.
- **Récupération :** Plans de récupération pour restaurer les opérations normales.

Plan

Définition de la politique de sécurité

- **Objectifs de sécurité** : Définir clairement les objectifs de sécurité en termes de confidentialité, intégrité et disponibilité des données.
- **Normes et réglementations** : Prendre en compte les exigences légales et les normes industrielles pertinentes (comme le RGPD).

Objectifs de sécurité

Établir des objectifs clairs en matière de sécurité des données, en se concentrant sur trois aspects principaux :

- la confidentialité,
- l'intégrité et
- la disponibilité.

Confidentialité

- **But :** Assurer que les données ne sont accessibles qu'aux personnes autorisées.
- **Stratégies :**
  - **Contrôle d'accès :** Mettre en place des systèmes d'authentification et de gestion des autorisations.
  - **Chiffrement :** Utiliser le chiffrement pour protéger les données en transit et au repos.
  - **Politiques de confidentialité :** Élaborer des directives claires sur la manipulation des données sensibles.

Intégrité

- **But :** Maintenir l'exactitude et la cohérence des données tout au long de leur cycle de vie.
- **Stratégies :**
  - **Vérifications de l'intégrité :** Implémenter des mécanismes pour détecter toute altération ou corruption des données.
  - **Gestion des modifications :** Suivre toutes les modifications apportées aux données et assurer la traçabilité.
  - **Sauvegardes régulières :** Effectuer des sauvegardes périodiques pour prévenir la perte de données.

Disponibilité

- **But :** Garantir que les données sont accessibles et utilisables lorsque nécessaire.
- **Stratégies :**
  - **Planification de la continuité :** Mettre en place des plans de continuité d'activité pour garantir l'accès aux données en cas de sinistre.
  - **Infrastructure robuste :** Assurer une infrastructure fiable avec des capacités de redondance et de récupération.
  - **Monitoring et maintenance :** Surveiller constamment les systèmes et effectuer une maintenance préventive pour prévenir les interruptions.

Plan

Exigences légales

- **Compréhension des lois :**
  - **Étude des réglementations :** Se familiariser avec les lois applicables telles que le RGPD pour la protection des données personnelles.
  - **Analyse juridique :** Consulter des experts juridiques pour comprendre les implications spécifiques pour l'entreprise.
- **Mise en pratique :**
  - **Politiques de conformité :** Développer des politiques internes qui reflètent les exigences légales.
  - **Formation du personnel :** Éduquer les employés sur les lois pertinentes et les bonnes pratiques à suivre.

Normes industrielles

- **Identification des normes :**
  - **Recherche de normes :** Identifier les normes industrielles pertinentes (ISO, NIST, etc.) pour la sécurité des données.
  - **Évaluation des standards :** Évaluer comment ces normes s'appliquent aux opérations de l'entreprise.
- **Intégration des normes :**
  - **Procédures standardisées :** Mettre en œuvre des procédures qui respectent les normes établies.
  - **Vérifications régulières :** Effectuer des audits réguliers pour s'assurer de la conformité continue.

Exemple : RGPD

- **Protection des données personnelles :**
  - **Consentement et transparence :** S'assurer que le consentement est obtenu pour la collecte de données personnelles et que les utilisateurs sont informés de l'utilisation de leurs données.
  - **Droits des sujets de données :** Faciliter l'exercice des droits des individus (accès, rectification, suppression des données).
  - **Sécurité des données :** Mettre en place des mesures techniques et organisationnelles pour protéger les données personnelles.
- **Responsabilisation et gouvernance :**
  - **Délégué à la protection des données :** Désigner un responsable pour superviser la conformité au RGPD.
  - **Documentation et registres :** Tenir des registres détaillés des activités de traitement des données.

Plan

Contrôle d'accès

- **Authentification des utilisateurs** : Mettre en place des mécanismes robustes d'authentification des utilisateurs (mots de passe, authentification multi-facteurs, etc.).
- **Gestion des rôles et des autorisations** : Attribuer des rôles spécifiques aux utilisateurs et définir des autorisations en fonction de ces rôles pour limiter l'accès aux données sensibles.

Authentification des utilisateurs

But

Renforcer la sécurité des systèmes en implémentant des mécanismes d'authentification solides et efficaces pour les utilisateurs.

Authentification par mot de passe

- **Création de mots de passe forts :**
  - **Politiques de mot de passe :** Établir des exigences pour la création de mots de passe (longueur, complexité).
  - **Renouvellement régulier :** Inciter les utilisateurs à changer leurs mots de passe périodiquement.
- **Stockage et gestion des mots de passe :**
  - **Chiffrement des mots de passe :** Utiliser le hachage et le salage pour stocker les mots de passe de manière sécurisée.
  - **Gestionnaires de mots de passe :** Encourager l'utilisation de gestionnaires de mots de passe pour une meilleure gestion.

Authentification Multi-Facteurs (MFA)

- **Principes de MFA :**
  - **Combinaison de facteurs :** Utiliser une combinaison de quelque chose que l'utilisateur sait (mot de passe), possède (token, smartphone) et est (biométrie).
  - **Diversité des méthodes :** Offrir différentes méthodes de MFA (SMS, applications d'authentification, tokens physiques).
- **Implémentation de MFA :**
  - **Intégration système :** Intégrer MFA dans les systèmes d'accès critiques (emails, bases de données).
  - **Formation et sensibilisation :** Éduquer les utilisateurs sur l'importance et l'utilisation de MFA.

Authentification biométrique

- **Utilisation de biométrie :**
  - **Types de biométrie :** Implémenter des méthodes biométriques (empreintes digitales, reconnaissance faciale, reconnaissance vocale).
  - **Sécurité des données biométriques :** Assurer la protection et le stockage sécurisé des données biométriques.
- **Considérations éthiques et légales :**
  - **Respect de la vie privée :** Prendre en compte la confidentialité et le consentement dans l'utilisation de la biométrie.
  - **Conformité réglementaire :** S'assurer que l'utilisation de la biométrie est conforme aux lois en vigueur.

Gestion des accès

- **Suivi et revue des accès :**
  - **Audit des accès :** Effectuer des audits réguliers pour surveiller et réviser les accès utilisateurs.
  - **Gestion des identités :** Utiliser des systèmes de gestion des identités pour contrôler l'accès aux ressources.

Gestion des rôles et des autorisations

But

Contrôler et limiter l'accès aux données sensibles en attribuant des rôles spécifiques aux utilisateurs et en définissant des autorisations appropriées pour ces rôles.

Établissement des rôles

- **Définition des rôles :**
  - **Identification des besoins :** Analyser les besoins d'accès des différents utilisateurs au sein de l'organisation.
  - **Création de rôles :** Définir des rôles distincts basés sur les fonctions et les responsabilités (par exemple, administrateur, utilisateur standard, auditeur).
- **Attribution des rôles :**
  - **Assignation des utilisateurs :** Attribuer chaque utilisateur à un ou plusieurs rôles en fonction de ses responsabilités.
  - **Gestion des changements de rôle :** Mettre en place un processus pour gérer les changements de rôles, promotions ou départs.

Définition des autorisations

- **Permissions par rôle :**
  - **Niveaux d'accès :** Déterminer les niveaux d'accès nécessaires pour chaque rôle (lecture seule, écriture, administration).
  - **Restrictions basées sur le rôle :** Limiter l'accès aux données sensibles en fonction du rôle attribué.
- **Mise en oeuvre des autorisations :**
  - **Systèmes de contrôle d'accès :** Utiliser des systèmes de contrôle d'accès basés sur les rôles (RBAC) pour gérer les autorisations.
  - **Révision périodique :** Réévaluer régulièrement les autorisations pour s'assurer qu'elles restent appropriées et sécurisées.

Sécurité et conformité

- **Principe de moindre privilège :**
  - **Application :** Assurer que les utilisateurs disposent uniquement des autorisations nécessaires pour effectuer leurs tâches.
  - **Réduction des risques :** Minimiser le risque d'accès non autorisé en limitant les privilèges.
- **Audit et surveillance :**
  - **Suivi des activités :** Surveiller l'utilisation des privilèges pour détecter toute activité suspecte ou non autorisée.
  - **Rapports d'audit :** Générer des rapports pour les audits de sécurité et les revues de conformité.

Chiffrement des données

- **Chiffrement au repos** : Utiliser des techniques de chiffrement pour protéger les données stockées.
- **Chiffrement en transit** : Assurer la sécurité des données lorsqu'elles sont transférées sur le réseau.

Sauvegarde et récupération des données

- **Stratégies de sauvegarde** : Établir des routines régulières de sauvegarde pour prévenir la perte de données.
- **Plan de récupération après sinistre** : Prévoir des procédures pour restaurer rapidement les données et les services en cas d'incident.

Surveillance et audit

- **Journalisation** : Enregistrer les activités des utilisateurs pour détecter les anomalies et les activités suspectes.
- **Audit** : Réaliser des audits de sécurité réguliers pour évaluer l'efficacité des mesures de sécurité et identifier les failles potentielles.

Maintenance et mise à jour

- **Mises à jour de sécurité** : Appliquer régulièrement des correctifs de sécurité et mettre à jour le SGBD pour se prémunir contre les vulnérabilités connues.
- **Réévaluation des risques** : Réévaluer périodiquement les risques et ajuster les mesures de sécurité en conséquence.

Formation et sensibilisation

- **Éducation des utilisateurs** : Former les utilisateurs aux bonnes pratiques de sécurité et à la reconnaissance des menaces potentielles.

Conformité et documentation

- **Conformité** : S'assurer que le concept de sécurité est en conformité avec les réglementations en vigueur.
- **Documentation** : Documenter toutes les procédures et politiques de sécurité pour une référence et un audit faciles.

Documentation des procédures et politiques de sécurité

But

Créer une documentation complète et accessible des politiques et procédures de sécurité pour faciliter la référence, la formation, l'audit, et le respect des normes.

Élaboration de la documentation

- **Contenu clair et structuré :**
  - **Information détailée :** Fournir des détails sur les politiques, les procédures, et les protocoles de sécurité.
  - **Organisation logique :** Structurer la documentation de manière logique et intuitive.
- **Langage et accessibilité :**
  - **Langage clair :** Utiliser un langage simple et clair pour assurer la compréhension.
  - **Accessibilité :** Rendre la documentation facilement accessible à tous les utilisateurs concernés.

Composants de la documentation

- **Politiques de sécurité :**
  - **Principes et objectifs :** Décrire les principes de sécurité et les objectifs de l'entreprise.
  - **Règles et standards :** Énoncer les règles, les standards, et les attentes en matière de sécurité.
- **Procédures et protocoles :**
  - **Procédures opérationnelles :** Documenter les étapes spécifiques pour les opérations de sécurité.
  - **Plans d'urgence :** Inclure des procédures pour les situations d'urgence et les incidents.
- **Guides et formations :**
  - **Matériel de formation :** Fournir des guides et des matériaux de formation pour les employés.
  - **FAQ et ressources :** Inclure une section FAQ et d'autres ressources utiles.

Mise à jour et maintenance

- **Révision régulière :**
  - **Planification des révisions :** Établir un calendrier pour la révision régulière de la documentation.
  - **Mises à jour continues :** Mettre à jour la documentation pour refléter les changements dans les technologies et les pratiques.
- **Audit et conformité :**
  - **Préparation pour les audits :** Assurer que la documentation est complète et à jour pour faciliter les audits.
  - **Conformité aux normes :** Vérifier que la documentation respecte les normes et réglementations pertinentes.

Bonnes pratiques

- **Collaboration et feedback :**
  - **Implication des parties prenantes :** Impliquer les différentes parties prenantes dans l'élaboration de la documentation.
  - **Collecte de feedback :** Obtenir des retours pour améliorer continuellement la documentation.
- **Sécurité de la documentation :**
  - **Protection des documents :** Assurer la sécurité des documents de politique et de procédure.
  - **Contrôle d'accès :** Limiter l'accès à la documentation aux utilisateurs autorisés.