SEC105 - Les 12 bonnes pratiques de la Cybersécurité

Valide le 18-01-2019

Code : SEC105

6 crédits

Responsabilité nationale :
EPN05 - Informatique / Véronique LEGRAND

Contact national :
EPN05 - Informatique
2 rue Conté
33.1.13A
75003 Paris
01 40 27 26 81
Safia Sider
safia.sider@lecnam.net

Présentation

Prérequis

Bac+2 informatique, BAC + 2 SI ou SHS

Objectifs pédagogiques

Maintenir la sécurité du système de base conformément aux politiques organisationnelles.

• Apprendre les bonnes pratiques de base à déployer sur un SI pour une hygiène informatique de base

• Comprendre les objectifs de sécurité, les bonnes pratiques, leurs applications et les mesures adaptées

• Être en mesure de prendre les décisions pour la mise en œuvre des bonnes pratiques dans l'entreprise

• Comprendre les mécanismes informatiques réseau et développement logiciel de base

• Rédiger des procédures de base pour la mise ne place des bonnes pratiques

• Apprendre à vérifier la mie en place des bonnes pratiques

• Apprendre à tester les bonnes pratiques

Compétences

- Maintenir la sécurité du système de base conformément aux politiques organisationnelles.
- Apprendre les bonnes pratiques de base à déployer sur un SI pour une hygiène informatique de base
- Comprendre les objectifs de sécurité, les bonnes pratiques, leurs applications et les mesures adaptées
- Être en mesure de prendre les décisions pour la mise en œuvre des bonnes pratiques dans l'entreprise
- Comprendre les mécanismes informatiques réseau et développement logiciel de base
- Rédiger des procédures de base pour la mise ne place des bonnes pratiques
- Apprendre à vérifier la mie en place des bonnes pratiques
- Apprendre à tester les bonnes pratiques

- Technicien sécurité : Mettre en place les bonnes pratiques
- Paramétrer et configurer les équipements informatiques impliqués dans les bonnes pratiques

Programme

Contenu

- Savoir paramétrer un équipement informatique de base
- Manager une équipe de techniciens,
- Savoir mettre en place les outils pour contrôler ou faire contrôler l'application des

bonnes pratiques

Temps 1

- Cours 1 : BP1 : Gestion des mots de passe
  - Principes d'authentification, serveurs et postes de travail, Gestion des identités,
  - Connaissance des architectures d'accès base sur les identités (e.g., public key infrastructure, Oauth, OpenID, SAML, SPML).
  - BP : Connaissance des politiques de sécurité des utilisateurs : création de compte, règles de mot de passe, contrôle d'accès
  - Installe, configure, dépanne et maintient les configurations des mots de passe et des serveurs (matériel et logiciel) pour assurer la confidentialité, l'intégrité et la disponibilité.
  - Gestion des comptes, contrôle de la création et de l'administration des comptes et des mots de passe.
  - Outils de génération automatique des mots de passe,
  - Tableau de bord et validation sur site de la bonne pratique
  - TD : installation de l'accès mot de passe et observation réseau des flux.
- Cours 2 : BP2 : Gestion des téléchargements des applications mobiles et logicielles,
  - Principe des architectures applicatives
  - Fonctionnement des protocoles réseaux (TCP / IP) pour le partage de ressources et services (Web, courrier, DNS), et comment ils interagissent pour fournir des communications réseau.
  - Connaissance des concepts, de la terminologie et des opérations d'un large éventail de supports de communication (réseaux informatiques et téléphoniques, satellite, fibre, sans fil).
  - Développement d'application du système de gestion des informations d'identification,
  - Connaissance des typologies à plusieurs niveaux (y compris les systèmes d'exploitation serveur et client).
  - Architecture client serveur, Front end/back end
  - Connaissance des correctifs et des mises à jour logicielles (difficultés pour certains périphériques en réseau)
  - BP 2 : Connaissance des bonnes pratiques d'installation logicielle
  - BP9 : Principes des mécanismes de mise à jour de sécurité.
  - Développement logiciel : principe d'une application et modèle de déploiement (Cloud, SaaS,…)
  - Technologies et des concepts de gestion des connaissances en cloud liés à la sécurité, à la gouvernance, à l'approvisionnement et à l'administration.
  - Concevoir ou intégrer des fonctionnalités de Installation des logiciels sur les systèmes d'exploitation : serveurs/postes de travail/mobiles
  - Tableau de bord et validation sur site de la bonne pratique
  - TD : créer une petite application WEB (partie 1)

Temps 2

- Cours 3 : BP3 : Gestion des habilitations et des droits
  - Concevoir des stratégies de groupe et des listes de contrôle d'accès pour garantir la compatibilité avec les normes organisationnelles, les règles métier et les besoins.
  - BP : Connaissance des politiques de sécurité concernant les droits des users,
  - Gérer les comptes, les droits de réseau et l'accès aux systèmes et à l'équipement.
  - Tableau de bord et validation sur site de la bonne pratique
  - TD : installer une ressource, bloquer les droits d'accès réseau et en local
- Cours 4 : BP4 : Gestion des sauvegardes
  - Architecture des systèmes de sauvegarde, connaissance des applications logicielles de base (par exemple, le stockage et la sauvegarde des données, les applications de base de données) et les types de vulnérabilités qui ont été

trouvés dans ces applications.
    - Concevoir ou intégrer des fonctionnalités de sauvegarde de données appropriées dans la conception globale du système
    - Identifier les exigences de reprise et de continuité des opérations après sinistre
    - BP : Connaissance des mesures de sécurité : planifier, exécuter et vérifier des procédures de sauvegardes et de restauration,
    - Tableau de bord et validation sur site de la bonne pratique
    - TD : installer et tester la sauvegarde et la restauration d'une sauvegarde
- Cours 5 : BP5 : Gestion et installation des accès WIFI
    - Architecture des réseaux existants (p. Ex. PBX, LAN, WAN, WIFI, SCADA)
    - BP : Mettre en place des mesures de sécurité de bases pour les accès et échanges WIFI,
    - Tableau de bord et validation sur site de la bonne pratique
    - TD : Paramétrer une borne WIFI et connecter un poste travail, chiffré et non chiffré
- Cours 6 : Solutions logicielles et applications mobiles :
    - BP6 : Gestion et installation des solutions mobiles (smartphone)
    - BP11 : Gestion des usages personnels et professionnels (BYOD)
    - Connaissance des systèmes électroniques (dispositifs de contrôle d'accès, appareils en réseau, capteurs en réseau, appareils photo numériques, scanners, imprimantes, copieurs, télécopieurs, stockage amovibles, disques durs, cartes mémoire, Smartphones, modems, téléphones, , etc.).
    - Connaissance des interfaces de programmation d'application d'accès à la base de données (par exemple, Java Database Connectivity [JDBC]).
    - Architecture de communication mobiles 3/4/5G
    - Architecture de communication cellulaires mobiles (par exemple, LTE, CDMA, GSM / EDGE et UMTS / HSPA).
    - BP : Connaissance des usages liés à la collaboration et à la synchronisation de contenu entre les plates-formes (par exemple, Mobile, PC, Cloud).
    - Tableau de bord et validation sur site de la bonne pratique
    - TD : créer une petite application WEB (partie 2)

Temps 3

- Cours 7 : BP6 : Gestion et protection des données en mobilité
    - Architecture service/embarqués
    - BP : Connaissance des cas d'utilisation liés à la collaboration et à la synchronisation de contenu entre les plates-formes (par exemple, Mobile, PC, Cloud).
    - Analyse et maintenance des données volatiles, des bases de données, portails et véhicules de diffusion associés.
    - Tableau de bord et validation sur site de la bonne pratique
    - TD : fuite de donnée, observation des flux en mobilité et expérimentation de l'insertion d'une clé USB automatique.
- Cours 8 : BP8: Gestion de la messagerie
    - Architecture, principes et fonctionnement des applications Internet (messagerie SMTP, messagerie Web, clients de chat, VOIP).
    - Fonctionnement des flux de messagerie Web,
    - Recherche, collecte et analyse des outils chat, VOIP, Media Over IP, VPN, VSAT / sans fil, courrier Web et les cookies.
    - TD : installation d'une messagerie et observation réseau des flux (port 25).

Temps 3

- Cours 10 : BP10 : Gestion des paiements sur Internet
    - Architecture, principes et fonctionnement des systèmes de paiement électronique
    - Terminaux de paiement
    - Présentation des modes de fonctionnement des cookie

    - Mise en œuvre de systèmes de gestions de clé pour le chiffrement des données
    - Tableau de bord et validation sur site de la bonne pratique
    - TD : suivi d’une transaction électronique
- Cours 12 : BP12 : Réputation et recommandation, gestion de son identité numérique
    - Tableau de bord et validation sur site de la bonne pratique
    - TD : installation d’une messagerie et observation réseau des flux (port 25).

Description des modalités de validation

Dossier cahier des charges d’analyse de risque ou d’une analyse de sécurité ou de vulnérabilité

Ou examen sur table

Ou les 2