ÉTAT DE L'ART DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION

Durée	3 jours	Référence Formation	3-SR-EBIO

Objectifs

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

Participants

A définir

Pré-requis

DSI, RSSI, RSI, Technicien sécurité

Moyens pédagogiques

Accueil des stagiaires dans une salle dédiée à la formation équipée d'un vidéo projecteur, tableau blanc et paperboard ainsi qu'un ordinateur par participant pour les formations informatiques.
Positionnement préalable oral ou écrit sous forme de tests d'évaluation, feuille de présence signée en demi-journée, évaluation des acquis tout au long de la formation.
En fin de stage : QCM, exercices pratiques ou mises en situation professionnelle, questionnaire de satisfaction, attestation de stage, support de cours remis à chaque participant.
Formateur expert dans son domaine d'intervention
Apports théoriques et exercices pratiques du formateur
Utilisation de cas concrets issus de l'expérience professionnelle des participants
Réflexion de groupe et travail d'échanges avec les participants
Pour les formations à distance : Classe virtuelle organisée principalement avec l'outil ZOOM.
Assistance technique et pédagogique : envoi des coordonnées du formateur par mail avant le début de la formation pour accompagner le bénéficiaire dans le déroulement de son parcours à distance.

PROGRAMME

- **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
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 législation
Les règles de confidentialité
L'usage des services Internet
Définir sa charte d'utilisation

Responsabilités du comité de coordination du SI
Responsabilités du conseil d'administration et des représentants