Référent CyberSécurité en TPE-PME

Modalités pédagogiques

Objectif : Comprendre et maîtriser les enjeux de la cybersécurité pour l'entreprise et être capable d'utiliser les outils nécessaires pour protéger efficacement son activité professionnelle des menaces et attaques informatiques.

Type de public : Dirigeant ou cadre en TPE/PME souhaitant acquérir les compétences lui permettant d'assurer le rôle de référent cybersécurité au sein de son organisation

Pré-requis : Connaissances techniques de base en informatique et en organisation d'entreprise

Moyens pédagogiques : présentation au vidéoprojecteur, support de cours remis aux stagiaires, exercices pratiques, études de cas tout au long du stage

Evaluation des acquis : à chaud, sous forme d'exercices pratiques et de questionnaires type QCM

Modalités d'exécution

Durée : 9 jours dont 3 jours obligatoires (63 heures dont 21 heures obligatoires)

Dates : à déterminer

Horaires : 9h00-12h30 / 13h30-17h00

Lieu : Rhône/Loire, locaux NETFORMATIC, salle extérieure ou au sein de l'entreprise bénéficiaire

Formateur : Experts en cybersécurité

Nombre de participants : 2 à 8 stagiaires

Modalités de suivi : feuille d'émargement, attestation de formation individuelle

Tarif : 490 € HT / jour / participant

Programme pédagogique

TRONC COMMUN OBLIGATOIRE (3 jours)

MODULE 1 - CYBERSECURITE : NOTIONS DE BASES, ENJEUX ET DROIT COMMUN (1 jour)

Objectifs :

- *Identifier l'articulation entre cybersécurité, sécurité économique et intelligence économique*
- *Comprendre les motivations et le besoin de sécurité des systèmes d'information (SI).*
- *Connaître les définitions et la typologie des menaces*

Programme détaillé :

- **Notions clés** : cybersécurité, intelligence économique, sécurité informatique
- **Enjeux de la sécurité des SI**
  - la notion de risque et économie de la cybercriminalité
  - panorama des menaces
  - typologie des principales vulnérabilités
  - le cas de l'ingénierie sociale
- **Composants de la sécurité des SI**
  - présentation de la démarche globale
  - critères DICP
  - notion de bien essentiel
- **Aspects juridiques et assurantiels**
  - responsabilités de l'entreprise
  - protection des données à caractère personnel
  - gérer une attaque d'un point de vue juridique
  - offre assurantielle
- **Paysage institutionnel**
  - les acteurs de la prévention : rôles et missions
  - traitement des cyberattaques et réponse judiciaire
- **EVALUATION DE FIN DE MODULE**

MODULE 2 - HYGIENE INFORMATIQUE POUR LES UTILISATEURS (1 jour)

Objectifs :

- ➲ *Appréhender et adopter les notions d'hygiène de base de la cybersécurité pour les organisations et les individus*

Programme détaillé :

- **Connaître et cartographier le SI**
- **Identifier le patrimoine informationnel de son ordinateur**
- **Maîtriser le partage de documents en interne et sur internet**
- **Définir une politique de mise à niveau des logiciels**
- **Authentifier les utilisateurs**
- **Gérer le nomadisme et le BYOD (Bring Your Own Device)**
- **EVALUATION DE FIN DE MODULE**

MODULE 3 - GESTION ET ORGANISATION DE LA CYBERSECURITE (1 jour)

Objectifs :

- ➲ *Appréhender les multiples facettes de la sécurité au sein d'une organisation.*
- ➲ *Connaître les métiers directement impactés par la cybersécurité.*
- ➲ *Anticiper les difficultés courantes dans la gestion de la sécurité.*

Programme détaillé :

- **Guides et recommandations**
  - → les acteurs à suivre
  - → les publications utiles
  - → l'importance de la veille informationnelle
- **Les métiers de l'informatique**
- **Les fondamentaux de la sensibilisation utilisateurs**
  - → pédagogie
  - → outils de communication
  - → plan de sensibilisation
- **Le rôle de l'image et de la communication dans la cybersécurité**
  - → e-réputation
  - → communication externe
  - → usage des réseaux sociaux
- **Evaluation du niveau de sécurité : la démarche d'audit**
- **L'actualité de la cybersécurité**
- **Gérer un incident de sécurité informatique**
- **EVALUATION DE FIN DE MODULE**

MODULES COMPLEMENTAIRES OPTIONNELS

MODULE 4 - PROTECTION DE L'INNOVATION ET CYBERSECURITE (0,5 jour)

Objectifs :

- ➲ *Appréhender la protection de l'innovation à travers les outils informatiques.*

Programme détaillé :

- **Modalités de protection du patrimoine immatériel de l'entreprise**
- **Droit de la propriété intellectuelle lié aux outils informatiques, droit des contrats informatiques**
- **Cyber-assurances**
- **Etude de cas réels**
- **EVALUATION DE FIN DE MODULE**

MODULE 5 - ADMINISTRATION SECURISEE DU SI INTERNE D'UNE ENTREPRISE (1 jour)

Objectifs :

- *Savoir sécuriser le SI interne*
- *Savoir détecter puis traiter les incidents*
- *Connaître les responsabilités juridiques liées à la gestion d'un SI*

Programme détaillé :

- **Analyse de risque**
  - principes généraux
  - méthodes Ebios et Mehari
- **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**
- **Aspects juridiques**
  - responsabilité en l'absence de conformité des infrastructures
  - cyber-assurances

MODULE 6 - CYBERSECURITE DES ENTREPRISES AYANT EXTERNALISE TOUT OU PARTIE DE LEUR SI (0,5 jour)

Objectifs :

- *Connaître les techniques de sécurisation d'un SI, partiellement ou intégralement externalisé.*

Programme détaillé :

- **Les différentes formes d'externalisation**
  - les contrats de services IaaS, PaaS, SaaS
  - enjeux du Cloud Computing
  - techniques de sécurité lors de l'externalisation
- **Choisir son prestataire de service**
  - les certifications et qualifications
- **Aspects juridiques et contractuels**
  - notions juridiques
  - obligations légales (localisation, transfert de données…)

MODULE 7 - SECURITE DES SITES INTERNET GERES EN INTERNE (2 jours)

Objectifs :

- ➲ *Connaître les règles de sécurité pour gérer un site internet*

Programme détaillé :

- **Menaces propres aux sites internet**
- **Approche systémique de la sécurité (versus 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 réglementaires**
  - → 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)

MODULE 8 - LE RGPD EN PME (2 jours)

Objectifs :

- ➲ *Comprendre les principes et les obligations liés à l'application du RGPD*
- ➲ *Démarrer la mise en œuvre du RGPD dans son organisation*

Programme détaillé :

- **Fondamentaux et concepts-clés**
  - → Historique et évolutions de la réglementation
  - → Avantages concurrentiels du RGPD
  - → Définitions clés
  - → Périmètre et champ d'application
  - → Acteurs et organes de régulation
- **Principes de la protection des données**
  - → Droit des personnes sur leurs données
  - → Finalité du traitement
  - → Licéité du traitement
  - → Minimisation des données
  - → Protection particulière de certaines données
  - → Conservation limitée des données
  - → Obligation de sécurité
  - → Transparence à l'égard des personnes concernées
  - → Encadrement des transferts de données hors de l'UE
- **Obligations des professionnels**
  - → Nouveau régime de responsabilité : l'accountability
  - → Partage des responsabilités
  - → La notion de "privacy by design and by default"
  - → L'analyse d'impact ou PIA
- **Sécurité des données :**
  - → Mesures techniques
  - → Mesures organisationnelles
  - → Violation des données
- **Mettre en œuvre le RGPD**
  - → Définir un pilote
  - → Constituer le registre des traitements
  - → Cartographier les données
  - → Evaluer les écarts
  - → Définir un plan d'action
  - → Engager les mesures correctives
  - → Documenter
  - → Le rôle de DPD