10, Place des Archives – 69002 LYON

Valérie Thoraval
04.72.32.50.60

contact@cpe-formation.fr
cpe-formation.fr

CYBERSÉCURITÉ

INTRODUCTION À LA CYBERSÉCURITE POUR LES DÉCIDEURS

OBJECTIFS

Informer sur les risques informatiques dans l'entreprise, les piratages et autres attaques possibles, détournements d'informations et des données. Sécuriser l'environnement informatique de son entreprise, les postes de travail et le réseau informatique. Définir le rôle des DSI, DSSI et autres acteurs. Connaitre le cadre juridique.

CONTENU PÉDAGOGIQUE

Jour 1

THÉORIE

Introduction la sécurité informatique.

Risques et menaces, processus d'authentification

Présentation des risques et des menaces courantes. Motivation et sociologie des pirates.

Présentation des menaces les plus courantes : exploitation de vulnérabilités, ransomware, phishing, exfiltration de données, attaques d'applications web, codes malveillants... exemples de piratages en entreprises et cas réels.

Introduction aux bonnes pratiques pour limiter les risques, cas d'usages.

Contrôle des accès, authentification et autorisation. Bonnes pratiques des mots de passe, certificats et token, connexions à distances et VPN

La cybersécurité par les réseaux et les failles inhérentes aux objets connectés, aux appareils en mobilité.

Informer le personnel et sécuriser les postes de travail

Comment sensibiliser et informer le personnel, faire prendre conscience qu'une négligence peut provoquer une catastrophe. Souligner les responsabilités de chacun.

Mettre en place les bonnes pratiques de base dans l'entreprise et les faire appliquer. Sécuriser les postes de travail. Agir pour une sécurité au quotidien et maintenir la vigilance dans le temps.

Rédiger et afficher une charte des bonnes pratiques et d'utilisation des ressources informatiques.

Introduction aux aspects sociaux et juridiques, à la cybersurveillance la protection de la vie privée.

Le cadre juridique

Découvrir et comprendre les contraintes juridiques et réglementaires, saisir leur intérêt .

Connaitre les différents acteurs de la sécurité informatique, leur rôle et les obligations à respecter quant aux pratiques et à la protection des données :

- La CNIL *(Commission Nationale de l'Informatique et des Libertés)* et la législation.
- La RGPD *(Règlement Général sur la Protection des Données)*, objet et objectifs
- L'ANSSI *(Agence Nationale de la Sécurité des Systèmes d'Information),* présentation

Savoir quoi faire en cas d'attaque constatée, dépôt de plainte et assurances spécifiques. Quels recours et protections en cas d'attaque informatique

Analyse des risques, des vulnérabilités et des menaces

Les pistes pour entamer une démarche d'analyse et d'évaluation de la maturité cybersécurité de son entreprise. Evaluation des conséquences en cas d'attaque et de perte des données pour son activité, arrêt momentané ou prolongé.

Comment définir et mettre en place une stratégie pour une meilleure protection des pratiques, de l'infrastructure et protection des données.

Décrire le rôle des DSI, DSSI et autres acteurs de la cybersécurité dans l'entreprise.

Jour 2

DEMONSTRATIONS ET TRAVAUX DIRIGES

DURÉE

2 jours
14 heures

SESSIONS

- 3 et 4 juillet 2023 en présentiel à Lyon

FRAIS D'INSCRIPTION (DÉJEUNER INCLUS)

1275 € HT

PRÉREQUIS & PUBLIC CONCERNÉ

Chefs d'entreprise, directeurs de services, personnels impliqués dans la gestion informatique, ingénieurs informatiques et réseaux. Connaissance de l'entreprise, connaissance générale de l'informatique

Décrire des cas pratiques, illustrer sur maquette les informations théoriques évoquées la veille et en faire découvrir d'autres. Compléter les apports théoriques.

Aider à définir la stratégie d'amélioration de la cybersécurité dans l'entreprise. Préciser le rôle des acteurs de l'informatique dans l'entreprise : DSI, DSSI, administrateur réseau...

Coordonnées

CPE Lyon Formation Continue

Campus Saint-Paul – Bâtiment F • 10, Place des Archives – 69002 LYON

04.72.32.50.60