SBP-14

CYBERSECURITE EN ENTREPRISE : MAITRISER LES FONDAMENTAUX DE LA CYBERSECURITE

OBJECTIFS PEDAGOGIQUES :

A l'issue de la formation, chaque participant devra mieux :

- Faire le point sur l'environnement de la cybercriminalité
- Identifier les failles informatiques qui rendent vulnérables les entreprises connectées
- Appréhender les techniques et méthodes permettant d'assurer la protection d'une entreprise face à une cyberattaque

CONTENU DU PROGRAMME DE LA FORMATION :

- **Initiation à l'environnement de la cybercriminalité et à son cadre juridique**
  - ✓ Cybercriminalité et entreprise : 5 chiffres clés à connaître
  - ✓ Définition du cyberespace et évolution des systèmes d'informations, l'augmentation de la surface d'attaque
  - ✓ La mise en place d'une charte informatique auprès de salariés
  - ✓ Le cas spécifique du vol de données

- **Identifier les menaces de cybercriminalité et ses conséquences pour une organisation**
  - ✓ Les risques majeurs pour une organisation, les organisations criminelles et associations de malfaiteurs
  - ✓ Attaques de masse VS Attaques ciblées
  - ✓ Les différents types de hacker, intérêts, motivations et facteurs déclencheurs
  - ✓ La méthodologie du hacker : La prise d'empreinte, le scan, l'anonymat, l'attaque : prise de contrôle, escalade des privilèges, exfiltration des données
  - ✓ Les principaux types d'attaques (programmes malveillants, attaques réseaux / web, failles applicatives, réseaux d'entreprise et réseaux sans fil, comptes / mots de passe, systèmes industriels et objets connectés)

- **Se représenter l'ingénierie sociale d'une cyberattaque**
  - ✓ Mécanisme de l'ingénierie sociale : Définition, modes d'action, leviers…
  - ✓ Les différentes techniques : phishing, risques de Faux Ordres de Virement, les autres techniques : SCAM, Malvertising, Rogues…
  - ✓ Identifier les différentes méthodes permettant de se protéger des attaques utilisant l'ingénierie sociale

- **Présentation des organismes Étatiques dans la cybercriminalité**
  - ✓ Enjeux et Objectifs : Présentation des motivations des centrales de renseignement
  - ✓ Organisation des structures étrangères et moyens associés
  - ✓ Présentation, par étude de cas, d'outils puissants utilisés en matière d'écoute et de cyber espionnage

- **Identifier les mesures de prévention pour les entreprises**
  - ✓ Le concept de défense en profondeur et de cloisonnement, la forteresse de Vauban appliquée au système d'information
  - ✓ Mise en oeuvre d'un Système de Management de la Sécurité de l'Information (Schéma d'un SMSI, la norme ISO 27001)
  - ✓ Principes incontournables d'une bonne politique de sécurité des systèmes d'information : Dispositifs de sécurité , chiffrement, Gestion des Identités et des Accès (IAM), sensibilisation des membres de l'organisation, politique de sauvegarde des données, plan de continuité d'activité, SMSI, Outil SIEM, SOC et gestion des incidents de sécurité en temps réel, automatisation de processus de sécurité, détection de préattaques ou cyber threat intelligence, tests de pénétration et Vulnerability Assessment, Bug Bounty, pots de miel, etc.
  - ✓ Focus sur la mobilité : Comment se protéger en déplacement, la protection physique et applicative, la sécurité des connexions sans-fil

- **La cyber résilience : Comment gérer et se remettre d'une cyberattaque ?**
  - ✓ Se préparer : Cartographier et analyser les interactions existantes, déterminer le patrimoine sensible, les facteurs de risques, les conséquences
  - ✓ Résister : Établir le contrôle sur son écosystème, mise en oeuvre de systèmes de détection intelligents

- ✓ Réagir : Prévoir un Plan de Continuité de l'Activité, réaliser des simulations, savoir gérer la communication interne et externe, signaler l'attaque aux autorités compétentes
- ✓ Se remettre : Recherche et analyse des traces, le Forensic, les techniques d'enquête, le cadre légal et le dépôt d'une plainte
- ✓ S'adapter : Retour d'expérience sur l'attaque, la cartographie des risques et des procédures opérationnelles

PUBLIC CIBLE

- DG, DAF, DGA, DSI, dirigeant ou cadre supérieur
- Ingénieur informatique
- Service DSI
- Ressources Humaines

DUREE DE LA FORMATION :

03 Jours de 8 heures chacune

ANIMATEUR :

Consultant spécialiste