RÉFÉRENT CYBERSÉCURITÉ

Durée	4 jours	Référence Formation	4-IT-WIN

Objectifs

Identifier et analyser des problèmes de cybersécurité dans une perspective d'intelligence et de sécurité économique
Connaître les obligations et responsabilités juridiques de la cybersécurité
Identifier et comprendre les menaces liées à l'utilisation de l'informatique et des réseaux internet, réseaux privés d'entreprises ou réseaux publics
Mettre en œuvre les démarches de sécurité inhérentes aux besoins fonctionnels
Savoir présenter les précautions techniques et juridiques à mettre en place pour faire face aux attaques éventuelles

Participants

Tout public

Pré-requis

Aucun prérequis

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

- **Cybersécurité : notions de bases, enjeux et droit commun**

Définitions
Intelligence économique, sécurité économique globale
Cybersécurité
Les enjeux de la sécurité des SI
La nouvelle économie de la cybercriminalité
Panorama des menaces selon une typologie
Les vulnérabilités (exemples, détermination, veille)
Focus sur l'ingénierie sociale
Les propriétés de sécurité
Présentation du principe de défense en profondeur

Identification et évaluation des actifs et des objectifs de sécurité
Aspects juridiques et assurantiels
Responsabilités
Préservation de la preuve
L'offre assurantielle
Le paysage institutionnel de la cybersécurité
La prévention
Le traitement des cyberattaques et la réponse judiciaire
Rôle et missions des acteurs étatiques chargés du traitement technique et judiciaire des attaques cybers

- **L'hygiène informatique pour les utilisateurs**
Connaître le système d'information et ses utilisateurs
Identifier le patrimoine informationnel de son ordinateur (brevets, recettes, codes, source, algorithmes□)
Maîtriser le réseau de partage de documents (en interne ou sur internet)
Mettre à niveau les logiciels
Authentifier l'utilisateur
Nomadisme-Problématiques liées au BYOD (Bring your Own Devices)

- **Gestion et organisation de la cybersécurité**
Présentation des publications/recommandations
Guides de l'ANSSI
Recommandations de la CNIL
Recommandations de la police et de la gendarmerie
Club de la sécurité de l'information Français, Club des experts de la sécurité de l'information et du numérique (CLUSIF/CESIN), etc.
Observatoires zonaux de la Sécurité des systèmes d'information (SSI)
Les CERTs (Computer Emergency Response Team)
Présentation des différents métiers de l'informatique (infogérance, hébergement, développement, juriste, etc.)
Méthodologie pédagogique pour responsabiliser et diffuser les connaissances ainsi que les bonnes pratiques internes (management, sensibilisation, positionnement du référent en cybersécurité, chartes, etc.)
Maîtriser le rôle de l'image et de la communication dans la cybersécurité
Surveillance de l'e-réputation
Communication externe
Usage des réseaux sociaux, professionnel et personnel
Méthodologie d'évaluation du niveau de sécurité
Actualisation du savoir du référent en cybersécurité
Gérer un incident/Procédures judiciaires

- **Protection de l'innovation et cybersécurité**
Les modalités de protection du patrimoine immatériel de l'entreprise
Droit de la propriété intellectuelle lié aux outils informatiques
Cyber-assurances
Cas pratiques

- **Administration sécurisée du système d'information (SI) interne d'une entreprise**
Analyse de risque (expression des besoins et identification des objectifs de sécurité-EBIOS/ méthode harmonisée d'analyse des risques □ MEHARI)
Principes et domaines de la SSI afin de sécuriser les réseaux internes
Politique et stratégie de sécurité
Gestion des flux, notamment réseaux sans fil/ architecture réseaux (cloisonnement du réseau)
Gestion des comptes, des utilisateurs, des privilèges selon le besoin d'en connaître

Gestion des mots de passe
Gestion des mises à jour
Journalisation et analyse
Gestion des procédures
Plan de continuité d'activité (PCA) / Plan de reprise d'activité (PRA)
Virtualisation / cloisonnement
Détecter un incident
Gestion de crise
Traitement technique de l'incident
Procédure organisationnelle et communication
Reprise d'activité
Méthodologie de résilience de l'entreprise
Traitement et recyclage du matériel informatique en fin de vie (ordinateurs, copieurs, supports amovibles, etc.)
Aspects juridiques
Responsabilités en l'absence de conformité des infrastructures
Cyber-assurances

- **La cybersécurité des entreprises ayant externalisé tout ou partie de leur SI**
Les différentes formes d'externalisation
Les contrats de services « classiques » : Infrastructure as a Service (IaaS), Platform as a Service (PaaS) et Software as a Service (SaaS)
Enjeux du Cloud Computing
Techniques de sécurité lors de l'externalisation (chiffrement des données)
Comment choisir son prestataire de service ?
Présentation du référentiel de l'ANSSI Maîtriser les risques de l'infogérance
Présentation de la qualification SecNumCloud applicable aux prestataires de services d'informatique en nuage
Aspects juridiques et contractuels
Connaître les bases juridiques pour protéger son patrimoine économique lors de l'externalisation d'un SI
Obligations en matière d'utilisation, de localisation et de transfert de données

- **Sécurité des sites internet gérés en interne**
Menaces propres aux sites internet
Approche systémique de la sécurité (éviter l'approche par patches)
Configuration des serveurs et services
HTTPS et infrastructure de gestion de clés (IGC)
Services tiers
Avantages et limites de l'utilisation d'un Content Management System (CMS ou Gestion des contenus) et/ou développement web
Sécurité des bases de données
Utilisateurs et sessions
Obligations juridiques règlementaires
Le e-commerce
La Loi pour la confiance dans l'économie numérique (LCEN), la CNIL, Payment Card Industry-Data Security Standard (PCI-DSS)
Règlement général sur la protection des données (RGPD)