CYBERSÉCURITÉ INITIATION

Référence
NEGCYB30

Durée
3 jours (21 heures)

Certification
Aucune

Modalités de formation
En présentiel
A distance
Intra et inter-entreprise

En partenariat

Objectifs de la formation

- Comprendre les motivations et le besoin de sécurité des systèmes d'information
- Connaitre les définitions de base et la typologie des menaces
- Appréhender et adopter les règles d'hygiène de base de la cybersécurité, pour les organisations et les individus

Prérequis

Connaissances de base sur les systèmes d'information (fonctionnement, etc.)
Connaissances de base sur le fonctionnement technique des réseaux, des systèmes d'exploitation et des applications

Programme :

CYBERSÉCURITÉ : NOTIONS DE BASE
Les enjeux de la sécurité des S.I.
La nouvelle économie de la cybercriminalité
Les impacts sur la vie privée
Quelques exemples d'attaques

Propriétés de sécurité
Disponibilité, Intégrité, Confidentialité, Preuve/Traçabilité
Exemples de mécanismes offrant des propriétés de sécurité

Présentation des notions de menaces, vulnérabilités, attaques
Notions de « Vulnérabilité », « Menace », « Attaque »
Exemple de vulnérabilité lors de la conception d'une application
Illustration de l'exploitation d'une vulnérabilité

Panorama de quelques menaces
Les principales sources de menaces
Hameçonnage & ingénierie sociale
Fraude interne
Intrusion informatique
Virus informatique
Déni de service

Le droit des T.I.C. et l'organisation de la sécurité en France
L'organisation de la sécurité en France
Le contexte juridique
Le droit des T.I.C.
Dispositif juridique français de lutte contre la cybercriminalité
Protection des données à caractère personnel

Quizz : notions de base à connaître

CYBERSECURITE : LES REGLES D'HYGIENE INFORMATIQUE
Connaître le S.I
Identifier et inventorier les composants du SI
Types de réseau et interconnexion

Maîtriser le réseau
Sécuriser le réseau interne
Accès distant
Sécuriser l'administration
Wifi

Sécuriser les terminaux
Applications et mises à jour logicielles et systèmes
Protéger contre les codes malveillants
Protéger les données
Durcir les configurations

Gérer les utilisateurs
Gestion des privilèges
Mots de passe et autres moyens d'authentification
Sensibilisation des utilisateurs

Sécuriser physiquement

Contrôler la sécurité du S.I.
Contrat de maintenance, d'assurance, de support
Surveiller et superviser et gérer les incidents de sécurité
Plan de secours
Audit

Quizz : recommandations et bonnes pratiques pour chacun et évaluation de la formation