Référent cybersécurité TPE & PME

Formation Labellisée SecNumedu-FC de l'ANSSI.

Les TPE/PME n'ont pas toujours la possibilité de recruter des profils dédiés uniquement à la sécurité informatique.

Leur approche de la gestion des infrastructures informatiques varie en fonction de l'utilisation qui en est faite, de leur taille, du secteur économique et du budget qui y est consacré. De fait, à l'exception de certains secteurs très spécifiques, le niveau de perception et de prise en charge du « cyberisque » dans les TPE/PME est souvent insuffisant.

Afin de les aider à maîtriser ce nouvel environnement, à aborder du mieux possible leur transformation numérique et à préserver leur patrimoine immatériel, il convient de mettre en place, dans une approche de sécurité économique globale, des solutions humaines et techniques de cybersécurité spécialement adaptées.

La formation de référents en cybersécurité au sein des TPE/PME permettra de répondre en partie à ce défi.

Objectifs

L'objectif général de la formation est de faire du participant un référent cybersécurité interne.

À la fin de la formation, le participant devra être en mesure de maîtriser les enjeux de la cybersécurité pour l'entreprise et d'utiliser les outils nécessaires pour protéger des informations sensibles (personnelles et professionnelles) sur les différents réseaux.

Il sera notamment à même de :

- Identifier et analyser des problèmes de cybersécurité dans une perspective d'intelligence et de sécurité économiques ;
- 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 oeuvre 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.

Référent cybersécurité TPE & PME

Programme

Ce programme s'organise autour d'un bloc de modules communs à l'ensemble des entreprises et de trois modules complémentaires en fonction de l'utilisation du numérique et des profils des entreprises.

- Administration sécurisée du SI interne d'une entreprise
- La cybersécurité des entreprises ayant externalisé tout ou partie de leur SI
- Sécurité des sites internet gérés en interne

FOCUS 1 **Cybersécurité : notions de base, enjeux et droit commun (3 heures)**

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 cyber-sécurité

- 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

FOCUS 2 **L'hygiène informatique pour les utilisateurs (3 heures)**

- 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)

FOCUS 3 **Gestion et organisation de la cybersécurité (3 heures)**

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)
- Méthodologie pédagogique pour res-ponsabiliser et diffuser les connaissances ainsi que les bonnes pratiques internes (management, sensibilisation, positionnement du référent en cybersécurité, chartes)
- 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

Référent cybersécurité TPE & PME

- Méthodologie d'évaluation du niveau de sécurité
- Actualisation du savoir du référent en cybersécurité
- Gérer un incident / Procédures judiciaires

FOCUS 4 **Protection de l'innovation et cybersécurité (3 heures)**

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

Modalités d'évaluation

Évaluation des acquis tout au long de la session par des travaux pratiques. Questionnaire de validation des compétences acquises en fin de formation.

Moyens techniques

En fonction du format, distanciel via l'outil Teams, en présentiel, salle de formation équipée de postes de travail informatiques disposant de tous les logiciels nécessaires au déroulement de la formation, salle moderne climatisée, accès à l'environnement numérique Efrei.

Prérequis

Aucun prérequis.

Pédagogie et ressources

La formation s'articule autour d'exposés, de démonstrations techniques, d'ateliers pratiques et de partages de retours d'expérience.

Sanction de la formation

Une attestation de fin de formation résumant les objectifs visés par la formation est remise au participant à l'issue de la formation.

Profil du participant

La formation à la cybersécurité peut toucher un public hétérogène parmi les salariés des entreprises, dirigeants ou DSI de PME/TPE, salariés utilisateurs, cadres, responsables de la gestion des risques.

Prix

1 400€ HT* par participant (tronc commun)
Consulter nos services pour les modules additionnels

Direction pédagogique

Salim NAHLE

Contact

executive.education@efrei.fr
06.23.18.43.22

* Prix HT, les déjeuners des jours de formation sont inclus.
Prix, dates, équipes pédagogiques et contenu des programmes sont susceptibles de changer.
Délai d'accès entre 3 et 5 jours ouvrés
Accessibilité : https://www.efrei.fr/ecole-ingenieur/efrei-for-good/
Contact : handicap@efrei.f

Format

Présentiel ou distanciel (via l'outil Teams)

Durée

2 jours (14 heures)

Possibilité de compléter votre formation avec les modules additionnels (pour plus de renseignements voir directement auprès de nos conseillers)

Dates

1ère session : 3 au 4 Juin 2024

2ème session : 28 au 29 Novembre 2024

INSCRIPTION

Référent cybersécurité TPE & PME I Modules complémentaires au choix

Module Administration sécurisée du système d'information (SI) interne d'une entreprise (7 heures)

- Analyse de risque (Expression des besoins et identification des objectifs de sécurité -EBIOS / Méthode
- Principes et domaines de la SSI afin de sécuriser les réseaux internes :
  - ✓Politique et stratégie de sécurité
  - ✓Gestion des flux : réseaux sans fil / architecture réseaux
  - ✓Gestion des comptes/utilisateurs/ privilèges
  - ✓Gestion des mots de passe / 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, cyber-assurances)

Module La cybersécurité des entreprises ayant externalisé tout ou partie de leur SI (3 heures)

- 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
  - ✓La CNIL
  - ✓Règlement général sur la protection des données (RGPD)

Module Sécurité des sites internet gérés en interne (10 heures)

- 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 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)