La cybersécurité - comment protéger ses actifs

La cyber délinquance a envahi notre quotidien. Jour après jour les médias nous annoncent des attaques de plus en plus pernicieuses. Nul ne peut se dire à l'écart de ces pratiques malveillantes et chacun peut se trouver confronté à des pertes de données.
Vol, panne de matériel, déni de services, cryptage de données, les risques sont présents pour toutes les entreprises. Il devient essentiel de définir une réelle politique de sécurité du système d'information adaptée à la structure de son entreprise.
Cette formation a pour objectif général 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.

Objectifs

- 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.

Prérequis

- Aucun pré-requis.

Public

- Tout employé d'une entreprise concerné par le développement des bonnes pratiques en matière de cyber sécurité.

Durée

- 5 journées consécutives : 9h00-17h00 - 35 heures
- Intégrant 1 pause matin et après-midi et pauses déjeuners

Déroulement pédagogique

Projection du cours sur vidéoprojecteur. Le support et la formation sont en langue française. Le support est livré sous PDF. Le cours est théorique à 70% et 30% pratique avec des discussions, partage d'expérience et étude de cas et quizz pour valider les acquis de formation. Une attestation de formation est délivrée en fin de formation.

Déroulement de l'examen

- Pas d'examen

Programme

- **La cybersécurité : notions de bases, enjeux et challenges (module 1 – ½ journée)**
  - Définition et notions de base : Sécurité, Cybersécurité, CIA (confidentialité, intégrité, authenticité), La sécurité des SI (prévention), La cyberdéfense (réaction), La cybercriminalité et cyberterrorisme (sanction)
  - La nouvelle économie de la cybercriminalité
  - Panorama des menaces selon une typologie
  - Les vulnérabilités (exemple, détermination, veille)
  - L'ingénierie sociale
  - Présentation du principe de défense en profondeur
  - Identification et évaluation des actifs et des objectifs de sécurité
  - Les aspects juridiques et assurantiels (CNIL, RGPD)
  - Le paysage institutionnel de la cybersécurité
- **Pratiques de base de la cybersécurité pour les organisations et les individus (module 2 – ½ journée)**
  - Connaître le système d'information et ses utilisateurs
  - Identifier le patrimoine informationnel de son ordinateur (brevets, recettes, codes source, algorithmes…) : Connaitre la valeur des actifs
  - Maîtriser le réseau de partage de documents (en interne ou sur internet)
  - Mettre à niveau les logiciels
  - Authentifier les utilisateurs et journaliser leurs activités : Techniques d'authentification (simple, multi-facteurs)
  - Problématiques liées au BYOD
- **Gestion et organisation de la cybersécurité (module 3 – ½ journée)**
  - Recommandations/guides/standards : ANSSI, CNIL, police et gendarmerie, CERTS, ISO 2700X, etc.
  - Métiers de l'informatique

- Méthodologie pédagogique pour responsabiliser et diffuser les connaissances
- Maîtriser le rôle de l'image et de la communication dans la cybersécurité
- Méthodologie d'évaluation du niveau de sécurité (les audits de la sécurité)
- Actualisation du savoir des experts en sécurité
- Gestion d'incidents, procédures judiciaires

- **Protection de l'innovation (module 4 – ½ journée)**
  - Les modalités de protection du patrimoine immatériel de l'entreprise : ZRR et PPST
  - Droit de la propriété intellectuelle lié aux outils informatiques : Cas du cloud computing
  - Cyber-assurances
  - Cas pratiques : Présentation de cas de cyber-attaques avérés, , attaques DoS par des équipements IoT, Anonymous (banques, assurances, gouvernements), Attaque AWS en 2011 et OVH en 2018 etc.
- **Administration sécurisée du système d'information (module 5 – 1,5 journée)**
  - Analyse de risque : Identifications des actifs, Identification des menaces et vulnérabilités, Calcul de risque, remédiations, Evaluation de la sécurité, Supervision, Analyse dynamique de risque
  - Principes et domaines de la SSI afin de sécuriser les réseaux internes : Développement de la notion de défense en profondeur. 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
  - Méthodologie de résilience de l'entreprise
  - Aspects juridiques
- **Sécurisation de SI partiellement ou intégralement externalisé (module 6 – ½ journée)**
  - Les différentes formes d'externalisation : Enjeux du cloud computing
  - Techniques de sécurité lors de l'externalisation
  - Comment choisir son prestataire de service : Présentation du référentiel de l'ANSSI, Présentation de la qualification SecNumCloud
  - Aspects juridiques et contractuels : Notion de propriété intellectuelle, CNIL, RGPD
- **Sécurité des sites internet (module 7 – 1 journée)**
  - Menaces propres aux sites internet
  - Approche systémique de la sécurité
  - 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 et/ou développement web
  - Sécurité des bases de données
  - Utilisateurs et sessions
  - Obligations juridiques réglementaires : Cas du e-commerce