CCI DEUX-SEVRES

FORMATION A LA CYBERSECURITE DES TPE ET DES PME

Durée : 30 à 35 Heures

OBJECTIFS

Devenir référent cybersécurité interne,
Connaitre les enjeux de la cybersécurité pour l'entreprise et utiliser les outils nécessaires pour protéger des informations sensibles (personnelles et professionnelles) sur les différents réseaux,
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 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.

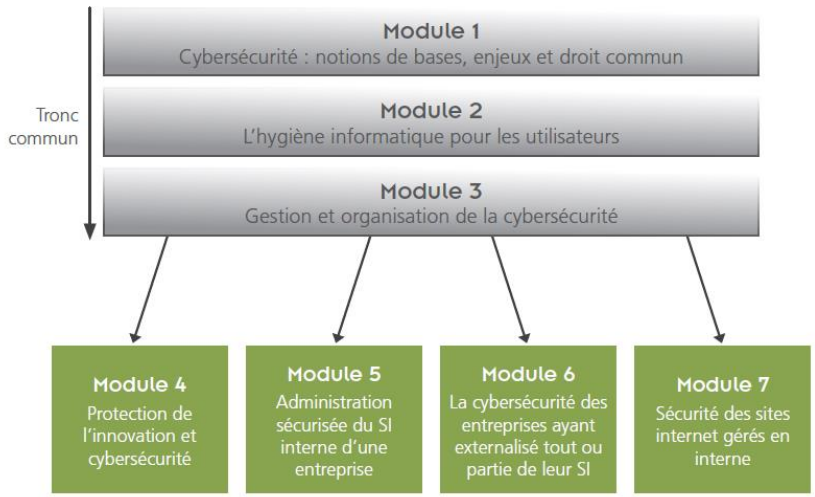
METHODES PEDAGOGIQUES

La formation utilisera les quatre méthodes d'apprentissage (démonstrative, expositive, interrogative et active) en fonction des objectifs.
La formation permettra une participation active de chacun basée sur un partage d'expérience au terme d'analyse de pratiques.
La formation sera basée sur la pédagogie par objectifs

CONTENU

STRUCTURE PEDAGOGIQUE :

Ce programme s'organise autour d'un bloc de trois modules communs à l'ensemble des entreprises, avec des notions d'ordre général, et de quatre modules complémentaires en fonction de l'utilisation du numérique et des profils des entreprises.
Il est préconisé que chaque module se termine par une évaluation, et qu'un ensemble de liens vers des ressources complémentaires (sites web, documents, statistiques, etc.) soit fourni aux participants désireux d'approfondir certains sujets de cybersécurité.



TRONC COMMUN :

Module 1 : Cybersécurité, notions de bases, enjeux et droit commun – 3 Heures

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.

10, place du Temple - BP 90314 - 79003 NIORT CEDEX
T. 05 49 28 79 79 - F. 05 49 24 57 11 - www.cci79.com

PUBLIC ET PRE-REQUIS

Salariés d'entreprises, référent cybersécurité, dirigeant, cadre, responsable informatique, etc...

BUDGET

599 € exo de TVA par jour de formation

VALIDATION

Attestation de présence,
Attestation de fin de formation.

Contenu pédagogique :

1 - Définitions :
- Intelligence économique, sécurité économique globale,
- Cybersécurité, Sécurité des SI (prévention) + Cyberdéfense (réaction) + Cybercriminalité (sanction) = Cybersécurité.

2 - Les enjeux de la sécurité des SI :
- La nouvelle économie de la cybercriminalité :
  Les déficiences en matière de cybersécurité peuvent engendrer des pertes financières directes ou indirectes (comme lorsqu'un site marchand est rendu indisponible ou lors d'espionnage économique sur des appels d'offres, par exemple),
- Panorama des menaces selon une typologie :
  Panel assez large des différentes menaces (attaques intrusives - injection SQL, passive – phishing, destructrices – virus, etc.),
  Détails sur les Advanced Persistent Threat (APT, Attaque persistante avancée) : rôle des entreprises dans ces attaques,
- Les vulnérabilités (exemples, détermination, veille) :
  Vulnérabilité : faiblesse d'un bien, que ce soit à la conception, la réalisation, l'installation, la configuration ou l'utilisation,
- Focus sur l'ingénierie sociale.

3 - Les propriétés de sécurité :
- Présentation du principe de défense en profondeur :
  Un logiciel spécialisé dans la cybersécurité n'est pas suffisant. La démarche de cybersécurité s'inscrit dans un processus global de sécurité économique (sécurité bâtimentaire, sécurisation des déplacements, contrôle d'accès, etc.),
  Cf. La sécurité économique au quotidien en fiches thématiques (SISSE).
- Identification et évaluation des actifs et des objectifs de sécurité :
  Arriver à identifier précisément le besoin,
  Un site internet marchand et un site internet « vitrine » n'ont pas les mêmes besoins en termes de sécurité,
  Déterminer les critères (disponibilité, intégrité, confidentialité, preuve / traçabilité) qui permettent d'évaluer le niveau de sécurité des SI.

4 - Aspects juridiques et assurantiels :
- Responsabilités :
  Quelles sont les responsabilités des entreprises qui n'ont pas assez sécurisé leurs SI ?
  Quels recours sont possibles vers les prestataires ?
  Réglementation européenne : analyse de risque obligatoire pour une entreprise dès qu'il y a une déclaration à la Commission Nationale de l'Informatique et des Libertés(CNIL),
- Préservation de la preuve :
  Que faire en cas d'attaques informatiques ?
  Comment préserver la preuve tout en restant opérationnel ?
  Qui faut-il contacter ?
  Le rôle de l'huissier,
- L'offre assurantielle :
  Le paysage institutionnel de la cybersécurité,
- La prévention :
  Rôle et missions des acteurs étatiques en charge de l'accompagnement des entreprises en matière de cyber,
- Le traitement des cyberattaques et la réponse judiciaire :
  L'agence nationale de la sécurité des systèmes informatiques (ANSSI), la Direction générale de la sécurité intérieure (DGSI), la Gendarmerie nationale,

- Rôle et missions des acteurs étatiques chargés du traitement technique et judiciaire des attaques cybers :
  L'ANSSI, la Direction centrale de la police judiciaire, sous-direction de la lutte-contre la cybercriminalité (SDLCOCLCTIC),
  La brigade d'enquêtes sur les fraudes aux technologies de l'information (BEFTI), la gendarmerie nationale (C3N, NTECH), etc...

Module 2 : L'hygiène informatique pour les utilisateurs - 3 Heures

Objectifs :
Appréhender et adopter les notions d'hygiène de base de la cybersécurité pour les organisations et les individus.

Contenu pédagogique :

1 - Connaître le système d'information et ses utilisateurs :
- Faire une cartographie des SI de l'entreprise.

2 - Identifier le patrimoine informationnel de son ordinateur (brevets, recettes, codes source, algorithmes...) :
- Connaître la valeur des informations contenues dans son ordinateur pour appliquer les différentes procédures de sécurité en fonction des documents utilisés.

3 - Maîtriser le réseau de partage de documents (en interne ou sur internet) :
- Identifier précisément les passerelles qui existent entre internet et le réseau interne pour éviter les failles qui permettront ou faciliteront une intrusion non détectée.

4 - Mettre à niveau les logiciels :
- Définir une véritable politique de mise-à-jour des logiciels (qui est en charge ? À quel moment ? etc.).

5 - Authentifier l'utilisateur :
- Présentation des différentes méthodes permettant d'authentifier les utilisateurs et ainsi de leur attribuer la méthode qui correspond le mieux aux documents qu'ils utilisent,
- Evoquer les bonnes pratiques pour les mots/phrases de passe (conception, fréquences d'utilisation, etc.).

6 - Nomadisme - Problématiques liées au BYOD (Bring your Own Devices) :
- Evoquer les risques liés à l'utilisation des terminaux mobiles personnels (PC et/ou Smartphone) dans la chaîne de sécurité de l'entreprise.

Module 3 : Gestion et organisation de la cybersécurité - 3 Heures

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.

Contenu pédagogique :

1 - 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) :
  Il s'agit ici de sensibiliser les PME à l'importance de la veille sur les différentes documentations disponibles.

2 - Présentation des différents métiers de l'informatique (infogérance, hébergement, développement, juriste, etc.)

3 - Méthodologie pédagogique pour responsabiliser et diffuser les connaissances ainsi que les bonnes pratiques internes (management, sensibilisation, positionnement du référent en cybersécurité, chartes, etc.) :
- Insister sur les messages que le référent en cybersécurité doit transmettre aux utilisateurs finaux des entreprises,
- Présenter le principe des chartes informatiques que chaque utilisateur doit connaitre.

4 - 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.

5 - Méthodologie d'évaluation du niveau de sécurité :
- Présentation d'un audit de sécurité (réglementation, avantages, coût etc.).

6 - Actualisation du savoir du référent en cybersécurité :
- Les découvertes en matière de cybersécurité sont nombreuses, rapides et les méthodes d'attaques évoluent en permanence. Il est donc nécessaire que le référent en cybersécurité connaisse les grandes actualités du domaine.

7 - Gérer un incident / Procédures judiciaires :
- Identifier clairement le point de contact dans l'entreprise ainsi que son rôle (lien avec les services de police, résilience du SI de l'entreprise etc.).

MODULES COMPLEMENTAIRES :

Module 4 - Protection de l'innovation et cybersécurité - 3 heures

Objectifs :
Appréhender la protection de l'innovation à travers les outils informatiques

Contenu pédagogique :

1 - Les modalités de protection du patrimoine immatériel de l'entreprise :
- L'objectif est de présenter les différentes mesures et éventuelles obligations en la matière, comme le dispositif de zone à régime restrictif (ZRR) concourant à la protection du potentiel scientifique et technique de la Nation (*PPST*).

2 - Droit de la propriété intellectuelle lié aux outils informatiques :
- Il s'agit ici de donner les moyens nécessaires aux entreprises ayant des données importantes pour connaitre les tenants et les aboutissants des contrats, comme par exemple l'infogérance et le Cloud Computing.

3 - Cyber-assurances :
- Présentation d'un domaine nouveau et émergent. L'objectif est de donner les clés nécessaires à une entreprise dans le cas où elle souhaiterait souscrire à une offre de cyber-assurance.

4 - Cas pratiques :
- Présentation de cas de cyber-attaques avérés.

Module 5 : Administration sécurisée de système d'information (SI) interne d'une entreprise – 6 à 9 heures

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

Contenu pédagogique :

1 - Analyse de risque (Expression des besoins et identification des objectifs de sécurité -EBIOS / Méthode harmonisée d'analyse des risques - MEHARI)
- Définir les besoins auxquels répondre à travers les principes et domaines de la SSI.

2 - Principes et domaines de la SSI afin de sécuriser les réseaux internes :
- Développement de la notion de défense en profondeur évoquée précédemment :
  . 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,
  . 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.

3 - Détecter un incident.

4 - Gestion de crise :
- Traitement technique de l'incident,
- Procédure organisationnelle et communication,
- Reprise d'activité.

5 - Méthodologie de résilience de l'entreprise.

6 - Traitement et recyclage du matériel informatique en fin de vie (ordinateurs, copieurs, supports amovibles, etc.).

7 - Aspects juridiques :
- Responsabilité en l'absence de conformité des infrastructures,
- Cyber-assurances.

Module 6 : La cybersécurité des entreprises ayant externalisé tout ou partie de leur SI - 3 heures

Objectifs :
Connaître les techniques de sécurisation d'un SI, partiellement ou intégralement externalisé.

Contenu pédagogique :

1 - 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…).

2 - Comment choisir son prestataire de service ?
- Quels sont les points clés, techniques et organisationnels, de sécurité à bien identifier lors du choix d'un prestataire ?
- Aborder la notion et le contexte de certification / qualification des produits :
- 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.

3 - Aspects juridiques et contractuels :
- Connaître les bases juridiques pour protéger son patrimoine économique lors de l'externalisation d'un SI,
  Exemple : qui est propriétaire des données (même après la fin du contrat) ?
- Obligations en matière d'utilisation, de localisation et de transfert de données :
  . La *CNIL,*
  . Règlement général sur la protection des données (*RGPD*).

Module 7 : Sécurité des sites internet gérés en interne - 9 à 12 heures

Objectifs :
Connaître les règles de sécurité pour gérer un site internet.

Contenu pédagogique :

1 - Menaces propres aux sites internet.

2 - Approche systémique de la sécurité (éviter l'approche par patches).

3 - Configuration des serveurs et services.

4 - HTTPS et Infrastructure de gestion de clés (IGC).

5 - Services tiers.

6 - Avantages et limites de l'utilisation d'un Content Management System (CMS ou Gestion des contenus) et / ou développement web.

7 - Sécurité des bases de données.

8 - Utilisateurs et sessions.

9 - 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*).

HORAIRES
9H-12H30, 13H30-17H

DATES
A déterminer

ANIMATEUR
Animateur agréé par la CCI Deux-Sèvres

LIEU
Chambre de Commerce et d'Industrie Territoriale des Deux Sèvres