Management SI

Etat de l'art de la sécurité des systèmes d'information

3 jours (21 heures)

Délai maximum : 2 mois.

Parcours concourant au développement des compétences. Action de formation réalisée en application des articles L 6313-1 et L 6313-2 du Code du travail.

Si vous êtes en situation de handicap, contactez-nous avant le début de votre formation pour que nous puissions vous orienter efficacement et vous accueillir dans les meilleures conditions.

Objectifs pédagogiques

- Comprendre les menaces sur les équipements de l'infrastructure
- Mettre en place une politique interne (technologique et humaine) de sécurité des informations
- Choisir les dispositifs et emplacements de sécurité
- Concevoir le Plan de Sécurité

Pré-requis

- Une réelle connaissance informatique est nécessaire

Modalités pédagogiques

Modalités de formation:

- Formation réalisée en présentiel, à distance ou mixte,
- Toutes nos formations peuvent être organisées dans nos locaux ou sur site
- Feuille de présence signée en demi-journée, questionnaires d'évaluation de la satisfaction en fin de stage et 60 jours après, attestation de stage et certificat de réalisation.
- Horaires de la formation: 9h - 12h30 et 13h30 - 17h.
- Les horaires de la formation sont adaptables sur demande.

Moyens pédagogiques

- Formateur expert dans le domaine,
- Mise à disposition d'un ordinateur, d'un support de cours remis à chaque participant,
- Vidéo projecteur, tableau blanc et paperboard,
- Formation basée sur une alternance d'apports théoriques et de mises en pratique
- Formation à distance à l'aide du logiciel Teams pour assurer les interactions avec le formateur et les autres stagiaires, accès aux supports et aux évaluations. Assistance pédagogique afin de permettre à l'apprenant de s'approprier son parcours. Assistance technique pour la prise en main des équipements et la résolution des problèmes de connexion ou d'accès. Méthodes pédagogiques : méthode expositive 50%, méthode active 50%.

Public visé

- DSI, RSSI, RSI, Technicien sécurité

Modalités d'évaluation et de suivi

- Evaluation des acquis tout au long de la formation : QCM, mises en situation, TP, évaluations orales…

Programme de formation

1. Domaines et contours de la sécurité

- Les systèmes de gouvernance
- Présentation des risques involontaires
- Cybercriminalité
- Le cycle de la gouvernance
- Les organes de contrôle

Contacts

Notre centre à **Mérignac**
14 rue Euler
33700 MERIGNAC
05 57 92 22 00
contact@afib.fr

Notre centre à **Périgueux**
371 Boulevard des Saveurs,
24660 COULOUNIEIX CHAMIERS
05 64 31 02 15
contact@afib.fr

- Le contrôle Interne
- Les audits externes
- Les acteurs de la sécurité
- Environnement juridiques
- Droits et obligations des entreprises en termes de sécurité
- La loi Sécurité Financière SOX (Sarbane Oxley) , La CNIL

2. Analyse des risques

- Connaître son SI
- PC final
- Serveur
- Utilisation d'une ferme de serveurs
- Quelles sont les données externalisées (cloud) ?
- Matériel réseau
- Méthodes d'accès aux réseaux
- Méthodes d'identification
- Gestion des autorisation
- Risques de piratage
- Risques de perte d'information
- Risques de vols d'information
- Risques naturels
- Les pannes matérielles
- Les risques d'ingénierie sociale

3. Mise en oeuvre d'une politique de sécurité

- La sécurité physique
- Accès aux installations
- Sécurité des installations (incendies, inondations, vols...)
- Prévision d'un plan de continuité et de reprise
- Contrôler les accès
- La sécurité des services
- Sécuriser les applications
- Cryptage
- Technologies VPN
- VPN SSL
- HTTPS
- Sécurité des protocoles Peer-to-peer
- Blocage des applications
- Sécurité des terminaux mobiles
- Utilisation d'une DMZ
- Comment intégrer la disponibilité et la mobilité des collaborateurs
- Généralités sur les outils disponibles

4. Les aspects organisationnels de la sécurité

- Définition des risques
- Confidentialité
- Intégrité
- Supervision
- La veille technologique
- Publication des failles
- Principe du modèle de maturité
- Sécurité du système d'exploitation
- Gestion des privilèges
- Documentation

5. Management de la sécurité

- Les méthodes Méhari EBIOS ISO 27001 Cobit
- Les limites de ces méthodes
- Les audits de sécurité
- Mener un audit dans une entreprise multisites
- Trop de sécurité tue la sécurité, comment éviter les faux-positifs
- Expliquer les enjeux de la sécurité aux utilisateurs finaux et aux directions
- La roue de la sécurité
- Mise en oeuvre technique de la sécurité
- Stress du système
- Amélioration de la sécurité
- Savoir protéger les investissements au meilleur coût pour les meilleures raison
- Communications sur la politique de sécurité
- Comment réagir à une attaque (en interne, en externe)
- Les limites du plan de sécurité et les dispositions juridiques
- Définition et rôle du RSSI

6. Méthodologie et technologie

- La vision de la sécurité selon les interlocuteurs
- Les objectifs
- Les moyens techniques et financiers mis en oeuvre
- La stratégie
- L'adaptation et la gestion du changement
- Elaboration du plan de sécurité
- L'audit de conformité
- Les indicateurs
- Les tableaux de bords à établir
- Les méthodologies d'audit

7. Les outils

- Fonction d'un firewall
- Documentation des accès autorisés sur le réseau
- Création d'une charte d'utilisation du réseau pour les collaborateurs
- Fonction d'un système de détection d'intrusion
- Les logiciels clients de sécurité (firewall, antivirus, antispyware...)
- Superviser la sécurité
- Faire évoluer la sécurité
- Contraction d'assurances : quelles sont les garanties ? qu'est ce qui peut et doit être assuré ? l'importance de la disponibilité du système
- Validation technique de l'architecture
- Formation des personnels du SI
- Formation des utilisateurs du SI
- Avenir de la sécurité informatique
- Les 6 idées les plus stupides selon Marcus J. Ranum
- La vision géostratégique de la sécurité
- Les phénomènes de monopole

8. Rédaction de chartes d'utilisation et / ou de configuration

- Le secret professionnel
- Le respect de la l